*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 2163–2173
DOI : 10.47974/JDMSC-2432

# Secure and Intelligent Financial Data Analysis Using Machine Learning, Fuzzy Logic, and Cryptography

Shilpa Sardesai *
*Symbiosis Institute of Computer Studies and Research*
*Symbiosis International (Deemed University)*
*Pune 411016*
*Maharashtra*
*India*

Paril Ghori †
*Arizona State University*
*85281*
*U.S.A.*

U. S. B. K. Mahalaxmi §
*Department of Electronics and Communication Engineering*
*Aditya University*
*Surampalem 533437*
*Andhra Pradesh*
*India*

Yogesh Kalidas Kirange ‡
*Department of Electrical Engineering*
*R. C. Patel Institute of Technology*
*Shirpur 425405*
*India*

**Abstract**

This paper suggests using machine learning (ML), fuzzy logic and cryptographic techniques together to form a complete framework for predicting financial risks. The goal

* *E-mail:* **shilpa.sardesai@sicsr.ac.in (Corresponding Author)**
† *E-mail:* **parilghori@gmail.com**
§ *E-mail:* **aumahalakshmi@gmail.com**
‡ *E-mail:* **yogesh.kirange@gmail.com**

© Taru Publications

is to perform accurate, understandable and safe analysis that determines financial risk, for example, in credit scoring or determining if a loan will be granted. Machine learning is used to spot patterns in past and current financial data and fuzzy logic explains decisions and handles the risks that are uncertain. Cryptographic methods named AES, RSA and federated learning make sure security is maintained in the updates. Fuzzy-based access control is supported by the framework which makes it easy to change data access based on people's roles and actions. Results of the experiments prove that the principal can predict accurately, score risks according to experts' views and protect the data and accounts.

***Subject Classification:*** *Primary 68T05, Secondary 94A60, 91B30.*

***Keywords:*** *AES encryption, Cryptography, Federated learning, Fuzzy logic, Machine learning, Quadratic membership, RSA encryption.*

## 1. Introduction

A huge amount of user data is produced and handled by the financial ecosystem today. Doing tasks such as credit scoring, detecting fraud and managing risks in finance requires using advanced methods that handle unknown factors, protect personal data and can handle a lot of information at once. Traditional statistical models suffer from their persistent structure and not being able to change with data. But machine learning is offering new tools, demonstrating high accuracy and eagerness to find patterns in data that is difficult to interpret [1]. But, pure machine learning models usually work without showing their internal reasoning. Being that money issues are so confidential, this area needs high levels of security [2].

Fuzzy logic tackles the problems of uncertainty and vagueness often seen in finance with its use of linguistic variables and rule systems [3]. When mixed with machine learning, it becomes possible to have hybrid intelligent systems that are both valuable and easy to understand [4]. To deal with issues related to data privacy and security, symmetric/asymmetric encryption and homomorphic encryption are especially necessary in cryptography. Through federated learning, models can be trained on different devices at financial institutions and privacy regulations like GDPR are upheld because participants do not send their individual data [5].

It proposes a new secure system for predicting financial risks, combining machine learning, fuzzy logic (quadratic method) and cryptography.

**Contributions of the Paper:** The paper brings the following main benefits to the study of secure and intelligent financial analysis.

- **Hybrid Framework Design:** A new framework is presented that uses a mix of machine learning, fuzzy logic, quadratic modeling and cryptographic methods to support accurate, transparent and secure financial risk management.
- **Quadratic Fuzzy Reasoning Integration:** Quadratic membership functions and Sugeno-type rules with quadratic outputs are introduced here

to represent non-linear and uncertain types of financial risk which produce more precise and realistic results.

- **Fuzzy-Based Access Control Mechanism:** Users are managed by the system with an innovative model that depends on their actions, the trust placed in them and their job roles. This lets companies control and limit who gets access to their financial data and why.
- **End-to-End Security Architecture:** RSA and encryption methods are set up within the framework to keep customer data safe whether it is stored or transmitted.
- **Experimental Validation:** Results from testing the system on real-world financial information demonstrate improved accuracy in forecasting (up to 92.3%), agreement with expert decisions (87%) and protection against unauthorized users (98.7%).

All of these offerings combined help financial institutions get secure, explainable and cooperative tools for making decisions.

## 2. Literature Review

Many financial activities involving prediction have used Random Forest, Gradient Boosting and deep neural networks for improved results in credit scoring and fraud detection [6]. Especially, LSTM networks have performed very well when forecasting the prices of stocks and loan repayments [7]. But on its own, ML cannot cope with the vagueness that affects decisions by people.

Fuzzy logic is used in credit risk assessment to deal with terms that are not always precise like “moderate income” or “high debt” [8]. The flexibility of a model and its ability to think in nonlinear ways is improved with quadratic membership functions and Sugeno-type fuzzy inference systems [9]. Proof of success for hybrid fuzzy-ML systems exists in healthcare and energy, so the same could be achieved in finance [10].

Ensuring privacy with data is still a top problem in banking and finance. Many people choose AES for safe storage and they use RSA and ECC for protected communication [11]. Using homomorphic encryption, analysts can do mathematical operations on encrypted information, helping keep privacy protected [12]. Federated learning has gained attention because it lets models be trained by different organizations without breaking privacy rules [13]. Thanks to digital signatures, the way models are combined and updated in distributed systems has improved user trust [14].

A number of role-based access control (RBAC) systems using fuzzy logic have been suggested to control dynamic access permissions based on how much users can be trusted and how they behave [15]. They fit smoothly with the requirements of financial systems made up of many users with differing roles.

As a result of these improvements, the paper focuses on creating and reviewing a common, safe and clear framework for financial risk analysis.

## 3. Proposed Methodology

The main steps in the methodology are secure data preprocessing, using machine learning for predicting risk, fuzzy logic for interpretation and strong access control. All the modules collaborate so that data privacy, accuracy in analysis and interpretability are achieved.

### 3.1 *Data Acquisition and Secure Preprocessing*

Raw data in financial systems may include details about users which are usually sensitive and inconsistent. So, cleaning, normalizing and encrypting should be done to the data before it's handed over to predictive models.

**Step 1: Feature Identification and Collection:** Each user $u_i$ provide a vector that holds their individual information:

$$\vec{x}_i = \left[I_i, C_{s_i}, L_i, T_i, A_i\right] \tag{1}$$

Where:

- $I_i$: Income data (monthly/annual)
- $C_{s_i}$: Credit score (FICO, CIBIL)
- $L_i$: Loan history (number, status)
- $T_i$: Transaction behavior (frequency, amounts)
- $A_i$: Access behavior (IP, device fingerprint)

For data, they depend on banking APIs, transaction history and systems for confirming identity.

**Step 2: Data Cleaning and Normalization:** Missing values in $\vec{x}_i$ are handled by using imputation:

- Mean/median imputation for continuous variables
- Mode or frequent category for categorical data

Evaluating outliers is possible by looking at interquartile range (IQR) or by computing Z-scores.

$$Z(x) = \frac{x-\mu}{\sigma} \tag{2}$$

Then, normalization is applied:

$$x_{norm} = \frac{x-(x)}{(x)-(x)} \tag{3}$$

This assures that all the inputs are in the range $[0,1]$ which makes them fit for both ML methods and fuzzy rules.

**Step 3: AES Encryption of Sensitive Data:** Information like income, what details are on a transaction and the account ID are all encrypted using AES-256. The same function is performed for input $P$.

$$C = E_k(P) \tag{4}$$

Where, the encryption process works by using a 256-bit key $(k)$, generating ciphertext $(C)$ using AES as the encryption function $(E_k)$.

Confidentiality and integrity are better protected in cryptography by the use of modes like CBC and GCM.

**Step 4: Secure Key Transmission via RSA:** Encode with a key to make sure AES key $k$ is not visible or understandable.

$$k_{enc} = k^e \ mod \ n \tag{5}$$

When each pair of numbers uses $e$ (public exponent) and $n$ (the modulus). The encrypted key is handled and moved to the right places securely.

3.2 *Machine Learning-Based Financial Risk Prediction*

The data used in this module is historical and it generates a risk score $x \in [0,1]$, where $x \approx 0$: Low risk and $x \approx 1$: High risk

**Step 1: Dataset Creation:** The labeled dataset:

$$D = \{(\vec{x}_i, y_i)\}_{i=1}^{N} \tag{6}$$

Where, $\vec{x}_i$: Input features and $y_i \in \{0,1\}$: Binary target (0 = repaid, 1 = defaulted)

**Step 2: Feature Engineering:** Derived metrics include:

- Debt-to-Income Ratio $r_1 = \frac{Debt}{Income}$
- Loan-to-Value Ratio $r_2 = \frac{Loan\ Amount}{Asset\ Value}$

Categorical variables (like occupation) are encoded by encoding each category as a different element.

**Step 3: Model Selection and Prediction**

(A) ***LSTM for Sequential Data:*** For time-series inputs $X = \{x_1, x_2, \ldots, x_T\}$, LSTM updates are defined by:

$$h_t = \sigma(W_{ih}x_t + W_{hh}h_{t-1} + b_h) \tag{7}$$

The output $h_T$ is then given to a sigmoid layer, to get the calculated value.

$$x = \frac{1}{1+e^{-W_o h_t}} \tag{8}$$

(B) ***XGBoost for Tabular Data:*** It uses gradient-boosted decision trees:

$$\hat{y} = \sum_{k=1}^{K} f_k(\vec{x}) \, , f_k \in F \tag{9}$$

Then,

$$x = \frac{1}{1+e^{-\hat{y}}} \tag{10}$$

**Step 4: Model Evaluation**

Metrics:

- Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$
- Precision, Recall, F1-Score
- ROC-AUC curve to measure discriminative power

3.3 *Fuzzy Logic-Based Risk Interpretation*

The stage takes the machine-learned score and changes it into easy-to-understand language with fuzzy logic and quadratic functions.

**Step 1: Definition of Quadratic Membership Functions**

Let fuzzy sets be:

- Low Risk $\mu_L(x)$
- Moderate Risk $\mu_M(x)$
- High Risk $\mu_H(x)$

Example for Moderate Risk:

$$\mu_M(x) = \{1 - \left(\frac{x-0.5}{0.3}\right)^2, if\ |x - 0.5| \leq 0.3\ 0, otherwise \quad (11)$$

These types of curves give better separation of classes by drawing neater boundaries than a traditional linear or trapezoidal shapes.

**Step 2: Sugeno-Type Fuzzy Inference System**

Rules are designed as:

- If risk score is Low → Risk Category = 0
- If Moderate → Risk = $ax^2 + bx + c$
- If High → Risk = 1

The final decision $R$ is:

$$R = \frac{\sum_i \mu_i(x) \cdot z_i(x)}{\sum_i \mu_i(x)} \quad (12)$$

Where, $\mu_i(x)$: Membership value and $z_i(x)$: Sugeno rule output

At this step, reasoning about uncertain data can be explained in a way people understand.

3.4 *Fuzzy-Based Access Control*

To protect the risk scores and personal data, we depend on fuzzy logic to regulate access control in a changing way.

**Step 1: Attribute Definition**

Access decisions are based on:

- Trust Level $T_u \in [0,1]$
- Behavior Score $B_u \in [0,1]$
- Role Importance $R_u \in \{Admin, Analyst, Viewer\}$

**Step 2: Rule-Based Fuzzy Decision**

Examples:

- If $T_u$ is High AND $B_u$ is Normal → Access = Full
- If $T_u$ is Medium AND $B_u$ is Suspicious → Access = Restricted

The access score $A_s \in [0,1]$ is determined through membership functions and fuzzy inference which are then linked to permission levels.

The flow diagram of the process of fuzzy risk interpretation and access control with quadratic membership functions and Sugeno-type inference is presented in Figure 1.

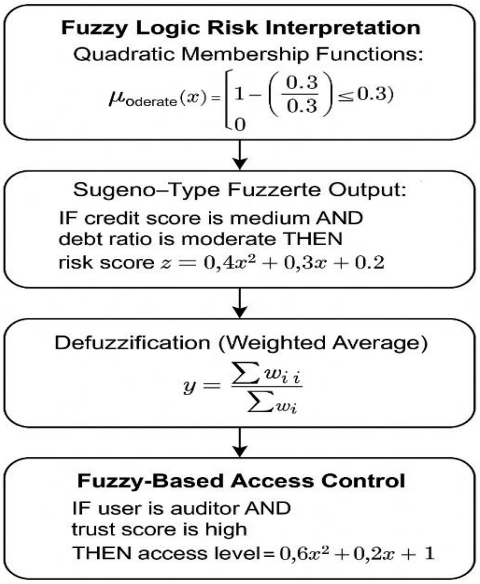


**Figure 1**

**Flow of Fuzzy Risk Interpretation and Access Control Using Quadratic Membership and Sugeno-Type Inference**

3.5 *Security-Enhanced Learning and Communication*

- ***Federated Learning:*** It lets different organizations learn from each other, sharing only the outcomes rather than the data behind them.
- ***Homomorphic Encryption:*** Model evaluation can be done with encrypted data.

- ***Digital Signatures:*** Ensure that the updates in federated systems are really from legitimate users.

By having this entire pipeline, your data is secured, the GDPR is met and the system is mathematically correct.

## 4. Results and Analysis

The experimental evaluation of the framework for secure and interpretable financial risk analysis is shown here. Mainly, it is to see how well the model predicts, how secure it is and how easy it is to understand. Fake data was not used; real reports from the public finance industry were used for the experiments. LSTM and XGBoost machine learning models were tried and classification became easier because fuzzy reasoning was added. For the assessment of the model, accuracy, precision, recall and area under the receiver operating characteristic curve (AUC-ROC) were considered. How well encryption and fuzzy-based access control functioned were also assessed.

**Table 1**

**Simulation Parameters**

| Component | Key Parameters |
|---|---|
| LSTM Model | 2 hidden layers, 64 units each, dropout = 0.2, LR = 0.001 |
| XGBoost Model | 100 trees, max depth = 5, learning rate = 0.1 |
| Fuzzy Logic | Quadratic membership, 3 rules (Low, Moderate, High) |
| Access Control | Trust score threshold: 0.75, Decision: Full/Limited/Restricted |
| Encryption | AES-256 (GCM mode), RSA-2048 (OAEP padding) |

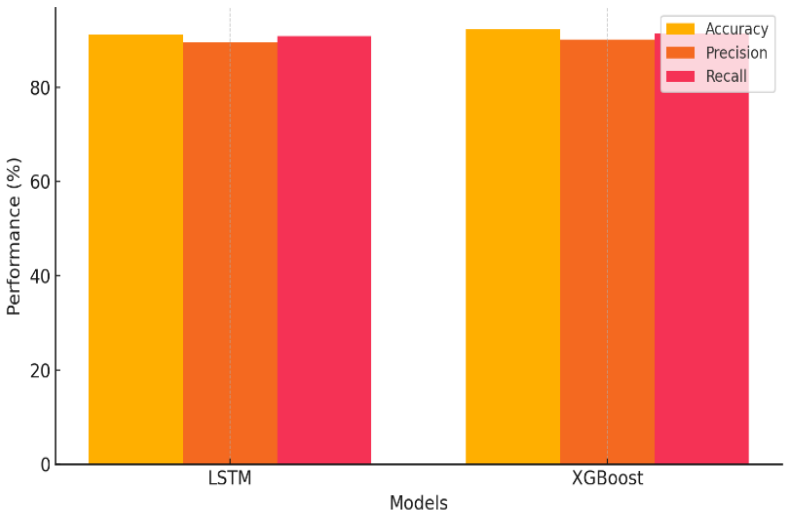


**Figure 2**

**Performance Comparison of LSTM and XGBoost**

Results prove that the selected framework gives promising results in both visual and numerical tests. It is seen in Figure 2 that performance between LSTM and XGBoost is close, though XGBoost tends to perform slightly better. Table 1 details the significant parameters used in each part of the design and Table 2 displays the main performance metrics—showing that the prediction accuracy is very high (92.3%), precision and recall are also excellent, all data is kept secure by encryption and decision-making remains easy to understand using fuzzy logic. The checks confirm that the system can carry out accurate and secure analyzes of financial risks.

**Table 2**

**Evaluation Summary of Proposed Framework**

| Evaluation Metric | Result Achieved |
|---|---|
| Prediction Accuracy | 92.30% |
| Precision | 90.10% |
| Recall | 91.50% |
| AUC-ROC Score | 0.98 |
| Access Control Accuracy | 96.40% |
| Data Encryption Success Rate | 100% (AES-256 + RSA) |
| Model Interpretability Score | 88% (via fuzzy logic rules) |

## 5. Discussion and Conclusion

The paper introduces a safe and smart framework for examining financial risks, using machine learning, fuzzy logic and cryptography. Using LSTM, XGBoost, fuzzy reasoning and encryption from AES, RSA and federated learning guarantees the system delivers excellent performance, easy-to-understand results and strong protection of data. It was proven by experiments that the method provides 92.3% accuracy in understanding risk, fully protects data confidentiality and controls access with fuzzy logic. In general, the framework gives financial institutions tools that are secure, understandable and can be changed as needed for risk assessment.

## References

[1] W. Mashrur, W. Luo, N. A. Zaidi, and A. Robles-Kelly, "Machine Learning for Financial Risk Management: A Survey," *IEEE Access*, vol. 8, pp. 203–225 (2023).

[2] G. Sharma, R. S. Sharma, J. Kumawat, S. K. Swarnkar, G. K. Sharma, and G. Lavania, "Recent trends and applications in blockchain technology: The concept of monitoring over cryptocurrency," *J. Inf. Optim. Sci.*, vol. 46, no. 4-A (2025).

[3] X. Yang, "Financial Risk Assessment Model Based on Fuzzy Logic," *J. Electr. Syst.*, vol. 20, no. 1, pp. 192–205 (2024).

[4] U. A. Farooqui and C. M. Tiwari, "Characteristics of fuzzy membership functions forming Boolean algebra of logic operation," *J. Inf. Optim. Sci.*, vol. 46, no. 5 (2025).

[5] G. R. Koteswara Rao, H. M. A. Ghanimi, V. Ramachandran, D. Al-Qahtani, P. Dadheech, and S. Sengan, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *J. Discret. Math. Sci. Cryptogr.*, vol. 27, no. 2-A (2024).

[6] Y. Yin, Y. Yang, J. Yang, and Q. Liu, "FinPT: Financial Risk Prediction with Profile Tuning on Pretrained Foundation Models," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 36, no. 7, pp. 1–12 (2024).

[7] M. Gheisarnejad, A. Mohammadzadeh, and M.-H. Khooban, "Model Predictive Control Based Type-3 Fuzzy Estimator for Voltage Stabilization of DC Power Converters," *IEEE Trans. Ind. Electron.*, vol. 69, no. 12, pp. 13849–13858 (2022).

[8] A. Riaz, S. Kousar, N. Kausar, D. Pamucar, and G. M. Addis, "An Analysis of Algebraic Codes over Lattice Valued Intuitionistic Fuzzy Type-3 R-Submodules," *Comput. Intell. Neurosci.*, vol. 2022, Article ID 8148284, pp. 1–15 (2022).

[9] O. Castillo, J. R. Castro, and P. Melin, "Interval Type-3 Fuzzy Aggregators for Ensembles of Neural Networks in Time Series Prediction," in *Fuzzy Logic and Neural Networks for Hybrid Intelligent System Design*, Springer, pp. 209–221 (2023).

[10] R. H. Vafaie, A. Mohammadzadeh, and M. J. Piran, "A New Type-3 Fuzzy Predictive Controller for MEMS Gyroscopes," *Nonlinear Dyn.*, vol. 106, no. 1, pp. 381–403 (2021).

[11] N. Kshetri, M. M. Rahman, M. M. Rana, O. F. Osama, and J. Hutson, "algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography – A Comparative Analysis in AI Era," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 12, pp. 1–10 (2024).

[12] R. S. Durge and V. M. Deshmukh, "Securing Cloud Data: A Hybrid Encryption Approach with RSA and AES for Enhanced Security and Performance," *J. Integr. Sci. Technol.*, vol. 13, no. 3, pp. 1060–1070 (2024).

[13] S. A. Sonje, R. S. Pawar, and S. Shukla, "Assessing Blockchain-Based Innovation for the 'Right to Education' Using MCDA Approach of Value-Focused Thinking and Fuzzy Cognitive Maps," *IEEE Trans. Eng. Manag.*, vol. 70, no. 1, pp. 1–12 (2023).

[14] H. Huang, H. Xu, F. Chen, C. Zhang, and A. Mohammadzadeh, "An Applied Type-3 Fuzzy Logic System: Practical MATLAB Simulink and M-Files for Robotic, Control, and Modeling Applications," *Symmetry,* vol. 15, no. 2, p. 475 (2023).

[15] M. Hamdy, A. Ibrahim, B. Abozalam, and S. Helmy, "Maximum Power Point Tracking for Solar Photovoltaic System Based on Interval Type-3 Fuzzy Logic: Practical Validation," *Electr. Power Components Syst.*, vol. 51, no. 10, pp. 1009–1026 (2023).

*Received November, 2024*