UDC 004.056.52:004.773.3:004.774

P.S. Myradov, D.M. Haytkulyyev
(The State Energy Institute of Turkmenistan, Mary, Узбекистан))

DEVELOPING A SECURE WEB APPLICATION FOR ANALYZES DATA LEAKS VIA EMAIL

Introduction

Email remains one of the most widely used communication tools in both personal and professional environments. However, its popularity makes it a prime target for cybercriminals and a frequent source of accidental data leaks. According to recent cybersecurity reports, a significant percentage of security breaches originate from compromised email accounts or phishing attacks.

Data leaks through email can occur due to weak authentication mechanisms, malware infections, social engineering attacks, or user negligence. Such incidents can lead to financial losses, reputational damage, and legal consequences. Therefore, developing a secure system that can analyze email traffic and detect potential data leaks is of critical importance.

This paper proposes a secure web application designed to monitor and analyze emails for potential data leakage. The system focuses on real-time detection, risk assessment, and preventive actions to enhance organizational security.

Related Work

Previous research has explored various approaches to email security, including spam filtering, phishing detection, and data loss prevention (DLP) systems. Traditional DLP solutions rely on predefined rules and pattern matching to identify sensitive information. While effective to some extent, rule-based systems often generate false positives and fail to detect new attack patterns.

Recent studies emphasize the use of machine learning algorithms for anomaly detection and content classification. Natural Language Processing (NLP) techniques have been applied to analyze email content and identify sensitive data. However, many existing solutions lack a comprehensive web-based interface and robust security architecture.

The proposed system builds upon existing research by integrating machine learning with secure web technologies to provide an efficient and user-friendly platform for data leak analysis.

System Architecture

The web application follows a modular architecture consisting of the following components:

1. User Interface (UI) – Provides a dashboard for administrators to monitor email traffic, view alerts, and generate reports.

2. Authentication Module – Implements multi-factor authentication and role-based access control to prevent unauthorized access.

3. Email Processing Engine – Extracts metadata and content from incoming and outgoing emails.

4. Data Analysis Module – Uses machine learning algorithms to classify emails based on risk level.

5. Security Layer – Applies encryption, secure APIs, and intrusion detection mechanisms.

6. Database – Stores encrypted logs, user data, and analysis results.

The system is hosted on a secure cloud infrastructure to ensure scalability and availability.

Methodology

1. Data Collection

Email data is collected through secure APIs or mail server integration. The system processes subject lines, message bodies, and attachments while complying with privacy regulations such as GDPR.

2. Feature Extraction

Key features include keyword frequency, file types, sender behavior, and anomaly patterns. NLP techniques are used to identify sensitive entities such as credit card numbers, personal identifiers, and confidential documents.

3. Machine Learning Model

A supervised learning model is trained using labeled email datasets. Algorithms such as Support Vector Machines (SVM), Random Forest, and Neural Networks are evaluated. The model classifies emails into categories: safe, suspicious, and critical.

4. Security Implementation

All data transmissions are encrypted using TLS protocols. Sensitive data stored in the database is protected with AES-256 encryption. Regular security audits and penetration testing are conducted.

Implementation

The application is developed using modern web technologies such as React for the frontend and Node.js for the backend. A RESTful API enables communication between system components. The machine learning model is deployed using Python and integrated via microservices.

Docker containers are used to ensure environment consistency, and continuous integration pipelines are implemented to maintain code quality.

Evaluation

The system is tested using real-world and synthetic datasets. Performance metrics include accuracy, precision, recall, and F1-score. Experimental results show an average detection accuracy of 92%, demonstrating high reliability in identifying data leaks.

User feedback indicates that the dashboard is intuitive and provides actionable insights for security teams.

Discussion

The proposed system effectively combines security best practices with intelligent data analysis. Unlike traditional DLP tools, the machine learning-based approach adapts to evolving threats. However, challenges remain in handling encrypted email content and minimizing false positives.

Future improvements may include deep learning models, real-time alert systems, and integration with enterprise security platforms.

Conclusion

This study presents a secure web application for analyzing data leaks via email. By integrating machine learning, encryption, and modern web technologies, the system offers a robust solution for detecting and preventing unauthorized data exposure. The results confirm its effectiveness and potential for real-world deployment.

As cyber threats continue to evolve, such intelligent and secure platforms will play a crucial role in protecting digital communication channels.

REFERENCES

1. Behl, A., & Behl, K. (2017). Cyberwar: The Gray Zone Between War and Peace. Oxford University Press.

2. Chandrasekaran, M., et al. (2006). Phishing email detection based on structural properties. NYU Technical Report.

3. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.

4. European Union. (2018). General Data Protection Regulation (GDPR).

УДК 51-3

Т.А. Котенева, ст. преп.
(Губкинский филиал БГТУ им. В.Г. Шухова, г. Губкин, Россия)

ОТ ЗАДАЧИ О КВАДРАТУРЕ КРУГА К СОВРЕМЕННЫМ ТЕХНОЛОГИЯМ ПАРАМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ

Относительная простота вычисления площади квадрата приводила к попыткам решить общую задачу о квадратуре других фигур. Квадратура фигуры – это построение квадрата с той же площадью, что и у данной фигуры, с помощью только циркуля и линейки. Если бы можно было построить такие квадраты, то это дало бы нам ценный