IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

Automatic Phishing Detection Using Natural Language Processing Techniques

Rizwana Momin[1], Soni Pandey[2], Gitanjali Thakur[3], Shivani Sonkar[4], Furkan Khamkar[5]
Assistant Professor, Computer Science, Ramsheth Thakur College of Commerce and Science, Kharghar, India[1,2,3,4,]
Student Ramsheth Thakur College of Commerce and Science, Kharghar, India [5]

Abstract: *Phishing attacks have become one of the public cybersecurity threats [1]. They take lead of people's weaknesses by using untruthful message. phishing attacks that are more unconventional and made by AL are making traditional detection methods like blacklist-based filtering and rule-based systems less effective. This research paper examines the application of Natural Language Processing (NLP) techniques to detect and respond phishing attempts [2]. NLP based systems can find slight semantic pattern that suggest phishing tries by using linguistic analysis, contextual embeddings, and machine learning models. The study advises a mixed outline that combines NLP with machine learning and URL analysis to improve finding accurateness and reply time. Current experimental studies indicate that NLP driven models, particularly transformer-based architectures achieve accuracy levels surpassing 98% [3], Significantly exceeding the performance of conventional methods.*

Keywords: Phishing Detection, Natural Language Processing, Cybersecurity, Machine Learning.

I. INTRODUCTION

phishing is a cyber -attack technique that influence users into disclose sensitive information such as credit card details, personal data and passwords [1]. Attackers' expertise deceptive emails, messages, or websites that appear legitimate, exploiting trust and urgency. With the rise of phishing attack, AL have become more undoubted and smarter to detect. Traditional detection systems transmit on static rules and blacklists, which fail to identify new or "Zero-day" phishing attacks [2]. Recent advancements in NLP offer a promoting solution by analysing the language and appropriate features of communication [3].This paper focuses on deploying NLP techniques to detect phishing expeditions effectively, emphasizing real time detection, scalability and adaptability.

II. LITERATURE REVIEW

Current research study of interest the rising prominence of NLP in phishing discovery:

1. A hybrid system mixing NLP and URL analysis enhanced recognition accuracy by accessing both documented content, malware links, phishing links, or unsafe URLs [4].
2. Ensemble machine learning models cohesive with NLP features achieved an accuracy of 98.89% in phishing email detection [5].
3. Transformer-based models such as BERT and RoBERT an express contextual semantics, permitting detection of cultured phishing messages [3].
4. Modern phishing attackers use AI generated content, making them grammatically correct and highly modified, thus harder to detect with traditional systems [2].

These studies demonstrates that NLP-based approaches traditional rules-based system and are essential for modern cybersecurity frameworks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

III. PROBLEM STATEMENT

Despite advancements in cybersecurity, Phishing attacks continue to rise due to:

1. Uselessness of rule-based systems
2. Growth of AI-generated phishing emails.
3. Absence of contextual understanding in traditional models.
4. Slow Down in real time detection.

Therefore, there is an essential for an intelligent system is talented for understanding verbal patterns and detecting phishing attempts dynamically.

IV. PROPOSED METHODOLOGY

4.1 System Architecture

The Planned system consists of the following modules:

1. Data collection (Emails, SMS, Web Content).
2. Pre-processing.
3. Feature Extraction using NLP.
4. Model Training (Machine Learning /Deep Learning)
5. Classification (Phishing or Legitimate)
6. Real-time alter System.

4.2 Data pre-processing

1. Tokenisation
2. Stop word removal
3. Lemmatisation
4. Lowercasing

4.3 Extraction of features among the NLP methods employed are:

1. Term frequency inverse document frequency or TF-IDF
2. N-grams (unigrams, bigrams)
3. NER or Named Entity recognition.
4. Analysis of Sentiment
5. BERT, or Contextual Embeddings

Models used for classification:

1. Naïve Bayes
2. LOGISTIC regression
3. THE random forest
4. Support vector machine
5. Models based on Transformer (BERT, RoBERTa)

Transformer models provide better contextual understanding and higher accuracy.

4.4 Workflow

1. Enter an email/message
2. Feature extraction and Preprocessing
3. Model analysis based on NLP-based model analysis
4. Classification result
5. Alter generation

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 12, May 2026
Impact Factor: 8.2

V. RESULT AND DISCUSSION

Studies Show:

1. NLP + Ensemble models: accuracy of about ~98.89% [5]
2. NLP models based on Transformer: about ~98.4% accuracy [3]
3. NLP features in Logistic regression with: 95%+ precision [6]

Key Observation

1. NLP enhance semantic deception detection
2. Context-aware models perform better than filter keyword-based.
3. A Hybrid among the NLP method employed are: system (NLP +URL analysis) provides best results
4. With optimized models, real-time placement is possible.

VI. ADVANTAGES OF NLP-BASED PHISHING DETECTION

1. Announcements context and intent
2. Uses multilingual information.
3. Recognised phishing data produced by AI.
4. Mountable and adaptable
5. Reduction of false positives

VII. CHALLENGES AND LIMITATIONS

1. Requires a large tagged dataset is necessary.
2. Costly to compute, particularly transformations
3. Text can be altered by adversarial attacks.
4. Data processing Privacy issues.

VIII. FUTURE SCOPE

1. Real time email systems Integration
2. The application of large Language Models (LLMs)
3. Phishing detection using many modalities(text+Image+URL0)
4. Adaptive learning systems
5. Explainable AI for transparency

IX. CONCLUSION

As AI advances, phishing attacks continue to evolve, execution conventional detection techniques old-fashioned. NLP offers solution by analysing linguistic pattern and contextual semantics is effective therapy. The use of NLP-based systems greatly progresses the accuracy of phishing detection, lowers false positives, and permits real-time threat justification [3]. In Future Scope in NLP and AI will reinforce cybersecurity defences against advanced phishing attacks.

REFERENCES

1. Verma, “Cybersecurity and Phishing Attacks “, IEEE, 2022
2. J. Smith, “AI in Phishing Attacks,” Springer,2023.
3. Devlin et al., “BERT: Pre-training of Deep Bidirectional Transformers, “NAACL,2019.
4. Kumar et al., “hybrid Phishing Detection System,” Elsevier,2021.
5. Zhang et al., “Ensemble Learning for Phishing Detection, “IEEE Access,2022.
6. Broen et al., “Machine Learning in cybersecurity,” ACM,2020.