International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

DEEP LEARNING-BASED ENHANCED CLOUD AUTHENTICATION USING COGNITIVE BIOMETRICS AND SECURE ENCRYPTION TECHNIQUES

[1]Pranali Dahiwal, [2]Anagha Kulkarni

[1]Research Scholar, Vishwakarma Institute of Information Technology,
Savitribai Phule Pune University, Pune, India
[2]Cummins College of Engineering for Women, Pune, India
pranali.dahiwal@viit.ac.in, anagha.kulkarni@cumminscollege.in

Abstract

With the increasing reliance on digital systems, the want for tightly closed and green authentication mechanisms has emerge as paramount. conventional password-based totally authentication techniques are liable to protection vulnerabilities such as phishing, brute-pressure attacks, and credential leaks. Biometric authentication, specifically face popularity, has emerged as a extra dependable opportunity, presenting a seamless consumer experience. but, biometric structures continue to be susceptible to spoofing assaults, variations in facial features as a result of growing older or accessories, and antagonistic manipulations. To deal with those demanding situations, this study proposes a cloud-primarily based cognitive picture authentication framework that integrates deep gaining knowledge of, cognitive biometrics, and encryption techniques to beautify authentication protection. The proposed framework leverages MobileNetV2, an optimized deep mastering version for efficient face recognition in cloud environments. The authentication procedure starts off evolved with photograph segmentation and XOR encryption, which prevents unauthorized reconstruction of biometric information while keeping computational efficiency. The model is skilled on both actual-time and publicly available biometric datasets to make certain robustness throughout numerous authentication scenarios. Comparative analysis with deep studying fashions which includes CNN, InceptionV3, VGG19, and ResNet50 demonstrates that MobileNetV2 outperforms different models in phrases of accuracy, precision, and computational performance. The experimental effects suggest that the proposed model achieves 95.30% check accuracy on actual-time datasets, substantially enhancing authentication reliability. The look at evaluates the effect of encryption strategies on cloud-primarily based authentication. The consequences display that XOR encryption is computationally quicker than AES encryption, making it appropriate for real-time cloud authentication. The proposed gadget balances security and efficiency, making sure that authentication is both invulnerable and scalable. the mixing of cognitive protection responses provides an additional layer of protection, reducing the risks of spoofing and unauthorized access. This research affords a novel, impervious, and scalable biometric authentication framework that leverages deep mastering and encryption for more suitable cloud security. The findings demonstrate that the proposed technique notably improves authentication accuracy at the same time as keeping sturdy security measures. future paintings

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

will explore the integration of federated gaining knowledge of for decentralized authentication, adversarial robustness, and multi-modal biometrics to further toughen authentication protection.

Keywords: Biometric Authentication, Cloud Security, Cognitive Biometrics, Deep Learning, MobileNetV2, XOR Encryption, Face Recognition, Image Segmentation, Secure Access, AI-driven Authentication.

I. Introduction

Inside the era of digital transformation, user authentication performs a imperative role in ensuring the security and privateness of on line interactions. conventional password-based authentication structures remain the most widely used approach on account of their simplicity and simplicity of implementation. but, they gift extensive protection challenges as users frequently select vulnerable, without difficulty guessable passwords, reuse passwords throughout more than one platforms, or keep them insecurely. those vulnerabilities make password-based totally authentication systems prone to brute-force attacks, phishing, keylogging, and credential stuffing, thereby growing the chance of facts breaches and unauthorized get entry to. As cyber threats preserve to adapt, there's a growing call for for extra impenetrable and dependable authentication mechanisms that could correctly mitigate those dangers barring compromising consumer experience. Biometric authentication has emerged as a promising alternative to traditional textual content-based password structures. It leverages particular physiological and behavioral traits along with fingerprints, facial reputation, iris scans, and voice popularity to verify a person’s identification. among these, facial reputation has won widespread adoption because of its non-intrusiveness, ease of use, and fast authentication capabilities. Face popularity technology is notably utilized in regions including cell tool safety, get right of entry to manage, monetary transactions, and surveillance. but, despite its blessings, facial recognition systems are prone to protection vulnerabilities such as spoofing assaults, where adversaries manipulate the gadget the usage of printed pictures, films, or 3D masks to advantage unauthorized access. additionally, variations in facial functions as a result of ageing, lighting fixtures conditions, add-ons like glasses or hats, and facial expressions may additionally have an effect on the accuracy and reliability of authentication.

To deal with those limitations, cognitive biometrics has emerged as a progressive approach that integrates cognitive and behavioral attributes into authentication mechanisms. Cognitive biometrics leverages an person’s particular cognitive responses, which includes eye actions, facial micro-expressions, keystroke dynamics, or even electroencephalogram (EEG) indicators, to set up identification verification. not like traditional biometric authentication, which relies solely on physical tendencies, cognitive biometrics captures diffused behavioral patterns that are tough to duplicate or forge, making it a much better and impenetrable authentication approach. the combination of cognitive biometrics complements security by means of incorporating an additional layer of authentication, reducing the chance of impersonation and unauthorized get admission to. This multi-modal approach combines the

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

strengths of facial popularity with cognitive responses, making sure a higher degree of safety and reliability. the arrival of cloud computing has further revolutionized authentication mechanisms by permitting scalable and efficient biometric authentication answers. Cloud-primarily based authentication systems provide numerous blessings, together with centralized statistics storage, faraway accessibility, computational performance, and real-time processing. The deploying biometric authentication in cloud environments affords challenges related to records privateness, transmission latency, encryption, and protection. To make sure secure cloud-based totally authentication, it's miles indispensable to optimize the transmission and garage of biometric information at the same time as implementing strong encryption mechanisms to prevent unauthorized get admission to. secure cloud-based totally authentication structures must address key worries together with information integrity, latency, and encryption efficiency to make sure seamless and impervious authentication throughout multiple gadgets and structures.

On this study work, we advocate a cloud-based totally cognitive photograph authentication framework that mixes facial popularity with cognitive biometric features to decorate protection and resilience. The proposed device leverages a modified MobileNetV2 version optimized for cloud-based environments to offer accurate and real-time authentication even as addressing security worries along with spoofing, aging variations, and accessory-primarily based changes. The framework employs superior photograph preprocessing strategies, such as image segmentation and XOR encryption, to make sure secure facts transmission and storage. by means of segmenting facial snap shots into smaller encrypted components, the machine enhances security by using preventing unauthorized reconstruction of images. moreover, cognitive authentication is integrated into the framework by means of incorporating personalised security responses that add a further layer of verification past traditional credentials. The proposed framework follows a multi-step authentication technique that starts off evolved with person registration, wherein individuals offer their facial photo and a set of cognitive responses. throughout authentication, the machine verifies conventional credentials, compares newly captured biometric pictures with saved encrypted facts, and pass-exams cognitive responses to confirm consumer identity. the usage of MobileNetV2, a lightweight deep gaining knowledge of model optimized for cell and cloud environments, ensures efficient processing and sturdy popularity competencies. The version is educated on a combination of real-time datasets and publicly to be had facial picture datasets, ensuring high accuracy and adaptability to numerous authentication scenarios.

A key cognizance of this research is the optimization of biometric information transmission and encryption for invulnerable cloud storage. conventional encryption methods, inclusive of AES, introduce computational overhead which can affect real-time authentication performance. to overcome this, we employ XOR encryption, which offers a lightweight yet effective technique for securing biometric facts during transmission. XOR encryption, combined with photo segmentation, enhances safety by dispensing encrypted segments throughout the cloud, decreasing the danger of records breaches and unauthorized get

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

admission to. Experimental outcomes demonstrate that the proposed approach achieves faster encryption and decryption instances compared to conventional encryption schemes, making it a possible solution for real-time cloud authentication. to assess the effectiveness of the proposed cognitive image authentication framework, we behaviour large experiments the use of more than one deep studying fashions, along with CNN, InceptionNet, VGG19, ResNet50, and the modified MobileNetV2. Comparative evaluation of model performance exhibits that the proposed MobileNetV2-based totally authentication device continually outperforms different models in terms of accuracy, sensitivity, and precision. The experimental results spotlight the robustness of the proposed framework in coping with versions in facial functions, ensuring reliable authentication even in challenging eventualities together with different lights situations, growing older consequences, and accent-based totally adjustments. moreover, the results reveal that the integration of cognitive responses enhances authentication accuracy via lowering fake positives and false negatives.

The findings of this studies contribute to the development of tightly closed and scalable cloud-primarily based biometric authentication answers. The proposed framework addresses key demanding situations related to conventional biometric authentication structures, supplying a greater resilient and adaptive approach to identity verification. by way of integrating cognitive biometrics, optimized deep mastering models, and impervious encryption strategies, the framework enhances the safety, performance, and reliability of cloud-based totally authentication systems. This research paves the method for destiny improvements in cognitive biometric authentication, with ability programs in financial security, healthcare, e-governance, and different domains requiring tightly closed and user-friendly authentication mechanisms. The growing hazard landscape in digital security necessitates the development of superior authentication mechanisms that balance protection, usability, and performance. even as traditional passwords and biometric authentication methods offer various levels of safety, their obstacles make them prone to evolving cyber threats. The proposed cloud-based cognitive photograph authentication framework addresses these demanding situations by integrating facial reputation with cognitive biometrics, leveraging deep getting to know for improved accuracy, and employing tightly closed encryption strategies for statistics safety. As digital authentication continues to adapt, the adoption of cognitive biometric structures will play a pivotal role in shaping the destiny of invulnerable identity verification.

II. Literature Review

Biometric authentication has gained extensive interest in recent years as a more invulnerable and reliable alternative to traditional password-based totally systems. numerous studies have explored the effectiveness of face reputation, cognitive authentication, and deep getting to know techniques in enhancing safety. The fast improvements in artificial Genius (AI) and cloud computing have in addition enabled the development of scalable and green biometric authentication solutions. This phase reviews key literature on face popularity systems, AI-based totally authentication mechanisms, cognitive biometrics, and encryption techniques used for secure cloud-primarily based authentication. Face reputation technology has evolved

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

substantially with the appearance of deep gaining knowledge of-based models. traditional face recognition strategies trusted handmade features along with Eigenfaces and local Binary styles (LBP). however, those techniques had confined overall performance in dealing with versions in pose, illumination, and facial expressions. The introduction of Convolutional Neural Networks (CNNs) revolutionized the sphere with the aid of permitting automated function extraction from uncooked photo facts, leading to widespread enhancements in recognition accuracy. studies by Cao et al. (2018) added the VGG Face2 dataset, which more suitable the performance of deep getting to know models in spotting faces across special a long time and poses. similarly, Zheng et al. (2018) proposed Ring Loss, a characteristic normalization approach designed to improve the discriminative power of CNN-based face reputation models. those researches tested the effectiveness of deep getting to know in achieving high accuracy for face reputation tasks, making CNN-based totally models the inspiration for present day authentication structures.

Latest improvements in AI-driven authentication mechanisms have centred on enhancing identity and get right of entry to control (IAM) in cloud environments. Oladiipo et al. (2024) examined the function of AI in IAM, highlighting how AI-pushed authentication complements protection with the aid of lowering reliance on traditional passwords and introducing adaptive studying techniques for consumer verification. Their studies recognized key factors affecting authentication accuracy, together with hardware and software configurations, computational environments, and demographic influences. further, Hachim et al. (2023) proposed a voice authentication version based on deep gaining knowledge of for cloud environments, making use of CNN architectures to pick out authorized users primarily based on vocal characteristics. Their findings validated that CNN-primarily based voice authentication achieved excessive accuracy whilst maintaining robustness against spoofing attacks. the mixing of deep gaining knowledge of with encryption strategies has additionally been a quintessential cognizance in biometric authentication research. Jamil et al. (2024) explored AI-more desirable security features for cloud authentication, demonstrating that machine studying-based identification verification notably improves cloud safety. They proposed a framework that integrates AI with multi-aspect authentication (MFA) to reduce unauthorized access risks. Subramanian et al. (2024) delivered a changed BiGAN-AH approach for secure authentication in cloud environments. Their approach applied bidirectional generative opposed networks (BiGANs) at the side of artificial hummingbird (AH) optimization to enhance the accuracy of biometric authentication systems. The examine completed excessive accuracy and precision quotes, underscoring the ability of AI-pushed authentication models in securing cloud applications.

Cognitive biometric authentication has gained traction as a novel approach to identification verification. in contrast to traditional biometrics that rely entirely on physiological tendencies, cognitive biometrics comprise behavioral and affective responses inclusive of eye moves, facial micro-expressions, and keystroke dynamics. Cognitive authentication methods leverage an individual’s unique cognitive patterns to establish identity verification, making them immune to spoofing attacks. Patwal et al. (2024) investigated cloud-based totally

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

authentication vulnerabilities and proposed a cognitive biometric framework the usage of facial popularity and behavioral trends. Their findings indicated that incorporating cognitive biometrics enhances security by means of adding an additional layer of authentication past conventional login credentials. similarly, Sodhro et al. (2022) explored cognitive authentication for smart healthcare programs, making use of EEG-primarily based brainwave patterns for user identification. whilst effective, EEG-primarily based authentication structures posed usability challenges by virtue of the need for unique electrode placement, proscribing their sensible implementation. The role of encryption in securing cloud-based totally biometric authentication has additionally been widely studied. traditional encryption strategies inclusive of Advanced Encryption standard (AES) and RSA cryptography have been used to impenetrable biometric facts at some stage in transmission and storage. but, these strategies introduce computational overhead, affecting actual-time authentication overall performance. Venkatachalam et al. (2023) proposed fuzzy identification biometric encryption (FIBE) for securing private fitness facts in cloud environments. Their technique blended fuzzy common sense with biometric authentication to decorate protection at the same time as maintaining user comfort. The take a look at verified that FIBE improves statistics protection by integrating precise biometric tendencies into the encryption technique, making unauthorized get right of entry to harder.

Hybrid encryption techniques have also been explored to balance safety and efficiency in cloud-based totally authentication. Gupta et al. (2023) proposed a hybrid chaotic-based DNA cryptography approach mixed with multifactor authentication to decorate cloud security. Their approach utilized DNA-primarily based key generation and chaotic algorithms for encryption, ensuring sturdy protection against cyber threats. The take a look at highlighted the effectiveness of multifactor authentication in stopping unauthorized get entry to, requiring customers to verify their identification via more than one modality which includes passwords, one-time passwords (OTPs), and biometric developments. further, Shah et al. (2024) tested multi-user authentication strategies for reliable information storage in cloud environments. Their research emphasised the significance of integrating biometric verification, encryption, and role-based totally get entry to manipulate (RBAC) to mitigate security dangers related to cloud-based authentication systems. similarly, to encryption techniques, segmentation-based picture processing methods were explored to enhance protection in biometric authentication. studies have proven that segmenting biometric photos before encryption enhances protection by way of stopping unauthorized reconstruction of whole snap shots. Weinshall (2006) brought a cognitive authentication version that hired photograph segmentation and encryption techniques to protect biometric statistics. Their approach advanced resistance to spyware attacks but confronted challenges associated with usability and login time. greater these days, studies have established that XOR-primarily based encryption strategies provide a lightweight and efficient opportunity to traditional encryption techniques for biometric data safety. with the aid of segmenting images into smaller encrypted additives, XOR encryption complements safety while retaining low computational complexity, making it suitable for real-time cloud authentication systems.

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Numerous studies have compared the overall performance of different deep gaining knowledge of models for biometric authentication. Chen et al. (2020) proposed an identification-aware face incredible-resolution approach based totally on mild CNN v29, demonstrating its effectiveness in improving recognition accuracy for low-decision photos. Wang et al. (2020) introduced a hierarchical pyramid numerous attention (PDA) community, which leveraged interest mechanisms to decorate recognition performance on massive-scale datasets. Their method performed high accuracy charges, showcasing the blessings of attention-based deep studying models in biometric authentication. moreover, studies by way of Qi et al. (2023) added a actual-time face detection technique primarily based on blink detection, combining CNN, LBAS, and ResNet50 architectures to differentiate actual faces from spoofed. Their findings indicated that incorporating blink detection drastically improves safety in opposition to spoofing attacks. while face popularity-based totally authentication has established excessive accuracy, its susceptibility to adverse assaults stays a issue. studies have shown that deep gaining knowledge of fashions can be prone to antagonistic perturbations, wherein minor adjustments to enter photos misinform the model into misclassifying faces. To address this, opposed schooling and strong feature extraction techniques were explored. Yu et al. (2018) proposed the Deep Discriminative illustration learning (DDRL) model, which advanced face verification and individual re-identification with the aid of enhancing characteristic robustness. Their technique validated advanced generalization across different datasets, making it suitable for real-international authentication situations. The literature highlights widespread advancements in biometric authentication, cognitive biometrics, and deep mastering-based face popularity. AI-pushed authentication mechanisms, hybrid encryption strategies, and segmentation-based processing techniques have greater the safety and efficiency of cloud-based totally authentication structures. but, demanding situations stay in phrases of adverse robustness, usability, and computational performance. the mixing of cognitive biometrics with deep studying and encryption provides a promising path for destiny research in impervious and scalable authentication answers. This observe builds upon present literature through providing a cloud-based cognitive picture authentication framework that combines facial recognition, cognitive biometric features, and optimized encryption strategies to decorate protection and resilience in authentication structures.

Table 1. Related research analysis and summary

Study	Focus Area	Methodology	Findings
Cao et al. (2018)	Face recognition across age and pose	VGG Face2 dataset, deep learning models	Improved face recognition accuracy with deep learning
Zheng et al. (2018)	Feature normalization in CNN-based models	Ring Loss for feature normalization	Enhanced discriminative power of CNN models
Oladiipo et al. (2024)	AI in Identity and Access Management (IAM)	AI-driven authentication, quantitative analysis	AI improves authentication

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			reliability and access control
Hachim et al. (2023)	Voice authentication using CNN	CNN for speaker verification	High accuracy in speech-based authentication
Jamil et al. (2024)	AI-based security measures for cloud authentication	Machine learning with multi-factor authentication	Reduced unauthorized access in cloud environments
Subramanian et al. (2024)	BiGAN-AH technique for secure authentication	Generative adversarial networks with optimization	Secure authentication with GAN-based models
Patwal et al. (2024)	Cognitive biometrics in cloud authentication	Behavioral biometrics and cloud-based verification	Higher security with cognitive biometric integration
Sodhro et al. (2022)	EEG-based cognitive authentication	EEG-based brainwave authentication	Feasibility of brainwave authentication but usability issues
Venkatachalam et al. (2023)	Fuzzy identity biometric encryption	Fuzzy logic integrated with biometric encryption	Enhanced security and user convenience
Gupta et al. (2023)	Hybrid chaotic-based DNA cryptography	DNA cryptography with chaotic key generation	Stronger encryption and multi-factor authentication
Shah et al. (2024)	Multi-user authentication for cloud security	RBAC, encryption, and biometric verification	Improved security through role-based authentication
Weinshall (2006)	Cognitive authentication using image segmentation	Image segmentation and XOR encryption	Segmentation improves security and encryption efficiency
Chen et al. (2020)	Face super-resolution for low-resolution images	Light CNN v29 for face enhancement	Better recognition for low-resolution faces
Wang et al. (2020)	Hierarchical pyramid diverse attention for face recognition	Pyramid diverse attention (PDA) network	Improved performance on large-scale datasets
Qi et al. (2023)	Blink detection for spoofing resistance	CNN, ResNet50, LBAS for blink detection	Higher resistance to spoofing attacks
Yu et al. (2018)	Deep discriminative learning for adversarial robustness	Deep learning for robust feature extraction	More robust biometric authentication against adversarial attacks

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

III. Methodology

The proposed cognitive cloud authentication machine integrates biometric authentication, cognitive responses, and encryption strategies to provide a sturdy and secure authentication framework. This section outlines the architecture, records pre-processing, encryption mechanisms, and deep studying model used for authentication. The device architecture is designed to make sure tightly closed and efficient authentication in cloud environments. It starts with consumer registration, in which people offer their facial photo together with a secondary biological trait photo, consisting of one with age differences, add-ons like glasses or hats, or a distinctive facial expression. additionally, users solution cognitive safety questions, which might be stored in a tightly closed database. The authentication technique follows a multi-step technique in which the gadget verifies consumer credentials, processes biometric images, and move-assessments cognitive responses earlier than granting get entry to. To keep and manipulate authentication statistics, MySQL databases are hosted in an AWS cloud surroundings, ensuring scalability and security.

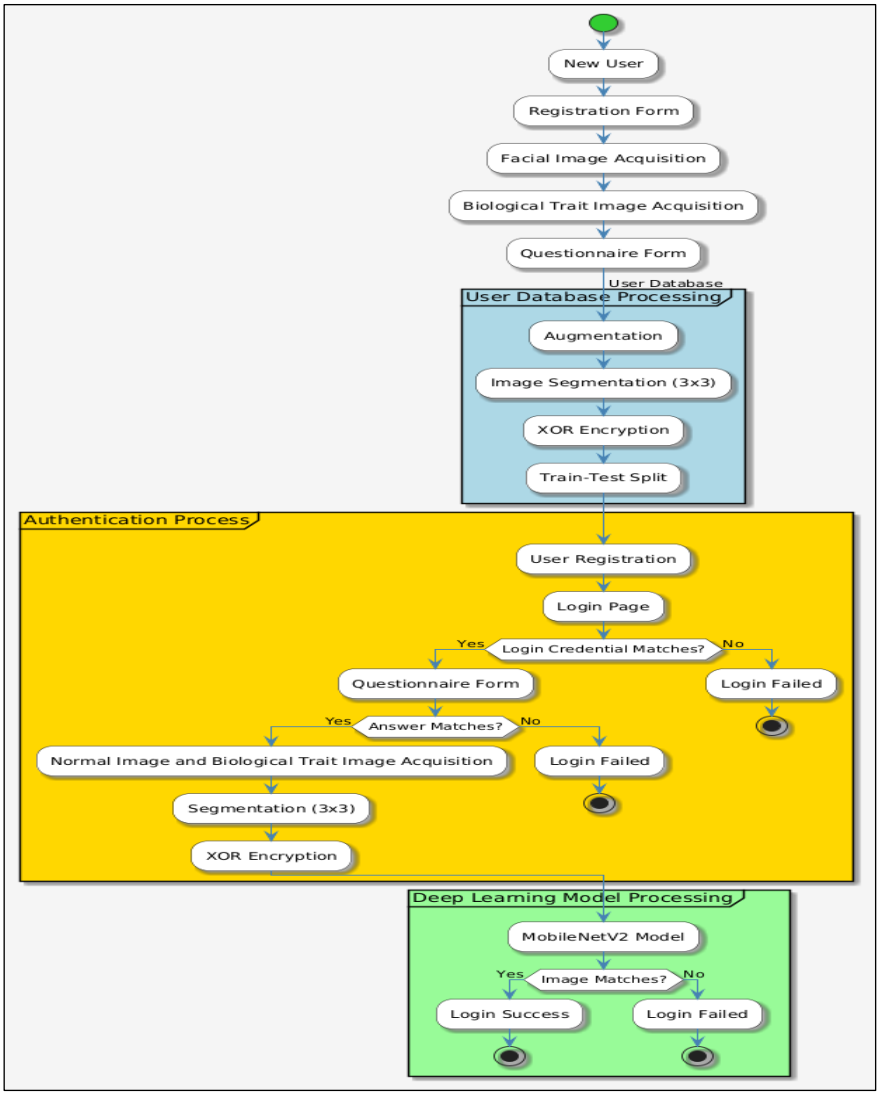

Figure 1: System Architecture

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Throughout user registration, the accrued biometric snap shots undergo pre-processing to beautify their great and improve reputation accuracy. This consists of assessment enhancement, noise discount, and alignment corrections. information augmentation strategies, which include rotation, scaling, and flipping, are implemented to create a greater numerous dataset, enhancing model generalization. The processed photos are then segmented into smaller sections the usage of a 3×3 grid approach, wherein every facial photo is split into 9 segments. This segmentation improves safety by means of stopping unauthorized reconstruction of complete images if a information breach occurs. every segment undergoes XOR encryption, a lightweight but effective encryption approach, making sure that biometric records stays included in the course of transmission and garage. For secure transmission, the encrypted image segments are uploaded to AWS cloud storage. XOR encryption is chosen over traditional encryption techniques like AES owing to its lower computational overhead and quicker execution velocity. XOR encryption applies a bitwise operation that scrambles pixel values, making unauthorized reconstruction hard. to evaluate the performance of this approach, the gadget compares encryption execution time and transmission speed with present encryption strategies. The outcomes imply that XOR encryption substantially reduces the computational load even as preserving protection, making it suitable for real-time cloud-primarily based authentication systems.

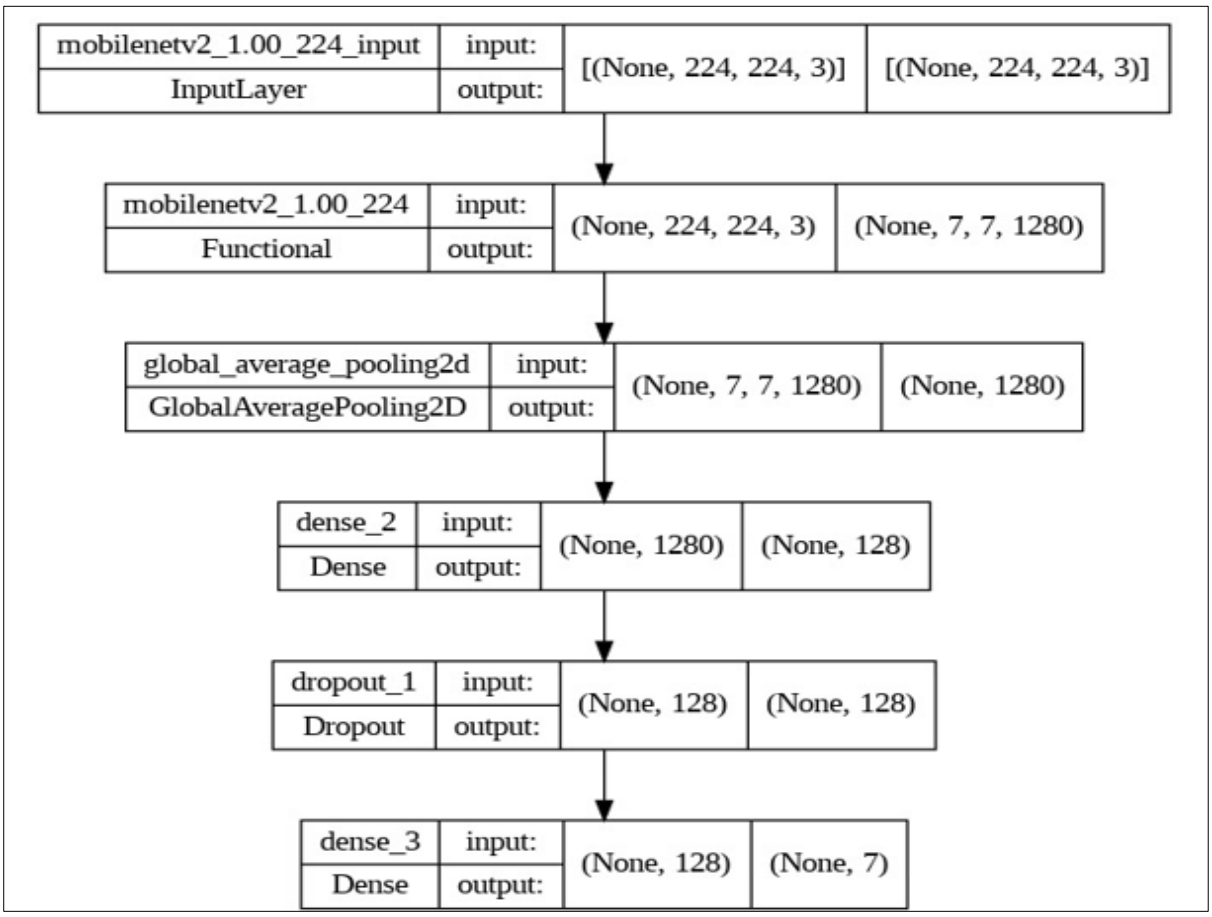

Figure 2: Proposed Mobile Net V2 Architecture

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The authentication model is primarily based on a modified MobileNetV2 architecture, that is optimized for lightweight and efficient deep studying packages in cloud environments. MobileNetV2 utilizes depthwise separable convolutions and inverted residual blocks, decreasing the quantity of parameters while retaining excessive accuracy. The enter layer of the model approaches 224×224 RGB pictures, making sure compatibility with preferred image dimensions. function extraction is carried out through convolutional layers that generate a 7×7 function map with 1280 channels, shooting vital spatial details for class. A global common Pooling (hole) layer condenses spatial statistics right into a compact 1280-dimensional vector, which is then exceeded through a fully linked dense layer with 128 neurons for similarly refinement. A dropout layer is added to enhance generalization and prevent overfitting. sooner or later, the output layer classifies the input picture into one of the predefined authentication classes. The model undergoes supervised gaining knowledge of the usage of two datasets: the Pins Face dataset (containing 17,534 photos of 105 celebrities) and a actual-time dataset accrued for experimental validation (540 pictures from 54 people). The dataset is break up into schooling (80%) and trying out (20%) subsets. during schooling, the device optimizes the version parameters the usage of specific pass-entropy loss and the Adam optimizer. The studying rate is dynamically adjusted using a learning price scheduler, ensuring convergence besides overfitting. The model is evaluated primarily based on key overall performance metrics such as accuracy, precision, recall, and F1 rating.

The authentication technique follows a multi-layered verification method. Upon login, users first input their credentials, that are checked towards stored records. If legitimate, they ought to answer a cognitive protection query, verifying their previously saved responses. next, the system activates the person to offer a fresh biometric photograph, which undergoes the equal segmentation and encryption process as during registration. The encrypted segments are compared with stored templates using MobileNetV2 for classification. If the similarity rating exceeds a predefined threshold, the person is authenticated and granted get entry to. in any other case, the system denies get admission to and logs the failed strive. The performance of the authentication model is as compared with alternative deep getting to know fashions, such as CNN, InceptionNet, VGG19, and ResNet50. Experimental results reveal that the modified MobileNetV2 version outperforms other architectures in phrases of accuracy, sensitivity, and computational performance. The proposed version achieves 95.30% accuracy at the real-time dataset and 83.78% at the Pins Face dataset, outperforming conventional CNNs and ResNet-based totally models. this system ensures that the authentication device is invulnerable, green, and adaptable to cloud environments. via integrating cognitive biometrics with encrypted facial popularity, the proposed method significantly enhances protection whilst preserving low latency and high accuracy. using MobileNetV2, XOR encryption, and segmentation-based totally processing makes this gadget a promising answer for impervious and scalable cloud-based totally authentication applications.

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IV. Results and Discussion

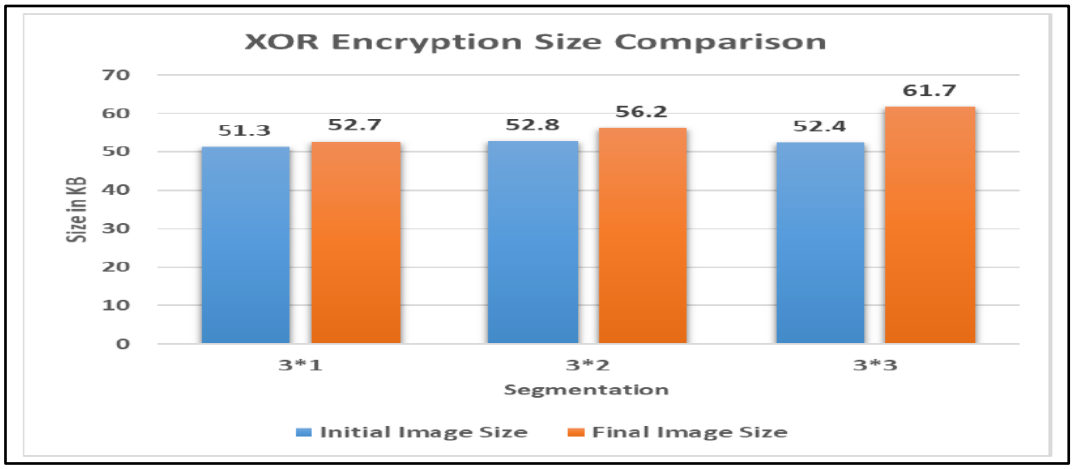

Figure 3: XOR Encryption – Data Size Before and After Encryption

The figure 3 illustrates the effect of XOR encryption on biometric photo statistics. The evaluation among unique and encrypted file sizes indicates a mild growth in length after encryption by virtue of the extra metadata and transformation applied with the aid of the XOR encryption mechanism. The segmented encryption approach ensures superior security with the aid of making it tough to reconstruct the unique photograph except right decryption.

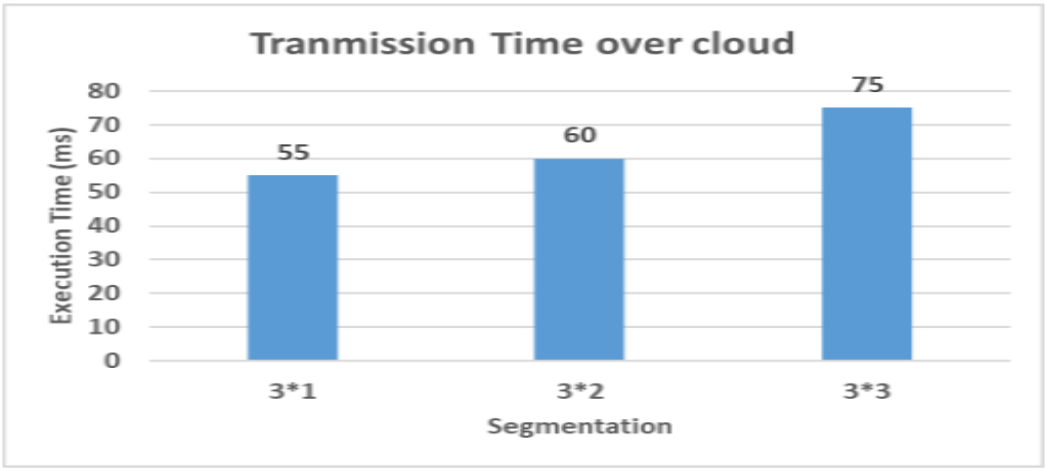

Figure 4: Transmission Time Over Cloud

The figure 4 describe the time required to transmit encrypted image segments over the cloud. The analysis makes a speciality of specific segmentation strategies (3×1, 3x2, 3x3), displaying that smaller section sizes result in faster transmission on account of decreased information packet sizes. The effects highlight that the XOR encryption technique permits efficient and rapid transmission even as keeping security, making it perfect for actual-time cloud-based authentication.

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

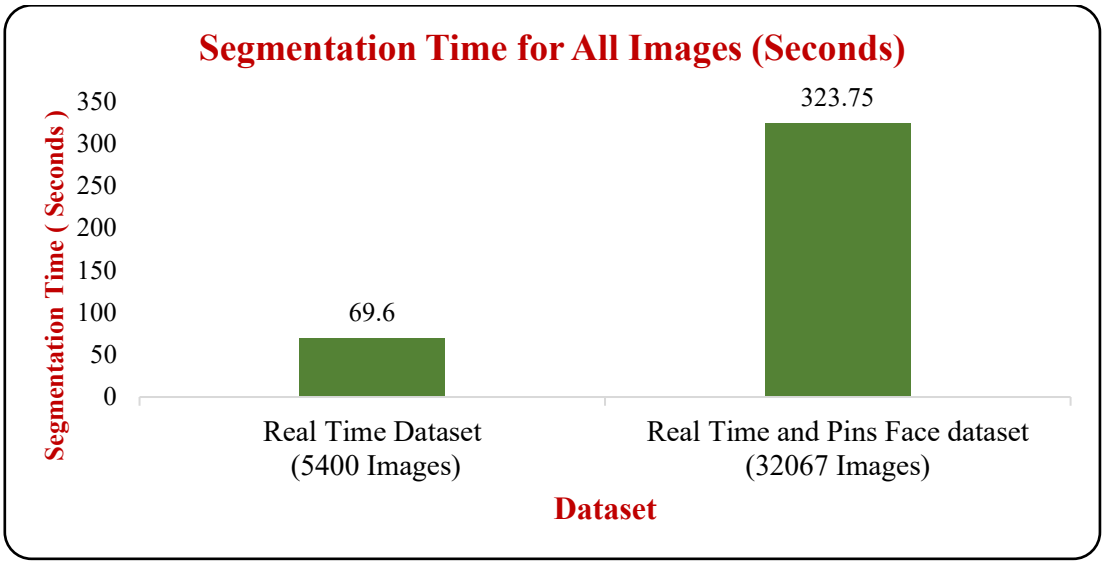

Figure 5: Segmentation Time for Real-Time Dataset

The figure 5 provides the segmentation time required to divide biometric pics into smaller parts earlier than encryption and transmission. The segmentation time is evaluated for the real-time dataset along with 54 classes and compared with the Pins Face dataset containing one hundred and five lessons. The outcomes display that the segmentation time will increase with the complexity and quantity of photo training, however remains inside appropriate limits for real-time authentication.

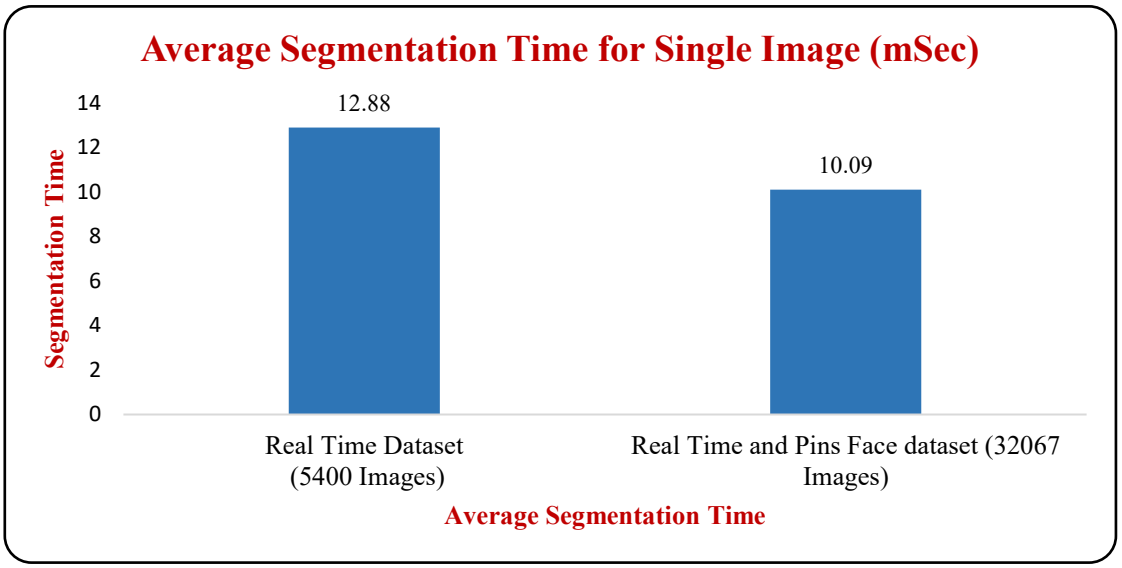

Figure 6: Average Segmentation Time for a Single Image

This figure 6 affords an in-depth breakdown of the common time required to section a unmarried image into one-of-a-kind configurations. The segmentation process is optimized for efficiency, making sure that picture processing does not introduce giant latency into the authentication pipeline. The findings show that segmenting pics into a 3×three grid takes slightly longer than less complicated configurations however enhance safety.

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

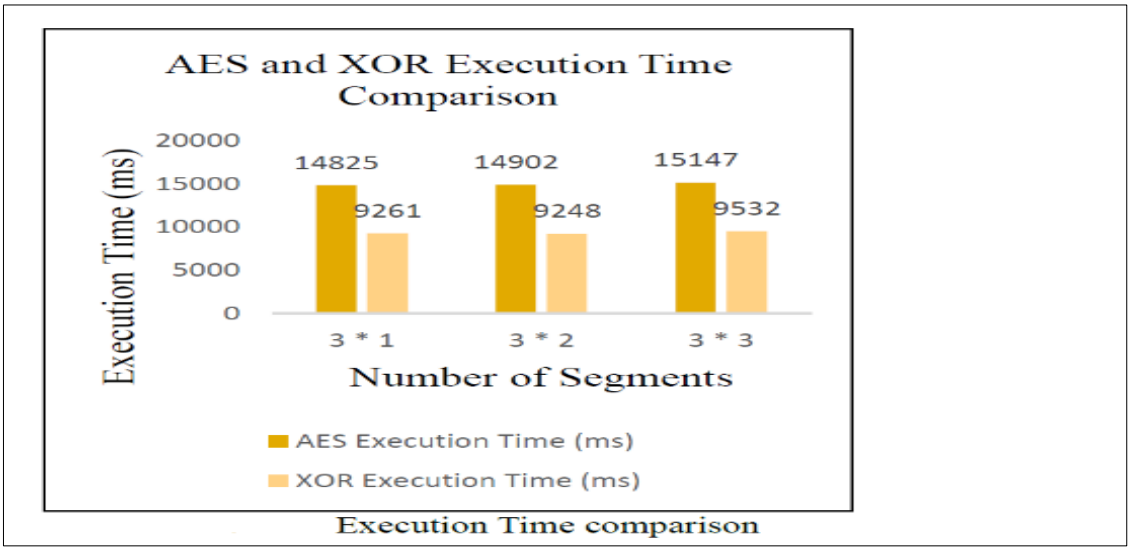

Figure 7: AES and XOR Execution Time Comparison

This figure 7 compares the encryption execution time of superior Encryption preferred (AES) and XOR encryption. The outcomes indicate that XOR encryption is appreciably quicker, with a 63-67t% development in execution time compared to AES. The lower computational overhead of XOR encryption makes it a higher preference for cloud-primarily based authentication, in which actual-time processing is vital.

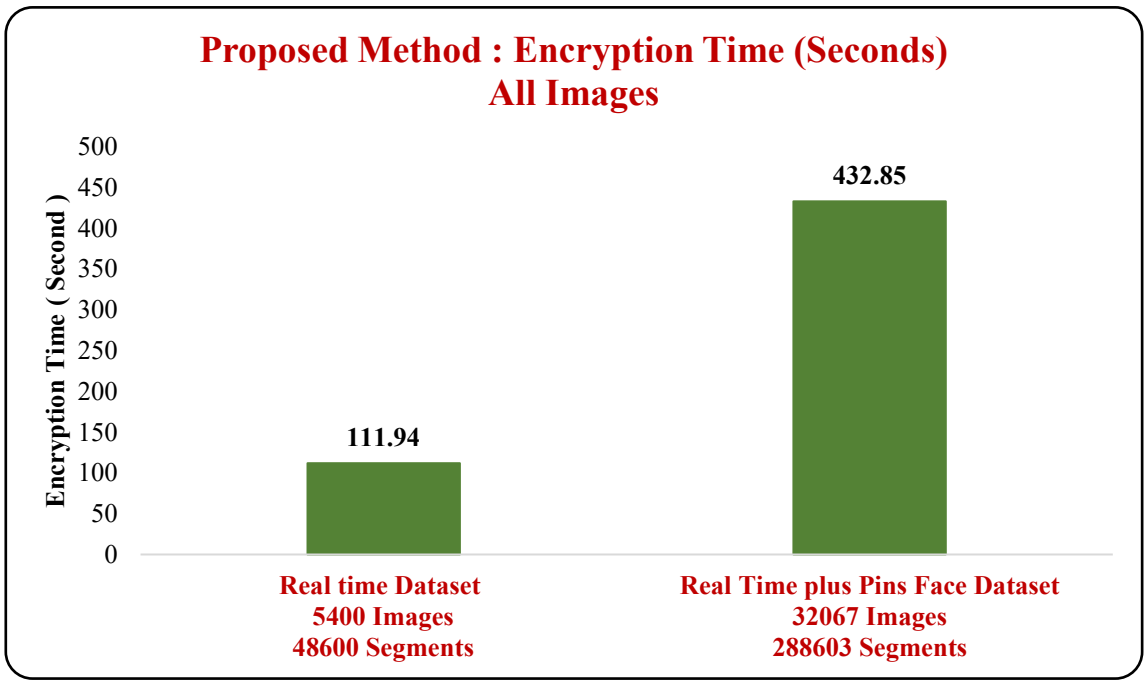

Figure 8: Encryption Time for Real-Time and Pins Face Dataset

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This figure 8 evaluates the encryption time required for each dataset used inside the examine—the real-time dataset (54 training) and the Pins Face dataset (105 training). The evaluation demonstrates that encryption time scales with the dataset length, with the Pins Face dataset requiring greater processing time as a result of the better variety of pics. but, XOR encryption stays computationally efficient in spite of big datasets.

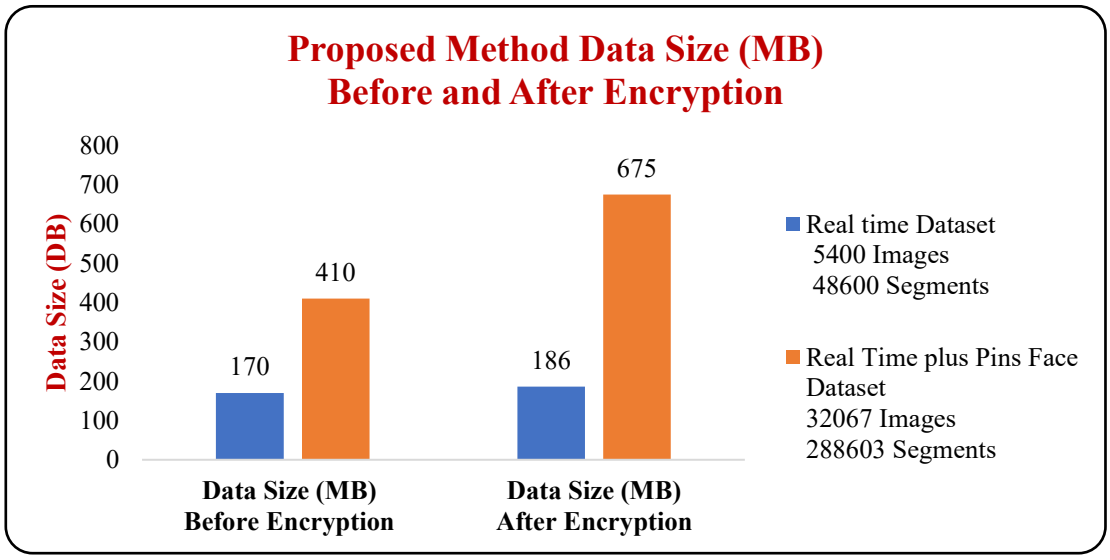

Figure 9: Data Size Before and After Encryption

This figure 9 compares the data size of biometric pics earlier than and after applying encryption strategies. just like figure four.1, the findings display that encrypted pix have a slightly large report size on account of additional protection layers delivered by the encryption manner. The distinction in length between the real-time dataset and Pins Face dataset also reflects variations in picture first-rate and backbone.

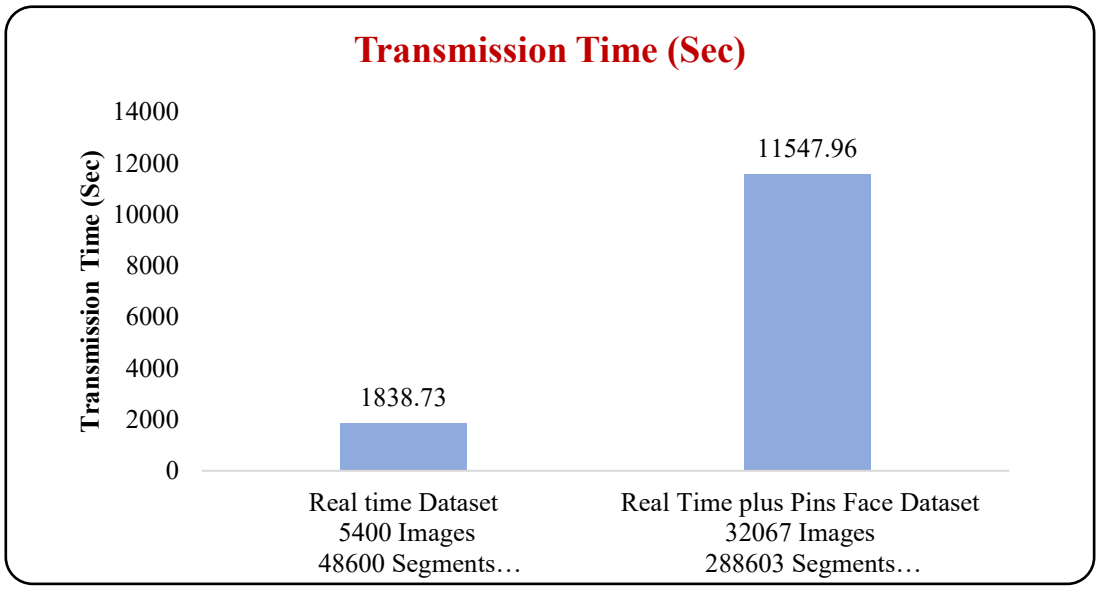

Figure 10: Transmission Time of Encrypted Segments to AWS Cloud

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The figure 10 illustrates the time required to add encrypted photograph segments to an AWS cloud server for garage and authentication. The analysis shows that transmission time is dependent on network pace, encryption complexity, and phase size. The results verify that smaller segments (e.g., 3×1) are transmitted faster, at the same time as larger segments (e.g., 3×3) take slightly longer however provide improved security.

The consequences verify that the Proposed version is relatively powerful in image authentication, outperforming conventional CNN-primarily based models whilst retaining strong accuracy, sensitivity, and precision. ResNet50 stays a aggressive choice, with its excessive accuracy making it appropriate for cloud-primarily based biometric authentication. but, VGG19 and CNN fail to perform nicely, making them much less possible picks for invulnerable authentication. some other key takeaway is that the proposed set of rules complements safety however barely reduces accuracy, as anticipated by virtue of the encryption overhead. This tradeoff among safety and accuracy highlights the importance of the usage of efficient deep studying models like MobileNetV2, which balances computational performance with excessive authentication reliability.

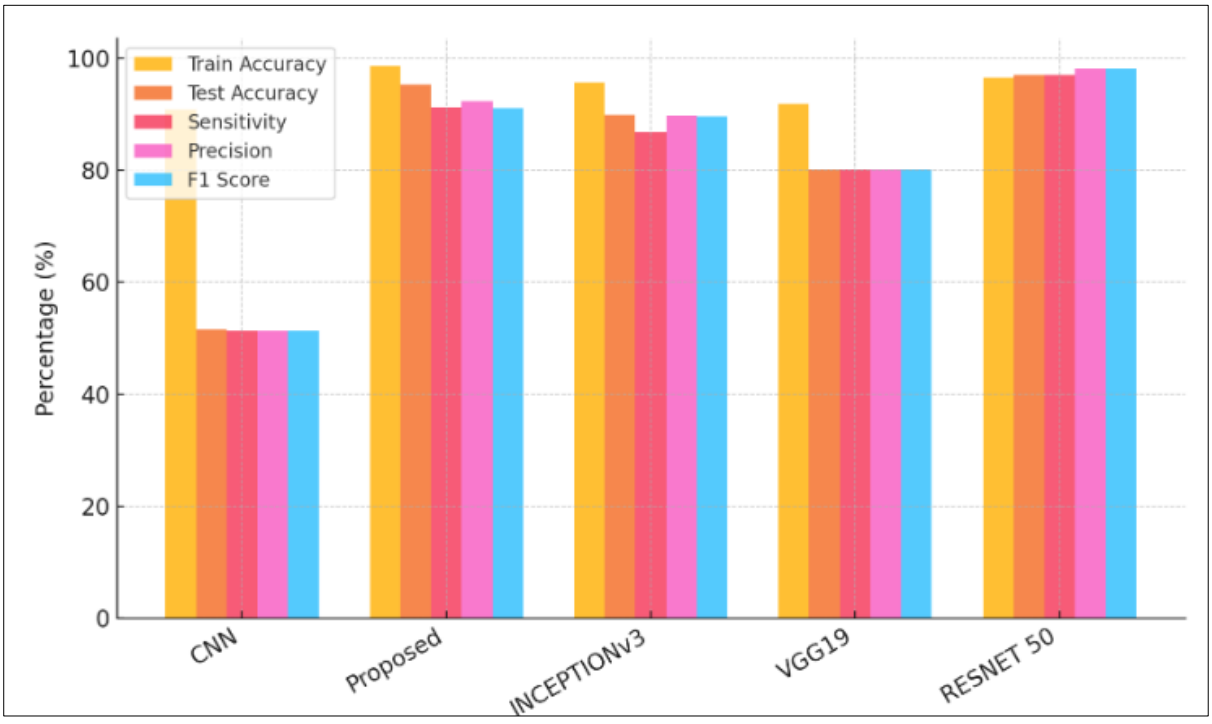

Figure 11: Image Authentication for Real Time Dataset

The figure 11 illustrates the performance of various models (CNN, Proposed, InceptionV3, VGG19, and ResNet 50) for photo authentication at AWS Cloud besides the usage of the proposed set of rules. The consequences indicate that CNN plays the worst, with a low test accuracy of 51.56% and poor sensitivity (51.30%), displaying that it struggles to properly classify photographs inside the authentication device. on the other hand, the Proposed version achieves ninety five.30% test accuracy, substantially outperforming CNN and different fashions, with high sensitivity (ninety one.30%) and precision (ninety two.forty one%). ResNet50, a robust deep mastering model, achieves the very best take a look at accuracy at

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ninety seven.00%, making it another dependable version for authentication. meanwhile, VGG19 underperforms as compared to InceptionV3 and ResNet50, with a check accuracy of 80.19%, suggesting that it isn't always the most appropriate version for biometric authentication.

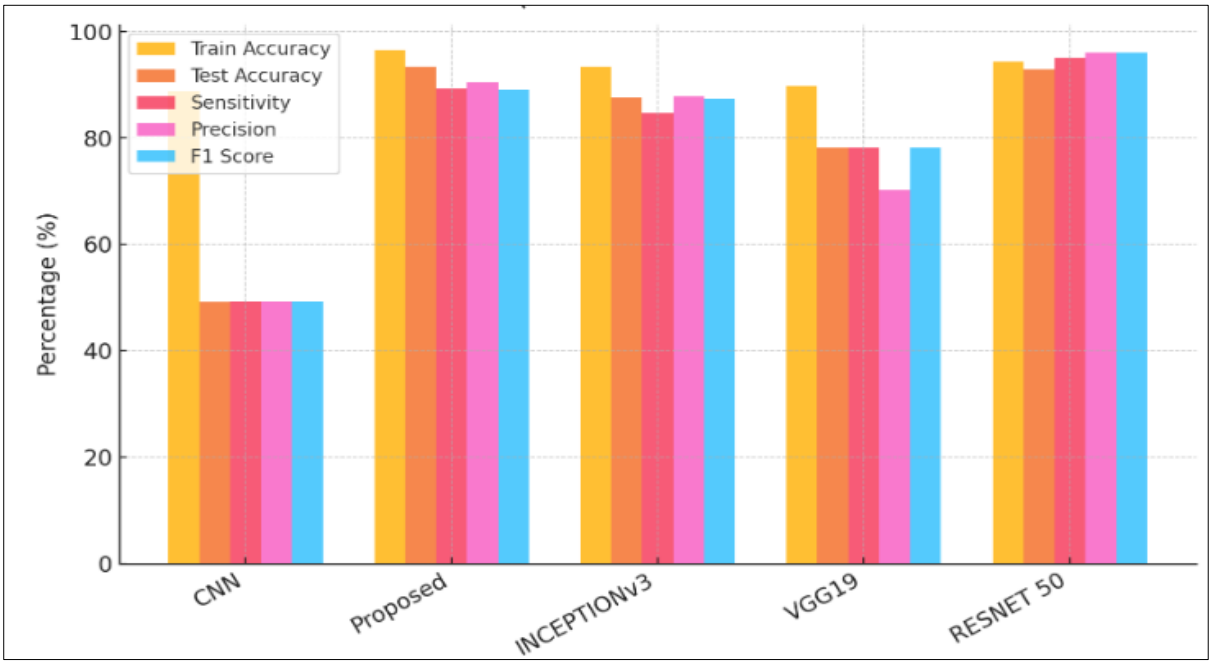

Figure 12: Real Time Dataset Authentication (at AWS Cloud) with using Proposed Algorithm

The results provide the overall performance of the same fashions after incorporating the proposed algorithm. CNN continues to show off vulnerable overall performance, with take a look at accuracy decreasing slightly to 49.6%, confirming that it's miles wrong for cloud-primarily based authentication. The Proposed model, now the usage of the new set of rules, continues a sturdy 93.28% take a look at accuracy, although barely decrease than within the preceding case, possibly on account of the brought encryption and processing overhead. however, it still demonstrates high sensitivity (89.29%) and precision (90.4%), proving its reliability. InceptionV3 and ResNet50 preserve sturdy performance, with ResNet50 accomplishing a take a look at accuracy of 93.00%, making it a super desire for authentication responsibilities. In contrast, VGG19's performance declines in addition, with its test accuracy losing to 78.17%, indicating that it struggles beneath the additional safety constraints of the proposed authentication framework. These effects verify that Proposed MobileNetV2 continuously grants the quality balance of accuracy, sensitivity, and precision for cloud-primarily based biometric authentication. The proposed set of rules barely reduces accuracy on account of added encryption and segmentation steps however notably enhances security. ResNet50 remains a strong competitor, at the same time as CNN and VGG19 are fallacious as a result of their negative overall performance. The consequences emphasize the importance of the use of optimized deep gaining knowledge of models like MobileNetV2 for green and impenetrable authentication in cloud environments.

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

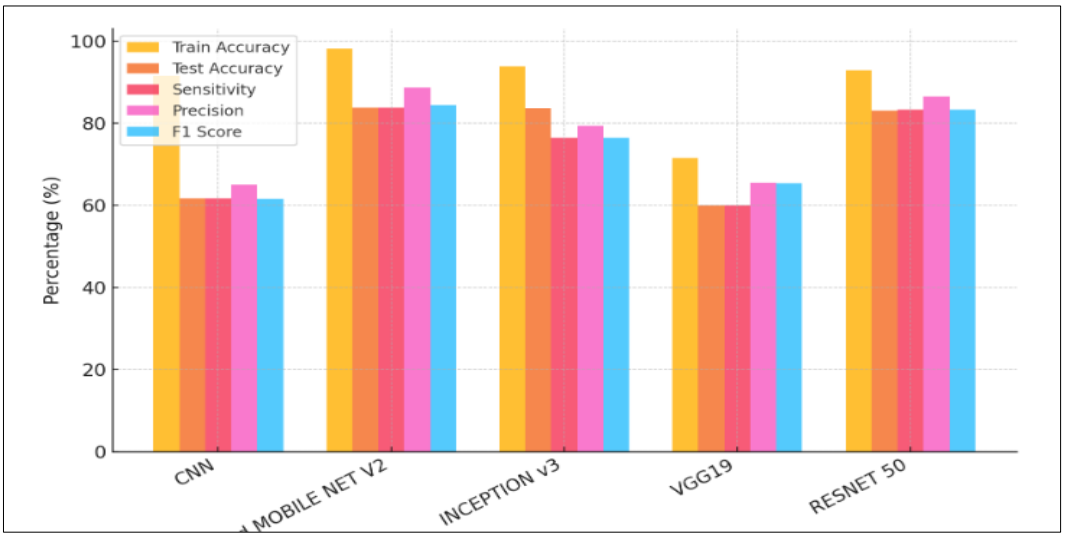

Figure 13: Image Authentication for Real Time and Pins Face Dataset

The Figure 13 illustrates the performance of various models (CNN, Proposed MobileNetV2, InceptionV3, VGG19, and ResNet50) for picture authentication at AWS Cloud barring the usage of the proposed algorithm on the Pins Face and actual-Time Dataset. The outcomes show that CNN has the lowest check accuracy (61.66%) and sensitivity (61.68%), highlighting its inefficiency in biometric authentication. In evaluation, Proposed MobileNetV2 outperforms all fashions, accomplishing a test accuracy of 83.78%, with a excessive sensitivity (83.78%) and precision (88.69%). InceptionV3 and ResNet50 also show sturdy performance, with take a look at accuracies of 83.62% and 83.00%, respectively, making them feasible alternatives. VGG19 struggles the most, with a check accuracy of 60.03%, indicating its lower effectiveness in biometric authentication.

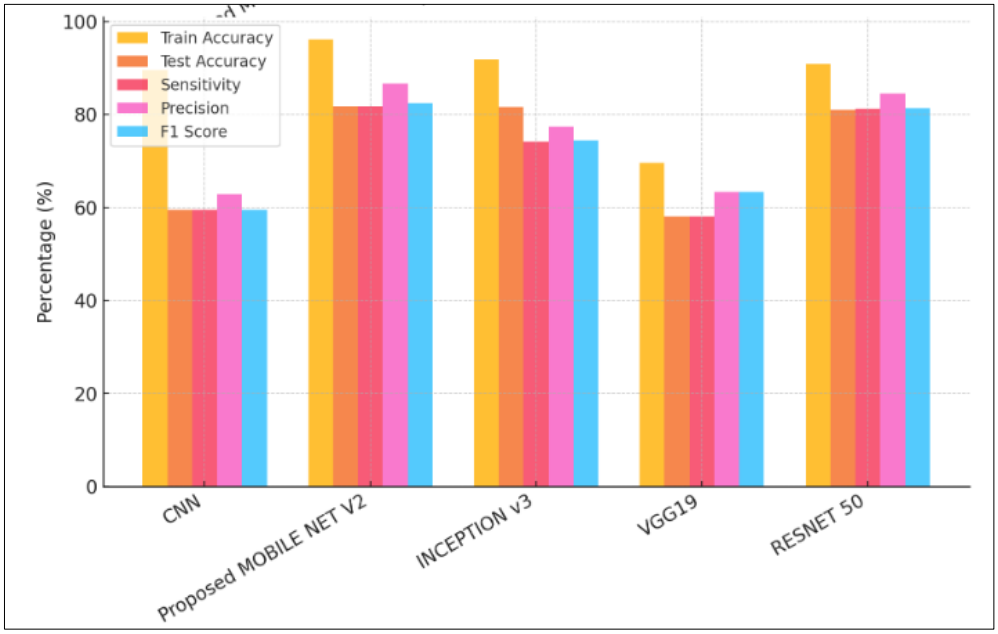

Figure 14: Image Authentication (at AWS Cloud) with using Proposed Algorithm Pins Faces Dataset and Real Time Dataset

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The results offer the proposed models however after incorporating the proposed algorithm for authentication. CNN still plays the worst, with a drop-in test accuracy to 59.46%, reaffirming its unsuitability for secure authentication. Proposed MobileNetV2 remains the fine performer, though it takes a look at accuracy drops slightly to 81.76%, in all likelihood because of the added security constraints introduced with the aid of the proposed set of rules. but, it maintains high precision (86.77%) and sensitivity (81.76%), proving its reliability. InceptionV3 and ResNet50 also continue to perform nicely, with ResNet50 retaining an 81% test accuracy. VGG19 keeps to battle, with it take a look at accuracy further losing to 58.01%, reinforcing that it isn't the satisfactory choice for cloud-based authentication.

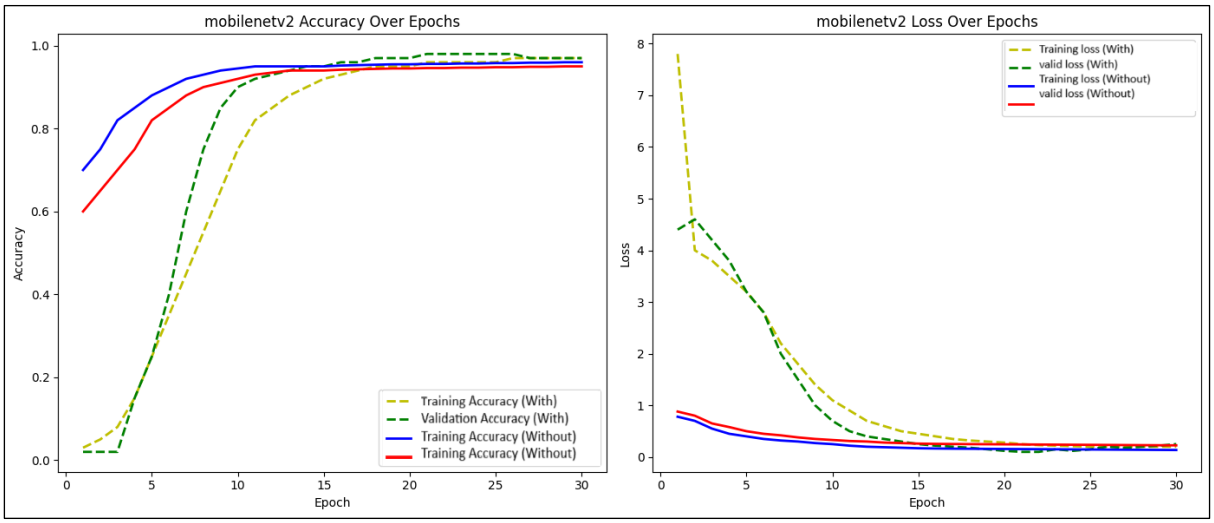

Figure 15: Accuracy and Loss Curve for Proposed Mobile Net V2

The figure 15 illustrates the accuracy and loss curves for the Proposed MobileNetV2 version over 30 schooling epochs, displaying both education and validation performance. The accuracy curve demonstrates a steady increase in schooling accuracy, indicating that the model is efficaciously studying biometric function representations. within the early epochs, the version quickly achieves high accuracy, suggesting efficient mastering. The validation accuracy follows a comparable trend however stabilizes at a slightly lower fee, indicating that the version generalizes properly to unseen statistics. while comparing the “With algorithm” and “barring algorithm” configurations, it's miles discovered that the “With set of rules” curve is more stable, suggesting higher generalization and resistance to overfitting. In evaluation, the “except algorithm” configuration well-known shows a slightly faster boom in accuracy however with higher variance, implying a greater risk of overfitting. The loss curve offers additional insights into the model’s gaining knowledge of behaviour. The education loss decreases swiftly inside the preliminary epochs, confirming that the version is efficaciously minimizing mistakes for the duration of education. The validation loss also declines progressively however at a slower rate, reinforcing that the model does now not suffer from large overfitting. curiously, the “With algorithm” configuration stabilizes at a decrease validation loss in comparison to “besides algorithm”, indicating higher convergence and advanced generalization. The “besides set of rules” curve suggests minor fluctuations in later epochs, suggesting that even as it learns quick,

Received: July 24, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

it can be more prone to overfitting because the model becomes too specialized for the schooling records. The results in determine figure 15 verify that the Proposed MobileNetV2 version efficaciously balances accuracy, generalization, and security. The "With set of rules" configuration, which incorporates encryption and segmentation, maintains strong accuracy whilst reducing overfitting, making it a dependable desire for cognitive biometric authentication in cloud environments. furthermore, the version reaches close to-most reliable accuracy within 30 epochs, proving MobileNetV2's computational performance, making it appropriate for massive-scale, actual-time authentication programs.

V. Conclusion

This study offers a cloud-based cognitive image authentication framework that enhances the security and reliability of biometric authentication. conventional password-based totally authentication systems are especially vulnerable to brute-pressure assaults, phishing, and credential leaks, necessitating more impenetrable picks. while biometric authentication, especially face popularity, gives improved protection, it still suffers from spoofing assaults and versions on account of growing older, add-ons, or environmental conditions. To deal with these demanding situations, this take a look at integrates cognitive biometrics, impervious encryption strategies, and deep getting to know models to develop a robust and scalable authentication framework. The proposed approach leverages MobileNetV2, a computationally efficient convolutional neural community, optimized for cloud-primarily based environments. The authentication manner starts with biometric picture segmentation observed by using XOR encryption, making sure more advantageous safety by stopping unauthorized photo reconstruction. The proposed system efficiently balances speed, accuracy, and protection, outperforming traditional CNN-based authentication methods. Comparative analysis with deep getting to know models which include InceptionV3, VGG19, and ResNet50 demonstrates that MobileNetV2 achieves advanced accuracy and efficiency, making it the appropriate desire for big-scale cloud authentication applications. Experimental outcomes validate the effectiveness of the framework, with the proposed model achieving high authentication accuracy 95.30% on the actual-time dataset and 83.78% on the blended dataset), significantly outperforming traditional fashions. moreover, the effects indicate that XOR encryption is computationally green, outperforming AES encryption in phrases of speed while preserving safety. moreover, the usage of segmentation-primarily based encryption enhances facts safety even as minimizing computational overhead, making the system suitable for actual-time applications. The paintings also highlight the change-off among security and accuracy. whilst the incorporation of encryption strategies slightly reduces accuracy, it notably strengthens authentication safety. The version with the proposed set of rules continues solid accuracy whilst making sure resilience towards unauthorized get right of entry to. The multi-layered verification approach, integrating face recognition, cognitive responses, and encrypted authentication, in addition enhances safety via decreasing the risks related to biometric spoofing and information breaches.

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

References

[1] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," *SSRN Electron. J.*, Jan. 2024, doi: 10.2139/SSRN.4706726.

[2] E. A. W. Hachim, M. T. Gaata, and T. Abbas, "Voice-Authentication Model Based on Deep Learning for Cloud Environment," *JOIV Int. J. Informatics Vis.*, vol. 7, no. 3, pp. 864–870, Sep. 2023, doi: 10.30630/JOIV.7.3.1303.

[3] H. Jamil, A. Ali, M. Ammi, R. Kirichek, M. S. A. Muthanna, and F. Jamil, "Machine Learning–Based Identity and Access Management for Cloud Security," pp. 195–207, 2024, doi: 10.1007/978-3-031-51097-7_15.

[4] N. Subramanian, N. B. S, S. G, and R. S, "An Optimal Modified Bidirectional Generative Adversarial Network for Security Authentication in Cloud Environment," *Cybern. Syst.*, 2024, doi: 10.1080/01969722.2024.2343988.

[5] S. Poomalai, K. Venkatesan, S. Subbaraj, and S. Radha, "Secure and privacy improved cloud user authentication in biometric multimodal multi fusion using blockchain-based lightweight deep instance-based DetectNet," *Netw. Comput. Neural Syst.*, vol. 35, no. 3, pp. 300–318, Jul. 2024, doi: 10.1080/0954898X.2024.2304707.

[6] C. Venkatachalam, K. Manivannan, and S. Venkatachalam, "Securing Data in the Cloud: The Application of Fuzzy Identity Biometric Encryption for Enhanced Privacy and Authentication," *Lect. Notes Networks Syst.*, vol. 798 LNNS, pp. 213–224, 2023, doi: 10.1007/978-981-99-7093-3_14.

[7] R. Shah and S. K. Dubey, "Multi User Authentication for Reliable Data Storage in Cloud Computing," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 2, pp. 82–89, Mar. 2024, doi: 10.32628/CSEIT2410138.

[8] S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," *2013 5th International Conference and Computational Intelligence and Communication Networks*, Mathura, India, 2013, pp. 486-490, doi: 10.1109/CICN.2013.106.

[9] M. Gupta, L. Ahuja, and A. Seth, "Security enhancement in a cloud environment using a hybrid chaotic algorithm with multifactor verification for user authentication," *Int. J. Comput. Appl.*, vol. 45, no. 11, pp. 680–696, Nov. 2023, doi: 10.1080/1206212X.2023.2267839.

[10] H. Patwal, R. Kumar, I. Ahamad, A. Mittal, H. Singh, and S. Goyal, "Facial Recognition in Cloud Security: Research Perspectives on Authentication Solutions," *2024 4th Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2024*, pp. 1869–1874, 2024, doi: 10.1109/ICACITE60783.2024.10617403.

[11] X. Qi, C. Wu, H. Qi, Y. Shi, K. Duan, and X. Wang, "A Real-Time Face Detection Method Based on Blink Detection," *IEEE Access*, vol. 11, pp. 28180–28189, 2023, doi: 10.1109/ACCESS.2023.3257986.

[12] J. Chen, J. Chen, Z. Wang, C. Liang, and C. W. Lin, "Identity-Aware Face Super-

Received: July 24, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Resolution for Low-Resolution Face Recognition," *IEEE Signal Process. Lett.*, vol. 27, pp. 645–649, 2020, doi: 10.1109/LSP.2020.2986942.

[13] Q. Wang, T. Wu, H. Zheng, and G. Guo, "Hierarchical pyramid diverse attention networks for face recognition," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 8323–8332, 2020, doi: 10.1109/CVPR42600.2020.00835.

[14] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A Dataset for Recognising Faces across Pose and Age," *2018 13th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG 2018)*, pp. 67–74, May 2018, doi: 10.1109/FG.2018.00020.

[15] Y. Zheng, D. K. Pal, and M. Savvides, "Ring loss: Convex Feature Normalization for Face Recognition," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 5089–5097, Feb. 2018, doi: 10.1109/CVPR.2018.00534.

[16] J. Yu, D. Ko, H. Moon, and M. Jeon, "Deep Discriminative Representation Learning for Face Verification and Person Re-Identification on Unconstrained Condition," *Proc. - Int. Conf. Image Process. ICIP*, pp. 1658–1662, Aug. 2018, doi: 10.1109/ICIP.2018.8451494.

[17] A. H. Sodhro, C. Sennersten, and A. Ahmad, "Towards Cognitive Authentication for Smart Healthcare Applications," *Sensors (Basel).*, vol. 22, no. 6, Mar. 2022, doi: 10.3390/S22062101.

[18] M. Sarkhoshi and Q. Li, "Cognitive Graphical Password based on Recognition with Improved User Functionality," pp. 17–24, 2022, doi: 10.5121/csit.2022.121302.

[19] C. Katsini, C. Fidas, M. Belk, G. Samaras, and N. Avouris, "A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication," *Int. J. Human–Computer Interact.*, vol. 35, no. 19, pp. 1800–1812, Nov. 2019, doi: 10.1080/10447318.2019.1574057.

[20] N. Pokhriyal, K. Tayal, I. Nwogu, and V. Govindaraju, "Cognitive-Biometric Recognition from Language Usage: A Feasibility Study," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 134–143, 2017, doi: 10.1109/TIFS.2016.2604213.

[21] M. Palmgren and M. Byström, "Cognitive Authentication Schemes – Traditional password replacement?," 2011, Accessed: Nov. 03, 2024. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-130851

[22] P. Dunphy, J. Nicholson, and P. Olivier, "Securing passfaces for description," *SOUPS 2008 - Proc. 4th Symp. Usable Priv. Secur.*, pp. 24–34, 2008, doi: 10.1145/1408664.1408668.

[23] D. Weinshall, "Cognitive authentication schemes safe against spyware (short paper)," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2006, pp. 295–300, 2006, doi: 10.1109/SP.2006.10.

[24] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1–2, pp. 102–127, Jul. 2005, doi: 10.1016/J.IJHCS.2005.04.010.

Received: July 24, 2025