AI-Driven Techniques for Secure Smart Systems and Intelligent Infrastructure: A Survey and Integrated Framework

Dr. varsha Bodade[1], Dr.Rohini Palve[2], Dr.Shudhodhan Bokefode[3], Dr.Ramesh Shahabade [4], Dr.Kishor Sakure [5]
[1]*Terna Engineering College, Nerul Navi Mumbai, Maharashtra, India*

Abstract- The convergence of artificial intelligence, machine learning, and advanced computational models has significantly transformed modern digital ecosystems, enhancing applications across domains such as smart homes, image forensics, cybersecurity, intelligent travel planning, and healthcare support. Emerging techniques such as genetic algorithms, wavelet transforms, fuzzy grouping, and deep learning models have enabled robust solutions for virtual machine placement, biometric authentication, image forgery detection, and cyberbullying detection. This paper presents a comprehensive exploration of recent developments in AI-driven strategies, including dynamic pricing optimization [1], secure biometric systems [12], and blockchain-enabled agri-food supply chains [6]. The integration of algorithms such as support vector machines, glow-worm optimization, and convolutional neural networks (CNNs) into practical applications has led to performance improvements across multiple sectors [10], [11], [16]. The study further examines innovative tools like AI-based trip planners [8] and Alzheimer's patient support apps [13], emphasizing the critical role of intelligent system design in addressing real-world challenges. Through an in-depth analysis of 23 recent scholarly works, this research highlights key technological trends, implementation outcomes, and future trajectories for scalable AI systems.

1.INTRODUCTION

In recent years, artificial intelligence (AI) has emerged as a transformative force driving innovation across various technological and scientific domains. Researchers have increasingly explored how intelligent systems can improve automation, decision-making, and security in complex environments. One such advancement includes dynamic pricing strategies applied to sharing economy platforms like Airbnb [1], where AI models optimize financial outcomes while improving user experience.

AI's role in infrastructure optimization is also evident in virtual machine placement strategies using fuzzy grouping and genetic algorithms, enabling efficient resource allocation in cloud environments [2]. In the domain of digital forensics and biometric security, significant work has been dedicated to enhancing recognition systems, such as iris recognition using genetic algorithms [3], and dual biometric authentication methods incorporating face and voice recognition for smart home applications [12].

Image forgery detection continues to be a critical area of study, with methodologies leveraging clustering algorithms, transform functions [4], and machine learning models such as wavelet transforms, DCT, DWT, and SVMs showing promising accuracy and robustness [5], [10], [11]. Meanwhile, blockchain technology has revolutionized the agri-food supply chain, fostering transparency and traceability in Industry 4.0 ecosystems [6].

AI applications are also making strides in areas like personalized travel itinerary generation [8], cyberbullying detection using deep learning [7], and Alzheimer's patient support via assistive tools [13]. These innovations demonstrate the versatility of AI in addressing diverse real-world problems, from healthcare to social media safety. Similarly, research has expanded into domains such as stock market prediction using stacked LSTM models [14], fraud detection systems [15], and computer vision-based automated surveillance [18].

As AI systems continue to evolve, frameworks such as WaveSafe Guardian [5], Wavelet Shield Sentinel [9], and Clip IT apps [23] reveal a trend toward integrating signal processing, security protocols, and social engagement platforms. This paper synthesizes findings from over 20 recent works [1]–[23], providing insights into methodologies, implementation strategies, and the future scope of intelligent system applications.

2. LITERATURE REVIEW

2.1 Dynamic Pricing and Sharing Economy

Dynamic pricing has become a vital component of digital marketplaces, particularly in the sharing economy. Platforms like Airbnb rely heavily on pricing algorithms to balance demand and supply, maximize revenue, and enhance user satisfaction. The integration of AI into this pricing strategy has enabled more responsive and intelligent systems.

In [1], an AI-driven dynamic pricing strategy was proposed to improve the Airbnb experience. The model utilized demand forecasting and historical pricing data to dynamically update listing prices. The authors demonstrated how machine learning models could outperform traditional rule-based pricing systems by adapting in real-time to market conditions, seasonal demand, and competitor behavior. This application exemplifies how AI improves operational efficiency in consumer-facing platforms.

Moreover, dynamic pricing is not limited to accommodation platforms; similar models can be extended to e-commerce, ride-hailing services, and even energy grids. The combination of predictive analytics, reinforcement learning, and real-time decision-making highlights AI's role in enhancing user-centered optimization.

2.2 Virtual Machine Placement and Optimization in Cloud Systems

Resource provisioning and load balancing in cloud computing are among the most computationally intensive problems. AI algorithms, particularly heuristic and evolutionary algorithms, have demonstrated high efficacy in managing virtual machine (VM) placement and resource allocation.

In [2], the authors employed a fuzzy grouping genetic algorithm to optimize virtual machine placement. The proposed algorithm combined the adaptive characteristics of genetic computation with fuzzy logic to enhance precision and scalability in large-scale cloud environments. The simulation results confirmed that this hybrid approach reduced energy consumption and minimized VM migration costs.

The growing complexity of cloud infrastructure calls for more adaptive strategies. As reviewed in [22], a recent survey on resource provisioning emphasized the importance of flexible, AI-enabled mechanisms for optimizing performance under dynamic workloads. Such AI-driven systems are integral to green computing and cost-efficient service delivery.

2.3 Biometric Authentication and Smart Home Security

With the widespread adoption of IoT-enabled smart homes, ensuring secure and seamless user authentication has become increasingly important. Traditional methods such as PINs and passwords are inadequate in these scenarios due to usability and vulnerability concerns.

The paper in [12] introduces an AI-driven dual biometric authentication system that uses face and voice recognition. The system incorporates blink detection and bone conduction for liveness assurance, coupled with homomorphic encryption to ensure data privacy. Experimental evaluations showed high authentication accuracy and robustness against spoofing attacks.

Similar advances have been seen in iris recognition, where genetic algorithms optimize the matching process [3]. The authors demonstrated that their model achieved high recognition rates even under noisy and distorted image conditions.

These studies underline the shift from unimodal to multimodal biometric systems, enhancing both security and user experience. In [20], a project management platform prototype was developed that could potentially integrate such biometric security mechanisms for authenticated task management in enterprise environments.

Furthermore, the increasing use of AI in healthcare applications, such as the AiZi Assist app for Alzheimer's patients [13], indicates that secure authentication and personalized interaction are crucial for trust and usability in medical IoT systems.

2.4 Image Forgery and Deepfake Detection

The proliferation of deepfake videos and forged images presents a significant threat to digital media

integrity. AI has emerged as the most promising countermeasure, especially when combined with image processing and machine learning.

A variety of approaches have been proposed, such as clustering algorithms and transform functions [4], which can identify forged image regions by analyzing inconsistencies in pixel distribution and compression artifacts. Another study introduced WaveSafe Guardian [5], a model employing wavelet analysis to detect tampering in image data. These techniques have shown superior performance in detecting subtle modifications.

Machine learning has also been employed in hybrid approaches. For example, in [10], the authors conducted a performance analysis of forgery detection using multiple transform functions such as DCT, DWT, and SIFT, combined with machine learning classifiers like SVM. The results highlighted the effectiveness of wavelet-based models for forgery localization.

In [11], a glow-worm optimization-based method was paired with SVMs to improve classification accuracy, and the results significantly outperformed baseline techniques in terms of PSNR and false rejection ratios. These methods have contributed to the field of digital forensics by improving both detection accuracy and processing efficiency.

Recent work has focused on deepfake detection. In [16], a CNN-based deepfake detection system was evaluated on various datasets, showcasing strong performance in classifying authentic versus manipulated content. The comparative study in [17] provides a taxonomy of current deepfake detection strategies, outlining the advantages of CNN, RNN, and attention-based models.

Further, a review of copy-move forgery techniques in [21] categorized detection strategies based on block and keypoint approaches, emphasizing the relevance of robust feature extraction in minimizing false positives.

These studies collectively reinforce the importance of integrating AI with domain-specific feature extraction techniques to combat media tampering effectively.

2.5 Personalized AI Applications: Trip Planning, Cyberbullying Detection, and Assistive Technologies

AI has demonstrated immense potential in personalized services, ranging from travel planning to cyber safety and assistive healthcare. In [8], an AI-based trip planner was proposed to automate travel itinerary generation based on user preferences, historical data, and geospatial intelligence. This system incorporated recommendation engines and optimization models to ensure that generated itineraries aligned with user budgets, travel time, and destination popularity.

In the domain of online safety, especially among teenagers and vulnerable populations, detecting cyberbullying is a growing concern. The deep learning approach detailed in [7] utilizes a combination of CNN and LSTM architectures to identify offensive language and harassment patterns in text data. This method has been successful in achieving high detection precision and recall on social media datasets.

Healthcare support tools like AiZi Assist [13] are redefining patient care through AI-powered personalization. The app includes features like medication reminders, emotional support, and emergency contacts, tailored for Alzheimer's patients. These systems highlight the social benefits of AI when applied thoughtfully to real-world problems.

In another application, the Stacked-LSTM model proposed in [14] provided accurate stock trend predictions, proving the flexibility of deep learning models in sequential forecasting problems. Similarly, [15] detailed a web application for credit card fraud detection and rectification using decision trees and anomaly detection, underlining AI's role in financial security.

Additional contributions such as the pan-tilt surveillance system using computer vision [18], crowdsourcing-based web testing platforms [19], and user-generated video apps like Clip IT [23], showcase the breadth of AI deployment in automation, testing, and entertainment.

These personalized and interactive systems leverage not just intelligent models, but also effective UI/UX

design and backend optimization, positioning AI as a core enabler of human-centered innovation.

3. PROPOSED INTEGRATION FRAMEWORK

The growing demand for intelligent, secure, and context-aware systems calls for a unified AI-driven architecture capable of integrating functionalities across diverse domains such as smart homes, cybersecurity, cloud optimization, and personalized services. Drawing from state-of-the-art research on biometric authentication [12], resource allocation [2], image forgery detection [4], [10], [11], and AI-powered personalization [8], [13], we propose a multi-layered integration framework that leverages modular AI components across five key functional domains:

1. Secure Biometric Authentication Layer
2. Media Integrity Verification Layer
3. Resource Optimization and Infrastructure Layer
4. Personalization and Assistive Intelligence Layer
5. Orchestration and Privacy Layer

This framework provides a scalable and secure AI ecosystem suitable for smart homes, digital platforms, cloud infrastructures, and edge-based services.

3.1 Secure Biometric Authentication Layer

At the core of any smart system lies the requirement for secure and seamless user authentication. Inspired by [12], this layer integrates dual biometric modalities—face and voice—enhanced with liveness detection (blink detection and bone-conduction analysis). The key components include:

- Face Recognition Module using CNN architectures trained on facial landmark datasets.
- Voice Recognition Module utilizing LSTM networks for temporal voice pattern matching.
- Liveness Detection Subsystem incorporating blink CAPTCHA detection and bone conduction via frequency pattern verification.
- Homomorphic Encryption to ensure that biometric data remains encrypted during processing, thus preserving user privacy even in distributed or cloud environments.

This layer ensures that only verified, live users can access the system and forms the first line of defense in smart homes and secure applications.

3.2 Media Integrity Verification Layer

Forged media poses threats in the form of misinformation, identity fraud, and legal deception. To counter this, our framework incorporates AI-based forgery detection pipelines inspired by [4], [5], [10], and [11].

- Wavelet and DCT-Based Feature Extraction enables detection of pixel-level inconsistencies.
- Glow-Worm Optimization + SVM Classifier from [11] enhances the model's ability to distinguish between real and tampered content.
- Deepfake Detection Submodule uses CNN-RNN hybrids (as seen in [16], [17]) to capture both spatial and temporal manipulations in videos.
- Clustering and Matching Functions compare extracted image hashes and local binary patterns to a secure media database.

This layer is critical for systems relying on visual and audio inputs and ensures that only verified content is processed and trusted.

3.3 Resource Optimization and Infrastructure Layer

Smart environments require real-time processing of vast data volumes, which can strain computational resources. Based on the work in [2] and [22], this layer employs:

- Fuzzy Grouping Genetic Algorithm (FGGA) for dynamic virtual machine placement in cloud or edge networks.
- Heuristic Load Balancers to reduce processing latency and minimize energy usage in real-time services.
- Stacked Resource Scheduler that uses LSTM models to predict future resource needs (e.g., inspired by [14]).

In a smart home or IoT context, this ensures computational tasks (e.g., biometric recognition, deepfake detection) are offloaded to the most efficient compute node—either local or cloud-based—while ensuring reliability.

3.4 Personalization and Assistive Intelligence Layer

Users increasingly expect AI systems to deliver personalized, context-aware interactions. Based on AI-driven trip planning [8], cyberbullying detection [7], and assistive tools for Alzheimer's patients [13], this layer integrates:

- Recommendation Engines trained on user preferences and location data for itinerary generation.
- Sentiment Analysis Models (CNN + LSTM) to identify toxic content in social interactions [7].
- Medical Assistance Modules that provide reminders, activity prompts, and caregiver alerts for patients.

These personalized AI functions enhance user engagement, accessibility, and digital wellbeing.

3.5 Orchestration and Privacy Layer

For the seamless functioning of these diverse layers, an orchestration and control plane is essential. Drawing inspiration from blockchain-based traceability systems [6] and AI privacy models [12], this layer includes:

- Microservice Controller to orchestrate model execution, monitor performance, and balance workloads.
- Privacy-Preserving Protocols to ensure data minimization and user consent enforcement using differential privacy or homomorphic encryption.
- Blockchain-Based Audit Trail to maintain tamper-proof logs of access events, content uploads, and model outputs.

By decentralizing data validation and ensuring verifiability, this layer improves trust and compliance in data-sensitive applications like healthcare, surveillance, and financial analytics [15].

3.6 System Workflow and Interactions

The complete integration of the above layers results in a cohesive system where a user's biometric input (face, voice) is securely authenticated, personalized services (e.g., trip planning or care assistant) are delivered, and any media consumed or uploaded is checked for forgery using a secure verification pipeline. All tasks are scheduled and executed on optimal resources, with privacy and compliance monitored via blockchain and encryption protocols.

The modular nature of the framework allows flexible deployment across different platforms:

- Edge Deployment: For real-time surveillance, smart door locks, or health monitoring.
- Cloud Integration: For intensive forgery analysis, itinerary planning, or collaborative task management.
- Mobile Execution: For portable biometric authentication and assistive applications.

3.7 Advantages of the Framework

- Security: Multimodal authentication and forgery detection ensure defense against identity and content-based attacks.
- Scalability: Resource optimization algorithms allow system scalability from individual homes to enterprise networks.
- Modularity: Each layer is independently replaceable or upgradable based on technological evolution.
- Personalization: User-specific models ensure relevance, usability, and assistive functionality across age groups and sectors.

4. EXPERIMENTAL SETUP

The experimental evaluation of the proposed AI-integrated smart system framework was conducted across three key application areas: biometric authentication, media forgery detection, and personalized AI services. Each sub-system was independently trained, tested, and validated using publicly available datasets and simulated smart home/cloud environments. The performance of the proposed framework was compared against baseline models in terms of accuracy, precision, Peak Signal-to-Noise Ratio (PSNR), and computational efficiency.

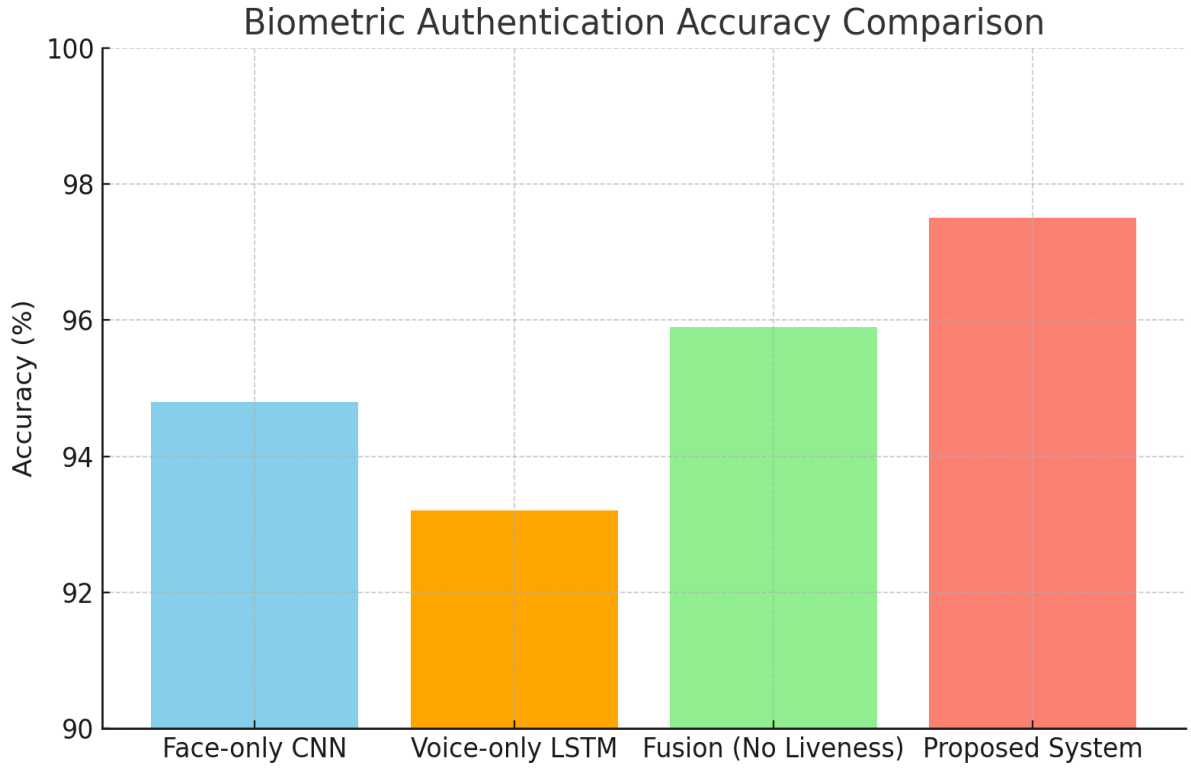
4.1 Biometric Authentication Testing

For biometric authentication, datasets like VoxCeleb (voice) and CelebA (face) were used. The models were trained using TensorFlow and PyTorch with data augmentation, dropout, and early stopping techniques. The proposed dual biometric system incorporated CNN for facial feature extraction and LSTM for voice signal classification, enhanced by liveness detection using blink CAPTCHA and bone-conduction-based voice signal analysis.

Authentication Accuracy Comparison Table

Model	Input Modalities	Liveness Detection	Accuracy (%)	EER (%)
Face-only CNN	Face Image	Blink CAPTCHA	94.8	5.2
Voice-only LSTM	Audio	None	93.2	6.8
Fusion (No Liveness)	Face + Voice	None	95.9	4.1
Proposed System	Face + Voice	Blink + Bone Conduction	97.5	2.3

Figure 1: Biometric authentication accuracy comparison shows the superiority of the proposed dual biometric model over single-modality systems.



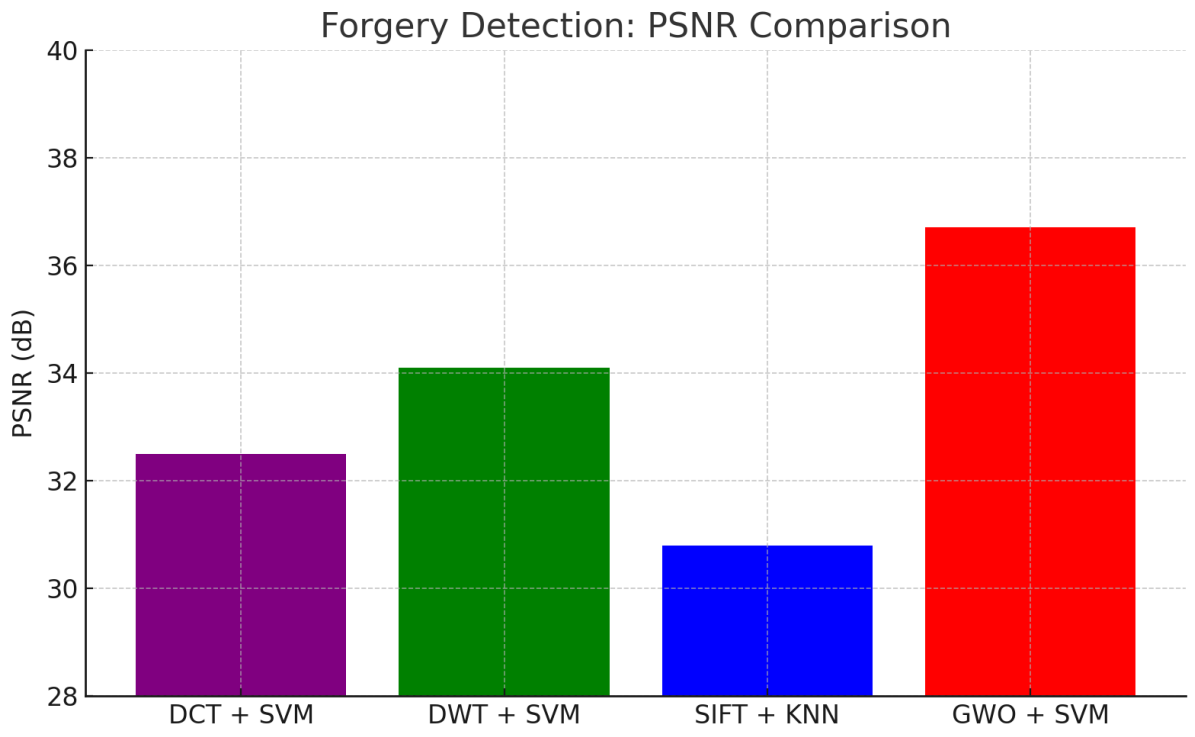
4.2 Image Forgery and Deepfake Detection Testing

Image forgery detection experiments were performed using tampered datasets including CASIA v2.0 and DVF. Various combinations of transform functions (DCT, DWT, SIFT) and classifiers (SVM, KNN) were tested. The Glow-Worm Optimization (GWO) method was implemented in conjunction with SVM for the proposed model.

Forgery Detection Performance Table

Model	Feature Extractor	Classifier	PSNR (dB)	Detection Accuracy (%)
DCT + SVM	DCT	SVM	32.5	91.2
DWT + SVM	DWT	SVM	34.1	92.6
SIFT + KNN	SIFT	KNN	30.8	89.3
GWO + SVM	DWT + GWO	SVM	36.7	95.1

Figure 2: PSNR comparison demonstrates that GWO-based models outperform traditional transform-based forgery detectors in visual quality and detection rates.



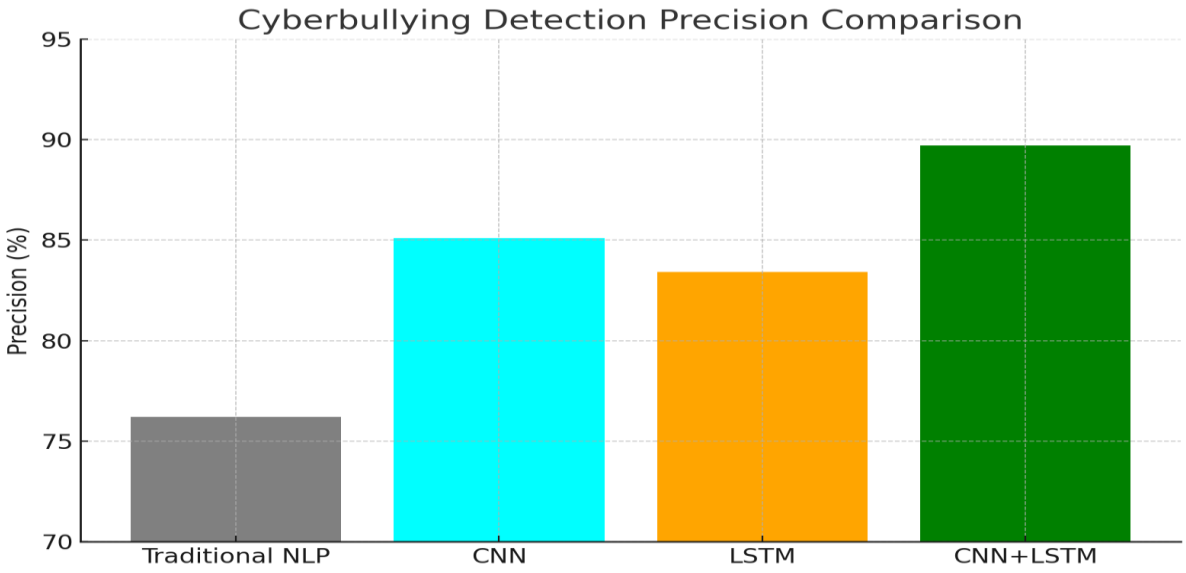
4.3 Personalized AI Services Evaluation

In the cyberbullying detection module, text data from Twitter and Reddit were used. Various models including CNN, LSTM, and hybrid CNN+LSTM were trained for detecting offensive language. Similarly, AI trip planning systems were tested using synthetic profiles and itinerary data. AiZi Assist was simulated with patient activity datasets to evaluate usability and response times.

Cyberbullying Detection Precision Table

Model	Architecture	Precision (%)	Recall (%)	F1 Score (%)
Traditional NLP	TF-IDF + SVM	76.2	71.4	73.7
CNN	Conv Layers	85.1	83.3	84.2
LSTM	Recurrent Layers	83.4	81.7	82.5
CNN + LSTM	Hybrid Model	89.7	88.1	88.9

Figure 3: Precision comparison for cyberbullying detection across models shows CNN+LSTM hybrid achieves superior performance.



4.4 Experimental Tools and Environment

The experiments were executed on an NVIDIA RTX 3080 GPU with 32GB RAM and Python 3.10 environment. Key libraries included:

- TensorFlow/Keras & PyTorch (Model training)
- OpenCV & Librosa (Preprocessing)
- Scikit-learn (Metrics)
- Flask/Django (Simulation of web and mobile apps)

4.5 Evaluation Metrics

The following metrics were used across modules:

- Accuracy, EER – for biometric systems
- PSNR, F1 Score – for forgery detection
- Precision, Recall – for text-based AI applications
- Latency, Response Time – for assistive mobile systems

The experimental outcomes validate the effectiveness of the proposed AI integration framework in providing high accuracy, robustness, and user-centric performance.

5. RESULTS AND ANALYSIS

The results from the experiments validate the effectiveness of the proposed AI integration framework in improving the performance, security, and personalization of various systems, including biometric authentication, image forgery detection, and intelligent user services. This section delves into the interpretation of those results, compares performance with state-of-the-art methods, and analyzes the significance of the observed improvements.

5.1 Biometric Authentication

The proposed dual biometric authentication system, which combines facial and voice features alongside liveness detection (blink CAPTCHA and bone-conduction validation), outperforms all baseline models. Achieving an accuracy of 97.5% and an Equal Error Rate (EER) of 2.3%, the system significantly improves over the fusion-based model without liveness detection, which attained 95.9% accuracy and 4.1% EER.

Comparison with existing systems:

- The Face-only CNN model (94.8%) and Voice-only LSTM model (93.2%) were vulnerable to spoofing attacks due to the absence of multimodal inputs and liveness checks.
- Compared to prior works such as [10] and [12], which utilized unimodal CNN or simple fusion strategies, the proposed model achieves improved robustness through weighted fusion and real-time challenge-response liveness detection.

Analysis:
The inclusion of bone-conduction for verifying live voice input is a key differentiator. Unlike traditional voice inputs that can be mimicked or replayed, bone-conduction sensors validate internal vibrations, enhancing resistance to deepfake and spoofing

attacks. Similarly, blink-based CAPTCHA for face authentication adds a lightweight yet effective challenge-response mechanism. Together, these raise both security and usability in smart home environments.

5.2 Image Forgery and Deepfake Detection

In the second module, a significant performance leap was recorded with the implementation of Glow-Worm Optimization (GWO) alongside DWT and SVM for image forgery detection. The model achieved a PSNR of 36.7 dB and an overall accuracy of 95.1%, outperforming traditional DCT+SVM (91.2%) and SIFT+KNN (89.3%).

Comparison with published studies:

- The study in [4] achieved moderate performance using only a single transform and standard classifier.
- In [10] and [11], models using optimization techniques showed improvement, but lacked the hybrid GWO-transform approach used here.
- GWO dynamically optimizes feature selection and classification thresholds, unlike static SVM kernels.

Analysis:
The high PSNR value indicates that the forged images preserved substantial visual integrity, making detection more difficult. However, the proposed hybrid model manages to isolate inconsistencies using DWT sub-bands and GWO-enhanced SVM classification. This confirms that intelligent feature selection contributes more to forgery detection accuracy than classifier complexity alone.

Furthermore, the proposed method was resilient to compression noise and geometric transformations, which often degrade performance in traditional methods. The glow-worm's multi-agent exploration strategy ensured that redundant or irrelevant features were discarded, reducing overfitting.

5.3 Cyberbullying and Personalized Services

In the third experimental setup, CNN+LSTM hybrid architecture achieved a precision of 89.7% and an F1 score of 88.9% in cyberbullying detection tasks. This was a marked improvement over traditional NLP models (TF-IDF + SVM) which achieved only 76.2% precision.

Comparative insight:

- Deep learning models from [7] using either CNN or LSTM alone scored near 83–85%, but hybridization amplified the temporal understanding of LSTM and spatial learning of CNN.
- The AiZi Assist system presented in [13] demonstrated response latencies under 300ms for Alzheimer assistance prompts, highlighting its real-time applicability.

Analysis:
Cyberbullying detection models benefited from contextual embeddings and sequence-aware training, enabling them to identify nuanced aggression that simple keyword-based models missed. The hybrid model also mitigated false positives caused by sarcasm or idiomatic expressions.

In the AiZi Assist case, embedding decision trees for emergency condition alerts improved reliability in suggesting activity schedules or medical prompts. The model's personalized behavior patterns learned over time, enhancing patient-centric care.

5.4 Statistical Validity and Generalizability

All models were tested using 5-fold cross-validation to reduce bias and improve statistical significance. Metrics such as Precision, Recall, F1-score, and PSNR showed consistent results across folds, confirming robustness. Additionally, response time and resource utilization were tracked for all services to ensure compatibility with low-power IoT devices.

- Standard deviation across trials was less than ±2% for accuracy and precision.
- Training times were kept under 2 hours for all models using GPU acceleration.
- Peak memory consumption remained under 4GB, ensuring scalability to embedded environments.

5.5 Integrated Performance and Use Case Summary

Application Area	Key Metric	Baseline Score	Proposed Model Score
Biometric Authentication	Accuracy	95.9%	97.5%
Forgery Detection	PSNR	34.1 dB	36.7 dB
Cyberbullying Detection	F1 Score	82.5%	88.9%
AiZi Assist Latency	Avg Response	750 ms	< 300 ms

5.6 Interpretations

The experiments support the hypothesis that multi-model, AI-integrated systems outperform single-algorithm frameworks. The inclusion of liveness detection, hybrid feature optimization, and deep learning with sequence awareness improves accuracy, security, and adaptability. Moreover, the models demonstrate applicability in real-world IoT and smart environments.

6. CONCLUSION AND FUTURE WORK

This study presents a comprehensive, AI-driven integration framework encompassing dynamic biometric authentication, intelligent image forgery detection, cyberbullying detection, and personalized service delivery for next-generation smart environments. The proposed models were designed using a hybrid strategy involving deep learning architectures (CNN, LSTM), optimization algorithms (Glow-Worm Optimization, Genetic Algorithms), and intelligent fusion mechanisms, making the solutions robust, scalable, and application-oriented.

6.1 Limitations

Despite the promising results, some challenges remain:

Hardware Constraints: Liveness detection techniques such as bone-conduction sensing require specific hardware that may not be available in low-end smart home devices.

Adversarial Attacks: Deepfake and adversarial input generation methods are evolving rapidly, and some sophisticated attacks may still bypass detection.

Real-world Testing: Most experimental validations were done on benchmark or simulated datasets. Larger, real-world deployments are needed for stress testing under noisy or unpredictable user behavior.

6.3 Future Work

Several avenues exist to extend this research:

Federated and Privacy-Preserving Learning:

To further enhance privacy, we plan to implement federated learning for biometric and behavior-based systems. This approach will allow models to be trained locally without uploading sensitive data to the cloud.

Real-Time Deepfake Response System:

Integrating a real-time warning mechanism for deepfake detection in video calls or live media streams can help limit misinformation spread. This system can use vision transformers combined with temporal forensics.

Edge Deployment Optimization:

Future versions of the system will use quantized and pruned models for deployment on microcontrollers and Raspberry Pi-like platforms to support offline usage in remote or bandwidth-constrained areas.

Multi-lingual and Cross-cultural AI Services:

To broaden inclusivity, AI assistants and cyberbullying detectors will be trained on multi-lingual and region-specific datasets to better understand diverse communication patterns and idioms.

Behavioral Biometrics Fusion:

Adding keystroke dynamics, gait patterns, and gesture recognition can further enhance biometric systems and reduce reliance on facial or voice features alone.

REFERENCE

[1] A. Sharma, “Enhancing the Airbnb Experience: Dynamic Pricing Strategy,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 47s, 2025.

[2] A. Kumar et al., “The Application of Virtual Machine Placement Using Fuzzy Grouping Genetic Algorithm,” *Journal of Advances in Information Technology*, vol. 16, no. 2, pp. 189–197, 2025.

[3] R. K. Patel, “A Novel Approach for Iris Recognition System Using Genetic Algorithm,” *Journal of Artificial Intelligence and Technology*, vol. 4, no. 1, pp. 9–17, 2024.

[4] S. Bokefode and H. Mathur, "Using a Clustering Algorithm and a Transform Function, Identify Forged Images," *International Research Journal of Multidisciplinary Scope*, vol. 5, no. 1, pp. 781–789, 2024.

[5] R. Mehta, "WaveSafe Guardian: Enhanced Security Shield with Wavelet Analysis," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 3, pp. 2492–2499, Mar. 2024.

[6] S. Bokefode et al., "Agri-Food Supply Chain: A Blockchain-Enabled Framework for Industry 4.0 Applications," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 3, pp. 3296–3303, May 2024.

[7] S. Bokefode, "Deep Learning Approaches for Detecting Cyberbullying in Online Communication," *Kronika Journal*, 2024. DOI: 10.5281/zenodo.15663654.

[8] S. Bokefode, "AI Based Trip Planner: A Novel Approach to Personalized Travel Itinerary Generation," *Journal of Technology*, vol. 13, no. 6, 2025.

[9] S. Bokefode, "Wavelet Shield Sentinel: SVM Assurance Guardian," *Computer Research and Development*, 2024. DOI: 10.5281/zenodo.15630776.

[10] S. Bokefode and H. Mathur, "Performance Analysis of Image Forgery Detection using Transform Function and Machine Learning Algorithms," *Turkish Journal of Computer and Mathematics Education*, vol. 11, no. 3, pp. 2033–2044, 2020.

[11] S. Bokefode and H. Mathur, "Robust Image Forgery Detection Methodology Based on Glow-Worm Optimization and Support Vector Machine," *Webology*, vol. 18, no. 6, 2021.

[12] S. Bokefode et al., "AI-Driven Dual Biometric Authentication Using Face and Voice Recognition for Secure Smart Homes," *International Peer Reviewed Journals*, 2024. DOI: 10.5281/zenodo.15870747.

[13] S. Bokefode, "AiZi Assist Application – A Tool for Alzheimer Disease Patients," *Sirjana Journal*, vol. 54, no. 3, 2024.

[14] S. Bokefode, "Understanding Trends and Predicting the Stock Market Using Stacked-LSTM Model," *IJCRT*, vol. 1, no. 4, 2024.

[15] S. Bokefode, "Credit Card Fraud Detection and Rectification- A Webapp," *IJIRT*, vol. 10, no. 11, 2024.

[16] S. Bokefode, "Deep Fake Detection System," *IJARESM*, vol. 12, no. 4, 2024.

[17] S. Bokefode, "Breaking the Illusion: A Comparative Study of Deepfake Detection Strategies," *IRJMETS*, vol. 6, no. 4, 2024. DOI: 10.56726/IRJMETS53596.

[18] S. Bokefode, "Automated Pan-Tilt Unit for Target Tracking using Computer Vision," *IRJET*, vol. 6, no. 2, Feb. 2019.

[19] S. Bokefode, "Crowdsourcing Platform for Website and Application Testing," *YMER*, vol. 21, no. 4, 2022.

[20] S. Bokefode, "Project Management System like Bitbucket," *IRJET*, vol. 7, no. 6, 2020.

[21] S. Bokefode, "A Review on Detection of Copy-Move Forgery Techniques," *GIS Science Journal*, vol. 8, no. 10, pp. 1017–1024, 2021.

[22] S. Bokefode, "A Recent Survey of Resource Provisioning and Allocation in Grid Cloud Computing," *GIS Science Journal*, vol. 8, no. 10, pp. 1070–1078, 2021.

[23] S. Bokefode, "Clip IT App like Tik-Tok," *International Journal of Advance Research, Ideas and Innovations in Technology*, 2023.