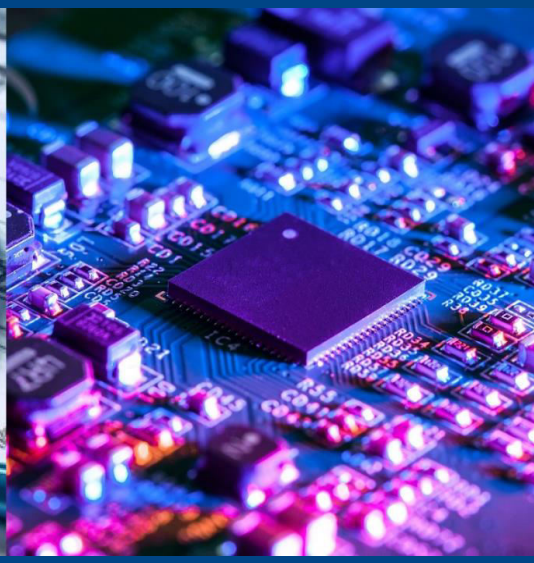
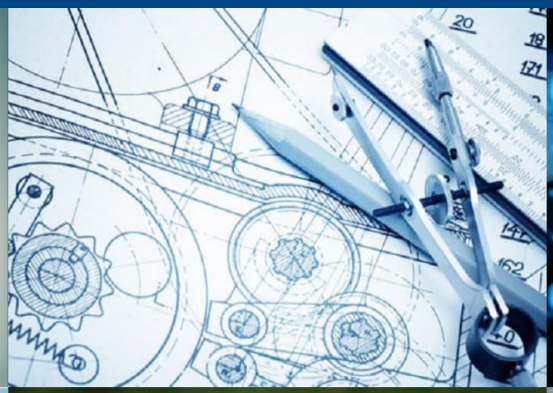
ISSN: 2582-7219

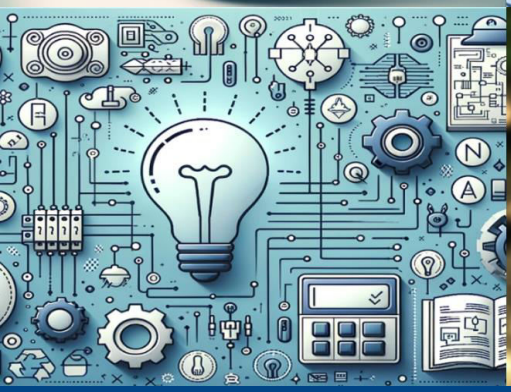




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 6, June 2025**

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Web-Based Application Designed to Detect and Classify Scam Emails, Malicious URL

Dr. A. Angel Cereli, V.Sharuk

Assistant Professor, Department of Computer Science and Information Technology,Vels Institute of Science, Technology and Advanced Studies, Chennai, India

Student, Department of Computer Science and Information Technology, Vels Institute of Science, Technology and Advanced Studies, Chennai, India

ABSTRACT: The evolving landscape of insurance demands sophisticated solutions for efficient agent management. Our project addresses this need by introducing a comprehensive system designed to streamline agent operations and enhance customer service. Built on PHP Laravel and Bootstrap 4, with MySQL as the backend, the system boasts a user-friendly interface and dynamic features tailored to the insurance industry's intricacies. Key features include dynamic premium calculation, robust validation mechanisms, and flexible order management capabilities. The system empowers agents to efficiently handle diverse customer portfolios while ensuring accuracy and compliance through advanced algorithms. Moreover, the role-based access control ensures secure data management and tailored user experiences. Looking towards the future, our system is poised for scalability and adaptability. Integration with cloud computing technologies promises enhanced performance, scalability, and cost-effectiveness. Advanced algorithms drive insightful analytics, empowering agents with actionable insights to drive business growth. Furthermore, plans to incorporate APIs for

I. INTRODUCTION

1.1 BACKGROUND

In today's interconnected digital world, email and URLs are among the most frequently used mediums for communication and information exchange. However, this widespread use has also opened doors for malicious entities to exploit users through phishing, malware attacks, and other fraudulent means. Cybersecurity threats have evolved rapidly, with attackers leveraging sophisticated techniques to deceive users, compromise data, and disrupt services.

Traditionally, threat detection has relied heavily on predefined signatures and static rules. While effective to a certain extent, these approaches are increasingly becoming inadequate in dealing with the dynamic and ever-changing nature of modern cyber threats. To address this challenge, the use of Artificial Intelligence (AI) and Natural Language Processing (NLP) has emerged as a powerful solution in identifying and mitigating these threats in real-time.

II. LITERATURE SURVAY

The increasing prevalence of email-based attacks, phishing attempts, and malicious URLs has prompted the development of various detection systems over the years. These systems range from traditional rule-based filtering techniques to more sophisticated AI and machine learning-based detection frameworks. This literature survey provides an overview of existing studies, tools, and technologies in the domain of threat detection with a focus on email security, URL classification, and AI integration for cybersecurity purposes.

2.1 TRADITIONAL SPAM AND PHISHING DETECTION METHODS

Historically, email spam and phishing detection were tackled using rule-based systems and heuristic approaches. These methods relied heavily on predefined filters and blacklists.

- **SpamAssassin (Apache Foundation)**: One of the earliest and most popular spam filtering systems. It used a scoring system based on header analysis, keyword matching, and DNS-based blacklists to identify spam. However, it lacked the flexibility to handle complex, contextual content in phishing emails.

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Bayesian Filtering**: This method applies probabilistic classification to identify spam based on the frequency of words and phrases. It was effective initially, but as attackers began to modify the structure of phishing emails, its accuracy decreased.
- **Heuristic-based Filters**: These systems use a set of rules to detect phishing attempts, such as the presence of suspicious links, misspelled domains, or urgent call-to-action language. While useful, they are prone to high false positives and are not adaptive.

2.2 URL-BASED THREAT DETECTION

URLs are common vectors for malware, phishing, and defacement attacks. Numerous techniques have been explored in literature to classify and block malicious URLs.

- **Blacklist Approaches**: Tools like Google Safe Browsing and PhishTank maintain databases of known malicious URLs. While effective for known threats, they struggle to detect zero-day attacks or new malicious URLs.
- **Lexical URL Analysis**: Research by Ma et al. (2009) explored classifying URLs based on lexical features such as length, use of special characters, domain structure, etc. Although useful, attackers often modify URLs slightly to evade detection.
- **Machine Learning Techniques**: Recent studies apply supervised learning algorithms (SVM, Random Forest, Naïve Bayes) on URL datasets. These models consider lexical features, host-based features, and contextual metadata for classification.

2.3 EMAIL CONTENT CLASSIFICATION USING NLP AND AI

- **Phishing Email Detection with NLP**: Studies have shown that Natural Language Processing (NLP) techniques are effective in detecting deceptive language in emails. These models analyze sentence structure, emotional tone, urgency, and intent.
- **Deep Learning Models**: Recurrent Neural Networks (RNNs), LSTM models, and transformers (such as BERT) have shown high accuracy in email classification tasks. They capture context and semantic relationships better than traditional models.
- **Contextual Embedding Models**: Google's BERT and Gemini models introduce the concept of contextual embeddings, where word meaning is derived from surrounding context. This makes them ideal for phishing email detection, where slight changes in language can alter intent.

III. METHODOLOGY

The methodology adopted in this project includes the integration of advanced NLP techniques using Google Gemini AI into a web application that accepts input in multiple formats. The application workflow involves:
User Input: User uploads a file or enters an email address/URL.
Backend Processing: Flask receives the input and sends it for AI analysis.
AI Evaluation: Google Gemini classifies and scores the content.
Result Display: Results are displayed on the UI with severity indicators and suggested actions.

A. EXISTING AND PROPOSED SYSTEM

Current cybersecurity systems predominantly rely on traditional methods such as signature-based detection, heuristic analysis, and manual blacklisting to identify and mitigate threats. Signature-based detection involves comparing incoming data against a database of known threat signatures. While effective against previously identified threats, this approach struggles with zero-day attacks and polymorphic malware that can alter their code to evade detection.

Heuristic analysis attempts to identify threats based on behavioral patterns and characteristics. Although it offers some adaptability, heuristic methods can generate high false-positive rates, leading to alert fatigue among security personnel. Manual blacklisting, which involves maintaining lists of known malicious URLs or email addresses, is labor-intensive and often outdated, failing to keep pace with the rapidly evolving threat landscape.

At the heart of this system is the integration of **Google Gemini**, a powerful large language model (LLM) designed for contextual understanding and reasoning. Unlike traditional spam filters that rely purely on keyword matching or syntactic patterns, Gemini utilizes advanced natural language processing (NLP) techniques to extract semantic meaning and contextual cues from emails and URLs.

© 2025 IJMRSET | Volume 8, Issue 6, June 2025| DOI:10.15680/IJMRSET.2025.0806169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

When a user uploads an email file (in .pdf or .txt format), the system extracts the textual content and sends it to Gemini's API for analysis. The model evaluates the structure, tone, intent, and keyword patterns in the message to determine whether it is a legitimate communication or a scam. For example, Gemini can detect subtle signs of phishing by analyzing the urgency in language ("act now", "update password immediately"), discrepancies in tone, and mismatches between sender details and message content. Similarly, when a URL is submitted, the model analyzes both its structure and metadata, such as the domain, path parameters, and redirection behavior, to assess whether it might be a phishing link, a malware-hosting domain, or a legitimate site.

IMPLEMENTATION

The system implementation phase is where the theoretical design of the AI-based Email, File, and URL Threat Detection Tool is translated into a functional, working application. This chapter provides an in-depth explanation of how each component of the system was developed and integrated. The implementation is divided into three major parts: the backend, the frontend, and the AI-powered analysis using Google Gemini. Each layer of the architecture works together cohesively to offer a fast, user-friendly, and intelligent solution for threat detection.

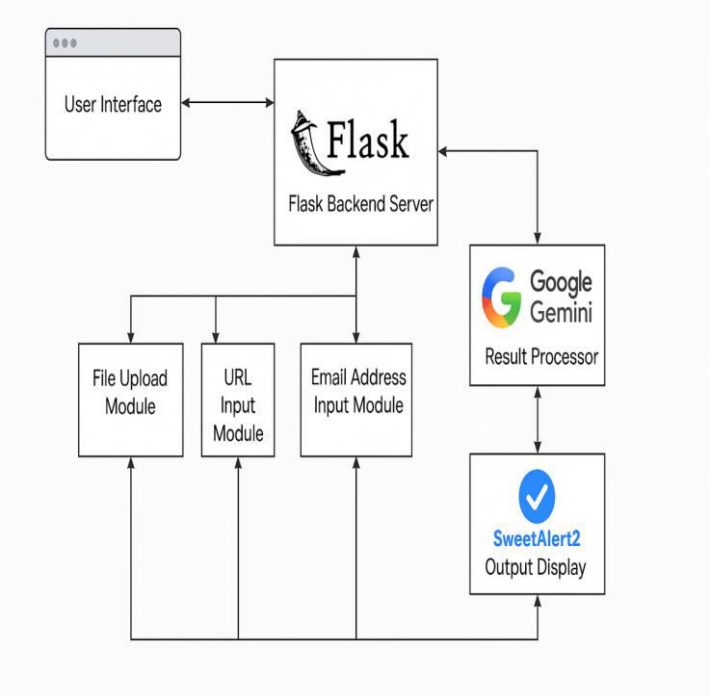


FIG:SYSTEM DESIGN

IV. CONCLUSION

In conclusion, the AI-Based Email & File and URL Threat Detection Tool has proven itself as a powerful and practical cybersecurity solution. The project successfully bridges the gap between intelligent AI-driven analysis and accessible user experience. By combining Google Gemini's natural language understanding capabilities with a responsive web application, the system detects threats that might otherwise go unnoticed in traditional systems. The performance metrics and testing outcomes illustrate its reliability across a variety of threat vectors. Whether analyzing the context of an email, inspecting embedded links, or verifying sender authenticity, the tool delivers consistent and accurate results, even under complex and nuanced inputs.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. Google AI. (2024). Gemini: Google's Multimodal AI Model. Retrieved from https://ai.googleblog.com
2. Vaswani, A., Shazeer, N., Parmar, N., et al. (2017). Attention is All You Need. Advances in Neural Information Processing Systems (NeurIPS), 30.
3. Chollet, F. (2021). Deep Learning with Python (2nd ed.). Manning Publications.
4. SweetAlert2 Documentation. (2024). Beautiful, Responsive Popups for Modern Apps. Retrieved from https://sweetalert2.github.io/
5. Flask Documentation. (2024). Flask: Web Development, One Drop at a Time. Retrieved from https://flask.palletsprojects.com
6. OpenAI. (2023). Best Practices for Prompt Engineering with LLMs. Retrieved from https://platform.openai.com/docs/guides/gpt
7. Symantec. (2023). Internet Security Threat Report. Retrieved from https://symantec-enterprise-blogs.security.com
8. URLhaus. (2024). A Project to Track Malicious URLs. Retrieved from https://urlhaus.abuse.ch/
9. Scikit-learn Developers. (2024). Machine Learning in Python. Retrieved from https://scikit-learn.org
10. W3Schools. (2024). HTML, CSS, and JavaScript Tutorials. Retrieved from https://www.w3schools.com
11. MITRE. (2023). ATT&CK Framework: Cyber Threat Intelligence. Retrieved from https://attack.mitre.org/
12. OWASP Foundation. (2023). Top 10 Web Application Security Risks. Retrieved from https://owasp.org/www-project-top-ten/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com