Enhancing Banking Access Control with Cloud-Integrated Neural Network Security

Ummadi. Surya Venkata Sekhar
Project Student, Department of Artificial Intelligence and Data Science
Lakireddy Bali Reddy College of Engineering (Autonomous), Mylavaram, AP, India
suryaelonm@gmail.com

Kalapala. Hema Chandana
Project Student, Department of Artificial Intelligence and Data Science
Lakireddy Bali Reddy College of Engineering (Autonomous), Mylavaram, AP, India
hemachandana.ds@gmail.com

Uddanti.Venu Gopala Rao
Project Student, Department of Artificial Intelligence and Data Science
Lakireddy Bali Reddy College of Engineering (Autonomous), Mylavaram, AP, India
uddantivenugopal5@gmail.com

Abstract- **By introducing a novel security paradigm that gets around the drawbacks of biometrics and video monitoring, this research solves shortcomings in conventional banking access control. To improve intrusion detection and tighten access control, the system combines neural net, google cloud, and network-messaging applications. The core is a multi-layered security system, where the first layer starts with picture capture. This layer uses transfer learning to validate people, allowing access to only verified humans. Convolutional Neural Networks (CNNs) are utilised in the second layer to process photos and verify the individual's identity as the locker owner. The image is instantly sent via cloud and network applications to the owner's device upon access denial. Users need to input a password at the third layer, and if they enter it correctly, an OTP is generated. After three failed tries at entering the password, the system alerts the owner with an OTP that contains the image that was collected. Opening the locker is part of the fourth layer, which is constantly watched. Strong security mechanisms are used by each layer, such as CNNs, transfer learning, and smooth network and cloud integration. This all-encompassing security solution, which is implemented using a web framework built on Python, is successful in strengthening access control at every level.**

Keywords: **Neural Nets, Mobilenet_V2, Cnn, Google Cloud, Transfer-Learning Access Control, Bank-Security, Multiple security layers.**

I. INTRODUCTION

Innovative solutions are more important than ever in the rapidly evolving field of financial security, where unauthorised access presents persistent problems and growing risks. This research, which is at the forefront of technical innovation, provides a revolutionary security paradigm dubbed "Enhancing Banking Access Control with Cloud-Integrated Neural Network Security" to secure vital domains.

To strengthen access control, the current state of traditional banking security systems combines security cameras, passwords, and biometric information. However, there are a number of serious issues with this strategy that frequently come up, such as complicated user interfaces, restricted real-time monitoring, and slow reactions to unwanted access. In light of these shortcomings, it is clear that a system that is intelligent, quick, and flawlessly responsive is required.

The system under consideration is a trailblazing solution to these problems, elegantly integrating state-of-the-art technologies to completely reimagine the financial security scene. The clever use of sophisticated neural networks, which purposefully take pictures of access attempts in real time using Personal Identification Numbers (PINs), is essential to its effectiveness. The careful processing of the neural network, which was trained on a large dataset, guarantees proficient user identity identification, strengthening access control fundamentally.

The benefits of the suggested approach underscore its need for financial security even more. This system impresses with its safe, fast, scalable, and incident-management capabilities. Its features include the ability to quickly dispatch images of unauthorised persons, records related to the users are maintained, better accuracy via the use of deep learning algorithms, and conduct thorough data analysis.

II. LITERATURE SURVEY

A novel method for filling up important security vulnerabilities in banking is presented in the paper "Cross-Domain Deep Face Matching for Real Banking Security Systems" [1]. Enhancing face matching accuracy for banking security applications is the methodology's top priority, and it makes use of

Convolutional Neural Networks (CNN) [1]. But this innovative endeavour highlights a number of difficulties, such as lengthy processing times, managing large amounts of data, and dealing with inadequate actual-time surveillance [1].

In the paper "Bank Locker Protection with Liveness Detection Using Machine Learning," researchers use technologies like Convolutional Neural Networks (CNN) and Haar Cascade to integrate face recognition with liveness detection mechanisms, offering a novel security solution [2]. Notwithstanding its improvements, the system has drawbacks, such as the incapacity to detect unsanctioned users visually and shortcomings in incident handling [2]. It is accepted that real-time monitoring is restricted, and the security system as a whole is thought to be somewhat straightforward [2].

Enhancing bank locker security is the goal of the "Cloud Computing based Intelligent Bank Locker System," which incorporates wirelessly switches, a Raspberry-Pi-3, GSM-technology, and a finger-print reader [3]. The system's clever approach to secure locker access is highlighted by the use of Cloud, IoT, and GSM technologies [3]. However, the suggested solution has some shortcomings, such as relying only on fingerprint verification, lacking live monitoring functionality, and without a user-maintained log history [3].

The study "Real-Time Object Detection Using SSD" uses Tensor-Flow (TF) and Opencv-Python to develop the Single Shot Multibox Detector (SSD) algorithm in the goal of real-time object detection for bank security [4]. The work's shortcomings, including its reliance on CCTV inputs and limited live monitoring, may limit its applicability and make it less suitable for high-end security requirements even with its creative methodology [4].

An SVM-based model for improving banking automation is introduced in the article "Intelligent Performance-Aware Adaptation of Control Policies for Optimising Banking Teller Process Using Machine Learning" [5]. Nevertheless, live maintenance is a challenge due to the model's proneness to overfitting or underfitting [5].

Our goal in the proposed effort is to fill the gaps that have been found and expand on the knowledge from the previous research. Motivated by the difficulties outlined in other studies, our strategy combines state-of-the-art technologies with innovative approaches to offer strong responses to the constraints mentioned in the literature.

III. METHODOLOGY

A. Dataset Collection:

1. Creating Datasets for Human Identification

The human detection dataset forms the basis of the first layer of the security system and is in charge of verifying the authenticity of users seeking to get access. There are 2000 photos in this dataset, divided into two groups: "Human" and "Not Human." There are 1000 photos per class, which helps to create a well-rounded and extensive collection. This dataset's photos are all saved in commonly used file formats, either jpg or png. This guarantees interoperability and simplicity of incorporation with different machine learning and image processing frameworks.

2.Collection Methodology:

The dataset was carefully selected to include a range of situations and differences in human presence. Various publicly accessible datasets were used to source the images, guaranteeing a wide range of human features, positions, and environmental circumstances. Furthermore, an attempt was made to incorporate difficult settings with various lighting, perspectives, and complicated backgrounds.

3. Creating Datasets for Owner Identification:

The second dataset, which is essential for the owner detection-focused second layer of the system, is made up of 4000 photos divided into two groups: "Owner" and "Not Owner." A balanced distribution is achieved within the dataset by carefully populating each class with 2000 photos. To maintain uniformity and ease of integration, this dataset's images are all saved in jpg or png format, just like the human detection dataset.

4. Collection Methodology:

An intentional strategy was used to gather photos in order to identify the owner. Images of authorised users make up the "Owner" class, which guarantees a complete picture of authorised users. These photos, which were taken in controlled settings, were added to the dataset to increase its diversity by include a range of stances and facial expressions. The "Not Owner" class comprises photos that show situations in which people try to enter unauthorised areas without authorization. This covers a range of situations, including somebody attempting to enter without the proper identification or PIN.

B. Implementation:

The four crucial layers of the neural network security system become visible as we move from theory to practice. Each layer is specifically created to strengthen access control within the context of banking security.

1. Layer 1: Accurate Human Verification Detection

The primary aim of our initial neural net security layer is to ascertain the requester's human identity. We've diligently sorted the dataset into categories reflecting humans and non-humans, organized within the 'individual_data' directory. Leveraging TensorFlow's image dataset tools, we've extensively processed the data, ensuring rapid loading, optimizing RGB values, and implementing consistent image resizing. This preliminary preparation phase ensures the creation of a meticulously selected dataset, laying the foundation for subsequent model training.

After the dataset preparation, the data is smartly divided into 70%-training, 20%-validation, and 10%-test subsets. This is a crucial stage in determining the model's capacity for generalisation. We use a strong feature extractor, a pre-trained MobileNetV2 model, to extract significant characteristics for human identification. Crucially, this model is meticulously set up to eliminate its uppermost classification layer, so preserving its acquired features and perfectly conforming to the binary classification requirements of our assignment.

The resulting framework integrates smoothly a dense layer featuring a sigmoid activation function with the powerful MobileNetV2 feature extractor. The integration can be expressed mathematically as follows: result = σ(Vm+d), where (V) for Weights, (m) for mobileNet characteristic extractor input, (d) for the prejudice element known as bias, and σ for the sigmoid activation function. With this setup, the system is configured for binary classification, differentiating between items that are human and those that are not. The model is compiled using the binary-cross-entropy loss using the 'Adam' optimizer during training. TensorBoard is used to provide comprehensive logging while its performance is tracked over 30 epochs. This first layer's resilience is demonstrated by the visualisation of training and validation losses as well as metrics like accuracy, precision, recall, and binary correctness. These measures reinforce the system's capacity to correctly detect and categorise entities that are seeking to get access.

2. Layer 2: Accurate Owner Verification Detection

In the second tier, our goal is to verify the person's identity as the owner of the safe locker. The 'Owner' dataset is carefully arranged to create a balanced dataset, containing 2000 photos each class ('Owner' and 'Not Owner'). Preprocessing entails resizing photos and maximising RGB values to guarantee consistency for efficient model training. Then, to enable thorough training and assessment, the dataset is logically split into training (70%), validation (20%), and test (10%) sets.

Convolutional Neural Network (CNN) layers are incorporated into a sequential model architecture in order to extract features. The 16-filter initial convolutional layer is where the architecture starts. Each filter uses a 3x3 kernel to mathematically execute a convolution operation on the input image. The network gains non-linearity from the ReLU activation function, enabling it to recognise intricate correlations in the data ($f(x) = \max(0, x)$). Using a stride of 1 is crucial since it makes sure that the convolution operation carefully examines the input's spatial dimensions and preserves detailed information.

The next stage is max-pooling, which is a downsampling method that minimises spatial dimensions while preserving important features. By helping to highlight the most important features of the picture, this procedure improves the network's capacity to identify pertinent patterns. With 32 filters in the second convolutional layer, which has a similar pattern but more, the network can capture more complex characteristics.

A third convolutional layer with sixteen filters is purposefully incorporated into the architecture to preserve a balance between computational efficiency and complexity. A max-pooling operation is added to each convolutional layer to guarantee that the network can comprehend characteristics at many sizes with subtlety because it learns interpretations that are organised hierarchically.

The convolutional layers are followed by the slanting phase, which turns the highest-level feature map into a one-dimensional array. Then, using 256 units, this compressed shape is placed into a densely connected layer. Here we apply the ReLU activation function after computing the weighted sum of the inputs mathematically. In this layer, the output formula of one neuron is g(x)=maximum (0, $\sum_{i=1}^{256}(pi * qi + d)$) where ($p_i$) stands Weights and ($q_i$) stands for inputs.

With a sigmoid activation function and a single unit, the final layer is dense. Because the sigmoid function produces values in the range of (0, 1), which represent the probability of ownership, this setup is appropriate for binary classification. The decision threshold is often set at 0.5, which means that values more than 0.5 indicate "the

proprietor," whereas values less than 0.5 indicate "Not Proprietor."

This architecture is trained over a predetermined number of epochs—each of which is a full run through the dataset. During training, accuracy measurements and the loss function—which is calculated using binary cross-entropy—are used to monitor the model's performance. An adaptive learning rate optimisation algorithm called an Adam optimizer manages the training process. Using criteria for binary accuracy, precision, and recall, a quantitative assessment is conducted throughout the evaluation phase.

To summarise, the convolutional and densely linked layers of this painstakingly designed CNN architecture are specifically designed to extract complex information from input photos, enabling the system to make imperceptible decisions on the right of ownership of those requesting entry.

Evaluation metrics in 1,2 Layers:

I. Precision (P) = $\frac{TP}{TP+FP}$

II. Recall (R) = $\frac{TP}{TP+FN}$

II. F1-Score (F1) = $\frac{2*(P*R)}{(P+R)}$

III. Accuracy (Acc) = $\frac{TP+TN}{Total\ Examples}$

3. Layer 3: Validating Passwords and Managing Incidents

The user is greeted by a strong password authentication process at the third layer of our system, which is essential to guaranteeing legitimate access to the locked locker. Here the user is given with three chances to enter the correct password. A strong protective feature, the password serves as a crucial entry point to the next tiers and the final admission to the locker room. The password entering process has been thoughtfully engineered to identify and authenticate every attempt.

The linked code makes use of a Flask web application to process and compare user-inputted passwords to a predefined, proper password. The system starts a sequence of events if the password that was entered meets the predetermined requirements. To ensure confidentiality and accessibility, the system first starts saving the taken image in Google Drive. This process is contained in the specific method `drive_link_generator()'. By connecting to the user's Google Drive account, this method makes use of Google Drive API authentication. After that, the captured facial image is uploaded and its sharing settings are set to allow public access. The uploaded image's unique link is created, offering a safe and direct path for further operations.

The `alert_send_pic(link)` function uses Twilio, a cloud communications provider, after the picture upload is successful. This feature makes use of Twilio's ability to instantly notify the specified user of the locker access. A link to the photo is included in the alert message so the owner may verify the person trying to gain access with their eyes. Real-time communication is ensured by Twilio's smooth integration, which improves the system's capacity to react quickly to security situations.

When three failed password attempts are more than is allowed, the system takes preventative action to make sure security is maintained. The photographed is immediately saved to Google Drive in case it is needed for forensic examination. Twilio-sms is used to alert the individual of the exceeded attempts and prompt them to report the incident for the police at the same time. Our innovative neural net system's general safety stance is strengthened by this multi-layered security strategy, which protects against unauthorised access and offers a strong foundation for individual warning and issue management.

4. Layer 4: Layers of Access and Monitoring

Final and fourth layer, called "Access and Monitoring Layer," serves as a doorway for authorised people to access the secured locker. Compared to the other levels, which focused on intricate safeguards and personal verification, this layer makes it simpler for individuals to get into the locker and retrieve or keep their belongings. Through the smooth integration of certified users into the physical access control procedures, the system guarantees a secure and convenient journey to the locker area.

The usefulness of this layer goes beyond simple access since it continuously tracks and logs the locker's status in real time. In addition to aiding security audits and keeping an exhaustive log of all access actions, the continuous monitoring offers insightful information about access occurrences. The Access and Monitoring Layer is an essential component of the entire security system because it offers an easy-to-use interface and robust surveillance features to quickly detect and address any possible threats related to security, even in spite of its straightforward role in enabling authorised access.

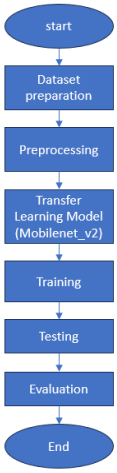

Fig 1: Layer 1: Mobilenet Model Development

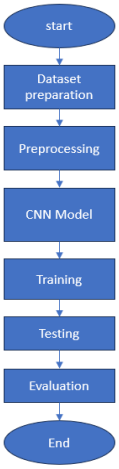

Fig 2: Layer 2: CNNs Model Development

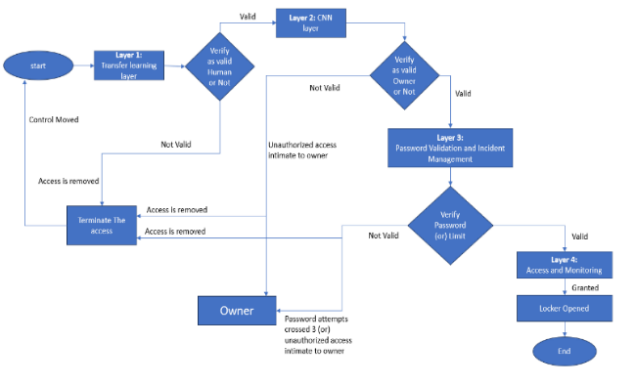

Fig 3: Architecture of the working system

IV. RESULTS

We carefully provide tables with key accuracy metrics, including precision, recall, F1-Score, and overall accuracy, in the results section. The performance of our Security System at each layer is provided in these tables in a comprehensive and quantitative manner. With the help of F1-Score balanced measurement calculations are given between recall and precision, Positive forecasts are accurate, according to the precision evaluation, while recall indicates the system's capacity to record all pertinent instances. Furthermore, the total accuracy statistic captures how well the system classifies entities that are attempting to gain access. This tabular format aims to provide an understandable and in-depth assessment of how the system performs across multiple metrics, enabling a more nuanced understanding of the system's capabilities. This thorough analysis seeks to demonstrate the strengths of each layer separately as well as their synergistic ability to strengthen our security system as a whole. Additionally, graphs and a variety of test-related output findings are included in this area.

Evaluation Metrics values	**Pre-trained Model (MobileNet_v2) (Epochs=50)**
Precision value	91.99%
Recall value	93.52%
F1-Score value	94.66%
Accuracy value	96.99%

Table 1: Metric for evaluating the primary layer using pre-trained model

Evaluation Metrics values	**CNNs Model (Epochs=50)**
Precision value	90.99%
Recall value	92.52%
F1-Score value	93.66%
Accuracy value	95.99%

Table 2: Evaluation Metrics for second layer using CNNs model

Fig 4: Outputs at Layer1 and Layer2

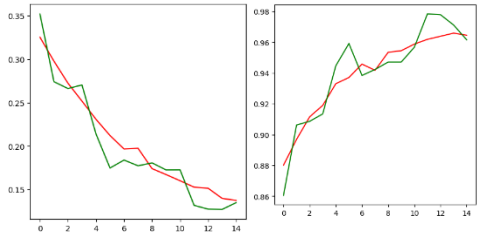

Fig 5: Graphs showing Loss and accuracy related to Mobilenet_V2 during Training

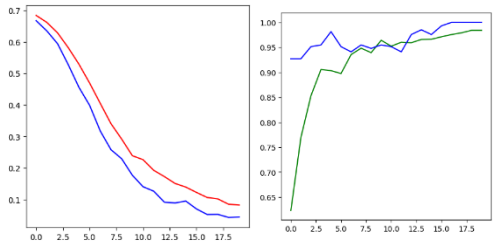

Fig 6: Graphs showing Loss and Accuracy related to CNN during Training

V. CONCLUSION

In conclusion, Enhancing Banking Access Control with Cloud-Integrated Neural Network Security is a cutting-edge and all-encompassing security paradigm. Sophisticated technologies like cloud computing, transfer learning, and Convolutional Neural Networks (CNNs) are all seamlessly integrated to provide strong password validation, effective alerting, and reliable identification of both owners and humans. The architecture with multiple layers guarantees a strong resistance against unwanted access attempts.

But with any developing technology, there's always potential for development. Subsequent improvements might concentrate on improving intrusion detection algorithms, offering different protection measures, adding more security layers to accommodate looking into fresh dangers and tracking capacities in instantaneously. These initiatives would support the system's continued development and guarantee its resistance to changing security threats in the banking industry.

VI. REFERENCES

[1] Oliveira, Johnatan S., et al. "Cross-domain deep face matching for real banking security systems." 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG). Ieee, 2020.

[2] Vishwakarma, Monika, et al. "BANK LOCKER PROTECTION WITH LIVENESS DETECTION USING MACHINE LEARNING."

[3] Devi, A., M. Julie Therese, and G. Premalatha. "Cloud computing based intelligent bank locker system." Journal of Physics: Conference Series. Vol. 1717. No. 1. IOP Publishing, 2021.

[4] Saji, Ruhin Mary, and N. V. Sobhana. "Real Time Object Detection Using SSD For Bank Security." IOP Conference Series: Materials Science and Engineering. Vol. 1070. No. 1. IOP Publishing, 2021.

[5] Tay, Bilal, and Azzam Mourad. "Intelligent performance-aware adaptation of control policies for optimizing banking teller process using machine learning." IEEE Access 8 (2020): 153403-153412.

[6] Kakadiya, Rutvik, et al. "Ai based automatic robbery/theft detection using smart surveillance in banks." 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2019.

[7] Mounika, N. Chnadra, and M. Vamsi Krishna. "ANDROID BASED SECURITY SYSTEM FOR BANK LOCKERS." Journal of Engineering Sciences 14.05 (2023).

[8] Tayade, Sejal, et al. "Face and Liveliness Detection Based Smart Bank Locker."

[9]https://tfhub.dev/google/tf2-preview/mobilenet_v2/feature_vector/4