International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I11P115

Volume 72 Issue 11, 117-130, November 2024

Original Article

A Multi-Factor Artificial Intelligence Enabled User Authentication System for Leveraging Integrity and Robustness in Online Examination System

Vallem Ranadheer Reddy[1], Gourishetty Shankar Lingam[2], Pulyala Mahipal Reddy[3], Nalla Rajender Reddy[4]

[1,2,3,4]*Department of Computer Science and Engineering, Chaitanya Deemed to be University, Telangana, India.*

[1]*Corresponding Author : ranadheerreddy5@gmail.com*

Received: 30 May 2024 Revised: 07 October 2024 Accepted: 24 October 2024 Published: 29 November 2024

Abstract *- The modern age has increased online education and examination requirements. In the process, several universities are offering courses besides conducting examinations online. There is a necessity for ensuring integrity and robustness in the online examination system due to the proliferation of technologies that may enable participants in online examinations to perform unauthorized activities and violate system rules. There are several ways in which students could violate the rules of integrity of examinations. In this context, ensuring that only authorized and genuine candidates will participate in the examinations is indispensable. The literature shows that there has been a certain effort to conduct online examinations with integrity. However, further leveraging the integrity and robustness of Artificial Intelligence (AI) enabled multi-factor authentication system is needed. We presented a paradigm in this research with mechanisms and algorithms towards a multi factor Artificial Intelligence (AI) enabled user authentication system for leveraging integrity and robustness in online examination systems. The system has multiple layers of authentication mechanisms with an approach that throws challenges like user ID and password, one-time passwords through handheld devices, and deep learning to recognize face models. I proposed an algorithm known as AI enabled Multi-factor Authentication (AIMA), which has the desired mechanisms to realize the proposed framework. Our investigational study demonstrated that the suggested framework can ensure the integrity and robustness of the online examination system regarding user authentication. The AI enabled space recognition system as part of multi factor authentication is superior to many existing methods, with the highest accuracy, 98.74%.*

Keywords *- Online examination, Multi-factor authentication, Security, Integrity and robustness, Deep learning.*

1. Introduction

The Multi-Factor Authentication (MFA) authentication system requires the user to provide two or more verification factors to connect to an application, online account, or VPN. MFA is essential to robust Identity and Access Management (IAM) strategies. With MFA, which requires one or more additional authentication components in addition to a login and password, the likelihood of a successful hack is decreased. Multi-Factor Authentication (MFA), which requires users to log in with more than simply a username and password, increases security for your business. Despite their importance, brute force attacks and other parties can steal usernames and passwords. Enforcing Multi-Factor Authentication (MFA) techniques, such as physical keys or fingerprints, will make your business feel safer knowing that hackers cannot access it. Further verification data, or factors, are required for MFA to work. One-Time Passwords (OTPs) are among the most common MFA factors users face. The four- to eight-digit numbers known as OTPs are what you usually receive by text message, email, or mobile apps. When employing OTPs, a new code is generated periodically or each time an authentication request is performed. In addition to a seed value given to the user at first registration, the code is generated using an incrementing time value or counter.

The advent of cloud computing has made MFA more necessary. As more and more systems are transferred to the cloud, businesses can no longer rely on a user being physically present on the same network as a system as a security safeguard. More security measures must be implemented to ensure that those obtaining access to the systems are not malevolent. MFA helps ensure users are who they say they are by requiring additional authentication factors that are more difficult for hackers to forge or break using brute force approaches, especially when users may access these systems from anywhere at any time. From the literature [1-30], it was observed that there have been efforts to improve authentication systems in online examinations. However, the traditional approaches for user authentication need to be coupled with AI enabled methods.

In this regard, we made the following additions to this study.

1. I proposed a framework with mechanisms and algorithms for a multi-factor AI-enabled user authentication system to leverage integrity and robustness in online examination systems.
2. I proposed an algorithm known as AI enabled Multi-factor Authentication (AIMA), which has the desired mechanisms to realize the proposed framework.
3. We implemented a prototype to demonstrate our framework and its multi-factor authentication with an AI-enabled approach.

This is how the rest of the paper is organized. Different methods and related concepts pertaining to user authentication in online examinations are reviewed in Section 2. Section 3 presents the materials and methods with mechanisms and AI enabled approaches for multi-factor user authentication. Section 4 presents our empirical study on the results observed when the system is operated and evaluated. Section 5 provides implications of the findings and limitations of the study. Section 6, conversely, provides conclusions of our research besides giving directions for future study areas.

2. Related Works

This section examines many current techniques and related concepts pertaining to user authentication in online examinations. Jaimes et al. [1] examined using ML/DL to identify intrusions in smart healthcare systems, focusing on anomaly-based techniques. In addition to discussing major security risks, it suggests Cloud-Fog-Edge-based methods for better detection. Zhang and Zhu [2] observed that, with its interconnected networks and numerous application goals, 6G calls for artificial intelligence (AI) to optimize resource usage. Principal concerns are discussed, with an emphasis on ML/DL applications. Zhou et al. [3] focused on edge computing and edge AI that have emerged due to current developments in AI and IoT, which drive the need for AI capabilities at the network edge. The history, designs, and prospects for Edge AI are covered in this overview. Benzaid et al. [4] observed that building trust is essential in rapidly changing 5G environments.

This essay focuses on the problems, new facilitators (like blockchain), and aspects of trust. Benzaid et al. [5] utilized SDN/NFV, AI, and model-driven interfaces. The ZSM framework developed by the ETSI seeks to achieve complete ANSMO in 5G networks. There is a discussion of security threats and countermeasures. Abdulrahman et al. [6] examined the use of AI and blockchain in aerospace, focusing on supply chain and operational effectiveness. Despite the promise, difficulties still exist. Chen et al. [7], with active auditory sensing and huge accuracy, presented EchoFace as a liveness detection system against media-based assaults. Zulfiqar et al. [8] utilized deep learning to achieve accuracy, and facial recognition is essential for a number of uses, including surveillance and biometric verification. Baqeel and Saeed [9] observed that while face detection on smartphones is commended for its security, there are usability issues, particularly regarding financial transactions and users who hide their heads. Saxena and Varshney [10] used voice and face recognition technology to develop a Smart Home Security service. With an accuracy rate of 82.71%, it provides real-time monitoring and notifications for illegal access. Zhang et al. [11] offered a multimodal biometric identification solution based on Android that uses voice and facial recognition.

It increases the accuracy of speech activity recognition and feature extraction. Jang and Cho [12] presented a cancellable biometrics face retrieval system based on CNN that guarantees template security and usability. Wati et al. [13] found that facial image processing is essential for biometrics, particularly for attendance systems. Viola-Jones is a face detector with a notable 88% accuracy rate while recording in groups. Fouratiu et al. [14] used motion cues and Image Quality Assessment, a unique anti-spoofing technique that surpasses previous approaches. The integration of CNN-based features is one area that needs potential enhancement. Nasution et al. [15] digitalized tendencies were accelerated when COVID-19 proclaimed a worldwide pandemic. With contactless payment options provided by biometric facial recognition, security is increased.Wang et al. [16] investigated by employing secure nearest neighbour and secret sharing homomorphism technologies, a face verification system that protects privacy using edge computing could improve security and efficiency. Wang et al. [17] investigated and found that although they provide many applications for convenience, mobile devices can present security issues. The two types of authentication techniques are multi-factor and knowledge-based. Integration will be given priority in future trends for improved security and usability. Weitzner et al. [18] opined that using grayscale coded light field imaging, a unique face authentication system offers quick anti-spoofing techniques without reconstruction. It delivers competitive outcomes and is valid for daily usage. Labayen et al. [19] ensured that identifying students online and avoiding cheating is essential. Scalability, affordability, and dependability are the solutions provided by a biometric authentication and proctoring system, which allay these worries.

The efficacy of its integration with learning management systems and user surveys is confirmed. Kim and Park [20] improved security in CCTV monitoring by combining RFID and face recognition. It tackles issues like low video quality and protecting privacy. Furthermore, a lightweight authentication mechanism increases the security and overall effectiveness of the system. Mansour et al. [21] utilized Two-Factor Authentication (2FA), authentication is essential in IT systems. However, the user experience may suffer as a result. An improved Autonomous Unimodal Biometric

Authentication System (AUBAS) is suggested using Markov chains. Vekariya et al. [22] enhanced biometric authentication security by feature-level fusion. High accuracy and efficiency are demonstrated by a unique approach that uses BCO-AKSVM. Yao et al. [23] looked at how age affects face authentication and found that older persons have superior accuracy. Improved synthetic aging techniques are investigated. Nakisa et al. [24] examined, using the Technology Acceptance Model (TAM), the variables influencing the adoption of biometric facial authentication.

Adoption is hampered by perceived risk, although positive user experiences, trust, and perceived utility are important variables. Li et al. [25] focused and said that with its evolution toward simplicity and security, biometric authentication is vulnerable to spoofing. Physiological cues that are not visible, such as the photoplethysmogram (PPG), provide a countermeasure. Although rigorous research is sparse, PPG's simplicity, uniqueness, and live detection improve authentication security. Ruiu et al. [26] observed that steady digitization raises the possibility of fraud; biometric authentication—particularly facial recognition—is promising but has practical performance problems. Security is greatly improved via a unique 3D-based authentication technique. Jiang et al. [27] investigated network security using the Zero Trust (ZT) paradigm, which strongly emphasises ongoing authentication. Partially Homomorphic Encryption (PHE)-based cloud-based facial authentication greatly minimizes computing overhead, improving scalability. Yao et al. [28] investigated how to test Facial Recognition (FR) resilience for low-power devices, harsh lighting conditions, and position changes. Relighting using GANs has an impact on FR performance. Robust authentication is possible by correcting flaws in FR networks through fine-tuning. Mitra et al. [29] sought to address urban issues by facilitating quick access to city services by people via digital IDs.

Vasanthi and Seetharaman [30] presented a multivariate correlation analysis-based biometric-driven facial recognition technique that combines geometric and visual information for precise identification and high F-score. The literature shows that there have been efforts to conduct online examinations with integrity. However, further leveraging the integrity and robustness of Artificial Intelligence (AI) enabled multi-factor authentication system is needed.

3. Materials and Methods

This research aims to develop a multi factor AI-enabled user authentication system for leveraging integrity and Robustness in online examination systems. The suggested system is presented in this section. It comprises multi-factor authentication to ensure that there is no possibility that an unauthorized person can take an online examination. The system is designed to have multiple layers of security to protect the sanctity of the online examination system. The reason for the different layers in the authentication system is that each layer adds security. With multi-factor authentication, the system can handle all kinds of security threats. With different layers in the authentication process, various security threats can be handled properly.To this effect, the proposal system is shown in Figure 1. As presented in the proposed system, three levels of risk are mentioned. The levels of risk include low risk, medium risk and higher risk. It is possible to rely on the security provided by Single Sign On (SSO) at low risk. Single sign-on is one of the popular authentication mechanisms by which a user can access multiple services with credentials like user ID and password. Single sign on is a great option for users or students who can access multiple subjects in examinations. However, it has a shortcoming if the credentials are disclosed to a third person, the security of the system is at risk. With respect to online examinations conducted for students studying various university courses, this will be a severe problem.

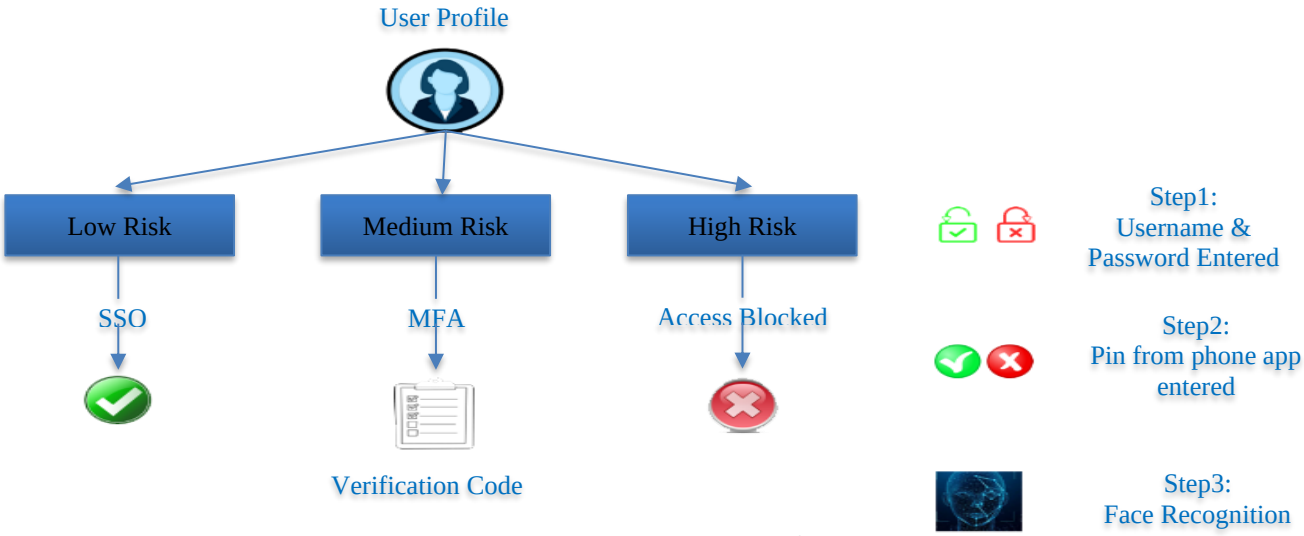

Fig. 1 Proposed system with AI enabled multi-factor authentication

Sometimes, there is a possibility that a student can appear for an exam on behalf of another student illegally. Therefore, though a single sign on is a great option to access multiple services, it has limitations in the security in case of leakage of credentials. When a system relies heavily on SSO, it has to pay the price of security risks. Therefore, another layer of security is indispensable. In the presence of a medium risk, it is ideal to enforce multi-factor authentication. Multi-factor authentication is the mechanism in which multiple means of authentication are followed. For instance, multi-factor authentication may include a traditional user name and password approach, a one-time password approach through handheld devices and a face recognition approach. For two-factor authentication, which includes a traditional username and password and one one-time password, a student may intentionally give both credentials to some intelligent student to attempt the examination to score more marks. In other words, students taking online examinations may misuse the two-factor authentication provision. Therefore, a third layer of authentication, which can be done with artificial intelligence techniques, is required. In this paper, we focused on students' face recognition as the third level of security as part of multi-factor authentication. The rationale is that face recognition ensures that an authorized student can only take the examination. This is the significance of the proposed system, which implements multi-factor authentication. At the same time, the face recognition model based on deep learning is enhanced with new convolutional neural network-based deep learning architecture. As discussed so far, when there is low risk, single sign on is preferred; when there is a medium risk, there is a need for multi-factor authentication. When there is a risk beyond a medium or a high-level risk, it is to be handled differently by completely denying access.

3.1. Single Sign On

Single sign on is the authentication approach that helps students to gain access to various services offered by the university. This authentication is based on the student's prior registration, with which the student gets a user ID and password. These credentials are given to the student to access various services linked to online examinations and learning platforms.

3.2. Multi-Factor Authentication

As discussed earlier, it is important to enable multi-factor authentication when there is medium level risk. Particularly with online examination systems, there is a higher risk of malpractice. Therefore, it is crucial to enable multi-factor authentication. In this paper, proposed a multifactor authentication system and implemented it with three layers of security. The first layer is known as traditional single sign on authentication. The second layer is known as a one-time password, done through a device's possession. The third layer is student face recognition, which authorizes students to participate in examinations or online learning platforms. With respect to the third layer, our convolutional neural network-based deep learning model is often employed in computer vision applications and analysing image or video content. In the proposal system, there is a need for continuous verification of the student for authentication and authorization to participate in the given examination. Towards this end, an artificial intelligence enabled solution is used in this paper.

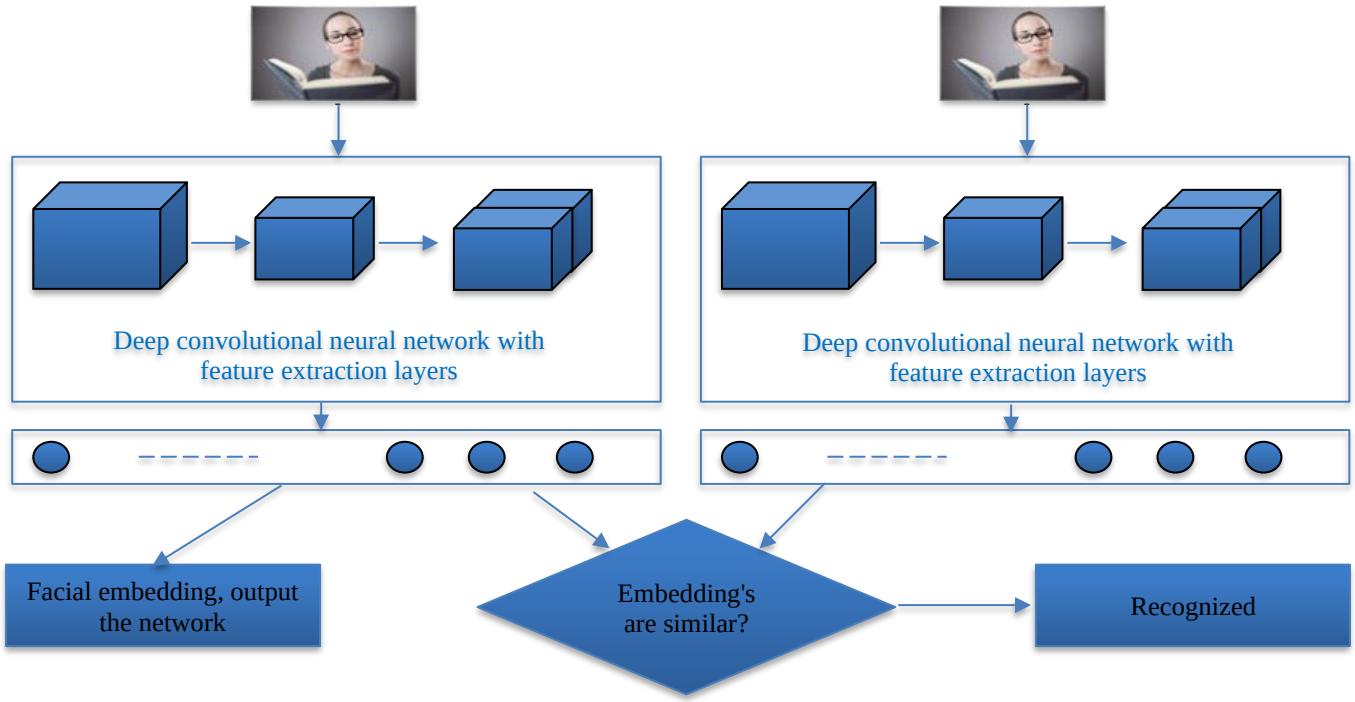

Fig. 2 Proposed AI enabled framework for face recognition

3.3. Artificial Intelligence Enabled Framework for Face Recognition

This section presents the proposed AI-enabled face recognition approach as part of multi-factor authentication in online examinations. In particular, the system is designed on top of deep learning models. Deep learning models are found suitable for computer vision applications. This paper finds the face recognition mechanism suitable for deep learning-based image processing. Figure 2 shows the AI enabled framework for face recognition. It uses a deep learning model that enables the system to extract the features from the participant's pace obtained from live video streaming. Once the face of the participant is identified, it has mechanisms to recognize the student and decide whether to allow or not to write an examination. This is the third layer or factor in the multi factor authentication system. Face recognition comes into the picture when the user ID and password are given correctly, and OTP is given correctly. Since it is the AI-enabled final step in the multi-phase authentication system, face detection and recognition quality are given higher importance. Towards this end, the framework presented in Figure 2 is designed and implemented.

A significant aspect of our technique in face recognition is the learning process that is end-to-end in nature, considering the proposed model as a black box. We employ the triplet loss to do face verification, identification, and grouping, which accurately represents our objectives. Find a given image x embedding f(x) is obtained, resulting in $\mathbb{R}^{\boldsymbol{d}}$ Which is the feature space with the aim of, independent of imaging settings, minimizing the measure known as squared distance among the faces linked to the same identity and increasing the measure between two face photos from different identities.

We found that the loss function named triplet loss is useful for verifying faces even though there is no direct comparison of it with different loss metrics, including the one that uses negative and positive pairs in Equation 2, as discussed in [14]. This is because the loss function had different aspects of an identity to be projected onto one location associated with the embedding space. On the other hand, the loss function used in this paper makes an effort to provide a space between each pair of faces and every other face. Because of this, the faces of one identity can live on a manifold without becoming associated with or discriminating against other identities. The effective at-scale learning of this triplet loss is described in the following section.

3.3.1. Embedding Representation

f(x) $\in \mathbb{R}^{d}$provides the embedding's representation. An image x is included in an Euclidean space of dimension d. Furthermore, we limit this embedding to live on $\|f(x)\|_2 = 1$, the d-dimensional hypersphere.[19] uses the nearest-neighbor classification framework to support this loss. In this instance, our goal is to ensure that one image, $x_i^a(anchor)$, of a certain individual is more like all other images, $x_i^p(positive)$, of the same individual than it is like any other image, $x_i^n(negative)$, of any other individual. Consequently, we desire,

$$\left\|f(x_i^a) - f\left(x_i^p\right)\right\|_2^2 + \alpha < \|f(x_i^a) - f(x_i^n)\|_2^2 \quad (1)$$

$$\forall \left(f(x_i^a), f\left(x_i^p\right), f(x_i^n)\right) \in T \quad (2)$$

Where the space between pairs of positive and negative values is represented by α. All triplets of cardinality N in the given training set are denoted as T. Afterwards, to lessen the loss,

$$L = \sum_i^N \left[\left\|f(x_i^a) - f\left(x_i^p\right)\right\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha\right]_+ . \quad (3)$$

Creating every existing triplet would lead to many triplets that readily satisfy the condition in Equation (1). Since these triplets would still be sent through the network, they would not aid in training and would cause a slower convergence rate. Selecting active and capable hard triplets is crucial to help advance the model. The many methods we employ for the triplet selection are covered in the following section.

3.3.2. Loss Function

Choosing triplets that break the triplet limitation in Equation (1) ensures rapid convergence. In other words, given x_i^a, we want to choose an x_i^p $(hard\ positive)$, such that $argmax_{x_i^p}\left\|f(x_i^a) - f\left(x_i^p\right)\right\|_2^2$ and similarly, we want to choose an $x_i^n(hard\ negative)$, such that $argmin_{x_i^n}\|f(x_i^a) - f(x_i^n)\|_2^2$. It is not practical to calculate the values for argmin and argmax for a given training set. Moreover, it may lead to insufficient training since inaccurately labeled and poorly depicted faces would overshadow the hard positives and negatives. Two clear solutions can get rid of the issue. For every step, argmax and argmin are computed on a given subset of data with the help of the most recent checkpoints. Generate triplets online. Selecting the most difficult exemplars of two kinds of sentiments from a given mini-batch is one method to do this. An online generation approach is preferred, considering mini-batches on a large scale for computing argmax and argmin linked to the mini-batch. In order to ensure an accurate representation of positives, it is imperative to ensure that each mini-batch has a minimum number of exemplars of each identity.

In our investigations, the training data is sampled so that in each mini-batch, about 40 faces are selected for each identity. Additional randomly chosen faces that are negative are associated with every mini-batch, and we employ all anchor-positive pairs to select the toughest negatives but not the hardest positives. Although we could not locate suitable comparisons of every pairing inside a mini-batch that was both hard and anchor-positive, in actuality, we found stability enhanced in the strategy, resulting in a quicker training

process. Furthermore, in addition to the online generation, we looked at the offline generation of triplets. Despite the contradictory findings of the investigations, this technique could make it possible to employ smaller batch sizes. In reality, choosing the toughest negatives might result in poor local minima at the beginning of training; more precisely, it can cause a collapsed model (f(x) = 0). It helps to choose x_i^n so that in order to lessen this.

$$\left\|f(x_i^a) - f\left(x_i^p\right)\right\|_2^2 < \|f(x_i^a) - f(x_i^n)\|_2^2. \quad (4)$$

Since the negative exemplars are farther from the anchor than the positive ones, we refer to them as semi-hard exemplars, even if their squared distance is still near the positive anchor distance. The margin α contains those negative values. Accurate triplet selection is essential for rapid convergence, as previously stated. Small mini-batches are preferred because they often improve convergence for Stochastic Gradient Descent (SGD) processes [20]. On the other hand, implementation details increase the efficiency of batches containing tens to hundreds of examples. However, our method for choosing tough, pertinent triplets from the small batches is the primary limitation of the batch size. We typically employ a batch size of 1,800 exemplars in our investigations.

3.3. Deep Convolutional Networks

Figure 3 shows the suggested facial recognition system's deep learning architecture-based authentication. This architecture is based on the CNN model. It has provisions for convolutional layers and max pooling layers. The convolutional layers progressively extract the features from a given video frame and generate feature maps. Conversely, in Max pooling, layers are used to optimize the feature maps generated by convolutional layers. The network architecture is designed in such a way that it has improved the quality of the learning process. The model is meant to improve the accuracy of face recognition.

This model is integrated with the proposed system to recognize every student as part of multi factor authentication to determine whether to allow or deny the student to write online examinations. We employ SGD with conventional AdaGrad and backpropagation [5] to train the CNN in all our trials. Most trials start at a 0.05 learning rate, which we decreased to complete the model.

The models were trained with a CPU-based system for 100–200 hours, starting at random, much as in [16]. The pace of accuracy gain and loss reduction drastically slows down after 100 hours of training, although further training can potentially leverage significant performance. The margin α has a constant value of 0.2.

3.4. Proposed Algorithm

I proposed an algorithm known as AI enabled Multi-factor Authentication (AIMA), which has the desired mechanisms to realize the proposed framework. Our investigational study demonstrated that the suggested framework can ensure the integrity and robustness of the online examination system regarding user authentication.

As president in Algorithm 1, it takes credentials, OTP and face image as inputs at various times appropriately and performs multi-factor authentication.

In the first layer of security, the algorithm challenges the user to provide correct credentials. The user is thrown an OTP challenge once the credentials are evaluated as valid.

Algorithm 1. AI enabled Multi-factor Authentication (AIMA)

Input: Credentials, otp, face image img
Output:

1. Begin
2. IF credentials match Then
3. Throw otp challenge
4. End If
5. If otp provided is correct Then
6. Throw face recognition challenge
7. End If
8. Load pre-trained enhanced CNN model (shown in Figure 3)
9. Result <- FaceRecognition(model, img)
10. IF result is satisfied Then
11. Allow user to continue online exam
12. Else
13. Deny online exam access to user
14. End If
15. End

The user must respond to the OTP challenge with the help of a personal device to which the OTP is sent. If the user responds with the correct OTP, then the third layer of security is applied. The third layer of security is throwing another challenge with face recognition.

With the proposed deep learning model trained with several face samples, the given input face image is tested for the final layer of authentication as part of a multi-factor authentication system. If users succeed in this authentication, then the user is allowed to continue with the online examination system. If the user fails to satisfy face recognition-based authentication, the user is denied access to the online examination system.

3.5. Evaluation Methodology

We test our technique on four datasets, and we test it on the face verification job, excluding Stated differently, a squared L_2 distance barrier for YouTube Faces and Labeled Faces in the Wild $D(x_i, x_j)$ is used to classify the two face pictures as similar or distinct. P_{same}, is used to indicate all face pairings (i, j) of the same identity, whereas P_{diff} is used to indicate all pairs of differing identities.

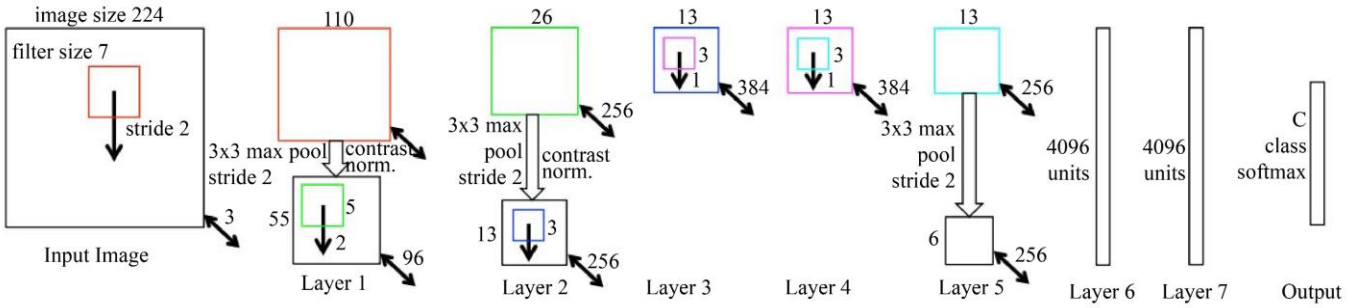

Fig. 3 Deep learning architecture based on the CNN model

The collection of all valid accepts is defined as

$$TA(d) = \{(i,j) \in P_{same}, with\ D(x_i, x_j) \leq d\}. \quad (5)$$

These face pairings (i,j) were identified at threshold d as the same by mistake. In a similar vein,

$$FA(d) = \{(i,j) \in P_{diff}, with\ D(x_i, x_j) \leq d\} \quad (6)$$

is the collection of all pairings that were mislabelled as identical. Therefore, the expression in Equation 7 is used to compute the false acceptance rate and validation rate considering face distance d.

$$VAL(d) = \frac{|TA(d)|}{|P_{same}|},\ FAR(d) = \frac{|FA(d)|}{|P_{diff}|}. \quad (7)$$

With disjoint identities, we maintain a holdout of thousands of images with the same distribution as our training set. We divided it into five sets, each with 200k photos, for examination. Next, 100k × 100k picture pairings are used to calculate the FAR and VAL rates. Over the five splits, the standard error is provided.

Although the distribution of this test set is comparable to that of our training set, it has been manually verified that it contains incredibly clean labels. It is made up of three individual photo sets totaling over 12,000 pictures. We calculate the VAL and FAR rates for every 12k squared picture pair.For face verification, According to [7], the de facto academic exam set is called Labelled Faces in the Wild (LFW). We present mean error and classification accuracy, adhering to the conventional procedure for unconstrained, labelled external data. YouTube Faces DB is a new dataset that has acquired prominence in the facial recognition field [21] [17, 15]. Although pairs of videos are utilized for verification instead of pairs of photos, the setup is identical to LFW.

4. Results and Discussion

Python implements the suggested system language, and deep learning-based libraries are available. The system is designed in such a way that it has an interface to collect the participant's user ID and password. This is the first mandatory level of authentication. Once this level of authentication is completed successfully, the system throws a challenge at the participant by providing a one-time password sent to a personal device. If the system fails to provide the correct OTP, the user is not authenticated. If the user successfully encounters the OTP challenge, then the system throws another challenge in terms of recognizing the face of the student. This third layer of authentication is based on artificial intelligence. In this phase, the system's camera captures the face of the participant and then uses a pretrained deep learning model to recognize the face. It is a supervised learning-based approach where the proposed deep learning model is trained to recognize the face of the participant accurately. The enhanced CNN model uses RMSprop as an optimization using a 0.001 learning rate of 50 epochs and batch size of 256. This model is compared with two existing models known as CNN and LSTM. This section presents the results of experiments made in this research.

4.1. Exploratory Data Analysis

This subsection offers an examination of exploratory data to reveal various aspects of data distribution dynamics. As shown in Figure 4, the number of samples in the data collection for each class is visualized. These four classes are used in the empirical study as part of a multi factor authentication system. As presented in Table 1, the data distribution for each class is provided. The first three classes have 2500 samples, while the last class has 2529 samples. As shown in Figure 5, an excerpt from the data set is provided with samples from the four classes. Experiments and observations are made with face image samples of these four classes.

Table 1. Different class and number of samples

Class Label	Count
1	2500
2	2500
3	2500
4	2529

One method is principal component analysis, which is used to analyse the data on different principal components linked to the four classes or presented in Figure 6. The data analysis using principal component analysis is presented in the form of scatter plot visualization. It shows the correlation dynamics among different variables linked to the data set considered.

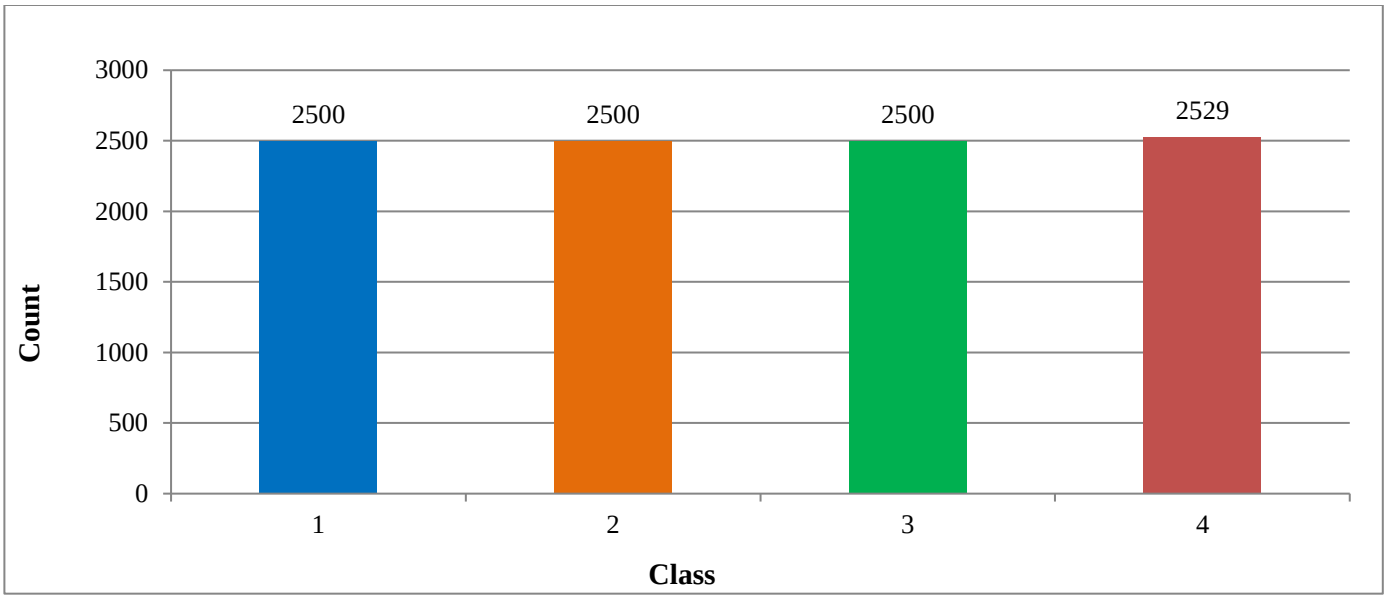

Fig. 4 Data distribution dynamics terms of four different classes

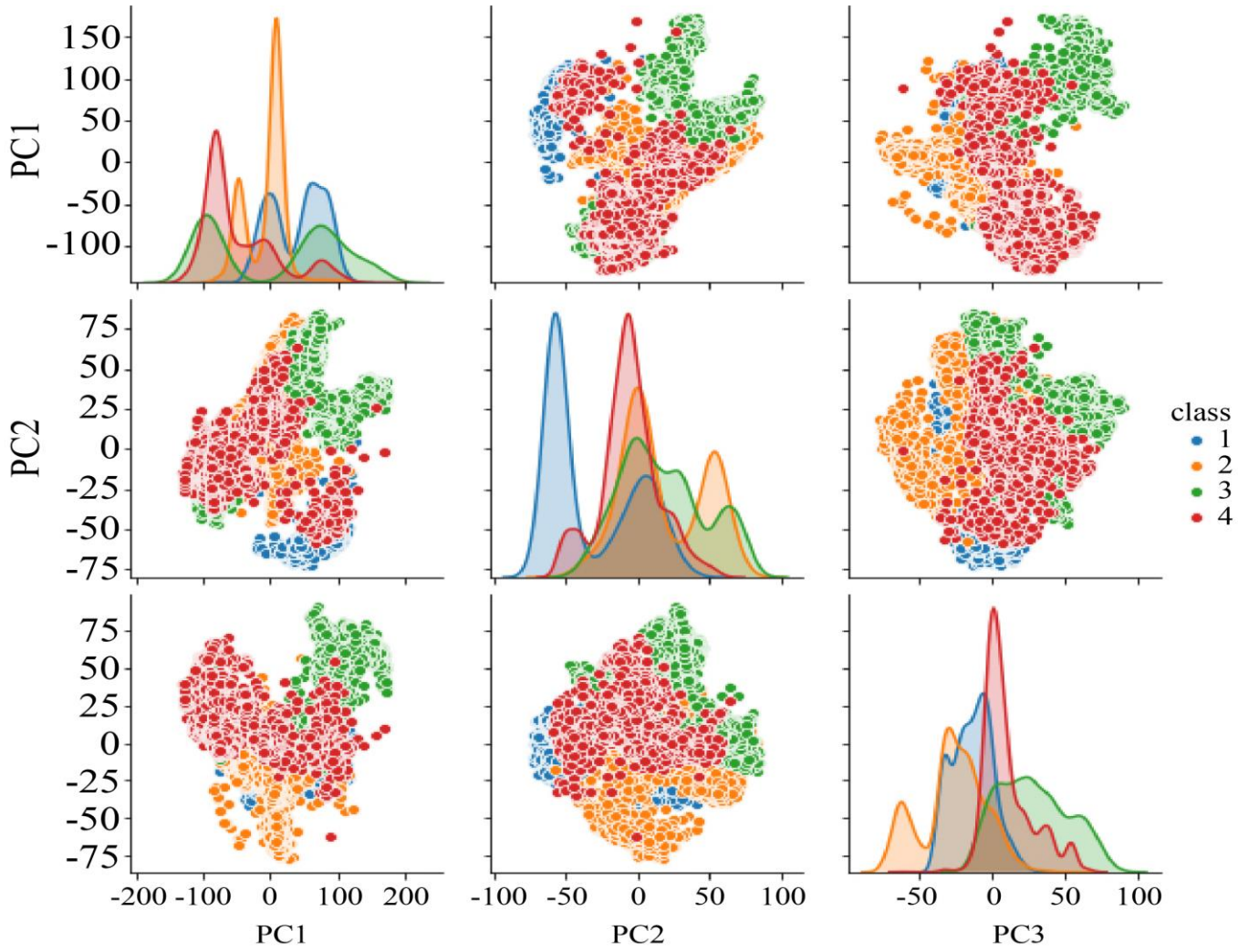

Fig. 5 An excerpt from the dataset

Fig. 6 Principal component analysis reflecting the four classeS

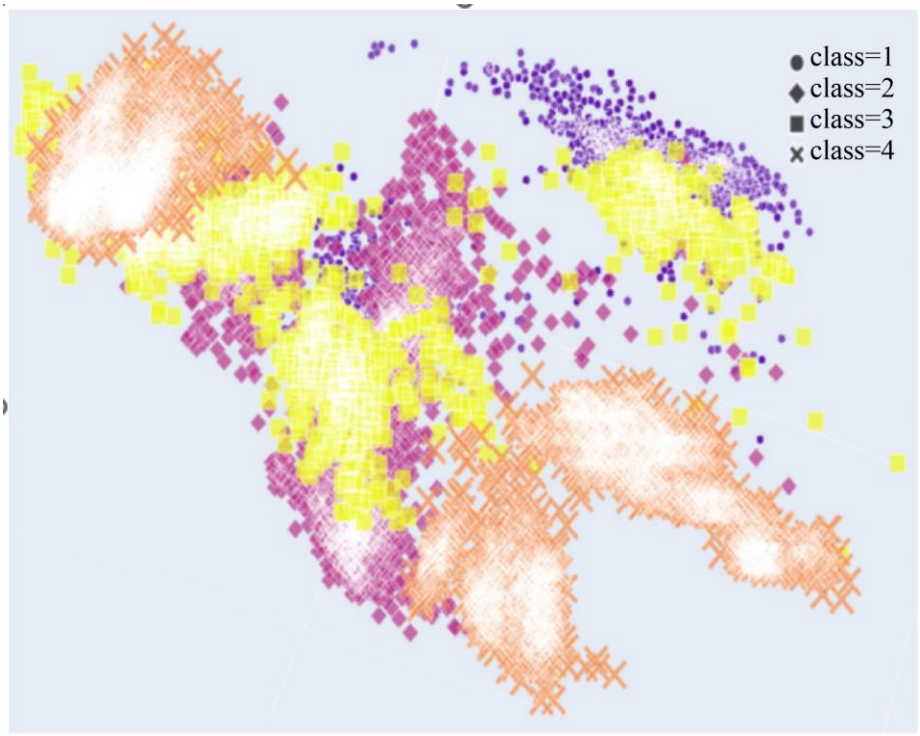

Fig. 7 The scatter plot reflecting the visualization of a data set consisting of four classes

4.2. Results of the Proposed Face Recognition Model

This section presents the results of our experiments pertaining to the face recognition model, which is an enhanced CNN model used in our empirical study.

Prior to the face recognition of the proposed system, the framework is evaluated using user credentials and OTP-based authentication. It is found from the empirical study that the system is able to handle challenges like credentials, OTP, and face recognition and process them correctly. More details about the face recognition results are as follows. The observations are made in terms of face recognition and the performance statistics related to face recognition evaluation.

The results of data augmentation are shown in Figure 8. For each class in the given sample, data augmentation is carried out to enhance data diversity and reduce the problem of overfitting in the process of supervised learning. As presented in Figure 9, a set of Eigen faces are generated in the process of principal component analysis. These are the faces that are derived from original human faces. These are useful in the process of mathematics and recognition of faces.

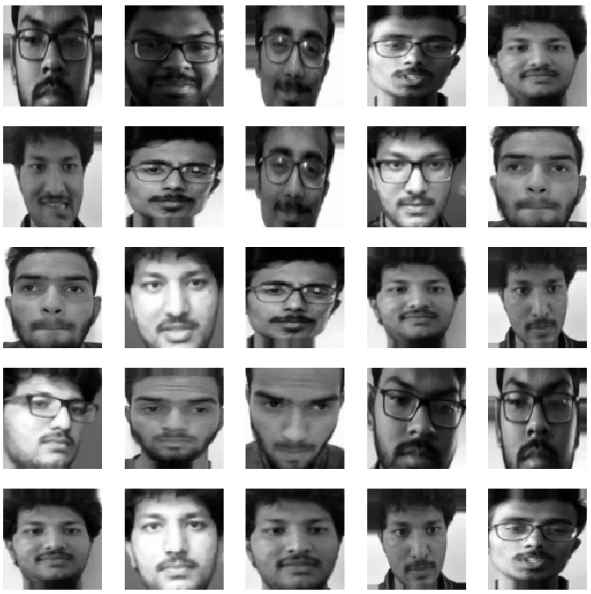

Fig. 8 Results of data augmentation

Fig. 9 Eigen faces generated as part of principal component analysis

The suggested augmented CNN model is utilized to handle facial picture data, as shown in Figure 10. Convolutional layers provide feature maps throughout this process that are helpful in identifying faces. The input picture is used to create feature maps by each convolutional layer. This is a progressive method where convolutional layers create feature maps, and max polling layers use the output to optimize the feature maps the convolutional layers have created.

Since it is a supervised learning process, it is very important to have ground truth samples. Figure 11(a) shows the ground truth for each class of samples provided in the dataset. An excerpt of the experimental results is provided in Figure 11(b), which shows the predictions made by the proposed enhanced CNN model. The results reveal that the ground truth is compared against the predicted value to reflect the correctness of the suggested framework.

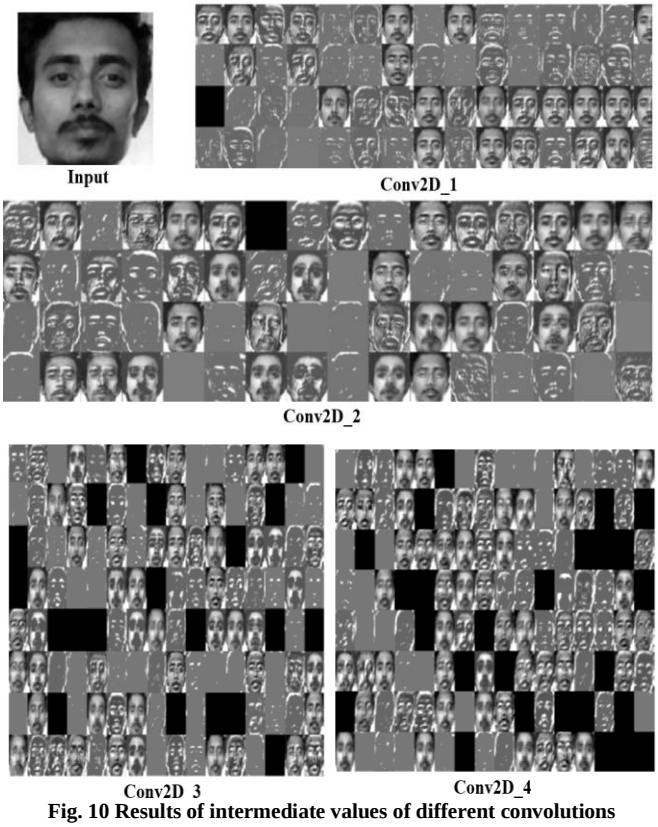

Fig. 10 Results of intermediate values of different convolutions

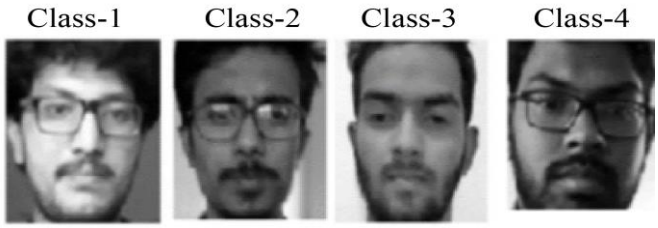

Fig. 11 (a) Ground truth of different classes

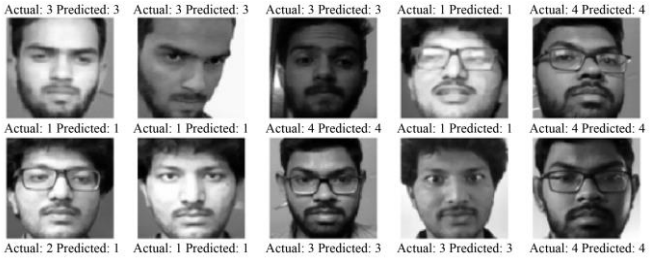

Fig. 11 (b) Results of face recognition showing ground truth label and predicted label

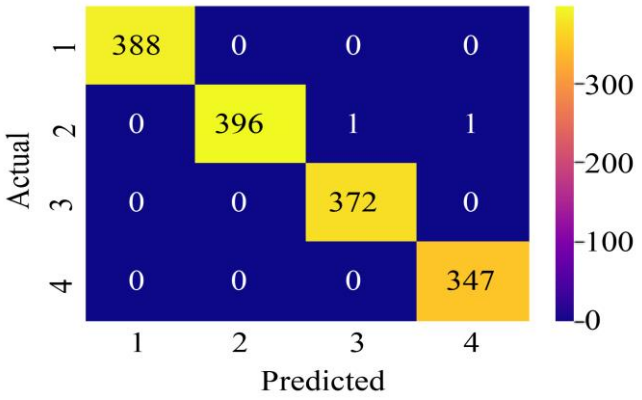

Fig. 12 Confusion matrix of the proposal enhanced CNN model

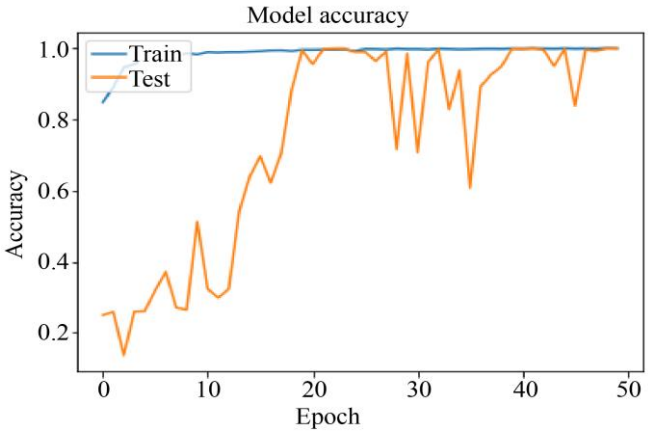

Fig. 13 (a) Modal accuracy dynamics against the number of epochs

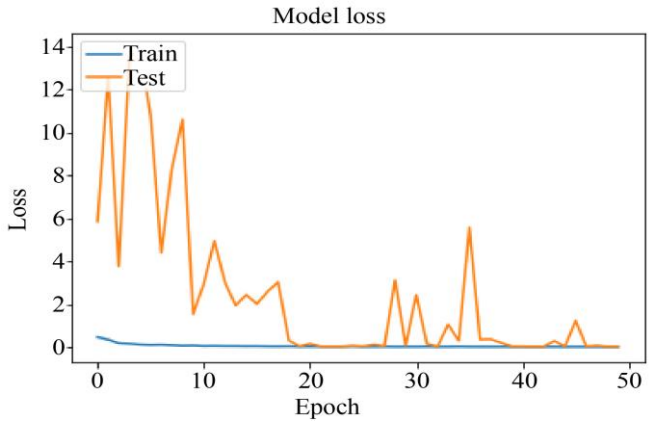

Fig. 13 (b) model loss dynamics against the number of epochs

Table 2. Results of the proposed CNN model

Model	Precision	Recall	F1-Score	Accuracy
Enhanced CNN	0.9876	0.9154	0.9501	0.9874

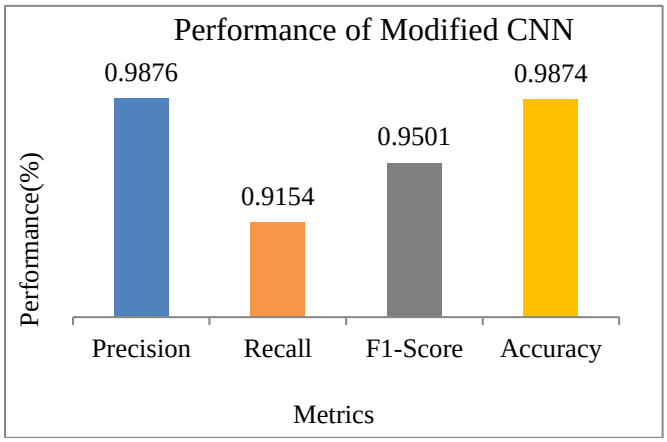

Fig. 14 Performance of the proposed enhanced CNN model

As presented in Figure 12, a confusion matrix is provided for each class, showing the predicted labels compared with ground truth labels. A different matrix is derived from the confusion matrix to assess how well the suggested model performs. The model's accuracy and loss dynamics are shown versus the number of epochs in Figures 13(a) and (b), respectively. The trials are conducted across 50 epochs. The model accuracy graph (left) illustrates how the accuracy of the model increases as the number of epochs increases. As the number of epochs increases, the model loss progressively decreases (right). At epoch number 50, the model accuracy and model loss converged to the best values. Table 2 displays the suggested CNN model's performance. Accuracy, F1-score, precision, and recall are measured for the model. The proposed deep learning model used in our empirical study is evaluated with different performance metrics. The results revealed that the model has achieved a significant level of accuracy in face recognition. It could achieve 98.76% precision, 91.54% recall, 95.01% F1-score and 98.74% accuracy.

4.3. Performance Comparison

The experimental outcomes of the suggested model are shown in this part compared with existing models like CNN and LSTM. The results of the proposed deep learning model in face recognition as part of a multi factor authentication system are compared against two existing baseline models known as CNN and LSTM.

Table 3. Performance comparison among different models

Face Recognition Model	Precision	Recall	F1-Score	Accuracy
CNN	95.44	95.81	95.62	94.12
LSTM	94.96	97.04	95.99	95.67
Enhanced CNN (Proposed)	96.03	94.66	95.34	98.48

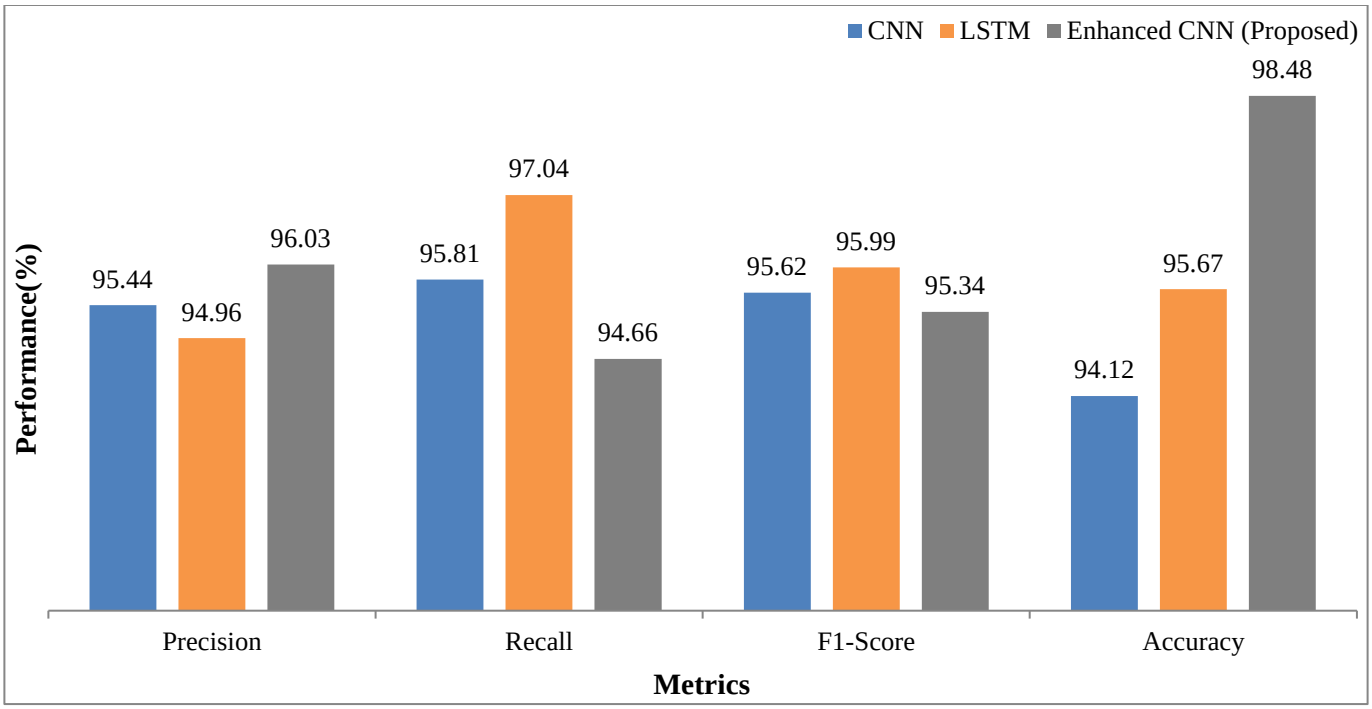

Fig. 15 Comparison of performance among different deep learning models

Figure 15 shows how the suggested model is contrasted with CNN and LSTM models. The precision of the CNN model is 95.44%, recall is 95.81%, F1-score is 95.62%, and accuracy is 94.12%. The precision of the LSTM model is 94.96%, recall is 97.04%, F1-score is 95.99%, and accuracy is 95.67%. The precision of the proposed model is 96.03%, recall is 94.66%, F1-score is 95.34%, and accuracy is 98.48%. From the results, it is observed that the proposed enhanced CNN model achieves the highest accuracy with 98.48%. Therefore, the proposed model can be used as part of multi-factor authentication systems of different entities that are involved in online education and examinations.

5. Implications of the Findings

Due to technological advancements in the needs of the real world, many educational institutions have been offering online courses and conducting examinations online. In this regard, it is indispensable to ensure integrity and robustness when conducting online examinations. In the wake of the recent COVID-19 pandemic, online education, under the usage of online collaboration platforms, has become quite common. Considering the advantages of different learning platforms bestowed by universities, the online education system has become very significant. However, there are many unresolved issues, including fraudulent behaviours of participants, technical issues while conducting online examinations and various kinds of few things' cases in computer vision applications and applications pertaining to education. In this context, the proposed research in this paper assumes importance. There have been many attempts to develop multi-factor authentication systems. However, from the literature, we found that there is a need for an AI-enabled approach integrated with traditional models to reach a greater degree of sophistication, security integrity and robustness in conducting online examinations. In the proposed system, the first layer of Securities challenges the user to provide correct credentials. The second level of challenge is to ask the user to provide a runtime password sent to the personal device. Once the user fulfils these two authentication factors, there is still a possibility that another user may try to participate in the examination of a specific user. In order to prevent this possibility, the proposed system will also have continuous monitoring of the participant with the help of live streaming video of the person. The face of the person is used to detect and recognize the person uniquely. Thus, the multi-factor authentication system with AI integration enables integrity and robustness when conducting online examinations. The proposed system has certain limitations, as discussed in section 5.1.

5.1. Limitations of the Study

The proposed system in this paper has AI enabled solution for authenticating users of online examinations fairly and accurately. However, there are certain limitations in the proposed system. The system has provision for human face recognition. Since human faces are part of biometrics, they are considered to be highly unique. The proposed system is evaluated with a relatively smaller number of samples, and there is a need to enhance the methodology with multiple data sets. Another important observation is that the proposed system lacks investigation into different cheating cases involved while conducting online examinations. Given these

limitations, there is a threat to the validity of the proposed system and its claims unless further research is done to overcome the limitations mentioned above.

6. Conclusion and Future Work

In this paper the proposed framework has mechanisms and algorithms for a multi-factor AI-enabled user authentication system to leverage integrity and robustness in online examination systems. The system has multiple layers of authentication mechanisms with an approach that throws challenges like user ID and password, one-time passwords through handheld devices, and face recognition with the assistance of deep learning algorithms. Our deep learning model for facial recognition was put out. The CNN model provides the basis for the model's architecture. It supports both max polling layers and convolutional layers. The convolutional layers produce feature maps as they gradually extract features from a given video frame. The Max pooling layers, on the other hand, are used to optimize the feature maps generated by convolutional layers. The network architecture is designed in such a way that it has improved the quality of the learning process. I proposed an algorithm known as AI enabled Multi-factor Authentication (AIMA), which has the desired mechanisms to realize the proposed framework. Our investigational study demonstrated that the suggested framework is capable of ensuring the integrity and robustness of the online examination system as far as user authentication is concerned. The AI enabled space recognition system as part of multi factor authentication is found to be superior to many existing techniques, with the highest level of precision at 98.74%. Going forward, our goal is to enhance the system by investigating different kinds of technical issues and fraudulent cases in online examinations and possible solutions to the problems.

References

[1] Mireya Lucia Hernandez-Jaimes et al., "Artificial Intelligence for IOMT Security: A Review of Intrusion Detection Systems, Attacks, Datasets and Cloud-Fog-Edge Architectures," *Internet of Things*, vol. 23, pp. 1-33, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Shunliang Zhang, and Dali Zhu, "Towards Artificial Intelligence-Enabled 6G: State of The Art, Challenges, and Opportunities," *Computer Networks*, vol. 183, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Zhi Zhou et al., "Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738-1762, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Chafika Benzaid, Tarik Taleb, and Muhammad Zubair Farooqi, "Trust in 5G and Beyond Networks," *IEEE Network*, vol. 35, no. 3, pp. 212-222, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Chafika Benzaid, and Tarik Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network*, vol. 34, no. 3, pp. 124-133, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Yusra Abdulrahman et al., "AI and Blockchain Synergy in Aerospace Engineering: An Impact Survey on Operational Efficiency and Technological Challenges," *IEEE Access*, vol. 11, pp. 87790-87804, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Huangxun Chen et al., "EchoFace: Acoustic Sensor-Based Media Attack Detection for Face Authentication," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2152-2159, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Maheen Zulfiqar et al., "Deep Face Recognition for Biometric Authentication," *2019 International Conference on Electrical, Communication, and Computer Engineering*, Swat, Pakistan, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hind Baqeel, and Saqib Saeed, "Face Detection Authentication on Smartphones: End Users Usability Assessment Experiences," *2019 International Conference on Computer and Information Sciences*, Sakaka, Saudi Arabia, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Navya Saxena, and Devina Varshney, "Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks," *International Journal of Cognitive Computing in Engineering*, vol. 2, pp. 154-164, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xinman Zhang et al., "An Efficient Android-Based Multimodal Biometric Authentication System with Face and Voice," *IEEE Access*, vol. 8, pp. 102757-102772, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Young Kyun Jang, and Nam Ik Cho, "Deep Face Image Retrieval for Cancelable Biometric Authentication," *2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance*, Taipei, Taiwan, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Vera Wati et al., "Security of Facial Biometric Authentication for Attendance System," *Multimedia Tools and Applications*, vol. 80, pp. 23625-23646, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Emna Fourati, Wael Elloumi, and Aladine Chetouani, "Anti-Spoofing in Face Recognition-Based Biometric Authentication Using Image Quality Assessment," *Multimedia Tools and Applications*, vol. 79, pp. 865-889, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Muhammad Irwan Padli Nasution et al., "Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic," *2020 3rd International Conference on Computer and Informatics Engineering*, Yogyakarta, Indonesia, pp. 48-51, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Xiang Wang et al., "A Privacy-Preserving Edge Computation-Based Face Verification System for User Authentication," *IEEE Access*, vol. 7, pp. 14186-14197, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Chen Wang et al., "User Authentication on Mobile Devices: Approaches, Threats and Trends," *Computer Networks*, vol. 107, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Dana Weitzner, David Mendlovic, and Raja Giryes, "Face Authentication from Grayscale Coded Light Field," *2020 IEEE International Conference on Image Processing*, Abu Dhabi, United Arab Emirates, pp. 2611-2615, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mikel Labayen et al., "Online Student Authentication and Proctoring System Based on Multimodal Biometrics Technology," *IEEE Access*, vol. 9, pp. 72398-72411, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jinsu Kim, and Namje Park, "Lightweight Knowledge-Based Authentication Model for Intelligent Closed-Circuit Television in Mobile Personal Computing," *Personal and Ubiquitous Computing*, vol. 26, pp. 345-353, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Abdeljebar Mansour et al., "A Lightweight Seamless Unimodal Biometric Authentication System," *Procedia Computer Science*, vol. 231, pp. 190-197, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Vipul Vekariya et al, "Multi-Biometric Fusion for Enhanced Human Authentication in Information Security," *Measurement: Sensors*, vol. 31, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Wang Yao et al., "A Study on the Effect of Ageing in Facial Authentication and the Utility of Data Augmentation to Reduce Performance Bias Across Age Groups," *IEEE Access*, vol. 11, pp. 97118-97134, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Bahareh Nakisa et al., "Using an Extended Technology Acceptance Model to Investigate Facial Authentication," *Telematics and Informatics Reports*, vol. 12, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Lin Li et al., "A Survey of PPG's Application in Authentication," *Computers & Security*, vol. 135, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Pietro Ruiu et al., "Enhancing eID Card Mobile-Based Authentication Through 3D Facial Reconstruction," *Journal of Information Security and Applications*, vol. 77, pp. 1-14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Tingcong Jiang et al., "FaceGroup: Continual Face Authentication via Partially Homomorphic Encryption & Group Testing," *2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems*, Toronto, ON, Canada, pp. 443-451, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Wang Yao et al., "Toward Robust Facial Authentication for Low-Power Edge-AI Consumer Devices," *IEEE Access*, vol. 10, pp. 123661-123678, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Alakananda Mitra et al., "iFace 1.1: A Proof-of-Concept of a Facial Authentication Based Digital ID for Smart Cities," *IEEE Access*, vol. 10, pp. 71791-71804, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] M. Vasanthi, and K. Seetharaman, "Facial Image Recognition for Biometric Authentication Systems Using a Combination of Geometrical Feature Points and Low Visual Features," *Journal of King Saud University - Computer and Information Sciences*, vol. 24, no. 7, pp. 4109-4121, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] John Duchi, Elad Hazan, and Yoram Singer, "Adaptive Subgradient Methods for Online Learning and Stochastic Optimization," *Journal of Machine Learning Research*, vol. 12, pp. 2121-2159, 2011. [Google Scholar] [Publisher Link]

[32] Gary B. Huang et al., "Labeled Faces in The Wild: A Database for Studying Face Recognition in Unconstrained Environments," *Workshop on Faces in'Real-Life'Images: Detection, Alignment, and Recognition*, Marseille, France, pp. 1-15, 2008. [Google Scholar] [Publisher Link]

[33] Yi Sun et al., "Deep Learning Face Representation by Joint Identification-Verification," *Advances in Neural Information Processing Systems*, vol. 27, 2014. [Google Scholar] [Publisher Link]

[34] Yi Sun, Xiaogang Wang, and Xiaoou Tang, "Deeply Learned Face Representations Are Sparse, Selective, And Robust," *2015 IEEE Conference on Computer Vision and Pattern Recognition*, Boston, MA, USA, pp. 2892-2900, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[35] Christian Szegedy et al., "Going Deeper with Convolutions," *2015 IEEE Conference on Computer Vision and Pattern Recognition*, Boston, MA, USA, pp. 1-9, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[36] Yaniv Taigman et al., "Deepface: Closing the Gap to Human-Level Performance in Face Verification," *2014 IEEE Conference on Computer Vision and Pattern Recognition*, Columbus, OH, USA, pp. 1701-1708, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[37] Kilian Q. Weinberger, and Lawrence K. Saul, "Distance Metric Learning for Large Margin Nearest Neighbor Classification," *Journal of Machine Learning Research*, pp. 207-244, 2009. [Google Scholar] [Publisher Link]

[38] D. Randall Wilson, and Tony R. Martinez, "The General Inefficiency of Batch Training for Gradient Descent Learning," *Neural Networks*, vol. 16, no. 10, pp. 1429-1451, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[39] Lior Wolf, Tal Hassner, and Itay Maoz, "Face Recognition in Unconstrained Videos with Matched Background Similarity," *CVPR*, Colorado Springs, CO, USA, pp. 1-6, 2011. [CrossRef] [Google Scholar] [Publisher Link]