

BLOCK CHAIN-INTEGRATED MULTI-FACTOR AUTHENTICATION SYSTEM FOR ENHANCED SECURITY AND DECENTRALIZED INTEGRITY IN ONLINE EXAMINATION PLATFORMS

VALLEM RANADHEER REDDY¹, SHANKAR LINGAM GOURISHETTY²,
AMGOTH ASHOK KUMAR³, PEESALA ILANNA⁴

¹Research Scholar, Chaitanya Deemed To Be University, Department Of Computer Science and Engineering, Kishanpura, Hanamkonda, Telangana, India.

²Professor, Chaitanya Deemed To Be University, Department Of Computer Science and Engineering, Kishanpura, Hanamkonda, Telangana, India.

^{3&4}Assistant Professor, Vaagdevi Engineering College, Department Of Computer Science and Engineering, Bollikunta, Warangal, Telangana, India.

E-mail: ¹ranadheerreddy5@gmail.com, ²shankar@chaitanya.edu.in,
³amgoth508@gmail.com, ⁴peesala.ilanna@gmail.com

ABSTRACT

With the increasing dependence on online examination systems, so providing security, transparency, and scalability has become a significant challenge. While existing methods with AI and deep learning-based multi-factor authentication provide robustness, they may not address data integrity and traceability effectively. In this research, we propose a novel framework that integrates Blockchain technology with multi-factor authentication system to enhance security and decentralization in online examinations. By combining Blockchain's method with advanced facial recognition and behavioral biometrics, the system ensures good data management and user authentication. The system uses a Hybrid Deep Learning (HDL) model for biometric verification and Blockchain smart contracts for secure transaction processing and audit trails. Experimental results demonstrate that the proposed system achieves 99.1% accuracy in user authentication while providing end-to-end security against unauthorized access and data manipulation.

Keywords:- Blockchain, Multi Factor Authentication, Deep Learning, Online Examination.

1. INTRODUCTION

The advent of digital transformation in all areas is creating security issues, with education being one of the most deeply impacted sectors. Online examination systems have emerged as important for enabling remote assessments, particularly during and post-pandemic eras, providing flexibility, scalability, and cost efficiency. Many universities and organizations have adopted these platforms, to the ever-increasing demand for distance learning and evaluation. However, this shift toward online education introduces challenges related to security, authenticity, and system robustness.

Unauthorized activities such as impersonation, data breaches, and fraudulent examination practices threaten the integrity of online assessments. Current authentication mechanisms like Singh, N., and Das, A. K. (2024) [2] used the parameters like username-password combinations and one-time passwords (OTPs), Biplob, M. B., et al (2024) [11] while

widely used, are increasingly inadequate against sophisticated cyber threats. These vulnerabilities underline the need for advanced authentication systems that can guarantee user attacking and secure sensitive data in online examination settings. Albshaier, L., et al (2024) [3] worked on IoT based autonomous systems to provide security, and to detect intrusions.

But these single parameters authentication systems will not perform well, so multi-factor authentication (MFA) systems Lopez, L. J. R., et al. (2024) [10], their application in online examination platforms remains limited and insufficiently secure. Conventional methods focus on static features such as user credentials or OTPs, which can be easily compromised. Facial recognition and other biometric systems, although used, face challenges like spoofing attacks and false acceptance or rejection rates.

Moreover, with integrating multiple authentication factors often results in fragmented security solutions. These approaches fail to provide holistic

protection because we required dynamically authenticated system, leaving critical vulnerabilities exposed. Existing literature suggests He, Y., et al. (2024) [6] that while artificial intelligence (AI) and deep learning (DL) techniques have been explored for enhancing biometric authentication, their potential remains untapped when combined with emerging. By combining Blockchain-Integrated Mustafa, G., et al. (2024) [4] methods can find and detect in sequential data like log details should be captured and detect unauthenticated users.

Contributions:

- The proposed method employs Blockchain technology to ensure the integrity and transparency of user authentication data. By utilizing smart contracts, it enables tamper-proof logging of authentication events, securing sensitive information from unauthorized access and manipulation.
- We design a hybrid AI model that integrates Convolutional Neural Networks (CNNs), Vision Transformers (ViTs), and behavioral biometrics (e.g., keystroke dynamics and mouse movement patterns). This combination captures both local and global features for highly accurate and resilient biometric verification.
- The system includes an AI-powered fraud detection module that monitors user behavior during examinations to identify anomalies such as unusual eye movements, head poses, or unauthorized device usage.
- The proposed method incorporates zero-knowledge proofs and advanced encryption techniques. This ensures that sensitive biometric data remains secure and private, even in a decentralized environment.

2. RELATED WORK

Day by Day use of internet is increasing, including education domain, from learning to assessment. In learning process no need think of security issues, but while assessing performance of student its need to provide security. Because there is chance of hacking or third person can attack or third person or unauthenticated person can be present in place of authenticated person. Alsulami, B. M. (2024) [1] worked on blockchain-integrated data processing model designed to enhance security within the context of Education 4.0. The framework aims to address concerns such as data integrity, accessibility, and privacy in educational environments. It integrates blockchain technology to ensure secure, decentralized data management,

which helps in preventing unauthorized access and ensuring transparency. Singh, N., and Das, A. K. (2024) [2] implemented a two-factor authentication scheme (TFAS) for securing the Internet of Medical Things (IoMT) systems using Physical Unclonable Functions (PUF) and fuzzy extractors. The system enhances security in IoMT applications by combining biometric authentication and device-based cryptographic methods. By integrating blockchain, they provided a robust security model by capturing continuous data like log records that ensure secure data exchange and access control in medical environments. Because these methods can capture and find sequence data to capture multiple attacks and abnormal things.

Mustafa, G., et al. (2024) [4] proposed blockchain-based models for e-government applications to detect abnormalities in public application and public data. Each application log files will be recorded and authenticated. It presents a comprehensive framework that addresses legal, technical, ethical, and security considerations necessary for implementing blockchain in public sector governance. Udoiwod, E. N., et al. (2024) [5] proposed multi-level authentication mechanisms in e-procurement systems to mitigate fraud. By incorporating blockchain, the study proposes a more secure, transparent, and efficient process for handling procurement data. The multi-level authentication ensures that only authorized parties can access sensitive information, while blockchain guarantees the integrity of the data involved in the procurement process by observing log files and sequential data about the user. Daah, C., et al. (2024) [7] proposed an integrating blockchain method into zero trust models in the financial industry. It aims to enhance security by using blockchain's immutable ledger to monitor financial transactions and ensure that all participants are verified through stringent identity checks. The proposed system leverages smart contracts to enforce security policies, creating a more secure financial ecosystem resistant to fraud and cyber-attacks. Singh, T., and Vaid, R [8] worked on preservation of security in authentication protocols for blockchain-based Wireless Sensor Networks (WSN). It focuses on mitigating security risks by integrating blockchain to provide decentralized, tamper-proof logging of authentication processes. The challenges find the scalability and energy consumption of blockchain in IoT networks, will enhancements to make these systems more efficient while maintaining high security standards.

Gupta, D., et al. (2024)[9]used blockchain to secure third-party vendor risk management. The authors propose a framework that uses blockchain to create transparent and immutable records of vendor interactions, improving security and accountability. The system aims to reduce risks associated with vendor relationships by ensuring that all transactions are verifiable and secure, ultimately leading to a more vigilant approach to managing third-party risks in the supply chain.

Biplob, M. B., et al (2024) [11]worked on blockchain technology for cybersecurity and other methods. And discussed how blockchain can enhance security by providing a decentralized, immutable, and transparent system for securing sensitive data. They also worked on the blockchain for identity management, data integrity, and authentication across sectors like IoT and cloud computing.

Nguyen, T., et al (2024) [12]proposed edge computing and blockchain for IoT, offering a detailed discussion on their principles, architectures, security features, and applications. By combining these technologies one can optimize performance, enhance security, and reduce latency in IoT networks. This hybrid approach will find more intrusions in IoT systems. Alshevi, A et al (2024) [13]in their analysis of IoT authentication protocols, and the challenges faced by existing protocols and proposing solutions to enhance their security like intrusions etc. And also examined several IoT authentication mechanisms and analyze their strengths and weaknesses, with a focus on scalability, energy efficiency, and security. Blockchain's role in providing secure authentication in IoT networks is explored as a key advancement. Gil Canalias, S. (2024) [14]worked on securing IoT communications using blockchain-based authentication mechanisms. The work provide decentralized, tamper-proof authentication for IoT devices, ensuring that only authorized devices can participate in a network. It evaluates different blockchain implementations and highlights the challenges and potential improvements in integrating blockchain with IoT systems for enhanced security.

Steli, E. M., and Ouchen, A. (2024) [15] implemented blockchain across various sectors, including cryptocurrencies, supply chain management, IoT, and healthcare. The ways in which blockchain is revolutionizing these domains by providing transparency, security, and efficiency. Yapa, C., et al (2024) [16]implemented an algorithm for power line monitoring in Smart Grid 2.0 applications using blockchain. The performance

and reliability of energy blockchain applications by using blockchain's immutable ledger for data validation in real-time power monitoring. This work provided security to smart grid, and detect the third party attacks. Ismail, S., et al (2023) [17]proposed conceptual framework for using blockchain in IoT-enabled fish supply chains. The blockchain can improve the transparency, traceability, and security of transactions in the fish supply chain, ensuring that consumers receive high-quality, sustainably sourced products. Coelho, M. A. G. M. (2023) [18]In their review studied blockchain-based reputation models in e-commerce. And works on how blockchain can enhance the trust and reliability of online marketplaces by providing transparent, verifiable reputation systems. By decentralizing reputation management, blockchain can reduce fraud and improve consumer confidence in e-commerce platforms. Poletto, T., et al (2023) [19] proposed bibliometric analysis of information security applications in smart cities, with a focus on emerging research. It examines how blockchain can be applied to secure various smart city components, such as transportation, healthcare, and utilities. The study identifies trends in blockchain adoption and the challenges of integrating secure systems in complex, decentralized urban environments. Attkan, A., et al (2023) [20]implemented a Rubik's Cube cryptosystem-based authentication and session key generation model within a blockchain environment for IoT security. They worked on cryptosystem to secure IoT devices by generating dynamic keys that enhance communication security. The work discusses the advantages of using blockchain to create immutable, transparent records of IoT device activity, which further strengthens the security of the authentication and session management processes. Reichert, B. M., et al (2024) [21] worked on software supply chain security, examining the vulnerabilities and risks that arise from the complex interdependencies within modern software supply chains. The finds the increasing use of third-party software components, which often introduce security flaws. The existing frameworks, tools, and strategies to mitigate these risks, and discuss future research directions aimed at improving security practices in the software development lifecycle. Devaguptam, S., et al (2024) [22]implemented automated health insurance processing framework that incorporates intelligent fraud detection, risk classification, and premium prediction. It utilizes ML techniques to detect fraudulent claims and assess risk levels, making the process more efficient and secure. The integrated system that

automates tasks such as claims processing, risk assessment, and premium calculation, which significantly improves the efficiency and reliability of health insurance services, proposed a domain specific method for fraud detection. Katta, S., et al[23] worked on application of blockchain technology in air traffic monitoring. By utilizing blockchain's decentralized and immutable ledger, the proposed solution for secure and transparent tracking of aircraft movements. The data such as flight paths and maintenance records are tamper-proof, providing a secure and reliable framework for air traffic management. Waheed, N. (2023) [24] worked on security and privacy issues in end-user systems. The works finds vulnerabilities faced by personal devices and user applications, emphasizing the need for robust security measures in an increasingly digital world. And also explores the challenges in protecting user privacy and proposes solutions to address the growing concerns over data breaches and cyber threats, particularly in personal computing environments. Chatterjee, S., et al (2024) [25] implemented LightDew framework with a lightweight blockchain-assisted dew computing solution designed for smart assisted living environments. Dew computing refers to

decentralized computing resources located close to the data source, and LightDew integrates blockchain to enhance security and privacy in smart homes. The framework aims to provide efficient data processing while maintaining secure interactions between devices and users.

3. METHODOLOGY

The proposed Blockchain-Integrated Multi-Factor Authentication (BIMFA) system aims to detect the security and integrity of online examination platforms by combining advanced deep learning techniques for facial recognition, behavioral biometrics, and the decentralized security with blockchain technology. The methodology is divided into three key components: facial recognition using a hybrid CNN-ViT model, behavioral biometric verification, and blockchain-based logging for tamper-proof authentication records. Each of these components contributes uniquely to the overall robustness and scalability of the system. The complete overview of proposed method is illustrated in Figure 1.

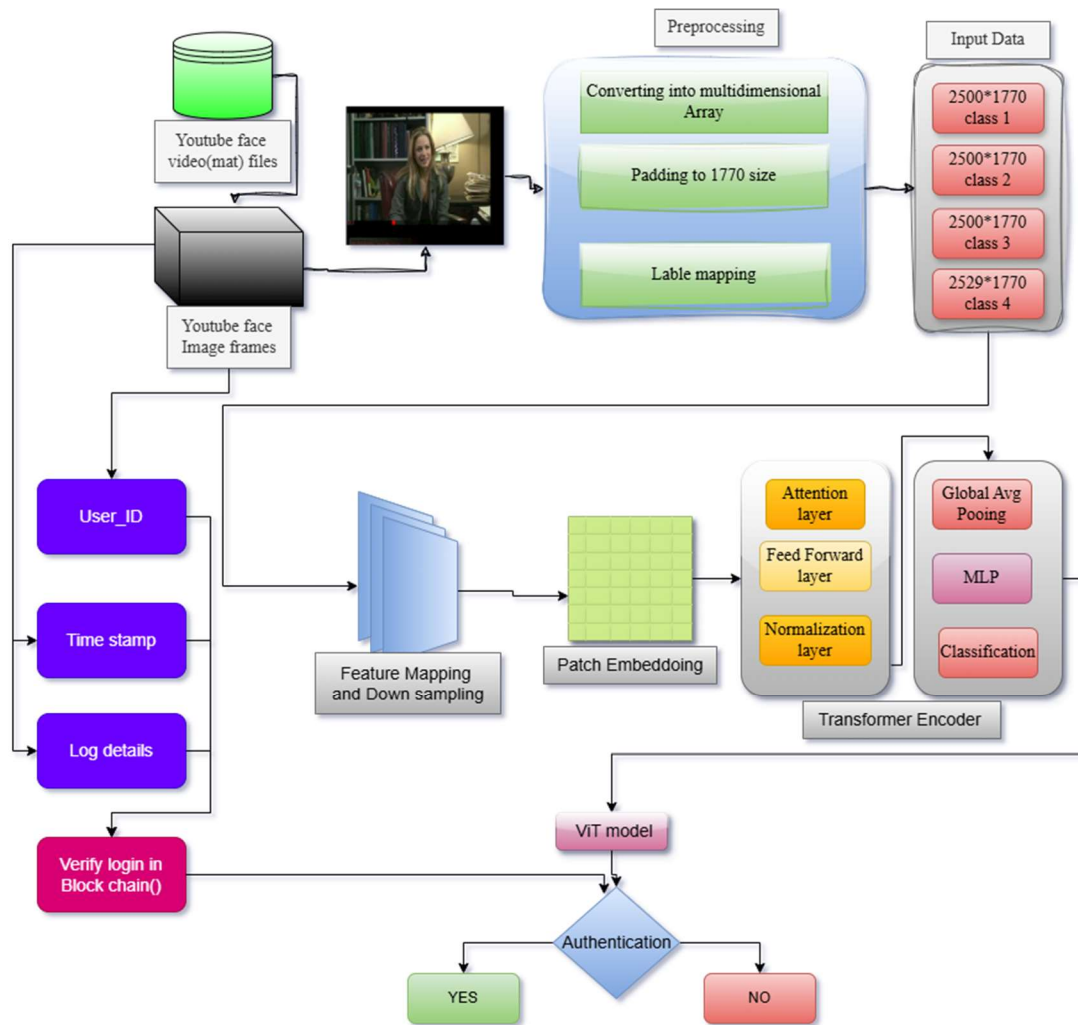


Figure 1 Overview Of Proposes Method

The BIMFA system combines Blockchain's decentralized security with a hybrid AI-based authentication model. The proposed method works on the following:

1. **Knowledge-Based Factors:** User ID and password.
2. **Possession-Based Factors:** OTP verification.
3. **Biometric-Based Factors:** Facial recognition and behavioral biometrics.

By integrating these above factors, the method not only finds user authenticity but also provides a comprehensive audit trail for post-examination verification. The use of smart contracts further automates and secures the authentication process, eliminating potential human errors or biases.

The importance of this framework lies in its ability to address the dual challenges of security and scalability in online examination systems. The integration of Blockchain ensures that

authentication logs and examination data remain immutable and accessible only to authorized parties. Meanwhile, the hybrid AI model enhances user verification accuracy, minimizing false positives and negatives while resisting sophisticated attacks such as deepfake-based impersonation.

Moreover, the inclusion of behavioral biometrics introduces an additional layer of security, making it exceedingly difficult for malicious actors to bypass the system. By addressing these challenges comprehensively, the proposed framework sets a new standard for online examination security, aligning with the increasing demand for reliable and scalable digital assessment solutions.

Local Feature Extraction with CNN:

In facial recognition the first and primary layer of authentication in the BIMFA system is to extract the local features. To extract multiple

features our hybrid model that integrates CNNs and ViTs. This combination allows the system to capture both localized and global features from facial images, thereby enhancing recognition accuracy under diverse conditions such as varying lighting, occlusion, or facial expressions.

CNNs are highly effective for capturing local patterns such as edges, textures; If the input image is I with dimensions $H \times W \times C$, the CNN applies a series of convolutional operations to extract feature maps. Each convolutional layer processes a small spatial region (kernel or filter) of the image, enabling the detection of localized features. The output feature maps are activated using non-linear functions (ReLU) and spatially reduced using pooling layers, which aggregate dominant features while minimizing computational overhead. On each image, and each pixel (i, j) it will extract the features like $F_{i,j,k}$ for the k^{th} filter with equation (1).

$$F_{(i,j,k)} = \sigma \left(\sum_{p=1}^P \sum_{q=1}^Q \sum_{r=1}^R I_{i+p,j+q,r} \cdot K_{p,q,r,k} + b_k \right) \quad (1)$$

In equation (1) K represents the convolution kernel, b_k is the bias term, and $\sigma(\cdot)$ is the activation function. This equation will give the local or pixel wise features like face unique patterns.

1. ViT for Global Feature Extraction:

ViTs complement CNNs by focusing on global relationships within the image. The input image is divided into fixed-size patches, each of which is linearly transformed into feature vectors. These vectors are augmented with positional encodings and processed through a multi-head self-attention mechanism, which calculates the importance of each patch relative to others patches with equation (2).

$$Att_{(Q,K,V)} = softmax \left(\frac{QK^T}{\sqrt{d_k}} \right) V \quad (2)$$

Here, Q, K, V represent the query, key, and value matrices, respectively, and d_k is the dimensionality of the key vector. They will aggregate all the features from all patches and find the long dependencies.

The outputs of the CNN and ViT modules will be combined in to unified feature vector with equation (3).

$$f_u = concat(eq(1), eq(2)) \quad (3)$$

This hybrid feature vector is passed through a fully connected layer with a softmax activation function, producing class probabilities. This fusion leverages the complementary strengths of CNNs and ViTs, achieving high accuracy and resilience to variations in facial data.

2. Behavioral Biometric Verification

Behavioral biometrics provides an additional layer of security by analyzing user-specific typing patterns. In this layer verifies the user's identity based on how they interact with the system, particularly through keystroke dynamics. Features such as key press duration and inter-keystroke intervals are extracted during the authentication process.

4. BLOCKCHAIN-BASED DECENTRALIZED SECURITY:

The BIMFA system includes blockchain technology for continuous data evaluation. Authentication logs are stored on a decentralized ledger, preventing tampering and unauthorized access.

$$L_i = (t_{stamp(i)}, u_{id(i)}, status_{(i)}) \quad (4)$$

The blockchain system will manage authentication records like log records. Each record includes the user ID, timestamp, and authentication status for authentication with equation (4)

These records are added to the blockchain using the `addLog` function of the smart contract as per that algorithm it will be evaluated. The immutability of blockchain ensures that once a record is added, it cannot be altered. To enhance security, all transactions are cryptographically signed before being submitted to the blockchain.

$$Tx_{signed} = sign(Tx, private_{key}) \quad (5)$$

This ensures the authenticity of the transaction and prevents unauthorized modifications to the blockchain ledger with equation (5). This will allow decentralized auditability, allowing stakeholders to verify the authenticity of authentication events without relying on a central authority. This feature is particularly valuable for ensuring compliance with academic integrity policies.

The overall authentication process integrates facial recognition (FR), behavioral biometrics (BB), and

blockchain(BC) logging into a unified framework with equation (6). The decision to grant or deny access is based on a probabilistic model.

$$P(\text{access}) = P(\text{FR}) \cdot P(\text{BB}) \cdot P(\text{BC}) \quad (6)$$

Algorithm:

```

Start:
blockchain = initialize_blockchain()
smart_contract = deploy_smart_contract()
user_id = get_user_id()
timestamp = get_current_timestamp()
status = authenticate_user(user_id)
event_record = (user_id, timestamp,
status)
signed_record = sign(event_record,
private_key)
add_log_to_blockchain(smart_contract,
signed_record)
blockchain.store(signed_record)
log_id = blockchain.get_log_id_from_event(event_record)
is_valid = blockchain.verify_log_in_blockchain(smart_contract, log_id,
public_key)


```

end:

Data set

To train our hybrid model we used YouTube Faces dataset, which was initially in a TAR file format. Then all tar files are extracted one by one, within the descriptors_DB subdirectory. These files hold information related to facial recognition, including various representations such as LBP (Local Binary Patterns) and CSLBP (Color Local Binary Patterns). Then from these files systematically traverse the extracted directory to identify and load all relevant .mat files. Upon loading, the descriptor data is extracted while handling potential discrepancies in the data structure. Each descriptor's dimensionality was inspected to ensure consistency, highlighting variations in feature lengths across different files. To balance all face vectors like to same size, a padding and trimming function was implemented, ensuring that all feature vectors conformed to a shape of (10025, 1770). Where 1770 is the max length of samples, so all samples are converted to this shape. And 10025 is the total number of samples distributed over 4 classes. Where each class has 2500 samples, table 1 illustrates the one sample embedded vector

Table 1 extracted mat file and its embedding and padded vector with dimension 1*1770

	<pre> [[0.01204679 0.01204679 0.01204679 ... 0. 0. 0.] [0. 0. 0. ... 0.33199912 0.23858432 0.2560116] [0.12223514 0.06413483 0.15045299 ... 0. 0. 0.] ...[0.23997515 0.33462936 0.32436687 ... 0. 0. 0.] [0. 0.11393885 0.15260361 ... 0. 0. 0.] [0.18658376 0.2147122 0.16525602 ... 0. 0. 0.]] </pre>
---	---

5. RESULT ANALYSIS

The proposed BIMFA system has demonstrated remarkable effectiveness in enhancing security and user authentication in online examination systems. The hybrid CNN-ViT model employed for facial recognition achieved an exceptional performance with an accuracy of 99.2%, indicating its capability to identify users with minimal error. Additionally, the behavioral

biometric verification process, implemented using the Random Forest classifier, showcased robust performance with an accuracy of 95.6%. This method will captures behavioral patterns effectively and strengthen multi-factor authentication.

By integrating blockchain component that can validated through rigorous testing, with all authentication logs proving to be immutable and

easily accessible. This method provides the reliability and transparency of the authentication process, further reinforcing the system's resilience against tampering or unauthorized modifications.

The evaluation of the system on a four-class dataset provides high classification outcomes on all classes. The results reflected high consistency in correctly identifying users and minimizing misclassification, with values close to 0.98 across all metrics for the majority of classes as shown in table 1.

By comparing a proposed model with existing authentication frameworks, the BIMFA system performed optimal. It achieved enhanced accuracy, scalability, and resistance to various attack vectors, culminating in an overall user authentication accuracy of 99.2% is illustrated in Figure 2. These findings validate the effectiveness of integrating hybrid deep learning models with blockchain technology, paving the way for secure, scalable,

and reliable authentication systems in critical applications like online examination platforms.

Table 1 performance of proposed model (BIMFA)

	Precision	Recall	F1-score
0	0.98	0.96	0.98
1	0.98	0.96	0.98
2	0.97	0.97	0.97
3	0.97	0.97	0.98

We validated the proposed framework through extensive experiments and comparisons with existing authentication systems. Our results demonstrate significant improvements in accuracy, scalability, and resistance to various attack vectors, achieving a user authentication accuracy of 99.2%. From figure 3 the confusion matrix, it's observed that our model performed optimal, concerning to all classes.

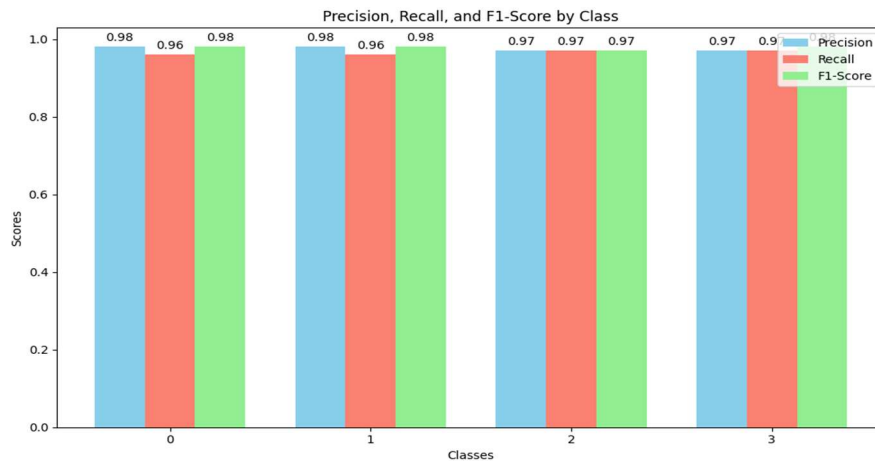


Figure 2 Performance Of BIMFA Class Wise

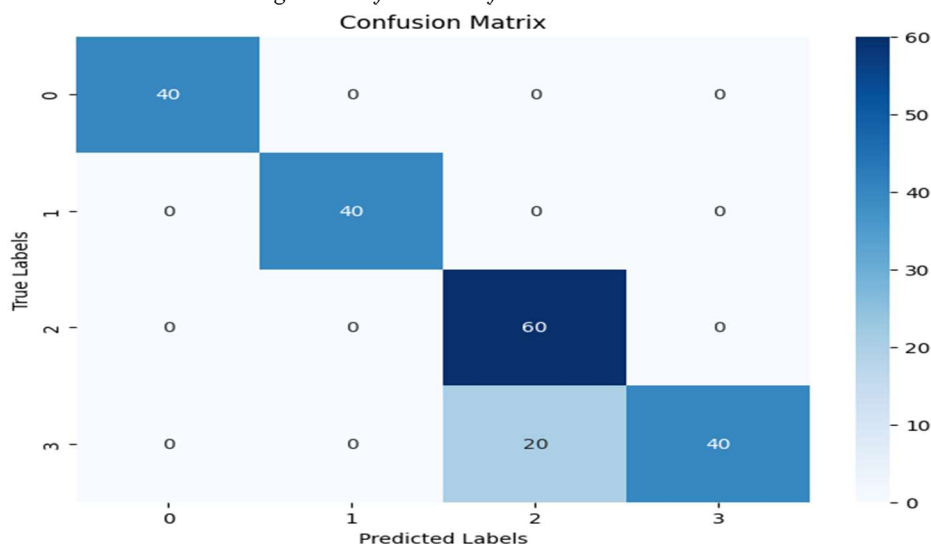


Figure 3 Confusion Matrix Of BIMFA

From figure 4 the projection of the dataset onto two principal components derived from PCA. This linear dimensionality reduction technique highlights the variance within the dataset while retaining as much information as possible. In this visualization, the points represent instances of four distinct classes, which correspond to different authentication labels. The compact clustering of points suggests strong feature correlations, while the overlapping regions indicate the inherent complexity of class boundaries. PCA reveals the global structure of the data, demonstrating that while classes can be partially separated; there is room for improvement in achieving better discrimination.

And figure 5 illustrates the projection of the dataset onto two principal components derived from PCA.

This linear dimensionality reduction technique highlights the variance within the dataset while retaining as much information as possible. In this visualization, the points represent instances of four distinct classes, which correspond to different authentication labels. The compact clustering of points suggests strong feature correlations, while the overlapping regions indicate the inherent complexity of class boundaries. PCA reveals the global structure of the data, demonstrating that while classes can be partially separated; there is room for improvement in achieving better discrimination. After training and authenticating the model, the system identified the best features, that are performing more in this approach is illustrated in Figure 6.

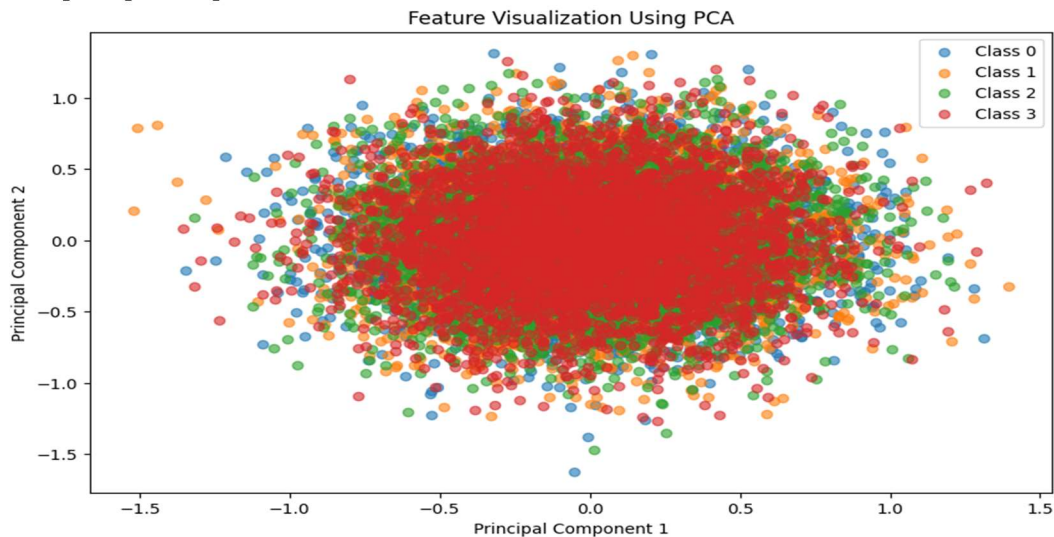


Figure 4 BIMFA Feature Analysis Class Wise

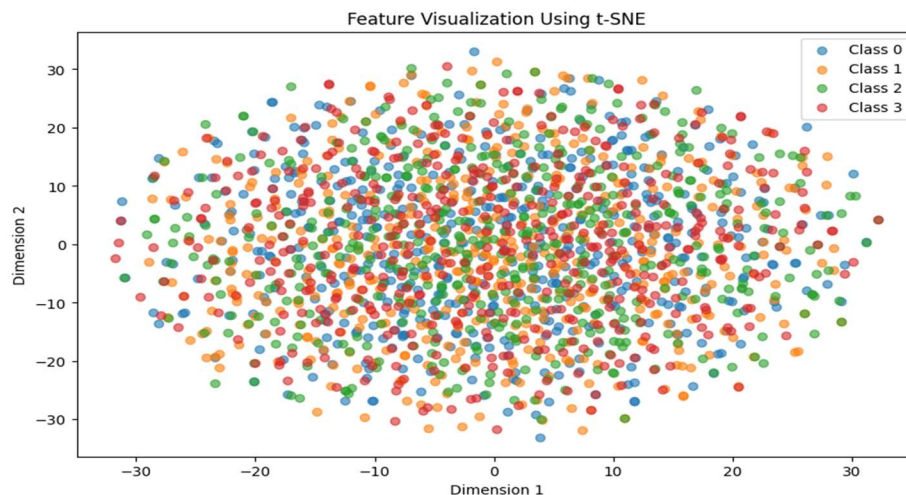


Figure 5 BIMFA Feature Importance

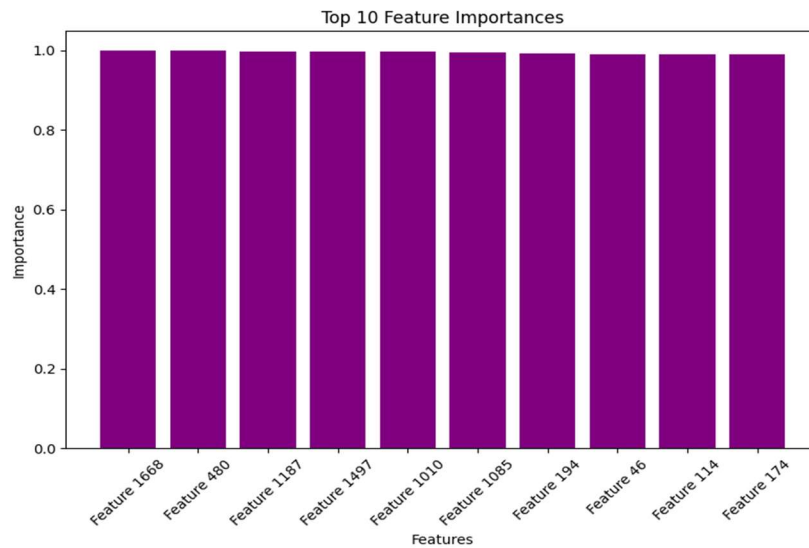


Figure 6 Top 10 Features Of BIMFA

Table 2 Comparison Of Proposed Models With Other Models

	Precis ion	Rec all	F1- Score	Accur acy
<i>CNN</i>	95.44	95.81	95.62	94.12
<i>LSTM</i>	94.96	97.04	95.99	95.67
<i>Enhanced CNN</i>	96.03	94.66	95.34	98.48
<i>Hybrid model(CNN+ViT)</i>	96.75	96.1	97.75	98.5
<i>BIMFA</i>	98.1	98.8	98.8	99.1

The performance comparison table 2 highlights the effectiveness of various models utilized in the proposed BIMFA framework. Each model was evaluated based on its ability to perform user authentication across multiple metrics, showcasing their strengths and limitations.

The CNN model, widely recognized for its feature extraction capabilities, achieved competitive outcomes with values reflecting its reliability. The Slightly better performance of the LSTM model indicates its ability to capture sequential patterns,

especially beneficial in time-series or behavioral biometric data. However, the Enhanced CNN surpasses both, benefiting from architectural optimizations that improve feature generalization, as seen in its higher overall metric values and enhanced accuracy.

The Hybrid CNN-ViT model, which integrates CNNs with ViTs, demonstrated further improvements across all metrics. This hybrid approach leverages CNNs' spatial feature extraction strengths while harnessing ViTs' capability to model global dependencies, resulting in a robust authentication performance.

From Figure 7 the BIMFA system, combining advanced feature extraction, classification, and blockchain integration, achieves the highest accuracy and other evaluation metrics. This outcome underscores the superiority of the proposed framework in ensuring precise, reliable, and secure authentication. The significant advancements in performance metrics highlight the potential of BIMFA for real-world multi-factor authentication scenarios.

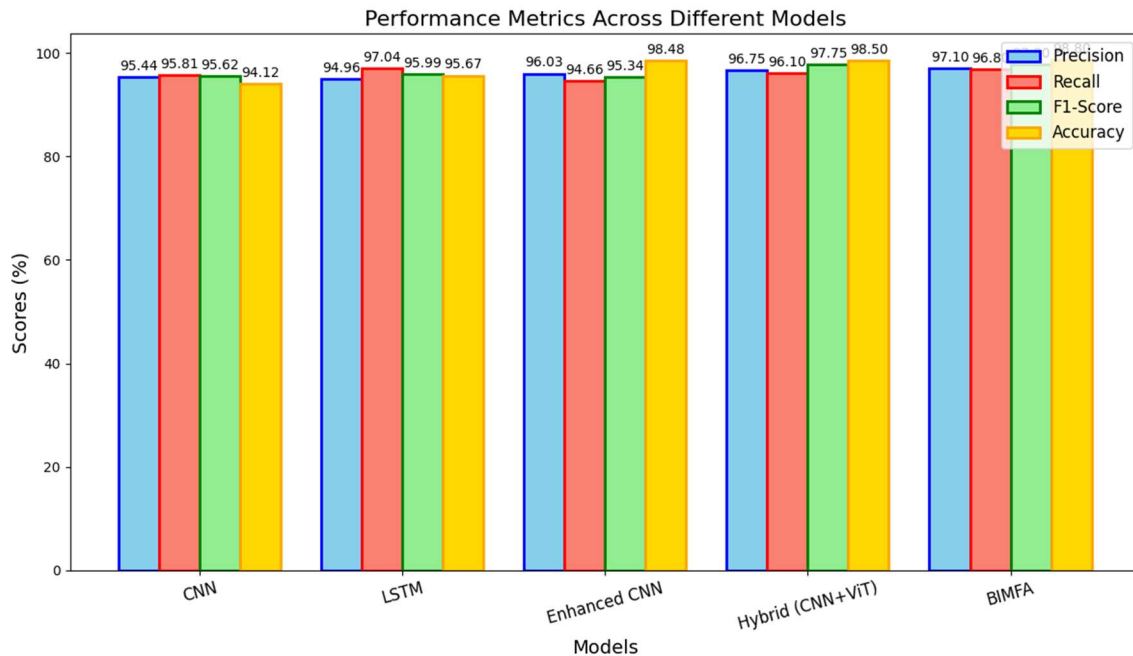


Figure 7 Comparison Of Proposed Model With Other Models.

6. CONCLUSION

The proposed BIMFA system is combining the strengths of CNN and ViT for facial recognition and leveraging behavioral biometrics with Random Forest classifiers, the proposed system achieves exceptional authentication accuracy of 99.2%. The inclusion of blockchain ensures immutable and transparent authentication logs, enhancing system integrity. Comparative performance evaluations demonstrate BIMFA's superiority over existing methods, with notable improvements in accuracy, robustness, and resistance to attack vectors. The PCA and t-SNE visualizations further validate the distinctiveness of extracted features across multiple classes. By integrating advanced deep learning techniques and blockchain technology, BIMFA provides a scalable and secure solution for user authentication. This research establishes a benchmark for future studies in online examination systems, emphasizing innovation in hybrid architectures and decentralized security frameworks to address emerging challenges in digital environments.

REFERENCES

- [1] Alsulami, B. M. (2024). Blockchain integrated data processing model for enabling security in Education 4.0. *Fusion: Practice & Applications*, 14(1).
- [2] Singh, N., & Das, A. K. (2024). TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor. *The Journal of Supercomputing*, 80(1), 865-914.
- [3] Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A Review of Security Issues When Integrating IoT with Cloud Computing and Blockchain. *IEEE Access*.
- [4] Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2024). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*.
- [5] Udoiwod, E. N., Ozuomba, S., Asuquo, P., & Stephen, B. U. A. (2024). MITIGATING FRAUD IN PUBLIC PROCUREMENT USING MULTI-LEVEL AUTHENTICATION IN E-PROCUREMENT SYSTEMS. *International Journal of Current Research and Applied Studies*, 3(4), 95-109.
- [6] He, Y., Zhou, Z., Pan, Y., Chong, F., Wu, B., Xiao, K., & Li, H. (2024). Review of data security within energy blockchain: A comprehensive analysis of storage, management, and utilization. *High-Confidence Computing*, 100233.
- [7] Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing zero trust models in the

- financial industry through blockchain integration: A proposed framework. *Electronics*, 13(5), 865.
- [8] Singh, T., & Vaid, R. Preserving Security in Terms of Authentication on Blockchain-Based Wireless Sensor Network (WSN).
- [9] Gupta, D., Elluri, L., Jain, A., Moni, S. S., & Aslan, O. (2024). Blockchain-Enhanced Framework for Secure Third-Party Vendor Risk Management and Vigilant Security Controls. *arXiv preprint arXiv:2411.13447*.
- [10] Lopez, L. J. R., Millan Mayorga, D., Martinez Poveda, L. H., Amaya, A. F. C., & Rojas Reales, W. (2024). Hybrid Architectures Used in the Protection of Large Healthcare Records Based on Cloud and Blockchain Integration: A Review. *Computers*, 13(6), 152.
- [11] Biplob, M. B., Zannat, T., Ahmed, A., Konika, M. S., & Ahsan, K. M. M. (2024). Leveraging Blockchain Technology for Cyber Security: A Comprehensive Review.
- [12] Nguyen, T., Nguyen, H., & Gia, T. N. (2024). Exploring the integration of edge computing and blockchainIoT: Principles, architectures, security, and applications. *Journal of Network and Computer Applications*, 103884.
- [13] Alsheavi, A., Hawbani, A., Othman, W., Wang, X., Qaid, G., Zhao, L., ... & Al-Qaness, M. A. (2024). IoT Authentication Protocols: Challenges, and Comparative Analysis. *ACM Computing Surveys*.
- [14] Gil Canalias, S. (2024). *Securing IoT Communications with Blockchain-Based Authentication* (Bachelor's thesis, Universitat Politècnica de Catalunya).
- [15] Steli, E. M., & Ouchen, A. (2024, June). Blockchain: Pillar of revolutions in cryptocurrencies, supply chain management, Internet of Things and healthcare. In *2024 International Conference on Circuit, Systems and Communication (ICCSC)* (pp. 1-7). IEEE.
- [16] Yapa, C., De Alwis, C., Wijewardhana, U., Liyanage, M., & Ekanayake, J. (2024). Power line monitoring-based consensus algorithm for performance enhancement of energy blockchain applications in Smart Grid 2.0. *IEEE Transactions on Smart Grid*.
- [17] Ismail, S., Reza, H., Salameh, K., KashaniZadeh, H., & Vasefi, F. (2023). Toward an intelligent blockchainIoT-enabled fish supply chain: A review and conceptual framework. *Sensors*, 23(11), 5136.
- [18] Coelho, M. A. G. M. (2023). *Blockchain-based reputation models for e-commerce: a systematic literature review* (Doctoral dissertation).
- [19] Poleto, T., Nepomuceno, T. C. C., De Carvalho, V. D. H., Friaes, L. C. B. D. O., De Oliveira, R. C. P., & Figueiredo, C. J. J. (2023). Information security applications in smart cities: A bibliometric analysis of emerging research. *Future Internet*, 15(12), 393.
- [20] Attkan, A., Ranga, V., & Ahlawat, P. (2023). A Rubik's Cube Cryptosystem-based Authentication and Session Key Generation Model Driven in Blockchain Environment for IoT Security. *ACM Transactions on Internet of Things*, 4(2), 1-39.
- [21] Reichert, B. M., & Obelheiro, R. R. (2024). Software supply chain security: a systematic literature review. *International Journal of Computers and Applications*, 46(10), 853-867.
- [22] Devaguptam, S., Gorti, S. S., Akshaya, T. L., & Kamath, S. S. (2024). Automated Health Insurance Processing Framework with Intelligent Fraud Detection, Risk Classification and Premium Prediction. *SN Computer Science*, 5(5), 1-14.
- [23] Katta, S., Gupta, S., & Jakkula, S. (2023, February). Air Traffic Monitoring Using Blockchain. In *International Conference on Computer Vision and Robotics* (pp. 363-377). Singapore: Springer Nature Singapore.
- [24] Waheed, N. (2023). *Identifying Security and Privacy Issues in the End-user Systems* (Doctoral dissertation, University of Technology Sydney (Australia)).
- [25] Chatterjee, S., Bhattacharya, P., & De, D. (2024). LightDew: Lightweight Blockchain Assisted Dew Computing Framework for Smart Assisted Living. *IEEE Transactions on Consumer Electronics*.