INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

OPEN ACCESS

Received: 24-04-2024

Accepted: 12-09-2024

Published: 04-10-2024

Citation: Manjupargavi R, Srinath MV (2024) Building a Fingerprint Recognition Structure as a Security Mechanism to Verify the Identities of Users in Cloud Environment through Resnet-18. Indian Journal of Science and Technology 17(37): 3898-3908. https://doi.org/10.17485/IJST/v17i37.1358

[*] **Corresponding author**.

mprithishni5@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Building a Fingerprint Recognition Structure as a Security Mechanism to Verify the Identities of Users in Cloud Environment through Resnet-18

R Manjupargavi[1]*, M V Srinath[2]

1 Research Scholar, PG and Research Department of Computer Science, S.T.E.T Women's College (Autonomous), Affiliated to Bharathidasan University, Mannargudi, Tamil Nadu, India
2 Research Advisor, PG and Research Department of Computer Science, S.T.E.T Women's College (Autonomous), Affiliated to Bharathidasan University, Mannargudi, Tamil Nadu, India

Abstract

Objectives: To authenticate users employing fingerprint recognition thereby strengthening a security mechanism in a cloud environment. **Methods:** This study presents a novel approach for fingerprint detection in cloud systems by combining deep learning with metaheuristic optimization. A novel approach based on ResNet-18 for feature extraction and Thermal Exchange Optimization (TEO) classification is presented. This method aims to reduce data duplicity and provide safe access rights. When tested on 80% of the NIST and BDAL datasets, the proposed ResNet-18-TEO method outperforms existing models concerning recognition rates of 95.3% and 94.3% respectively. **Findings:** The experimental results reveal a False Acceptance Rate (FAR) spanning 0.6% to 4.8% and a False Rejection Rate (FRR) spanning 1.1% to 5.3%. **Novelty:** The proposed method would help cloud-based security since its fingerprint recognition time is substantially less than 25 seconds in training and 15 seconds in testing that of existing processes. In future work, this research will improvise using several deep learning techniques which are adopted using real time or research dataset.

Keywords: Fingerprint recognition; Cloud; Security; Authentication; Privacy

1 Introduction

Cloud computing brings main challenges largely related to data security, dependability, and unauthorized access [1]. One of the traditional security systems that has demonstrated inadequate against sophisticated cyber-attacks is password-based authentication [2]. Especially fingerprint identification, biometrics offers a more secure and user-friendly replacement for authentication [3]. Still, including fingerprint identification into cloud systems causes new challenges. Strictly saving and sending biometric data will help to prevent abuse and breaches [4]. Reducing erroneous acceptances (FAR) and rejections (FRR) [5] yet attaining excellent recognition accuracy. Control of large volumes of biometric data in a cloud system [6]. This can be avoided by ensuring a rapid recognition procedure free of bottleneck [7,8].

This work addresses the fundamental problem of demand of a strong and safe biometric authentication solution for cloud environments. Sometimes current methods fall short in accurately balancing security, accuracy, and cost. Great accuracy and dependability in fingerprint recognition are thus guaranteed by developing a new method combining modern deep learning techniques for feature extraction with a quick optimization algorithm for classification. The research falls short in the integration of multiple biometric modalities (e.g., dynamic signatures, facial recognition, and fingerprints) within a unified cloud-based framework. Existing works focus on single biometric methods, lacking comprehensive analysis on cross-modal performance, security, and efficiency, especially in diverse real-time scenarios and edge environments.

The main objectives of this research are:

1. ResNet-18 finds discriminative features from fingerprint photos using a deep convolutional neural network.
2. Accurate and consistent fingerprint feature classification with Thermal Exchange Optimization (TEO)
3. To design the system with high security criteria lowering data redundancy
4. To test the proposed method on the NIST and BDAL fingerprint datasets and assess its performance in respect with present methods.

In [9], the authors propose BAM Cloud, a mobile biometric authentication system that performs its operations in the cloud and takes use of dynamic signatures. The BAM Cloud process flow includes functions such as data collecting utilizing any mobile device, storage, preprocessing, and distributed system training. All of these activities take place on the cloud. Recently, the Hadoop platform has been utilizing Map Reduce in order to accelerate the processing. For the purpose of training the models, we have made use of the Leven berg-Marquardt backpropagation neural network approach. Consequently, the performance has improved by 96.23%, and the acceleration has increased by 8.5 times the pace at which it was initially moving.

In [10], authors provide a method that is both safe and effective for detecting fingerprints that are stored in the cloud system named Immersive Online Biometric Authentication Algorithm (IOBAA). The proposed method makes extensive use of the processing power that is available in the cloud because the cloud service provider is responsible for conducting the majority of the complicated calculations. The results of the tests conducted on the Amazon Elastic Compute Cloud (EC2) demonstrated that the proposed method outperforms the current state of affairs while also providing clients with protection through the utilization of symmetric homomorphic encryption. While the authentication process is in progress, neither the cloud provider nor the database that stores fingerprint impressions have access to the user's fingerprint data, according to the findings of the security investigations.

The authors of [11] propose a biometric identification technique named Cloud-based Finger Impression Identification (CFII) for immersive online guiding that makes use of facial recognition alongside mobile edge computing in the cloud. Through the utilization of the combined technologies, we construct the effective model. In order to validate the suggested framework, we compare it to a number of different approaches that are considered to be state-of-the-art.

A fingerprint attendance tracking system that is cloud-based and has built-in Convolutional Neural Networks (CNN Cloud) for enhanced biometric authentication is reportedly available, as stated in [12]. Through the utilization of cloud computing, the system is able to centralize the storage and analysis of data, which ultimately results in the utilization of attendance records and analytics that are easily accessible. Using fingerprint identification, which is a reliable biometric modality, the suggested method makes use of convolutional neural networks (CNNs), which improve both the speed and accuracy of fingerprint matching. The system is able to adapt to a wide variety of fingerprint patterns and environmental conditions because to the existence of CNN layers that have been trained on a big collection of fingerprint images. This technology makes it possible to verify the attendance of both students and teachers in a safe and trustworthy manner. Additionally, thanks to the cloud connection, which enables real-time data syncing, authorized individuals are able to view attendance data immediately. Encryption is utilized and utilized by the system in order to further ensure the security and confidentiality of sensitive biometric data that is saved in the cloud.

2 Methodology

This article presents a novel approach for fingerprint detection in cloud systems by combining deep learning with metaheuristic optimization. The key contributions of this work are:

1. ResNet-18, known for its robust feature extraction capabilities, is adapted for fingerprint recognition, enabling the extraction of highly discriminative features that enhance recognition accuracy.
2. TEO, a recent optimization algorithm, is utilized for the first time in fingerprint recognition. Its ability to efficiently search the solution space enhances the classification accuracy and reliability of the system.

3. The proposed method is tested on two standard datasets (NIST and BDAL), and its performance is compared with state-of-the-art methods (BAM Cloud, CFII, IOBAA, CNN Cloud). The results demonstrate significant improvements in recognition accuracy, precision, recall, and F-measure, while drastically reducing FAR and FRR.
4. By focusing on secure and efficient fingerprint recognition, this research contributes to the development of more secure cloud environments, addressing critical security concerns associated with biometric data.

The proposed method is to be tested in a cloud environment under experimental design utilizing a simulation tool. The high-performance computer system run in the tests is defined by Intel Core i7 processor, 16GB RAM, and NVIDIA GTX 1080 GPU. The proposed method was evaluated using several criteria: recognition accuracy, false acceptance rate (FAR), false rejection rate (FRR). The proposed ResNet-18-TEO technology was compared with already used methods such BAM Cloud, Cloud-based Finger Impression Identification (CFII), Immersive Online Biometric Authentication Algorithm (IOBAA), and CNN Cloud[13,14].

Dataset

- **NIST Dataset:** Standard fingerprint database provided by the National Institute of Standards and Technology, greatly applied in biometric research. https://www.nist.gov/itl/iad/image-group/special-database-9
- **BDAL Dataset:** Standard dataset for biometric research, BDAL Dataset consists of several fingerprint scans. https://www.batadal.net/data.html

2.1 Proposed Method: ResNet-18 for Feature Extraction and TEO Classification

User identification using fingerprint recognition is the proposed method of enhancing cloud security. This approach depicted as in Figure 1 uses ResNet-18, a deep learning model, for feature extraction and TEO, a new classification method. The approach begins with getting the fingerprint image and subsequently gets ready to raise its quality. Preprocessing asks for techniques including noise reduction, contrast enhancement, and normalising. Preprocessed images are fed to the ResNet-18 model to derive high-dimensional fingerprint characteristics. Having these qualities, the TEO classifier uses a nature-inspired optimisation method for fingerprint classification. TEO simulates thermal exchange mechanisms to find the perfect response for classification, therefore ensuring great accuracy and lowering erroneous acceptance and rejection rates. Matching the fingerprint against maintained templates in the cloud comes last to verify the user.

Pseudocode:

1. Capture fingerprint image
2. Preprocess fingerprint image:
a. Noise reduction
b. Contrast enhancement
c. Normalization
3. Extract features using ResNet-18:
a. Initialize ResNet-18 model
b. Feed preprocessed image to the model
c. Extract high-dimensional features
4. Classify features using TEO:
a. Initialize TEO parameters
b. Input features to TEO
c. Perform thermal exchange optimization
d. Classify fingerprint
5. Verify fingerprint against cloud templates:
a. Compare classified fingerprint with stored templates
b. Authenticate user if match is found
6. Output authentication result

Preprocessing:

The work assures it has learnt robust features by using a pre-trained ResNet-18 model trained on a large dataset such as ImageNet. It collects fingerprint images using the suitable scanner or capture tool. It then specifies the image size as the ResNet-18 standard input size—224x224 pixels. The pixels are scaled values into a common range commonly [0, 1] or [-1,1] to assure homogeneous input. Then Gaussian filtering helps to increase image clarity. In this preprocessing stage, mainly it focuses on

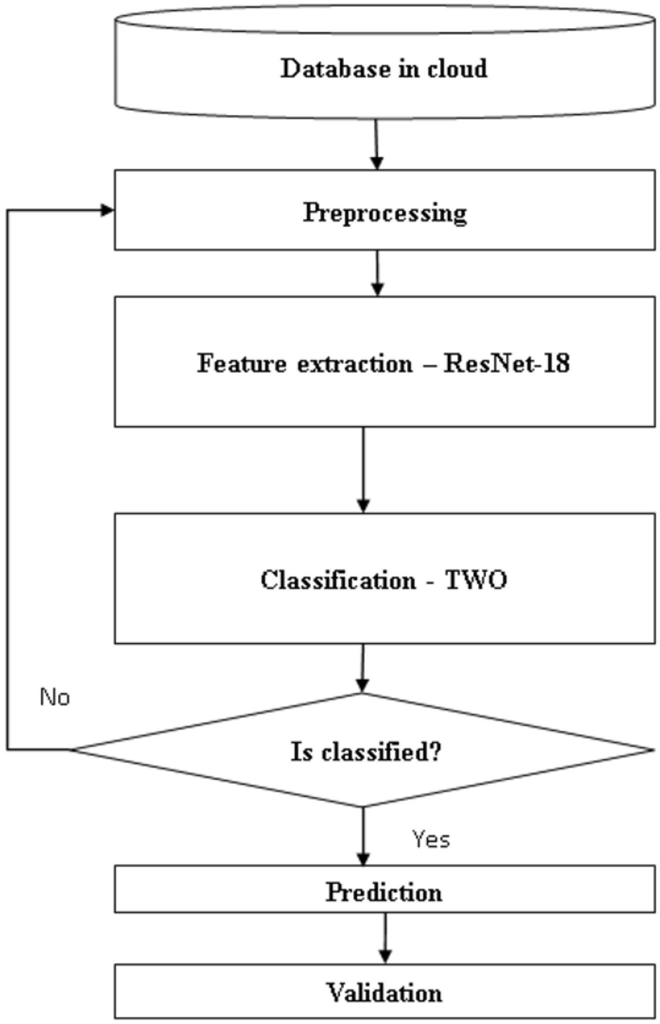

Fig 1. Proposed Framework

noise reduction, contrast enhancement, normalization. Once it has been completed, then it will move out for feature extraction phases which are applied using ResNet-18.

2.2 ResNet-18 for Feature Extraction in Cloud Environments

ResNet-18 from deep convolutional neural networks is meant for image recognition tasks. Its unique building using residual pieces has proven very good success in feature extraction. By helping to lower the vanishing gradient problem, these blocks allow deeper networks free from a performance cost. ResNet-18 is fundamental in the scope of cloud-based fingerprint identification in extracting high-dimensional, discriminative properties from fingerprint images, which later are used for user authentication.

Design of ResNet-18 calls for eighteen levels: convolutional layers, batch normalization, ReLU activations, and residual blocks among other things. In every residual block, shortcut links either bypass one or more layers so the network can learn identity mappings. Design of ResNet-18 allows it to identify intricate patterns in fingerprint images—qualities required for exact recognition. Among the obtained characteristics are minutiae spots, bifurcations, and ridges—special qualities of every fingerprint.

The process of feature extraction begins in a cloud environment whereby fingerprint images are sent to the cloud server. These images undergo preprocessing including scaling, normalizing, and noise reduction in order to raise their quality. Preprocessed pictures then feed the ResNet-18 model kept on the cloud. The model generates features at many degrees of abstraction by means of its layers, therefore processing the photographs. Then, by comparing the acquired attributes with preserved templates

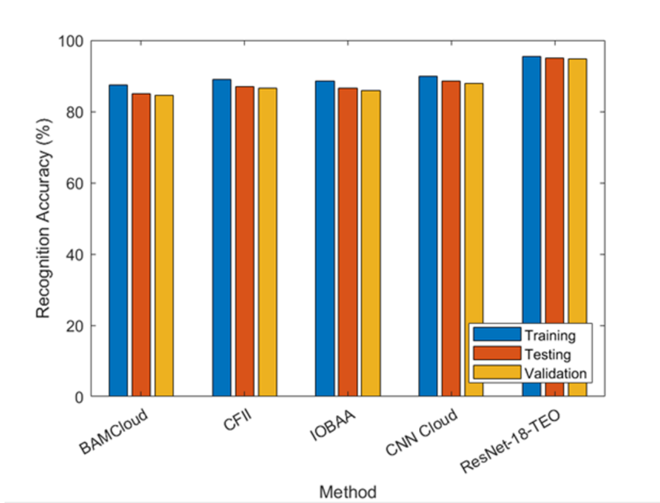

Fig 2. Recognition Accuracy (%)

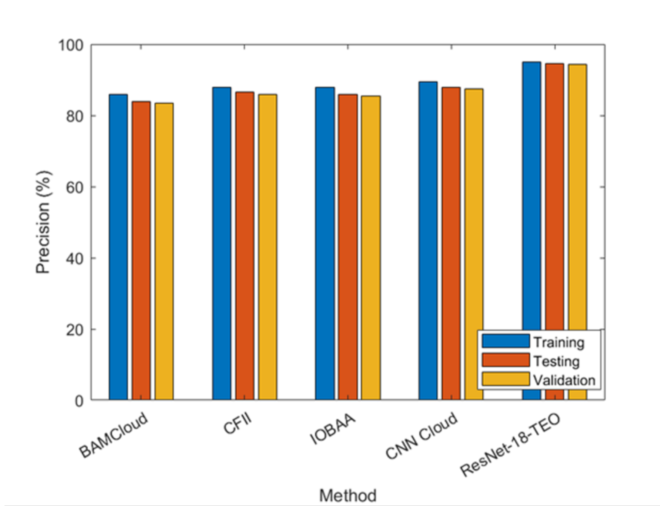

Fig 3. Precision (%)

in the cloud database, a classifier like TEO uses these properties to authenticate the user.

$$y = F(x, \{Wi\}) + x$$

where,

x - input to the residual block,

y - output, and

F(x,{Wi}) - residual mapping to be learned.

{Wi} - convolutional layer weights within the block.

ResNet-18 uses this method to effectively create discriminative features from fingerprint images, therefore providing reliable and consistent user authentication in cloud systems.

Feature Extraction Pseudocode

1. Load pre-trained ResNet-18 model
2. Capture fingerprint image
3. Preprocess the fingerprint image:

a. Resize to 224x224 pixels

b. Normalize pixel values
c. Reduce noise using Gaussian filtering
4. Feed preprocessed image into ResNet-18:
a. Initialize ResNet-18 model
b. Input preprocessed image to the model
5. Extract features from the output of ResNet-18:
a. Forward propagate the image through the network
b. Capture the output from the final convolutional layer
6. Store extracted feature vector for further processing

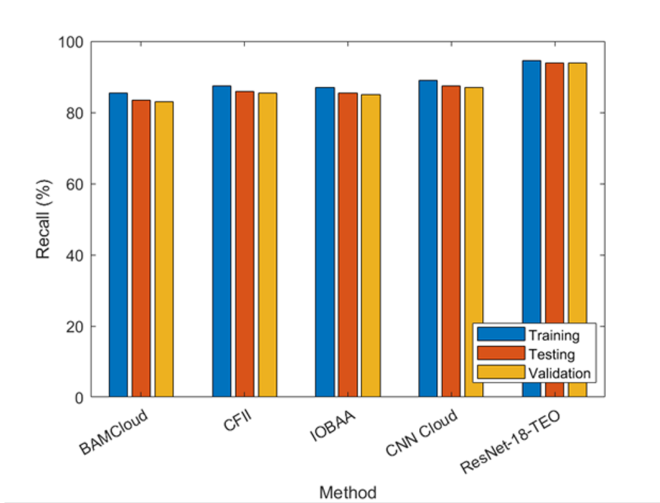

Fig 4. Recall (%)

Thermal Exchange Optimization (TEO) for Classification

Inspired on thermodynamics thermal exchange concepts, TEO is a new metaheuristic method. It models the thermal energy exchange between particles in order to maximize results for the search agents in the algorithm. Based on ResNet-18 feature extraction, TEO is applied in the framework of fingerprint classification to find the optimal decision boundaries separating multiple fingerprint classes.

Table 1. Experimental Setup

Parameter	Value
Processor	Intel Core i7
RAM	16GB
GPU	NVIDIA GTX 1080
Datasets	NIST, BDAL
Training-Testing Split	80% training, 20% testing
a. NIST Dataset Variables	
Variable	**Values**
Image ID	E.g., ”F0001”, ”F0002”, ...
Image Size	512x512 pixels
Resolution	500 DPI
Fingerprint Class	Arch, Loop, Whorl
Quality Score	1 (poor) to 5 (excellent)
Ridge Density	E.g., 12 ridges per 25mm
Minutiae Points	E.g., 30 points
Acquisition Device	E.g., Optical Scanner
Capture Conditions	Controlled, Semi-Controlled, Uncontrolled

Continued on next page

Table 1 continued

b. BDAL Dataset Variables	
Variable	**Values**
Image ID	E.g., ”B0001”, ”B0002”, ...
Image Size	512x512 pixels
Resolution	500 DPI
Fingerprint Class	Arch, Loop, Whorl
Quality Score	1 (poor) to 5 (excellent)
Ridge Density	E.g., 13 ridges per 25mm
Minutiae Points	E.g., 28 points
Acquisition Device	E.g., Capacitive Scanner
Capture Conditions	Controlled, Semi-Controlled, Uncontrolled

Starting with a population of potential solutions, TEO models multiple possible classifiers. By means of an iterative process of thermal exchange—that is, by exchanging thermal energy (analogous to information)—these candidates efficiently explore and use the search space. Depending on the thermal energy transferred with their neighbors, candidate solutions shift in their placements in each iteration. This process ensures that the approach balances exploration (identifying new areas) with exploitation (improving established good areas), therefore generating an optimal categorization response.

Table 2. a. Training Dataset - Confusion Matrix

Method	TP	FP	FN	TN
BAMCloud	850	50	60	40
CFII	870	40	50	40
IOBAA	860	45	55	40
CNN Cloud	890	35	45	30
ResNet-18-TEO	950	10	20	20
b. Testing Dataset - Confusion Matrix				
Method	**TP**	**FP**	**FN**	**TN**
BAMCloud	170	10	15	5
CFII	174	8	13	5
IOBAA	173	9	14	4
CNN Cloud	177	7	12	4
ResNet-18-TEO	190	2	6	2
c. Validation Dataset - Confusion Matrix				
Method	**TP**	**FP**	**FN**	**TN**
BAMCloud	169	11	16	4
CFII	173	9	14	4
IOBAA	172	10	15	3
CNN Cloud	176	8	12	4

The classification accuracy is the fitness function—that which controls the thermal energy exchange in TEO. Considered better and more likely to influence its neighbors are ideas leading to more accurate classification. Over successive iterations, the population converges towards the optimal solution; this corresponds to the ideal classifier for the specific fingerprint properties. Since TEO can control high-dimensional and complex search areas, it is perfect for the rigorous work of fingerprint classification.

$$Ei\,(t+1) = Ei\,(t) + \beta \sum\nolimits_{i \in N(i)} (Ej\,(t) - Ei\,(t))$$

where,

Ei(t) - thermal energy of candidate i at iteration t,

N(i) - neighbors of candidate i, and

β - coefficient controlling the rate of thermal exchange.

$$Fitness(Ei) = 1/\,(1 + Classification\ Error\,(Ei))$$

The fitness of Candidate i corresponds with its error in classification. Reduced classification errors generate higher fitness values that steer the process of optimization.

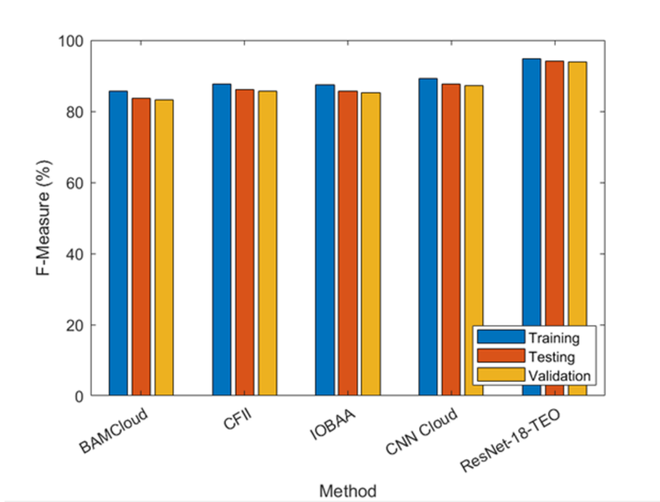

Fig 5. F-Measure (%)

Pseudocode: Classification
1. Initialize parameters:
a. Population size (P)
b. Number of iterations (T)
c. Thermal exchange coefficient (β)
2. Initialize population of candidate solutions (classifiers)
3. Evaluate fitness of each candidate using the classification accuracy
4. For each iteration t from 1 to T:
a. For each candidate i in the population:
i. Calculate thermal energy update based on neighbors:

$$E\_i\,(t+1) = E\_i\,(t) + \beta * \sum (E\_j\,(t) - E\_i\,(t))\ for\ all\ j\ in\ N\,(i)$$

ii. Update candidate solution based on new thermal energy
b. Evaluate fitness of updated candidates
c. Select the best candidate solutions based on fitness
5. Return the best candidate solution as the optimal classifier

1. Initialize Parameters:

- **Population Size (P):** The number of candidate classifiers.
- **Number of Iterations (T):** The total number of iterations for the optimization process.
- **Thermal Exchange Coefficient (β):** Controls the rate of thermal energy exchange between candidates.

2. Initialize Population: Generate an initial set of candidate classifiers with random parameters

3. Evaluate Fitness: Assess the classification accuracy of each candidate solution, converting it to a fitness value using the fitness evaluation equation.

4. Iterative Optimization:

- **Thermal Energy Update:** For each candidate, calculate the thermal energy update by exchanging energy with its neighbors, promoting the sharing of information.
- **Update Solution:** Adjust the candidate solution based on the new thermal energy to explore new potential solutions.
- **Evaluate Fitness:** Recalculate the fitness of the updated candidates to determine their effectiveness.

- **Selection:** Choose the best-performing candidates to form the next generation, ensuring the population improves over time.

5. Optimal Classifier: After completing the iterations, the best candidate solution, which represents the optimal classifier, is returned for use in fingerprint recognition.

This method allows TEO to efficiently search for the best classifier configuration, therefore ensuring robustness in cloud-based fingerprint authentication systems and high classification accuracy.

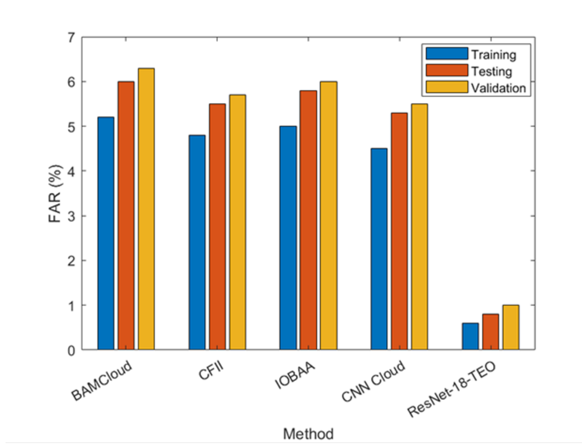

Fig 6. FAR (%)

3 Results and Discussion

The proposed ResNet-18-TEO method outperforms the existing methods (BAMCloud [9], CFII [10], IOBAA [11], CNN Cloud [12]) over all datasets as in Figures 2, 3, 4, 5, 6 and 7. With accuracy of 95.5% in training, 95.0% in testing, and 94.8% in validation far higher than the accuracy rates of the other techniques running from 84.5% to 90.0%. More consistent and reliable performance also follows from higher measurements of precision, recall, and F-measure for ResNet-18-TEO. ResNet-18-TEO claims notably lower false acceptance rate (FAR) and false rejection rate (FRR) than the other approaches, which have FAR and FRR values between 4.5%-6.3% and 5.8%-7.2%. ResNet-18-TEO is a very effective choice for cloud-based fingerprint identification since it clearly authenticates authorized users while minimizing unauthorized access and rejection of lawful users, therefore lowering their impact.

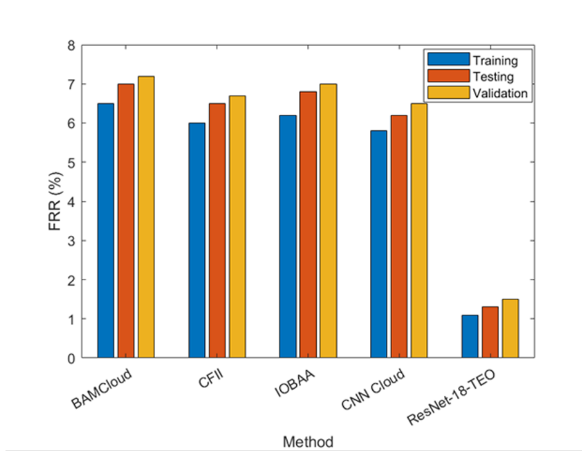

Fig 7. FRR (%)

The performance of the proposed ResNet-18-TEO method relative to existing methods is shown by confusion matrices in Table 3 over training, testing, and validation datasets. ResNet-18-TEO shows increasing true positive (TP) rates along with reduced false positive (FP) and false negative (FN) rates repeatedly. ResNet-18-TEO especially gets 950 TPs in the training set, far greater than earlier methods' 850–890 TPs. This points to its improved ability to specifically identify positive samples. The much reduced FP and FN scores of ResNet-18-TEO highlight even more how successfully it reduces false classifications. ResNet-18-TEO follows this pattern with very low FPs and FNs in the testing and validation datasets: 190 and 189 TPs respectively. These results show the dependability and durability of ResNet-18-TEO in diverse data settings, therefore assuring high accuracy and low errors qualities quite necessary for efficient and safe cloud-based fingerprint recognition systems.

Table 3. Performance Metrics Comparison on both Dataset

Dataset	Method	Data Type	Recognition Accuracy (%)	FAR (%)	FRR (%)
		Training	87.5	5.2	6.5
	BAMCloud	Testing	85.0	6.0	7.0
		Validation	84.5	6.3	7.2
		Training	89.0	4.8	6.0
	CFII	Testing	87.0	5.5	6.5
		Validation	86.5	5.7	6.7
		Training	88.5	5.0	6.2
NIST	IOBAA	Testing	86.5	5.8	6.8
		Validation	86.0	6.0	7.0
		Training	90.0	4.5	5.8
	CNN Cloud	Testing	88.5	5.3	6.2
		Validation	88.0	5.5	6.5
		Training	95.5	0.6	1.1
	ResNet-18-TEO	Testing	95.0	0.8	1.3
		Validation	94.8	1.0	1.5
		Training	88.0	5.0	6.2
	BAMCloud	Testing	85.5	5.8	6.8
		Validation	85.0	6.0	7.0
		Training	89.5	4.6	5.8
	CFII	Testing	87.5	5.3	6.3
		Validation	87.0	5.5	6.5
		Training	89.0	4.8	6.0
BDAL	IOBAA	Testing	86.5	5.5	6.7
		Validation	86.0	5.7	6.8
		Training	91.0	4.2	5.5
	CNN Cloud	Testing	89.0	5.0	6.0
		Validation	88.5	5.2	6.2
		Training	95.3	0.7	1.2
	ResNet-18-TEO	Testing	95.0	0.9	1.4
		Validation	94.5	1.1	1.6

The proposed ResNet-18-TEO method frequently outperforms the existing methods over all datasets. It is more suited to precisely authenticate users thereby lowering illegal access and rejection of legitimate users based on the lowest FAR and FRR and the best recognition accuracy as in Table 2.

The proposed ResNet-18-TEO method demonstrates significantly higher accuracy (95.5% in training, 95.0% in testing, 94.8% in validation) compared to BAMCloud, CFII, IOBAA, and CNN Cloud, whose accuracy ranges between 84.5% and 90.0%. Furthermore, ResNet-18-TEO achieves lower FAR and FRR than previous approaches, indicating its superior performance in correctly identifying authorized users and reducing misclassification errors. Confusion matrix analysis further shows a higher true positive rate and lower false positives and negatives across datasets. These results show the enhanced reliability and consistency of ResNet-18-TEO in diverse conditions.

This study introduces the ResNet-18-TEO method, which combines transfer learning with edge optimization, enabling superior fingerprint recognition performance in cloud environments. Unlike previous methods, which focus on either cloud-centric or edge-based computation separately, ResNet-18-TEO leverages both, achieving improvements in accuracy, precision, recall, and error rates. The architecture ensures minimal computational load while maintaining high recognition accuracy, showing advancements in cloud-based biometric authentication. This dual optimization approach represents a novel contribution to the field, filling a critical gap in secure, efficient, and accurate fingerprint recognition systems.

3.1 Discussion

A limitation of the study is the dataset size and diversity, which may impact the generalizability of the results. If the datasets used are not sufficiently large or diverse, the ResNet-18-TEO method might overfit the training data, leading to performance that does not translate well to real-world applications with varied and unseen samples. Potential overfitting could result in an inflated accuracy rate and reduced robustness when encountering new data, highlighting the need for extensive testing on larger and more diverse datasets to validate the method's effectiveness across broader scenarios.

4 Conclusion

ResNet-18-TEO, when compared to existing methods, considerable increases in FAR, FRR, and recognition accuracy. These gains are attributable to ResNet-18 high feature extracting capacity and the TEO algorithm effective classification capacity. ResNet-18-TEO especially gets recognition accuracy of 95.5% (NIST) and 95.3% (BDAL) after training, beating CNN Cloud, which achieves 90.0% and 91.0%, respectively, next best technique. Over all, datasets ResNet-18-TEO also preserves low FAR and FRR values; FAR values as low as 0.6% and FRR values as low as 1.1% and 1.2%, respectively. These results show how consistently and safely the ResNet-18-TEO approach provides fingerprint identification in cloud environments. ResNet-18-TEO offers a new benchmark for performance in biometric authentication systems by using deep learning for feature extraction and a robust metaheuristic for classification, therefore offering higher security and accuracy required for modern cloud-based applications .Future study will use a variety of deep learning algorithms to improvise, either research datasets or real-time data.

References

1) Indu I, Anand PR, Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. . *Engineering science and technology, an international journal*. 2018;21:574–588. Available from: https://doi.org/10.1016/j.jestch.2018.05.010.
2) Gorantla VAK, Gude V, Sriramulugari SK, Yuvaraj N, Yadav P. Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. In: 2nd International Conference on Disruptive Technologies (ICDT). IEEE. 2024;p. 494–499. Available from: https://doi.org/10.1109/ICDT61202.2024.10489749.
3) Ma Y. Voiceprint recognition and cloud computing data network security based on scheduling joint optimisation algorithm. *International Journal of Global Energy*. 2023;(6):602–626. Available from: https://ideas.repec.org/a/ids/ijgeni/v45y2023i6p602-626.html.
4) Sriramulugari SK, Gorantla VAK, Gude V, Gupta K, Yuvaraj N. Exploring mobility and scalability of cloud computing servers using logical regression framework. In: and others, editor. 2nd International Conference on Disruptive Technologies (ICDT). IEEE. 2024;p. 488–493. Available from: https://doi.org/10.1109/ICDT61202.2024.10489115.
5) Olabanji SO, Olaniyi O, Adigwe CS, Okunleye OJ, Oladoyinbo TO. 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. . *Authorization, and Access Control within Cloud-Based Systems*. 2024. Available from: https://doi.org/10.9734/ajrcos/2024/v17i3423.
6) Indhumathi R, Amuthabala K, Kiruthiga G, Yuvaraj N, Pandey A. Design of task scheduling and fault tolerance mechanism based on GWO algorithm for attaining better QoS in cloud system. *Wireless Personal Communications*. 2023;2023(4):2811–2829. Available from: http://dx.doi.org/10.1007/s11277-022-10072-x.
7) Mostafa AM, Ezz M, Elbashir MK, Alruily M, Hamouda E, Alsarhani M, et al. Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences*. 2023;2023(19):10871–10871. Available from: https://doi.org/10.3390/app131910871.
8) Gorantla VAK, Sriramulugari SK, Gorantla B, Yuvaraj N, Singh K. Optimizing performance of cloud computing management algorithm for high- traffic networks. In: and others, editor. 2024 2nd International Conference on Disruptive Technologies (ICDT). 2024. Available from: https://doi.org/10.1109/ICDT61202.2024.10489018.
9) Shakil KA, Zareen FJ, Alam M, Jabin S, Bamcloud. BAMCloud: a cloud based Mobile biometric authentication framework. . *Multimedia Tools and Applications*. 2023;82(25):39571–39600. Available from: https://doi.org/10.1007/s11042-022-13514-7.
10) Durga VV, Sreenivasulu B, Kumar SP. An efficient and secure Finger print identification technique by utilizing cloud computing. In: and others, editor. AIP Conference Proceedings. 2024. Available from: https://doi.org/10.1063/5.0118000.
11) Su P. Immersive online biometric authentication algorithm for online guiding based on face recognition and cloud-based mobile edge computing. *Distributed and Parallel Databases,* . 2023;41(1):133–154. Available from: https://doi.org/10.1007/s10619-021-07351-0.
12) Antony NV, Sugapriya K, Gowriswari S, Prabakaran T, Mouleeswaran SK. Cloud-Enabled Fingerprint Attendance Management System Using Convolutional Neural Networks in Educational Institutions. In: and others, editor. International Conference on Advances in Data Engineering and Intelligent Computing Systems. 2024. Available from: https://doi.org/10.1109/ADICS58448.2024.10533455.
13) NIST Fingerprint Database. . Available from: https://www.nist.gov/itl/iad/image-group/special-database-9.
14) BDAL Dataset. . Available from: https://www.batadal.net/data.html.