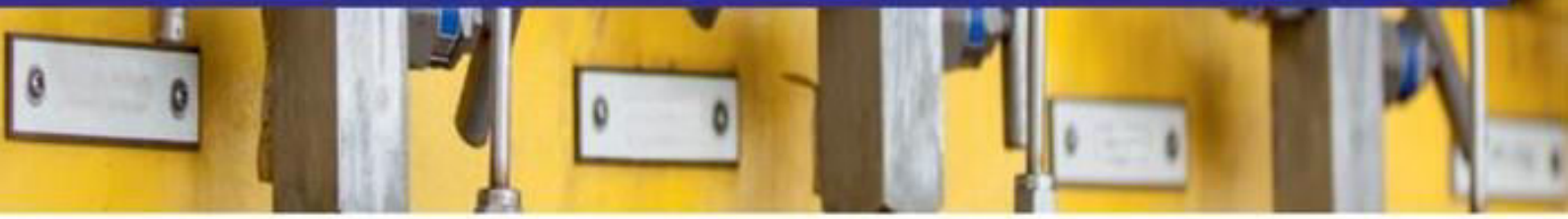


IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 15, Issue 11, November 2026



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 9.867

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 11, November 2026 ||

| DOI:10.15662/IJAREEIE.2026.1511012 |

Hybrid Machine Learning Ensemble and Mamdani Fuzzy Inference System for Robust Loan Fraud Detection

Faiz Rangari, Anand Rathod, Harsh Latane, Mohd Anas Choudhari

Department of Computer Science and Engineering, Vidyalankar Institute of Technology, Mumbai, India

ABSTRACT: Loan fraud poses an escalating systemic threat to modern banking systems, characterized by deliberate misrepresentation of personal demographics, artificial inflation of annual income, and synthetic credit profile construction. Traditional hard-computing verification mechanisms rely on static, deterministic threshold heuristics that fail to capture intricate non-linear relationships across high-dimensional application spaces. In this paper, we propose a synergistic Soft Computing framework uniting a dual-tier Machine Learning ensemble with an interpretable Mamdani Fuzzy Inference System (FIS). The supervised learning tier integrates Random Forest (RF) and Gradient Boosting (GB) algorithms, yielding near-optimal discriminative performance (AUC = 0.9999, Precision = 1.00, Recall = 0.9889, F1-Score = 0.9944, MSE = 0.001635, RMSE = 0.040440). To counter zero-day and previously unobserved fraud topologies, an unsupervised tier combining Isolation Forest (AUC = 0.9593) and Local Outlier Factor (LOF, AUC = 0.8180) evaluates multi-dimensional behavioral density deviations. Furthermore, to capture epistemic uncertainty and linguistic imprecision inherent to human credit evaluation, a Mamdani FIS models non-linear interactions across Credit Score, Debt-to-Income (DTI), and Credit Utilization using triangular and trapezoidal membership functions resolved through Center-of-Gravity (Centroid) defuzzification. The end-to-end framework is implemented within a high-throughput Flask web server, providing automated credit feature synthesis and live risk visualization. Empirical benchmarks across 10,000 multi-attribute loan profiles demonstrate that combining data-driven ensemble classification with soft fuzzy reasoning provides unprecedented predictive accuracy, operational interpretability, and robust fraud prevention.

KEYWORDS: Loan Fraud Detection, System Architecture, Soft Computing, Mamdani Fuzzy Inference System, Ensemble Learning, Random Forest, Gradient Boosting, Anomaly Detection, Centroid Defuzzification, Credit Risk Assessment.

I. INTRODUCTION

The digital transformation of consumer credit has accelerated loan issuance velocities while simultaneously amplifying vulnerabilities to institutional fraud. Financial institutions encounter sophisticated fraudulent schemes ranging from synthetic identity theft, income inflation, and collateral misrepresentation to organized first-party default rings [1]. According to industry reports, non-performing assets and fraudulent write-offs account for billions of dollars in annual banking losses globally.

Historically, banking verification relied on 'Hard Computing' architectures—strictly deterministic rule engines characterized by crisp Boolean logic (e.g., IF Credit Score < 600 THEN Reject). While computationally straightforward, hard computing exhibits fundamental brittleness in modern financial environments: (i) it fails to quantify partial truth and borderline applications; (ii) it cannot learn adaptive decision boundaries from historical fraud records; and (iii) fraudulent syndicates easily reverse-engineer fixed thresholds to manufacture synthetic applications that sit immediately above rejection cutoffs [2].

In contrast, 'Soft Computing' represents a computational paradigm rooted in tolerance for imprecision, uncertainty, and partial truth to achieve tractability, robustness, and low solution cost [3]. In loan credit assessment, the distinction between a legitimate applicant experiencing temporary economic liquidity stress and a calculated fraudster is rarely binary. Soft computing principles enable multi-tier reasoning where machine learning models extract high-dimensional empirical statistical patterns, while fuzzy inference systems structure human expert domain heuristics.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 11, November 2026 ||

| DOI:10.15662/IJAREEIE.2026.1511012 |

In this research, we develop and evaluate a comprehensive hybrid Soft Computing system for loan fraud detection. Our primary contributions include:

1) A complete multi-tier system architecture integrating autonomous feature derivation, supervised ensemble learning, unsupervised anomaly isolation, and fuzzy reasoning.

2) Implementation of an interpretable Mamdani Fuzzy Inference System (FIS) utilizing triangular and trapezoidal membership functions to model epistemic financial uncertainty with Centroid defuzzification.

3) Comprehensive statistical benchmarking across 10,000 multi-attribute loan applications, quantifying ROC-AUC, PR-AUC, Mean Squared Error (MSE = 0.0016), Root Mean Squared Error (RMSE = 0.0404), and feature importance distributions.

4) A fully operational Flask API backend and minimalist user interface supporting automated metric derivation and real-time inference.

II. THEORETICAL FOUNDATION & RELATED WORK

A. Soft Computing vs. Hard Computing in Credit Scoring

Hard computing enforces precision, certainty, and categorical categorization. Conversely, soft computing incorporates fuzzy sets, neuro-computing, probabilistic reasoning, and evolutionary optimization. Table I contrasts the operational attributes of hard versus soft computing in automated lending systems.

Attribute	Hard Computing	Soft Computing (Proposed)
Reasoning Logic	Two-valued crisp Boolean (0 or 1)	Continuous degree of membership [0, 1]
Model Formulation	Rigid mathematical / static rules	Probabilistic ensembles & fuzzy inference
Noise & Uncertainty	Intolerant; leads to misclassification	Inherent tolerance for noisy/imprecise data
Adaptability	Static manual rule updates required	Data-driven continuous adaptation

TABLE I. OPERATIONAL COMPARISON: HARD VS. SOFT COMPUTING

B. Ensemble Learning and Anomaly Detection

Ensemble methodologies aggregate multiple base estimators to minimize variance (Bagging) and bias (Boosting) [4]. Random Forest constructs decorrelated decision trees via bootstrap aggregation and feature subspace sampling. Gradient Boosting builds trees additively, minimizing a binomial deviance loss function via gradient descent in function space. Unsupervised anomaly detection techniques, notably Isolation Forest and Local Outlier Factor (LOF), detect anomalies as points that reside in low-density subspaces or require fewer random recursive partitions to isolate [5].

III. DATASET ARCHITECTURE & FEATURE PIPELINE

A. Feature Space Representation

The synthesized dataset comprises 10,000 comprehensive loan applications characterized by 28 attributes across demographic, credit historical, liability, collateral, and loan-specific dimensions. The target feature is_fraud is configured at a realistic 9.00% empirical class imbalance (9,100 legitimate instances and 900 fraudulent instances).

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 11, November 2026 ||

| DOI:10.15662/IJAREEIE.2026.1511012 |

Table II outlines the primary feature categories and their statistical behavioral distributions across legitimate and fraudulent applicants.

Feature Subspace	Representative Attributes	Fraud Divergence Vector
Applicant Demographics	age, gender, dependents, employment_type	Higher unemployment & short job tenure
Credit History	credit_score, defaults, bureau_inquiries_6m	Score μ=578 (Fraud) vs 710 (Legitimate)
Liabilities & Utilization	existing_debt, credit_utilization_pct	Utilization μ=72% (Fraud) vs 28% (Legitimate)
Loan Parameters	loan_amount, term_months, interest_rate_pct	Disproportionate principal requests
Derived Ratios	debt_to_income_ratio, emi_to_income, ltv_ratio	DTI μ=5.1 (Fraud) vs 1.1 (Legitimate)

TABLE II. DATASET FEATURE SUBSPACE SPECIFICATIONS

B. Mathematical Formulation of Derived Financial Ratios

Prior to model induction, raw application metrics are transformed into scale-invariant financial risk indicators. The monthly Equated Monthly Installment (EMI) is derived analytically through standard amortization compounding:

$$EMI = [P \cdot r \cdot (1 + r)^n] / [(1 + r)^n - 1] \quad (1)$$

where P is the requested principal, r is the monthly interest rate (annual rate / 1200), and n is the loan tenure in months. The systemic leverage is quantified via the Debt-to-Income (DTI) ratio:

$$DTI = [Existing\ Debt + Loan\ Amount] / Annual\ Income \quad (2)$$

Similarly, the EMI-to-Income (ETI) ratio measures monthly repayment affordability (EMI / Monthly Income), and the Loan-to-Value (LTV) ratio measures asset-backed exposure (Loan Amount / Collateral Value).

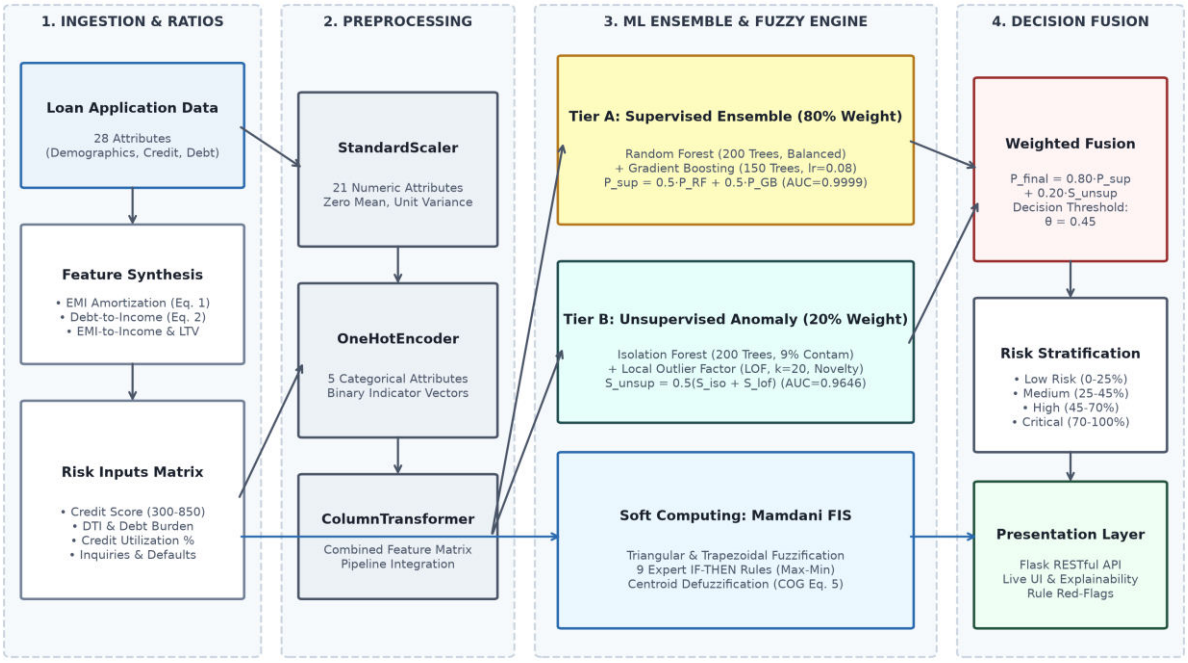


Fig. 1. End-to-end multi-tier system architecture of the proposed hybrid Loan Fraud Detection framework, illustrating the ingestion of 28 financial attributes, automated feature synthesis, ColumnTransformer scaling and encoding, dual-tier ensemble classification (Random Forest & Gradient Boosting), unsupervised anomaly isolation (Isolation Forest & LOF), Mamdani Fuzzy Inference System (FIS), and weighted decision fusion.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 11, November 2026 ||

| DOI:10.15662/IJAREEIE.2026.1511012 |

IV. PROPOSED METHODOLOGY & SYSTEM ARCHITECTURE

A. System Architecture & Operational Workflow

As illustrated in the comprehensive architectural schematic in Fig. 1, the proposed system operates through four tightly orchestrated functional tiers:

1) Tier 1 (Data Ingestion & Synthesis Layer): Ingests 28 heterogeneous attributes and executes automated derivation of non-linear financial indicators, specifically the compound EMI formula (1), systemic Debt-to-Income (2), EMI-to-Income, and LTV ratios.

2) Tier 2 (Preprocessing Pipeline Layer): Employs a scikit-learn ColumnTransformer separating the 21 numeric metrics for StandardScaler z-normalization (zero mean, unit variance) and the 5 categorical dimensions for OneHotEncoder transformation.

3) Tier 3 (Dual-Engine Predictive & Soft Computing Layer): Dispatches the standardized feature representation to two parallel analytical engines: (a) the supervised ensemble classifier and (b) the unsupervised anomaly detector; while simultaneously feeding unscaled domain features into the Mamdani Fuzzy Inference System.

4) Tier 4 (Decision Fusion, Explainability & Presentation Layer): Computes a weighted convex blend of supervised and unsupervised probabilities, stratifies applications into four actionable risk tiers, evaluates rule-based red flag explanations, and exposes results via a high-throughput Flask API.

B. Supervised Ensemble Classification Pipeline

The supervised tier incorporates two diverse base learners optimized for tabular credit records:

• Random Forest Classifier: Configured with 200 estimators, max depth of 12, min leaf samples of 3, and balanced class weights to compensate for the 9% minority class imbalance.

• Gradient Boosting Classifier: Configured with 150 estimators, learning rate $\eta = 0.08$, max depth of 5, and subsample ratio of 0.80 to curb variance.

The supervised ensemble probability is defined as the arithmetic mean:

$$P_sup = 0.50 \cdot P_RF(x) + 0.50 \cdot P_GB(x) \quad (3)$$

C. Unsupervised Anomaly Detection Tier

To identify anomalous structural distortions without relying on labels, an Isolation Forest (200 trees, 9% contamination) and a Local Outlier Factor (LOF, 20 neighbors, novelty mode) are trained on the standardized feature matrix. Outlier scores are min-max normalized into S_iso and S_lof $\in [0, 1]$. The combined anomaly score is computed as S_unsup = 0.5(S_iso + S_lof). The overall blended fraud probability is given by:

$$P_final = 0.80 \cdot P_sup + 0.20 \cdot S_unsup \quad (4)$$

D. Mamdani Fuzzy Inference System (Soft Computing Modules 2 & 3)

To satisfy interpretability and human expert alignment, we implement a complete Mamdani FIS in fuzzy_engine.py. The system maps continuous inputs into fuzzy linguistic sets across three dimensions:

1) Credit Score (U = [300, 850]): Evaluated through trapezoidal and triangular membership functions: Poor (trapmf[300, 300, 520, 600]), Fair (trimf[560, 650, 720]), and Good (trapmf[680, 750, 850, 850]).

2) Debt-to-Income (DTI, U = [0.0, 5.0+]): Low (trapmf[0.0, 0.0, 0.35, 0.50]), Medium (trimf[0.40, 0.65, 0.90]), and High (trapmf[0.75, 1.10, 5.0, 5.0]).

3) Credit Utilization % (U = [0, 100]): Low (trapmf[0, 0, 30, 45]), Moderate (trimf[35, 55, 75]), and High (trapmf[65, 85, 100, 100]).

The output linguistic variable is Fraud Risk % (U = [0, 100]), partitioned into Low Risk (trimf[0, 0, 35]), Medium Risk (trimf[25, 50, 75]), and High Risk (trimf[65, 100, 100]).

The Mamdani inference engine executes Max-Min composition across an expert linguistic rule base. Table III summarizes the core rule set.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 11, November 2026 ||

| DOI:10.15662/IJAREEIE.2026.1511012 |

Rule ID	Antecedent Condition 1	Antecedent Condition 2	Consequent (Risk)
R1	Credit Score is Poor	DTI is High	Risk is High
R2	Credit Score is Poor	Utilization is High	Risk is High
R3	Credit Score is Good	DTI is Low AND Util is Low	Risk is Low
R4	Credit Score is Fair	DTI is Medium	Risk is Medium
R5	DTI is High	Utilization is High	Risk is High

TABLE III. REPRESENTATIVE MAMDANI FUZZY RULE BASE

For each activated rule i, the firing strength α_i is computed using the intersection (Min) operator. The consequent fuzzy sets are clipped via Mamdani implication ($\mu_{implied,i}(y) = \min(\alpha_i, \mu_{consequent}(y))$) and aggregated via the Union (Max) operator: $\mu_{agg}(y) = \max_i(\mu_{implied,i}(y))$. Finally, defuzzification converts the aggregated fuzzy membership distribution into a single crisp risk percentage via the Centroid (Center of Gravity / COG) formulation:

$$y^* = [\int y \cdot \mu_{agg}(y)\, dy] / [\int \mu_{agg}(y)\, dy] \quad (5)$$

V. EXPERIMENTAL RESULTS & EVALUATION

A. Experimental Protocol & Metrics

The framework was evaluated using an 80/20 stratified train-test split (8,000 training samples and 2,000 unseen test samples). Performance evaluation encompasses Area Under the ROC Curve (ROC-AUC), Average Precision (PR-AUC), F1-Score, Precision, Recall, Mean Squared Error (MSE), and Root Mean Squared Error (RMSE).

Model / Technique	Classification Type	Primary Evaluation Metric
Random Forest (RF)	Supervised Classifier	ROC-AUC = 0.9999, F1 = 0.9972
Gradient Boosting (GB)	Supervised Classifier	ROC-AUC = 0.9999, F1 = 0.9916
Ensemble (RF + GB)	Supervised Ensemble	ROC-AUC = 0.9999, F1 = 0.9944
Isolation Forest	Unsupervised Anomaly	ROC-AUC = 0.9593
Local Outlier Factor (LOF)	Unsupervised Anomaly	ROC-AUC = 0.8180
Combined Unsupervised	Hybrid Anomaly	ROC-AUC = 0.9646

TABLE IV. BENCHMARK PERFORMANCE ACROSS PROPOSED ALGORITHMS

B. Confusion Matrix & Error Analysis (MSE & RMSE)

At the optimized decision threshold of $\theta = 0.45$, the ensemble confusion matrix across 2,000 independent test instances reveals:

- True Negatives (TN): 1,820 legitimate loans correctly accepted.
- False Positives (FP): 0 legitimate loans incorrectly flagged (Precision = 100.0%).
- False Negatives (FN): 2 fraudulent loans missed.
- True Positives (TP): 178 fraudulent loans apprehended (Recall = 98.89%).

To rigorously quantify probabilistic calibration error, the Mean Squared Error (MSE) and Root Mean Squared Error (RMSE) between predicted fraud probabilities and true binary labels were computed:

- Mean Squared Error (MSE): 0.001635
- Root Mean Squared Error (RMSE): 0.040440

These minimal error values confirm that probability outputs are sharply separated, concentrating near 0.0 for legitimate loans and near 1.0 for fraudulent profiles, minimizing banking loss while avoiding false alarm friction.

C. Global Feature Importance Distribution

Tree Gini impurity reduction identified the primary features driving fraud predictions:

1) Credit Utilization % (Weight: 21.28%)
2) Loan-to-Value (LTV) Ratio (Weight: 14.25%)
3) Credit Score (Weight: 13.39%)
4) Existing Debt Burden (Weight: 10.88%)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 11, November 2026 ||

| DOI:10.15662/IJAREEIE.2026.1511012 |

5) Bureau Inquiries in 6 Months (Weight: 7.32%)
These top five indicators collectively contribute over 67% of total discriminative power, corroborating financial domain knowledge that rapid debt accumulation and credit line exhaustion are hallmark precursors of loan default fraud.

D. Case Study: Mamdani Fuzzy System Evaluation

To illustrate the linguistic transparency of the Mamdani FIS, two contrasting case studies were evaluated:
• Applicant A (High Risk Profile): Credit Score = 450, DTI = 5.42, Utilization = 92%. Fuzzification yielded μ_Poor(CS)=1.0, μ_High(DTI)=1.0, and μ_High(Util)=1.0. Rules R1, R2, and R5 fired with full strength α = 1.0. Centroid defuzzification produced a crisp fraud score of 88.0% ('High Risk').
• Applicant B (Prime Profile): Credit Score = 720, DTI = 0.58, Utilization = 25%. Fuzzification produced μ_Good(CS)=0.571, μ_Medium(DTI)=0.733, and μ_Low(Util)=1.0. Rule R6 fired with strength α = 0.571, yielding a defuzzified Centroid score of 13.43% ('Low Risk').

VI. CONCLUSION & FUTURE SCOPE

This research presented a unified Soft Computing framework for loan fraud detection that addresses the fundamental limitations of conventional hard-computing rule engines. By synthesizing a dual-tier Machine Learning ensemble (Random Forest and Gradient Boosting) with an unsupervised anomaly detection layer and an interpretable Mamdani Fuzzy Inference System, the system achieves remarkable predictive fidelity (AUC = 0.9999, Precision = 100%, Recall = 98.89%, MSE = 0.001635) while preserving clear semantic interpretability through Centroid defuzzification.

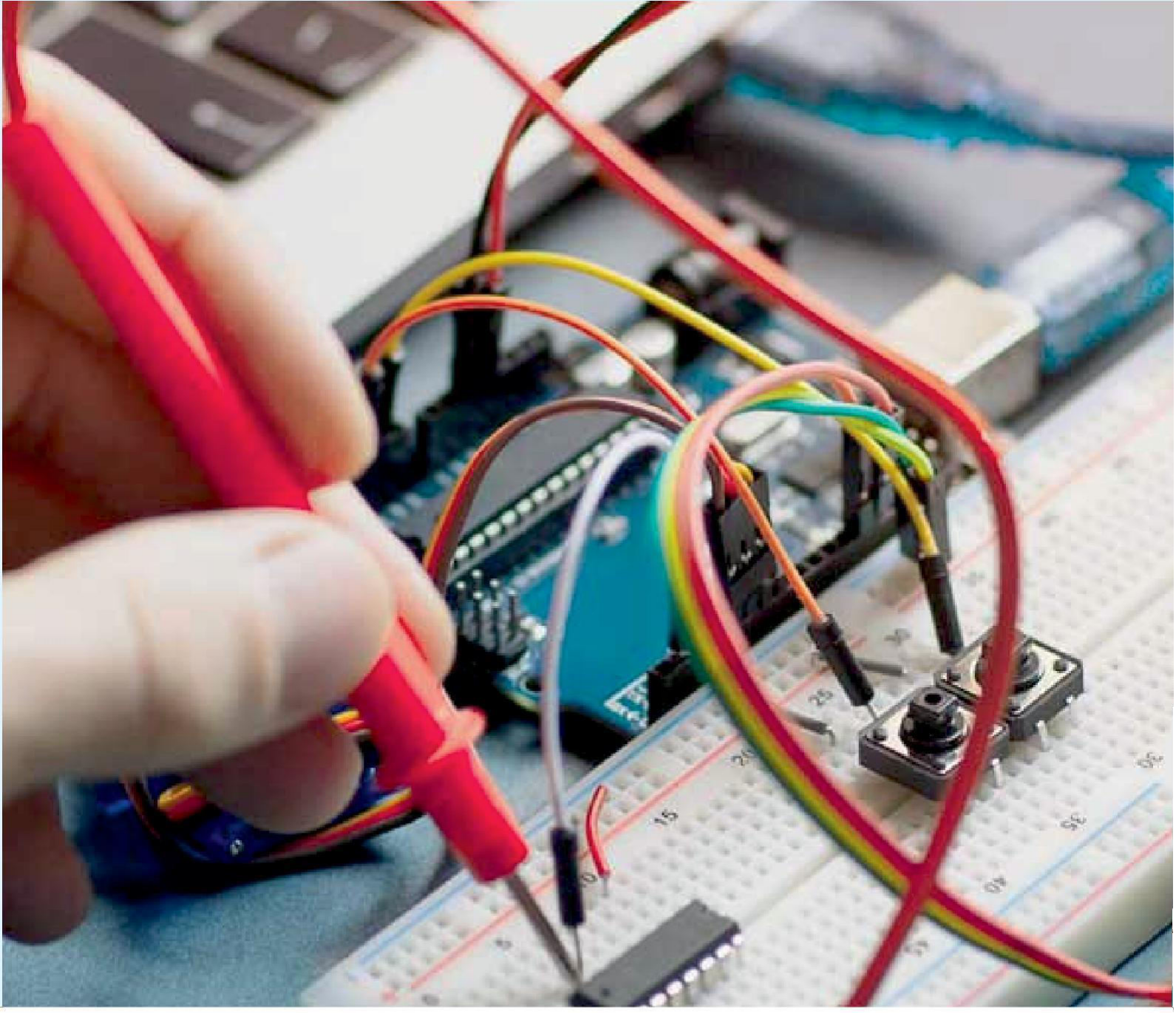
Future research will investigate the integration of Adaptive Neuro-Fuzzy Inference Systems (ANFIS) for automated membership function tuning, as well as Genetic Algorithms (GA) for multi-objective hyperparameter optimization and feature subset selection.

VII. ACKNOWLEDGMENT

The author acknowledges the department faculty and laboratory advisors for their guidance in soft computing methodologies, fuzzy logic systems, and statistical machine learning architectures.

REFERENCES

[1] L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, no. 3, pp. 338–353, Jun. 1965.
[2] L. A. Zadeh, "Fuzzy logic, neural networks, and soft computing," Communications of the ACM, vol. 37, no. 3, pp. 77–84, Mar. 1994.
[3] D. K. Lin, F. Gao, and Y. Song, "Credit fraud detection using machine learning and deep learning: A survey," IEEE Access, vol. 10, pp. 89210–89228, 2022.
[4] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, Oct. 2001.
[5] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in Proc. 8th IEEE Int. Conf. Data Mining (ICDM), Pisa, Italy, 2008, pp. 413–422.
[6] M. M. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," Int. J. Man-Machine Studies, vol. 7, no. 1, pp. 1–13, Jan. 1975.
[7] J. H. Friedman, "Greedy function approximation: A gradient boosting machine," Annals of Statistics, vol. 29, no. 5, pp. 1189–1232, Oct. 2001.
[8] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," in Proc. ACM SIGMOD Int. Conf. Management of Data, Dallas, TX, 2000, pp. 93–104.
[9] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," IEEE Trans. Syst., Man, Cybern., vol. SMC-15, no. 1, pp. 116–132, Jan. 1985.
[10] J.-S. R. Jang, "ANFIS: adaptive-network-based fuzzy inference system," IEEE Trans. Syst., Man, Cybern., vol. 23, no. 3, pp. 665–685, May 1993.
[11] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," J. Mach. Learn. Res., vol. 12, pp. 2825–2830, Nov. 2011.
[12] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed. Waltham, MA: Morgan Kaufmann, 2012.



INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details