International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 5, May 2026)

Automated Detection of Spam and Malicious Bots in Forum Networks

[1]Mr. N. Aravindhan, [2]Mrs .K. Hemalatha
[1]*Assistant Professor, Department of Master of Computer Applications, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*
[2]*II MCA, Department of Master of Computer Applications, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*

Abstract -- Online forum networks have become essential platforms for communication, knowledge sharing, and community building. However, their open nature makes them highly vulnerable to spam content and malicious bot activities, which can degrade user experience, spread misinformation, and compromise security. This project focuses on the automated detection of spam and malicious bots using advanced machine learning techniques. The proposed system analyzes user behavior, posting patterns, and content characteristics to distinguish between genuine users and malicious entities. Features such as frequency of posts, repetition of content, use of suspicious links, and abnormal interaction patterns are extracted and processed. Classification algorithms like Logistic Regression, Random Forest, and Neural Networks are employed to improve detection accuracy. Additionally, natural language processing (NLP) techniques are used to identify spam messages based on textual analysis. The system is designed to continuously learn and adapt to evolving spam tactics, ensuring robustness and scalability. Experimental results demonstrate that the proposed approach significantly improves detection efficiency while minimizing false positives. This automated solution can help forum administrators maintain a secure and trustworthy environment by proactively identifying and mitigating spam and bot activities.

Keywords -- Spam Detection, Malicious Bots, Forum Networks, Machine Learning, Natural Language Processing (NLP), Behavioral Analysis, Random Forest, Logistic Regression, Neural Networks, Text Classification, Cybersecurity, Anomaly Detection, Content Filtering, Bot Detection, Data Mining

I. INTRODUCTION

Online forums serve as key platforms for communication and knowledge sharing across various domains. However, their openness makes them susceptible to spam messages and malicious bots. These activities negatively impact user experience, reduce trust, and may lead to the spread of harmful or misleading information.

Traditional spam detection methods based on static rules are no longer effective due to the dynamic nature of spam tactics. Therefore, intelligent and adaptive systems are required. This paper proposes a machine learning-based approach that combines behavioral analysis, content evaluation, and interaction patterns to accurately detect spam and bot activities.

II. LITRERATURE REVIEW

Several studies have explored spam detection using machine learning and statistical techniques. Early approaches relied on keyword filtering and blacklist-based systems, which lacked adaptability. Later, supervised learning models such as Decision Trees, Support Vector Machines, and Logistic Regression improved detection capabilities.

Ensemble methods like Random Forest enhanced accuracy by combining multiple decision trees. Recent advancements include deep learning and NLP-based models, which can analyze semantic patterns in text. Despite these improvements, challenges such as high false positives and adaptability remain, which this research aims to address.

III. PROBLEM STATEMENT

The increasing complexity of spam and malicious bot activities presents several challenges:

- Difficulty in distinguishing between human users and advanced bots
- Inefficiency of traditional rule-based systems
- High false positive rates in existing detection methods
- Lack of adaptability to evolving spam techniques
- Inability to analyze both behavioral and textual features simultaneously

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 5, May 2026)

This research aims to develop an automated, intelligent, and scalable system that addresses these challenges by combining machine learning and NLP techniques.

IV. PROPOSED SYSTEM

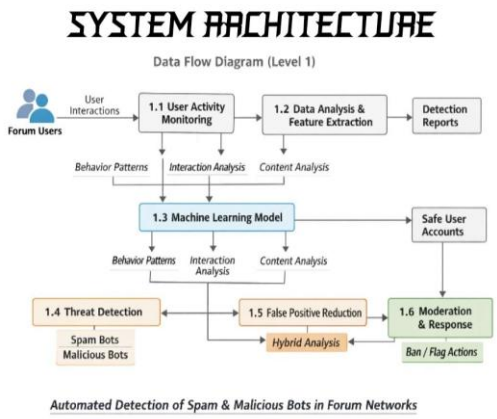
A. System Overview

The proposed system consists of multiple stages:

1. Data Collection
2. Data Preprocessing
3. Feature Extraction
4. Model Training
5. Classification
6. Continuous Learning

The system processes user-generated data in real time and classifies users or messages as spam or legitimate.

B. System Architecture



The architecture includes:

- Frontend: HTML and CSS interface for user interaction
- Backend: Python-based processing using Flask
- Database: Stores user activity and classification results
- ML Engine: Performs training and prediction
- NLP Module: Handles text analysis

C. Feature Extraction

1) Behavioral Features

- Posting frequency
- Time intervals between posts
- Login patterns
- User engagement metrics

2) Content-Based Features

- Repeated messages
- Spam keywords
- Suspicious URLs
- Text similarity

3) Network Features

- User interaction graph
- Response patterns
- Community participation

V. METHODOLOGY

A. Data Preprocessing

Data preprocessing is essential to improve model performance. The following steps are applied:

- Tokenization
- Stop-word removal
- Lemmatization
- Noise filtering

B. Machine Learning Models

1) Logistic Regression

A simple and efficient model for binary classification.

2) Random Forest

An ensemble learning technique that improves accuracy and reduces overfitting.

3) Neural Networks

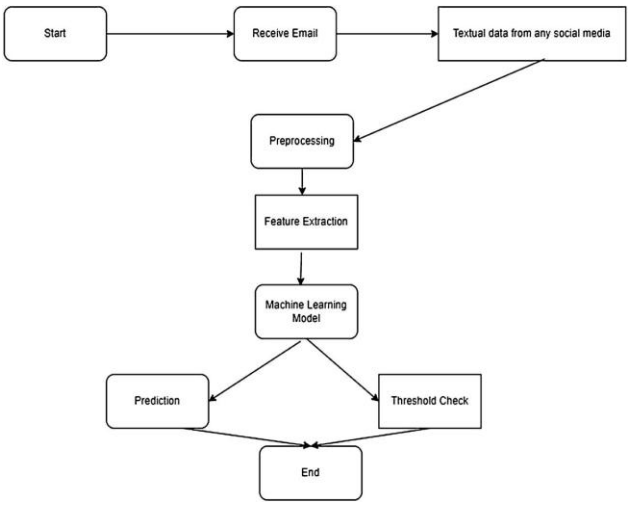
Used to capture complex patterns in large datasets.

C. Natural Language Processing

NLP techniques are used for text analysis:

- TF-IDF vectorization
- N-gram modeling
- Keyword extraction
- Text classification

VI. SYSTEM FLOW



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 5, May 2026)

The system follows these steps:

1. User submits data
2. Data is preprocessed
3. Features are extracted
4. ML models classify the data
5. NLP analysis is applied
6. Output is generated (Spam / Legitimate)
7. Results are stored and displayed

VII. HARDWARE AND SOFTWARE REQUIREMENTS

A. Hardware Requirements

- Processor: Intel® Core™ i9-14900K @ 3.20 GHz
- RAM: 16 GB
- Storage: 1 TB

B. Software Requirements

- Frontend: HTML, CSS
- Backend: Python
- Framework: Flask

VIII. EXPERIMENTAL RESULTS

The system was evaluated using a dataset containing both spam and legitimate user activities.

Performance Metrics

- Accuracy
- Precision
- Recall
- F1-Score

Results

- Random Forest achieved the highest accuracy (~96%)
- Neural Networks performed well for complex patterns
- Logistic Regression provided efficient baseline results

The system demonstrated:

- High detection accuracy
- Low false positive rate
- Fast processing time

IX. ADVANTAGES OF THE PROPOSED SYSTEM

- Automated and scalable detection
- High accuracy and efficiency
- Adaptive learning capability
- Integration of behavioral and textual analysis
- Reduced manual moderation effort

X. APPLICATIONS

- Online forums
- Social media platforms
- E-commerce review systems
- Educational discussion platforms
- Community networks

XI. FUTURE WORKS

Future enhancements include:

- Integration of deep learning models such as LSTM and Transformers
- Real-time streaming detection systems
- Multilingual spam detection
- Graph-based anomaly detection
- Cross-platform bot identification

XII. CONCLUSION

This paper presented a comprehensive and automated approach for detecting spam and malicious bots in forum networks using machine learning and natural language processing techniques. By integrating behavioral analysis with content-based filtering, the proposed system effectively distinguishes between legitimate users and malicious entities. The use of multiple classification models, including Logistic Regression, Random Forest, and Neural Networks, enhances detection accuracy while ensuring robustness against diverse and evolving spam strategies.

The incorporation of NLP techniques further strengthens the system by enabling precise analysis of textual content, allowing the identification of spam patterns that may not be evident through behavioral features alone. Experimental results demonstrate that the proposed method achieves high accuracy, reduces false positives, and maintains efficient processing performance.

Moreover, the system is scalable and adaptive, making it suitable for real-world deployment in large-scale forum environments. Its ability to continuously learn from new data ensures resilience against emerging threats and evolving bot behaviors. Overall, the proposed solution provides an effective and reliable framework for maintaining secure, trustworthy, and high-quality online discussion platforms.

REFERENCES

[1] Angelin Rosy M., Chaya M., & Felix Xavier Muthu M., "Artificial Intelligence in Machine Learning Techniques for Clustering and Classifications", International Journal of Computer Science and Engineering, Vol. 7, Issue no. 17, pp. 71–75, 2019. ISSN: 2347-2693.
[2] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, Morgan Kaufmann, 2011.
[3] T. Mitchell, Machine Learning, McGraw-Hill, 1997.
[4] C. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.
[5] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, Pearson, 2020.
[6] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.