River Publishers

Next Generation Email Security: AI Based Spam Detection

Editors:

Ramjee Prasad, Founder President, CTIF Global Capsule (CGC), Denmark

Vikas S Kadam, Marathwada Mitra Mandal's College of Engineering Karvenagar, Pune Maharashtra, India

Vandana Rohokale, Sinhgad Institute of Technology and Science Narhe, Pune, India

This book presents AI-driven approaches for combating spam, phishing, and malware in email systems. It reviews classical techniques, identifies their limitations, and introduces two novel frameworks?FLIDA and G-SFO with adaptive capsule networks. It also highlights the role of quantum machine learning in enabling scalable and resilient email security.

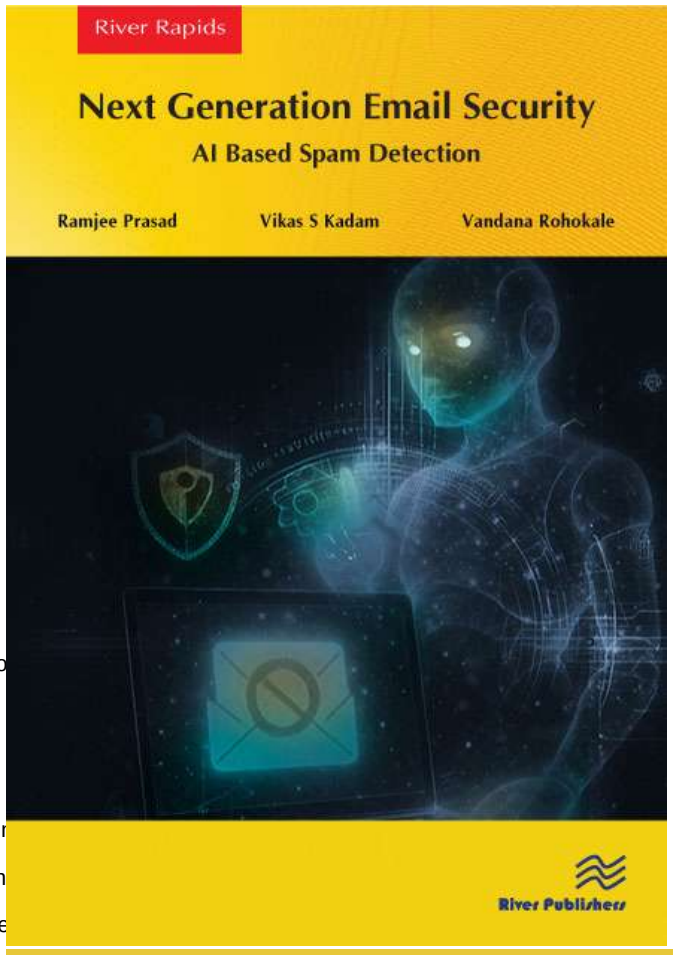
Key Features

- Concise review of classical and AI-based spam detection.
- Innovative frameworks: FLIDA and G-SFO-ACapsNet.
- Insights into quantum paradigms for cybersecurity.
- Empirical evaluations and comparative performance analyses.
- Open research issues and future perspectives.

This is a valuable resource for researchers, postgraduate students, and professionals in cybersecurity, AI, and data science, as well as industry practitioners and policymakers working on secure communication technologies.

TABLE OF CONTENTS

1. 1. Introduction
    1. 1.1 Emergence of Online Social Networks
    2. 1.2 Challenges of Social Network Security
    3. 1.3 Email Spam An Issue in Cyber Security
    4. 1.4 Origins of Email Spam
    5. 1.5 Types of Spam
    6. 1.6 Spam Avoiding Techniques
        1. 1.6.1 Technical Techniques
        2. 1.6.2 Non-Technical Techniques
    7. 1.7 Filtering Techniques for Email Spam Detection
    8. 1.8 Existing Email Spam Detection Models
    9. 1.9 Summary
2. 2. Email Spam Detection Models Overview
    1. 2.1 Supervised Deep Learning Based Models
    2. 2.2 Supervised Machine Learning Based Models
    3. 2.3 Enhanced Heuristic-Based Models
    4. 2.4 Unsupervised Clustering-Based Models
    5. 2.5 Hybrid Spam Detection Models
    6. 2.6 Unaddressed Challenges
3. 3. Email Spam Detection Approach I (FLIDA)
    1. 3.1 Introduction
    2. 3.2 Architecture of FLIDA Email Spam Detection Technique
    3. 3.3 Datasets Description
    4. 3.4 Extraction of Text Features using TFIDF
    5. 3.5 Extraction of Visual Features using GLCM and Color Correlogram
    6. 3.6 Selection of Optimal Features
    7. 3.7 Optimal Feature Selection and Classification Using Levy Impro Dragonfly Algorithm
    8. 3.8 Conventional Dragonfly Algorithm
    9. 3.9 Implementation of FLI-DA
    10. 3.10 Classification of Image and Text Features using Hybrid Model
4. 4. Performance Analysis of FLIDA
    1. 4.1 Experimental Setup and Parameter Setting
    2. 4.2 Performance Analysis of FLIDA in Terms of Accuracy with Differer Algorithms
    3. 4.3 Performance Analysis of FLIDA Using Different Machine Learn Learning Models
    4. 4.4 Performance Analysis of Proposed FLI-DA-CRNN Email Spam Dete
    5. 4.5 Performance Analysis of FLIDA with Ensemble Approaches
    6. 4.6 Error and Feature Analysis of Email Spam Detection Techniques
    7. 4.7 Analyzing Implementation Time
    8. 4.8 Conclusion
5. 5. Email Spam Detection Approach II (Adaptive Capsule Network)
    1. 5.1 Introduction
    2. 5.2 Architecture of Proposed Email Spam Detection Technique using G-
    3. 5.3 Extraction of Visual Features
        1. 5.3.1 Walsh-Hadamard Transform Matrix
        2. 5.3.2 Fisher Discriminate Analysis
        3. 5.3.3 Color Correlogram
    4. 5.4 Extraction of Text Features
        1. 5.4.1 TV
        2. 5.4.2 TFIDF
    5. 5.5 Architecture of A-CapsNet Framework for Email Spam Detection
    6. 5.6 G-SFO Grey Sail Fish Optimization Algorithm
        1. 5.6.1 MFOS Multi-Objective Feature Selection
6. 6. Performance Analysis of G-SFO with ACaps Network
    1. 6.1 Experimental Setup and Parameter Setting
    2. 6.2 Dataset Used
    3. 6.3 Evaluation Metrics
    4. 6.4 Algorithmic Evaluation of the Suggested G-SFO with ACapsNet Mod
    5. 6.5 Performance Analysis with Machine and Deep Learning Models
    6. 6.6 Performance Analysis with Existing Metaheuristic Algorithms
    7. 6.7 Performance Validation against Traditional Classifiers
    8. 6.8 Summary
7. 7. Comparative Analysis of FLIDA and G-SFO ACapsNet
    1. 7.1 Introduction
    2. 7.2 Comparative Analysis on Dataset 1
    3. 7.3 Comparative Analysis on Dataset 2
    4. 7.4 Comparative Analysis on Dataset 3
    5. 7.5 Comparative Analysis on Dataset 4
    6. 7.6 Summary
8. 8. Quantum Machine Learning for Email Spam Detection
9. 9. Conclusion and Future Scope
    1. 9.1 Conclusions
    2. 9.2 Major Findings
    3. 9.3 Future Scope
10. References



River Publishers Series in Computer Engineering and Information Science and Technology

ISBN: 9788743810377
e-ISBN: 9788743810360
Available From: June 2026
Price:

KEYWORDS:
Email security, spam detection, phishing prevention, malware defense, artificial intelligence, machine learning, FLIDA framework, G-SFO, adaptive capsule networks, quantum machine learning, scalable cybersecurity, anomaly detection, empirical evaluation, cybersecurity frameworks.

www.riverpublishers.com
marketing@riverpublishers.com