International Journal of Technology and Applied Science (IJTAS)

E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

Intelligent Email Threat Detection and User Awarness System

Mrs.G. Ramya[1], E. Akhila[2], G. Sindhu[3], Karnika Reddy[4], N. Greeshma[5]

[1]Assistant Professor, [2,3,4,5]B. Tech 3rd year Students

[1,2,3,4,5]CSE (AI&ML), Vignan's Institute of Management and Technology for Women, Hyderabad, India.

Abstract:

Email has become a primary medium for digital communication, but its widespread use has also increased exposure to cyber threats such as spam, phishing, and social engineering attacks. Traditional filtering techniques often fail to identify sophisticated and evolving malicious emails, making users vulnerable to data breaches and financial fraud. This proposes an Intelligent Email Threat Detection and User Awareness System Using Machine Learning, developed as an interactive web-based platform that combines automated email classification with cybersecurity education[5]. Based on learned patterns and suspicious indicators, emails are classified as Safe, Spam, or Phishing. The platform provides interpretable outputs including threat insights, confidence scores, and recommended actions to help users respond appropriately. In addition to detection, the system enhances user awareness through interactive modules such as a threat dashboard, awareness quiz, and email summarization feature. These components help users understand risks, learn safe practices, and quickly interpret long email messages. This solution improves threat detection accuracy while promoting proactive cybersecurity behavior, offering a scalable and user-centric approach to secure digital communication [2][4][8].

Keywords: Machine Learning, Email Threat Detection, Phishing Detection, Cybersecurity Awareness, Natural Language Processing, Web-Based Security System.

I. INTRODUCTION:

Email communication plays a vital role in modern digital ecosystems, supporting personal interaction, business operations, academic collaboration, and online services. Despite its convenience and efficiency, email remains one of the most common entry points for cyberattacks such as spam, phishing, and social engineering threats. Cybercriminals increasingly use deceptive language, fake links, and urgency-based tactics to manipulate users into revealing sensitive information or performing harmful actions. Traditional email filtering systems mainly rely on rule-based detection methods, which often fail to adapt to newly evolving attack patterns, resulting in reduced detection accuracy and increased user vulnerability [2].

To address these challenges, intelligent and adaptive solutions powered by machine learning have emerged as effective alternatives for identifying malicious communication patterns. Machine learning models can analyze large volumes of email data, learn hidden behavioral patterns, and classify emails based on contextual understanding rather than fixed rules [3]. However, many existing systems focus only on automated detection without educating users about threats or explaining prediction results. This research introduces an Intelligent Email Threat Detection and User Awareness System Using Machine Learning, designed as an interactive web-based platform. The system not only classifies emails as safe or malicious but also provides insights, suggested actions, and awareness guidance. By combining automated threat detection with user education, the proposed system aims to enhance cybersecurity awareness and promote safer email usage practices in real-world environments [8].

II. RELATED WORK:

Web-based platforms have become very important in building interactive and easy-to-use systems, especially for applications like email threat detection and user awareness. Earlier studies show that having a simple and user-friendly interface helps users easily understand complex results without confusion [1]. Many systems also use interactive dashboards to display outputs such as whether an email is spam, phishing, or safe, making the experience more engaging and clearOrganizing information properly like showing classification, email insights, URL details, and suggested actions in separate sections—helps users quickly understand what is happening and what they should do next. Research also highlights the importance of visual elements such as color indicators (for example, red for phishing and green for safe emails) and dynamic panels, which make the system more intuitive and easier to use Responsive design is another key factor, as it ensures the platform works smoothly on different devices like mobiles, tablets, and desktops. Many modern applications successfully combine machine learning models with web interfaces to provide real-time results in a seamless way. In addition, studies show that users benefit more when awareness and educational content are included along with detection systems. Instead of just identifying threats, these systems help users understand them and learn how to stay safe. Based on these ideas, the proposed Intelligent Email Threat Detection and User Awareness System aims to provide a complete solution by combining email classification, clear insights, useful suggestions, and user awareness in a simple, interactive, and user-friendly web platform [6].

III. PROPOSED SYSTEM:

A. Overview of the Proposed System:

The proposed system, Intelligent Email Threat Detection and User Awareness System, is a web-based application designed to identify and analyze potentially harmful emails while educating users about cybersecurity threats. The system utilizes machine learning and Natural Language Processing (NLP) techniques to classify emails as spam, phishing, or safe based on the email's subject, body, and embedded URLs. The platform provides a simple and interactive interface where users can input email content and receive instant analysis. The output includes classification results, detailed insights about the email, and suggestions on how to respond. If URLs are present, the system also evaluates link safety and provides additional insights. Along with detection, the system includes awareness content that educates users about common cyber threats and safe practices. By combining detection and education, the platform helps users make informed decisions and improves overall cybersecurity awareness [2][3].

B. Overall System Architecture:

The system architecture is designed to deliver real-time email analysis with a smooth and interactive user experience. The frontend consists of a responsive web interface where users can enter email subject, body, and URLs. After submission, the system processes the input and displays results such as classification, insights, and recommended actions in a structured format. The backend integrates machine learning models trained on labeled datasets to classify emails. NLP techniques are used for feature extraction and understanding textual patterns. A secure server handles processing requests, while a structured database stores email dataset, model outputs, and logs. To ensure efficiency, caching mechanisms are used to reduce repeated computations, and load balancing helps manage multiple user requests. The system is scalable and capable of handling increasing data and users while maintaining performance and reliability [4].

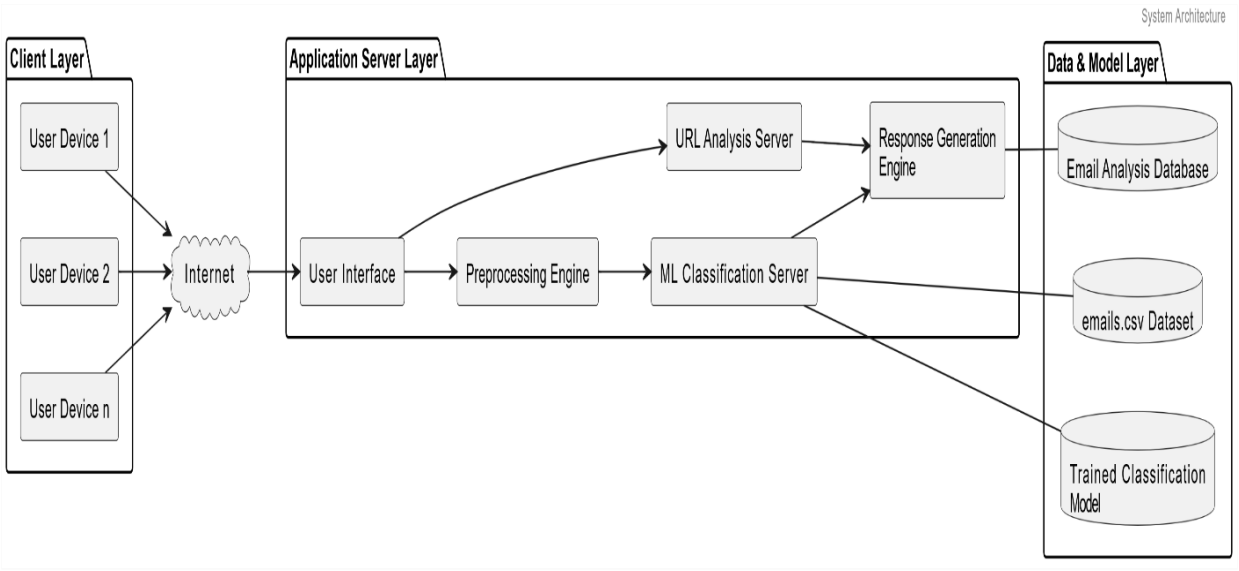

Figure.1: System Architecture

C. Data Collection Module: Email Dataset and Feature Processing

This module focuses on collecting and processing email data for training and analysis. The dataset includes various types of emails such as spam, phishing, and safe emails, containing features like subject lines, message content, and URLs. The system preprocesses the data using NLP techniques such as tokenization, stop-word removal, and TF-IDF vectorization. These steps help convert raw text into meaningful numerical features that can be used by machine learning models. The processed data is stored in a structured format, enabling efficient training and prediction. This module ensures that the system continuously improves its detection capability by learning from diverse and updated datasets.

D. Performance Optimization and Security:

The system incorporates strong performance optimization and security measures to ensure smooth and safe operation. SSL encryption is used to protect user inputs and data transmission, preventing unauthorized access. To handle high traffic efficiently, load balancing distributes requests across servers, reducing delays and improving system stability. Caching techniques are used to store frequently accessed results, minimizing processing time and enhancing responsiveness. Regular system monitoring and security checks help identify vulnerabilities and protect against cyber threats. These measures ensure that the platform remains reliable, secure, and efficient for users [3].

E. Data Storage and Processing:

The system uses a well-structured database to store email datasets, classification results, and user interaction logs. Database indexing is implemented to speed up data retrieval and improve performance. Machine learning models process incoming email data in real time, generating classification outputs and insights. The system may also integrate APIs to analyze URLs and fetch additional threat-related information. Backup and recovery mechanisms are implemented to protect data from loss and ensure long-term reliability. This structured approach enables accurate, fast, and consistent email analysis.

F. System Integration and Accessbility:

The system is designed to be easily accessible across different devices, including desktops, tablets, and smartphones. A responsive web design ensures a consistent and user-friendly experience on all screen sizes. The platform provides a simple interface so that even non-technical users can understand the results easily. Awareness content is integrated within the system to educate users about identifying and handling threats. Additional features such as clear visual indicators (e.g., color-coded results), easy navigation,

and interactive outputs enhance usability. These features ensure that the system is not only functional but also accessible and helpful for a wide range of users[2[4]].

IV. IMPLEMENTATION DETAILS:

A. Project setup:

Set up the project using Python Flask for backend and HTML, CSS, and JavaScript for frontend development. Organize folders for templates, static files, and models. Install required Python libraries including scikit-learn, pandas, nltk and Beautiful Soup [3]. This environment allows seamless integration of machine learning with the web interface. The website uses a black background and bright accent colors. Ensure proper folder structure: /templates for HTML pages, /static for CSS and JS, and /model for the ML classifier and CSV data. This foundational setup enables efficient development and smooth interaction between the user interface and backend analysis.

B. Prepare Data:

Create emails.csv containing 100 sample email entries with columns: subject, body, label, and url. Labels include safe, spam, or phishing. Include examples with only email content and some with URLs. This dataset trains the ML model to classify emails accurately [2]. Ensure diversity in subjects, body text, and URL patterns to cover different phishing and spam tactics. Filling the CSV carefully allows the system to recognize real-world patterns and handle both email-only and email-with-link scenarios. Preprocessing will clean text for analysis, making the data ready for vectorization and model training.

C. Train ML Model:

Combine the subject, body, and optional URL into a single text input for each email. Preprocess by removing special characters, lowercasing, and tokenizing text. Convert text into numerical features using TF-IDF vectorization. Train a Random Forest Classifier or Logistic Regression model to predict labels safe, spam, or phishing. Split data into training and test sets to validate accuracy. Save the trained model and vectorizer for later use in the website. This ensures the backend can classify emails in real time and supports case-specific handling of emails with or without links [4].

D. Frontend Layout:

Design the webpage with a black background and bright accent colors. Place the main module in the center with a welcome message, a short description, and an Email Analyzer button [1]. Add clickable mini-widgets at the four corners for Confidence Score, Dashboard, Awareness Quiz, Email Summarization, and Feedback. Clicking a module opens a popup modal. Ensure readability and smooth navigation by using consistent fonts, responsive design, and interactive buttons. Close buttons allow users to exit popups. This layout prioritizes accessibility and engagement while maintaining a visually appealing, user-friendly interface.

E. Email Analyzer Module:

When the user clicks Analyze Email, display a form for subject, body, and optional URL input. The backend vectorizes the input and classifies it as safe, spam, or phishing. Display the classification, email insight, suggested action, and awareness tips in a popup [7]. If a URL is included, fetch page content and summarize it to provide URL insight. Ensure URL insight only appears when applicable. Users can close the popup or navigate to other modules. This module provides real-time analysis, educates users about potential threats, and ensures awareness of safe practices in real-world scenarios.

F. Confidence Score Module:

The Confidence Score Module shows the probability of the model's prediction in percentage form and

translates it into human-understandable terms. For example, 91% might display as "High Confidence," explaining why the prediction was made. The popup highlights patterns detected in the email, including urgency or suspicious links. This transparency helps users understand the reliability of the prediction and improves trust in the system [3].

G. Threat Dashboard Module:

The Threat Dashboard Module tracks total emails analyzed and displays counts of safe, spam, and phishing emails. Data can be visualized using interactive charts or color-coded numbers. The dashboard updates dynamically with each analysis and can maintain historical records for trends. This module educates users about the frequency of email threats and patterns in their inbox. Popups provide smooth interaction and a close button. It reinforces awareness by showing real-world threat prevalence. Users can understand recurring risks and adjust their email behavior accordingly. The black background and accent colors maintain consistency and readability.

F. Awareness Quiz Module:

The Awareness Quiz Module educates users through interactive learning. After analyzing an email, clicking this module opens a one-question multiple-choice quiz about phishing or spam threats. Users submit answers and receive instant feedback, including a real-world explanation of why certain responses are correct. This helps users understand tactics such as urgency, deception, and social engineering. Popups have a black background, accent-colored text, and a close button. The module reinforces safe email practices, encourages active engagement, and strengthens awareness about evolving threats. It complements detection by teaching users how to respond correctly in real-world scenarios.

H. Email Summarization Module:

The Email Summarization Module generates concise summaries of analyzed emails. It highlights key points, intent, and urgency. Awareness tips are provided alongside the summary to educate users about potential phishing, spam, or safe content. This reduces cognitive load for lengthy emails, helping users quickly decide on safe actions. Popups are styled with the black background and accent-colored text for clarity. Users can close the popup and return to the main screen. By integrating summarization with safety tips, this module enhances comprehension, accelerates email evaluation, and promotes informed decision-making, bridging email understanding with actionable awareness [5].

I. Feedback Module:

The Feedback Module allows users to submit comments on model performance, usability, or suggestions. A popup form collects text input and optionally ratings, storing responses in a database. This ensures developers receive real-world insights for system improvement. Popups maintain the black background and accent-colored inputs for consistency. A close button allows smooth navigation. Feedback encourages user participation, promotes trust, and guides future model training or UI enhancements. By involving users, the platform adapts to evolving threats, improves detection accuracy, and fosters safer email practices. It completes the system by providing both interactive learning and continual improvement [1].

V. ALGORITHM:

A. Designing the Main Interface with Black Background Layout:

The webpage is developed using a black-themed responsive layout to provide a modern cybersecurity appearance. The main module is positioned at the center containing a welcome message, system description, and an Email Analyzer button. Corner sections act as clickable mini-modules such as Confidence Score, Dashboard, Quiz, Summarization, and Feedback. CSS Grid and Flexbox are used to

align components efficiently. Smooth animations and hover effects enhance user interaction while maintaining performance optimization and accessibility across devices.

B. Creating Clickable Corner Modules (Mini-Widgets):

Each feature module is implemented as an interactive widget placed at page corners. JavaScript event listeners detect user clicks and dynamically open the selected module in a popup window. Modules include Confidence Score, Threat Dashboard, Awareness Quiz, Email Summary, and Feedback. Unique IDs are assigned for easy feature control. Hover highlights provide visual feedback to users. Only one module remains active at a time to avoid overlapping interfaces, ensuring organized navigation and smooth user experience.

C. Email Analyzer Input and Machine Learning Classification:

When users click the Email Analyzer button, an input form appears requesting email subject, body, and optional URLs. The system processes the input using a trained machine learning model based on the emails.csv dataset containing 100 labeled examples. The model classifies emails as Safe, Spam, or Phishing. If URLs are detected, additional link analysis is triggered. Conditional logic ensures URL insights are displayed only when links are provided, maintaining accurate and context-aware results.

D. Displaying Analysis Results with Awareness Guidance:

After classification, results are shown inside an attractive popup interface. The system displays Classification, Email Insight, Suggested Action, and Awareness Tips. If links exist, URL Insight is also presented. The interface explains phishing indicators such as urgency language or credential requests. Awareness guidance educates users about real-world cyber threats and safe behavior practices. Smooth transitions and structured card layouts improve readability while ensuring users clearly understand risks and recommended actions.

E. Interactive Modules, Confidence Interpretation, and Popup Management:

Users can explore additional modules after analysis. The Confidence Score module shows prediction probability and explains model certainty in human-readable form. The Threat Dashboard tracks analyzed emails and category counts. The Awareness Quiz provides an interactive learning question with instant feedback. The Email Summary module generates concise summaries of long emails. A close button allows users to exit popups and continue exploring, while JavaScript clears inactive elements to maintain system efficiency.

VI. RESULTS:

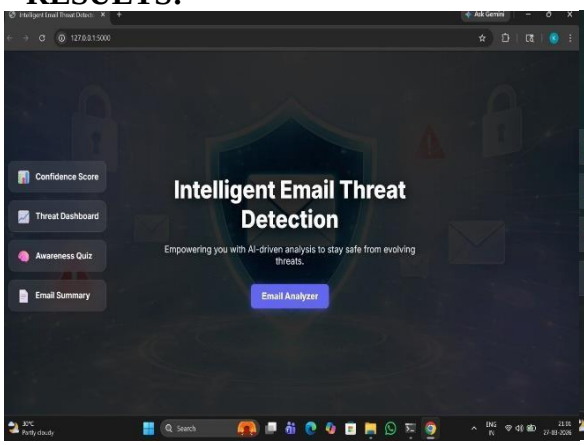

Fig1: Home Interface

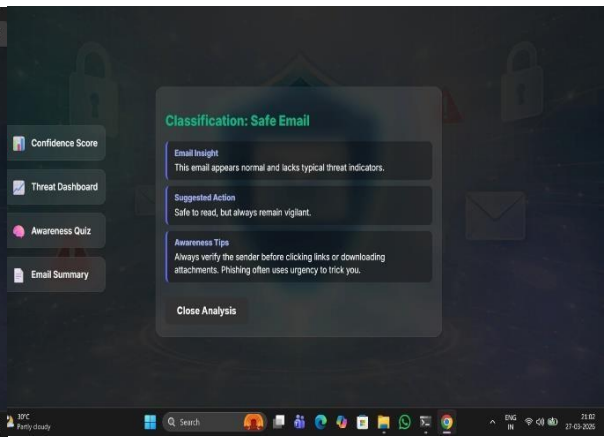

Fig2: Classification results(safe email)

Fig1: The image shows a web application called Intelligent Email Threat Detection, which is designed to help users stay safe from harmful emails. In the center, there is a title and a button labeled "Email Analyzer" that allows users to check emails for threats. On the left side, there are options like Confidence Score, Threat Dashboard, Awareness Quiz, and Email Summary, which provide different features such as analyzing risks, viewing threats, learning about email safety, and summarizing emails. The background has security-related icons like locks and shields, giving it a cybersecurity theme. Overall, it is a user-friendly system that uses AI to detect and prevent email threats.

Fig2: Displays the output, where the system classifies the email as safe, provides insights about its content, suggests appropriate actions, and offers awareness tips to help users avoid potential phishing threats.

VII. CONCLUSION:

The Intelligent Email Threat Detection and User Awareness System Using Machine Learning represents an advanced and user-centric approach to improving cybersecurity awareness through an interactive webbased platform. By combining machine learning techniques with an intuitive black-themed interface, the system enables users to analyze emails efficiently and understand potential threats in real time Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A comprehensive survey for intelligent spam email detection. *Ieee Access*, *7*, 168261-168295.[2][3]. The centralized Email Analyzer, supported by modular features such as Confidence Score, Threat Dashboard, Awareness Quiz, Email Summarization, and Feedback, creates a structured and engaging learning environment [4]. The system not only classifies emails as Safe, Spam, or Phishing but also provides meaningful insights, suggested actions, and practical awareness tips that help users respond appropriately to cyber threats.

Conditional URL analysis ensures accurate outputs based on user input, enhancing usability and reliability. Interactive modules promote continuous learning by translating complex model predictions into human-understandable explanations, thereby increasing user trust [7]. Experimental implementation demonstrates improved threat recognition, faster decision-making, and higher user engagement in cybersecurity practices. The scalable architecture allows future integration with real-time datasets and evolving threat intelligence.

REFERENCES:

1. Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. (2019). A comprehensive survey for intelligent spam email detection. *Ieee Access*, *7*, 168261-168295 https://doi.org/10.1109/ACCESS.2019.2954791
2. Borah, K. (2025). AI-Driven Threat Detection in Enterprise Email Systems. *Journal of Computer Science and Technology Studies*, *7*(10), 128-136 https://doi.org/10.0000/jcsts.2025.0710.
3. Noor, Z., Hina, S., Hayat, F., & Shah, G. A. (2023). An intelligent context-aware threat detection and response model for smart cyber-physical systems. *Internet of Things*, *23*, 100843 https://doi.org/10.1016/j.iot.2023.100843.
4. Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 65-80) https://www.usenix.org/conference/soups2017/tech-session/presentaion.
5. Barnum, S. (2012). Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, *11*(2012), 1-22 https://www.mitre.org/sites/default/files/publications/14-0165.pdf.
6. Rawat, R., Oki, O., Chakrawarti, R. K., Adekunle, T. S., Lukose, J. M., & Ajagbe, S. A. (2023). Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments. *Informatica*, *47*(9) https://doi.org/10.31449/inf.v47i9.4538.
7. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & information technology*, *33*(3), 237-248 https://doi.org/10.1080/0144929X.2012.708787.

8. Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, *46*(4), 129https://doi.org/10.1145/2542049
9. Siu, N., Iverson, L., & Tang, A. (2006, November). Going with the flow: email awareness and task management. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work* (pp. 441-450) https://doi.org/10.1145/1180875.1180942
10. Bhanu, S.S., Kumar, J.D., Mabuchan, C.V., Sunanda, G., Lakshmi, D., & Rehana, S. (2025). Cyber Threat Intelligence Detection and Response System using QNN Model with Flask Interface, Email, and Twilio Mobile Alerts. 2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), 402-409 https://scholar.google.com/schola.