

# A SURVEY ON SECURESCAN 360: CYBER INTEGRATED SYSTEM FOR THREAT DETECTION AND IMAGE AUTHENTICATION

Aparna Sunil, Niranjana K V, Jeeva C V, Pranav S Plavida

*Aparna Sunil Student, Computer Science and Engineering, Holy Grace Academy of Engineering,  
Kerala, India*

*Niranjana K V Student, Computer Science and Engineering, Holy Grace Academy of Engineering,  
Kerala, India*

*Jeeva C V Student, Computer Science and Engineering, Holy Grace Academy of Engineering,  
Kerala, India*

*Pranav S Plavida Student, Computer Science and Engineering, Holy Grace Academy of Engineering,  
Kerala, India*

*Irfana Parveen C A Assistant Professor, Computer Science and Engineering, Holy Grace Academy of Engineering,  
Kerala, India*

*Sanam E Anto Head of Department, Computer Science and Engineering, Holy Grace Academy of Engineering,  
Kerala, India*

## ABSTRACT

*The rapid expansion of digital communication and internet-based services has significantly increased the occurrence of cyber threats such as phishing websites, spam emails, and manipulated digital images. These attacks pose serious risks to individuals and organizations, including data theft, financial fraud, and the spread of misinformation. Traditional cybersecurity solutions often focus on detecting a single type of threat, resulting in fragmented protection and limited effectiveness against modern multi-vector attacks.*

*To address these challenges, this paper proposes SecureScan 360, a multi-faceted cybersecurity detection platform that integrates multiple threat detection mechanisms within a unified system. The proposed system incorporates three primary modules: phishing website detection, spam email classification, and image forgery detection. The phishing detection module utilizes the Random Forest algorithm to analyze URL features and identify fraudulent websites. The spam detection module employs Natural Language Processing (NLP) techniques with Long Short-Term Memory (LSTM) to categorize emails as spam or legitimate. Additionally, the image forgery detection module applies digital image processing techniques to detect manipulated or tampered images.*

*The platform also includes a role-based interface that allows users to access detection services, submit complaints, and view activity reports, while administrators can monitor users, analyze reports, and manage system notifications. By integrating machine learning and image analysis techniques into a single platform, SecureScan 360 enhances cybersecurity protection and improves the reliability of digital communication systems.*

*redistribution platforms represent a scalable and replicable model for achieving zero hunger and environmental sustainability across developing nations. The system is designed with scalability and usability in mind, ensuring efficient threat detection for both individuals and organizations. Experimental evaluation indicates that the proposed model achieves reliable detection performance across multiple threat categories. By combining machine learning algorithms with image analysis techniques, the platform provides a comprehensive approach to modern cybersecurity challenges. The unified framework improves response time, enhances threat visibility, and supports proactive monitoring of suspicious activities. Overall, SecureScan 360 demonstrates the potential of intelligent security systems in creating safer and more trustworthy digital environments.*

**Keywords :** *Cybersecurity, Phishing Website Detection, Spam Email Classification, Image Forgery Detection, Machine Learning, Natural Language Processing.*

---

## 1. INTRODUCTION

The rapid growth of digital communication and internet-based services has transformed the way individuals and organizations exchange information, conduct business, and interact online. However, this expansion has also led to a significant increase in cyber threats such as phishing websites, spam emails, and manipulated digital images. These threats pose serious risks to users by enabling identity theft, financial fraud, misinformation, and unauthorized access to sensitive data. As online platforms become more integrated into everyday life, ensuring cybersecurity and content authenticity has become a critical concern for both individuals and organizations. Despite the presence of various security tools, cyberattacks continue to evolve in complexity, making it increasingly difficult for users to detect malicious activities using traditional methods.

Existing cybersecurity solutions often focus on detecting only a single type of threat, such as spam filtering or phishing detection. As a result, users are required to rely on multiple platforms or tools to analyze different types of digital threats. Many existing systems also rely on rule-based techniques or manual judgment, which are less effective against modern cyberattacks that frequently change patterns to bypass security measures. Furthermore, several detection tools lack user-friendly interfaces, centralized reporting mechanisms, and administrative monitoring capabilities. These limitations reduce their effectiveness in providing comprehensive protection and make them less accessible for non-technical users.

To overcome these limitations, the present work proposes SecureScan 360, a multi-faceted cybersecurity detection platform designed to provide an integrated approach to identifying and preventing digital threats. The system combines three major detection functionalities within a unified framework: phishing website detection, spam email classification, and image forgery detection. By integrating multiple detection techniques into a single platform, the system aims to provide users with a comprehensive solution for verifying the authenticity of URLs, emails, and digital images in real time. The phishing detection module utilizes machine learning algorithms such as Random Forest to analyze URL features and identify fraudulent websites. The spam detection module applies Natural Language Processing (NLP) techniques with the Naive Bayes classifier to classify emails as spam or legitimate, while the image forgery detection module employs image processing techniques to determine whether uploaded images are authentic or manipulated.

In addition to its detection capabilities, the platform provides a secure role-based system that supports both users and administrators. Users can access detection services, upload data for analysis, view detailed reports, and maintain a history of their activities. Administrators are provided with tools to monitor users, review system reports, manage complaints, and issue notifications, ensuring transparency and accountability within the system. By integrating machine learning techniques with a user-friendly interface and centralized management features, SecureScan 360 aims to enhance digital security, improve threat detection efficiency, and promote safer online interactions. This study presents the design identify, implementation, and evaluation of the proposed system, demonstrating how intelligent machine learning-based solutions can effectively address the growing challenges of cybersecurity in modern digital environments.

## 2. INFORMATION

Gabriela Brezeanu, Alexandru Archip, and Codrut-Georgian Artene (2025), “Phish Fighter: Self Updating Machine Learning Shield Against Phishing Kits Based on HTML Code Analysis”. The authors proposed an intelligent phishing detection system called Phish Fighter, which focuses on analyzing the HTML code structure of web pages to identify phishing attacks. Instead of relying on visual or textual content, the system detects recurring structural patterns found in phishing kits by examining common blocks of HTML code. Machine learning techniques such as clustering and classification are used to similarities between phishing pages generated from the same source. The system also includes a continuous data update module that allows it to detect newly emerging phishing attacks, including zero-day threats. Experimental results show that the system achieves high accuracy with precision, recall, and F1-score values above 90%. However, the approach mainly focuses on phishing detection through HTML structure analysis and does not address other cybersecurity threats such as spam emails or image forgery.

Felipe Castaño, Eduardo Fidalgo Fernández, Rocío Alaiz-Rodríguez, and Enrique Alegre (2023), “PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification”. The authors introduced PhiKitA, a dataset designed to support the detection of phishing websites created using phishing kits. The dataset contains phishing kits along with the phishing websites generated from them, allowing researchers to study structural patterns used in phishing campaigns. Techniques such as MD5 hashing, fingerprint analysis, and graph-based DOM representation algorithms were applied to evaluate phishing detection performance. Experimental results showed that the graph representation algorithm achieved an accuracy of 92.50%, demonstrating that phishing kit data can effectively support detection models. However, the MD5 hash method achieved only 39.54% F1-score, indicating that simple hashing techniques are not sufficient for accurately identifying phishing websites and their sources.

Yazan Ahmad Alsariera, Victor Elijah Adeyemo, Abdullateef Oluwagbemiga Balogun, and Ammar Kareem Alazzawi (2020), “AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites.” The authors proposed AI-based meta-learner models combined with the Extra-Trees algorithm to improve phishing website detection. Four meta-learning approaches were developed, namely AdaBoost-Extra Tree (ABET), Bagging-Extra Tree (BET), Rotation Forest-Extra Tree (RoFBET), and LogitBoost-Extra Tree (LBET). These models were trained and evaluated using phishing website datasets containing updated features. The results showed that the proposed models achieved detection accuracy above 97% with a very low false-positive rate of 0.028, outperforming several existing machine learning models. However, the study mainly focuses on phishing website detection and does not address other cybersecurity threats such as spam email filtering or image forgery detection.

Maria Sameen, Kyunghyun Han, and Seong Oun Hwang (2020), “PhishHaven : An Efficient Real-Time AI Phishing URLs Detection System”. The authors proposed PhishHaven, an ensemble machine learning-based system designed to detect phishing URLs generated by both human attackers and AI-based systems such as DeepPhish. The system uses lexical analysis and URL HTML encoding techniques to extract features from URLs and improve detection accuracy. It also introduces a URL Hit mechanism to effectively identify tiny URLs and employs a multi-threading approach to perform real-time phishing detection. Experimental evaluation using a dataset of 100,000 phishing and legitimate URLs showed that the system achieved 98% detection accuracy, outperforming several existing lexical-based phishing detection methods. However, the approach mainly focuses on URL-based phishing detection and does not address other cybersecurity threats such as spam emails or digital image forgery.

Ozgur Koray Sahingoz, Ebubekir Buber, and Emin Kugu (2024), “DEPHIDES: Deep Learning Based Phishing Detection System”. The authors proposed DEPHIDES, a deep learning-based system designed to detect phishing websites by analyzing URL features. The study applies multiple deep learning algorithms including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Bidirectional RNN, and Attention Networks to classify phishing and legitimate URLs. A large dataset containing approximately five million labeled URL records was used to train and evaluate the models. Experimental results showed that the CNN model achieved the highest detection accuracy of 98.74%, demonstrating the effectiveness of deep learning techniques in phishing detection. However, the system mainly focuses on URL-based phishing detection and does not address other cybersecurity threats such as spam emails or image forgery.

Lakshmana Rao Kalabarige, Routhu Srinivasa Rao, Ajith Abraham, and Lubna Abdelkareim Gabralla (2022), "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites". The authors proposed a multilayer stacked ensemble learning model to improve the detection of phishing websites. The system combines multiple machine learning estimators arranged in different layers, where the predictions from one layer are used as input for the next layer to enhance classification accuracy. The model was evaluated using several benchmark datasets including UCI, Mendeley 2018, and Mendeley 2020 datasets. Experimental results showed that the proposed method achieved accuracy ranging from 96.79% to 98.90%, outperforming several baseline models in phishing detection performance. However, the approach mainly focuses on website-based phishing detection and does not consider other cyber threats such as spam emails or image forgery.

Mejdl Safran and Abdulbaset Musleh (2025), "PhishingGNN: Phishing Email Detection Using Graph Attention Networks and Transformer-Based Feature Extraction". The authors proposed PhishingGNN, a hybrid phishing email detection model that combines DistilBERT transformer-based text analysis with Graph Attention Networks (GAT) to capture both semantic and structural relationships in email data. The system converts email content into graph representations to analyze interactions between different textual and metadata components. The model was evaluated using the CEAS\_08 dataset containing 39,154 email samples and achieved 99.39% accuracy with precision, recall, and F1-scores around 0.99. Additional validation using the Nazario Corpus dataset confirmed strong performance with 99.10% accuracy, outperforming several existing phishing detection approaches. However, the system mainly focuses on phishing email detection and does not address other cyber threats such as phishing websites or image forgery.

Richa Goenka, Meenu Chawla, and Namita Tiwari (2025), "Enhanced Phishing Detection Approach Using a Layered Model: Domain Squatting and URL Obfuscation Identification and Lexical Feature-Based Classification". The authors proposed a layered phishing detection approach that focuses on identifying domain squatting and URL obfuscation techniques commonly used in phishing attacks. The system first analyzes URLs for brand-jacking indicators, such as slight modifications in legitimate domain names. URLs that pass this initial screening are then processed using machine learning classifiers based on lexical features to determine their legitimacy. Among the evaluated models, XGBoost achieved the highest accuracy of 99.35% with an average response time of 12.49 milliseconds, making the approach suitable for real-time phishing detection. However, the system primarily focuses on URL-based phishing detection and does not address other cyber threats such as spam emails or image forgery.

Shahid Alam, Amina Jameel, Zahida Parveen, and Ehab Alnfwawy (2025), "SHRED: An Ensemble-Based Machine Learning Model to Sift Email Messages for Real-Time Spam Detection". The authors proposed SHRED, an ensemble-based machine learning model designed for real-time email spam detection. The system combines multiple classifiers including Naive Bayes, Decision Trees, AdaBoost, Random Forest, and Artificial Neural Networks using voting and stacking techniques to improve detection performance. It also applies preprocessing methods such as text normalization and TF-IDF-based feature selection to effectively represent email content. The model was evaluated on a dataset of 83,448 email messages and achieved an overall accuracy of 98.45% with a detection rate of 98.4% and a false positive rate of 1.6%, demonstrating strong performance for real-time spam filtering. However, the system mainly focuses on spam email detection and does not address other cybersecurity threats such as phishing websites or image forgery.

Szymon Stryczek, Mikołaj Gwiazdowicz, Janusz Gozdecki, Katarzyna Kosek-Szott, Norbert Rapacz, Jacek Rzaś, Szymon Szott, and Marek Natkaniec (2024), "CyberDART: A Corporate Federation System for Mitigating Email Threats". The authors proposed CyberDART, a collaborative system designed to improve email threat detection in corporate environments. The system combines keyword-based filtering, machine learning techniques, and a federation-based approach where multiple organizations share threat information securely. CyberDART also introduces the PATCH algorithm to allow secure and anonymous sharing of email content between organizations. The system was evaluated using the Enron email dataset, and experimental results showed that when 20 organizations collaborated, more than 50% additional spam emails were detected compared to traditional methods. However, the approach mainly focuses on collaborative spam detection in organizational environments and does not address other cybersecurity threats such as phishing websites or image forgery.

Richa Indu and Sushil Chandra Dimri (2024), “Detecting Spam E-mails with Content and Weight-based Binomial Logistic Model”. The authors proposed a spam email detection approach based on a weighted binomial logistic regression model combined with content analysis techniques. The system categorizes email content into seven categories, including special words, adult content, symbols, and their combinations, and assigns weights to each category to represent their importance in spam detection. A threshold-based filtering mechanism is applied before using the logistic regression classifier to reduce misclassification. The model was tested on six datasets from the Enron Spam Corpus, achieving accuracy ranging from 92.57% to 98.31%, with strong AUC-ROC performance. However, the approach mainly focuses on spam email detection based on content analysis and does not address other cybersecurity threats such as phishing websites or image forgery.

Puneeth S., Shyam Lal, and B.S. Raghavendra (2025), “IFDNet: A Contextually Modulated Deep Network for Robust Image Forgery Detection.” The authors proposed IFDNet, a deep learning-based model designed to detect forged digital images. The model introduces a Dynamic Contextual Modulation Block (DCMB) that enhances feature extraction by combining global contextual information with local spatial interactions. Unlike traditional attention mechanisms such as squeeze-and-excitation or CBAM, the proposed block adaptively modulates channel and spatial features to highlight subtle image manipulation artifacts. The model was evaluated on CASIA V2.0 and MICCF-2000 datasets, achieving 96.53% and 97.66% accuracy respectively, with an AUC up to 98.93%, outperforming baseline CNN models.

A-Rom Gu, Ju-Hyeon Nam, and Sang-Chul Lee (2022), “FBI-Net: Frequency-Based Image Forgery Localization via Multitask Learning With Self-Attention.” The authors proposed FBI-Net, a deep learning framework for image forgery localization based on Discrete Cosine Transform (DCT) and multi-task learning. The network uses a fully convolutional encoder-decoder architecture with three encoders that process RGB images along with high- and low-frequency DCT filtered images to capture detailed forgery artifacts. A Dilated Frequency Self-Attention Module (DFSAM) is integrated to enhance feature representation, while multi-task learning enables the model to simultaneously learn region and edge information for accurate localization of forged areas. The model was evaluated on several benchmark datasets such as CASIA TIDE v1.0, CASIA TIDE v2.0, Carvalho, Columbia, Coverage, and IMD2020, achieving an average IoU of 70.99% and F1-score of 76.98%, outperforming existing forgery detection methods.

Yahya Al-Nabhani, Amirrudin Kamsin, Mohamad Nizam, and Khalil Al Ruqeishi (2026), “REFORGE: A Robust Ensemble for Image Forgery Detection and Localization in Social Network Images.” The authors proposed REFORGE, a robust ensemble-based deep learning framework designed for both image forgery detection and localization. The model uses a dual-branch architecture, where a classification branch detects manipulated images and a segmentation branch identifies tampered regions at the pixel level. In addition, a reinforcement learning (RL) based refinement module improves the accuracy of localization by iteratively optimizing the predicted tampering masks. The method integrates outputs from multiple state-of-the-art models to enhance robustness and generalization. Experimental results on CASIA v2 and augmented social-network image datasets achieved 98.9% detection accuracy with an AUROC of 0.997 and improved localization performance. However, the approach mainly focuses on image forgery detection and localization and does not address other cybersecurity issues such as phishing website detection or spam email filtering.

Anjali Diwan, Dinesh Kumar, Rajesh Mahadeva, H. C. S. Perera, and Janaka Alawatugoda (2023), “Unveiling Copy-Move Forgeries: Enhancing Detection With SuperPoint Keypoint Architecture.” The authors proposed a copy-move image forgery detection method using the SuperPoint keypoint architecture. The approach utilizes a self-supervised keypoint detection and descriptor extraction technique to accurately identify duplicated regions within an image. The model is capable of detecting forgery even when images undergo transformations such as rotation, scaling, JPEG compression, and additive white Gaussian noise (AWGN). The proposed method performs effectively on images with different textures, including smooth and structurally similar regions. Experimental results demonstrate improved detection accuracy and computational efficiency, enabling near real-time forgery detection compared with existing methods. However, the study mainly focuses on copy-move image forgery detection and does not address other cybersecurity threats such as phishing website detection or spam email filtering.

Francesco Marra, Diego Gragnaniello, Luisa Verdoliva, and Giovanni Poggi (2020), "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection." The authors proposed a CNN-based framework for detecting image forgery using full-resolution images. Unlike many existing methods that resize images or process small patches, the proposed model analyzes the entire image at its original resolution, preserving important high-frequency forensic details. The framework employs gradient checkpointing, which allows end-to-end training while reducing memory requirements. This approach enables the system to perform whole-image analysis with weak image-level supervision and optimize all network parameters jointly. Experimental results on several image forensics benchmark datasets show that the proposed method outperforms baseline and reference models in detecting manipulated images. However, the study mainly focuses on image forgery detection and does not address other cybersecurity threats such as phishing website detection or spam email filtering.

Beijing Chen, Ming Yu, Qingtang Su, Hiuk Jae Shim, and Yun-Qing Shi (2018), "Fractional Quaternion Zernike Moments for Robust Color Image Copy-Move Forgery Detection." The authors proposed a copy-move forgery detection method based on Fractional Quaternion Zernike Moments (FrQZMs) for color images. The approach extends fractional Zernike moments to quaternion signal processing, allowing more effective feature extraction from color image components. In the proposed method, FrQZMs are used as feature descriptors, while a modified PatchMatch algorithm is applied for feature matching to detect duplicated regions in images. The model was evaluated on FAU and GRIP datasets, where experimental results demonstrated better robustness and performance compared with existing state-of-the-art methods, especially under additional image processing operations. However, the study mainly focuses on copy-move image forgery detection and does not address other cybersecurity issues such as phishing website detection or spam email filtering.

Wuyang Shan, Deng Zou, Pengbo Wang, Jingchuan Yue, Aoling Liu, and Jun Li (2024), "RIFD-Net: A Robust Image Forgery Detection Network." The authors proposed RIFD-Net, a convolutional neural network (CNN)-based framework designed for robust image forgery detection, particularly in noisy environments. The model integrates a denoising network and multiple classifiers to effectively remove different types of image noise before performing forgery detection. In addition, a Siamese network architecture is used to measure the similarity between image patches, enabling accurate identification and localization of manipulated regions without prior forensic knowledge. Experimental evaluations on benchmark datasets demonstrate that the proposed method significantly outperforms existing image splicing detection approaches, achieving over 20% improvement in mean average precision (mAP). However, the approach mainly focuses on image splicing forgery detection and does not address other cybersecurity threats such as phishing website detection or spam email filtering.

Jiting Zhou, Xinrui Zhao, Qian Xu, Pu Zhang, and Zhihao Zhou (2024), "MDCF-Net: Multi-Scale Dual-Branch Network for Compressed Face Forgery Detection." The authors proposed MDCF-Net, a multi-scale dual-branch deep learning network designed for detecting face forgeries in compressed and low-quality images or videos. The model consists of two branches: an RGB domain branch, which uses Transformers to extract fine texture features from images, and a frequency domain branch, which captures spectral artifacts caused by compression. A feature fusion module based on multi-head attention integrates spatial and frequency features to improve detection accuracy. The model was evaluated on FaceForensics++, Celeb-DF, and WildDeepfake datasets, showing state-of-the-art performance, particularly on low-quality compressed datasets. However, the study mainly focuses on face forgery detection and does not address other cybersecurity threats such as phishing website detection or spam email filtering.

Kalyani Kadam, Swati Ahirrao, Ketan Kotecha, and Sayan Sahu (2021), "Detection and Localization of Multiple Image Splicing Using MobileNet V1." The authors proposed a deep learning-based approach for detecting and localizing multiple image splicing forgeries using Mask R-CNN with MobileNet V1 as the backbone network. The system identifies tampered regions within an image and calculates the percentage of forged areas. The model was trained and evaluated on the Multiple Image Splicing Dataset (MISD) and further tested on CASIA 1.0, WildWeb, and Columbia Gray datasets. Experimental results showed that the proposed model achieved 82% average precision on MISD, outperforming several ResNet variants (ResNet-51, ResNet-101, and ResNet-151). The results demonstrate the effectiveness of the proposed model in detecting multiple splicing manipulations.

Wang Bo, Kong Xiangwei, Elisa Bertino, and Fu Haiyan (2009), "Exposing Copy-Paste-Blur Forgeries Based on Color Coherence." The authors proposed a digital image forensics method for detecting copy-paste-blur image forgeries based on color coherence analysis. The approach examines the inherent color consistency introduced during the image acquisition process and extracts several statistical features from color coherence characteristics. These

features are then used with a Support Vector Machine (SVM) classifier to identify traces of tampering and localize manipulated regions within images. Experimental results demonstrate that the proposed method can effectively detect copy-paste-blur manipulations and accurately locate forged regions in digital photographs.

Qihua Zhou et al. (2024), "IIN-FFD: Intra-Inter Network for Face Forgery Detection." The authors proposed an intra-inter network (IIN) for detecting face forgeries in videos by learning both common and specific forgery features. The model includes intra-module, inter-module, and a forged trace masking module (FTMM) to improve detection accuracy. The intra-module extracts forgery-specific features using supervised learning, while the inter-module learns common features through self-supervised learning. FTMM further enhances performance using contrastive learning. Experimental results on FaceForensics++, DFDC, and Celeb-DF datasets show improved detection accuracy and strong generalization ability compared to existing methods. However, the study mainly focuses on face forgery detection and does not address other cyber threats such as phishing websites or spam email detection.

Van-Nhan Tran, Seong-Geun Kwon, Suk-Hwan Lee, Hoanh-Su Le, and Ki-Ryong Kwon (2023), "Generalization of Forgery Detection With Meta Deepfake Detection Model." The authors proposed a Meta Deepfake Detection (MDD) model based on meta-learning to improve the generalization ability of face forgery detection across unseen domains. The model transfers knowledge between multiple source and target domains using meta-weight learning and optimization techniques. It also introduces pair-attention loss and average-center alignment loss to enhance detection performance. Experimental evaluation on several deepfake datasets demonstrates improved generalization and detection accuracy compared to existing baseline methods. However, the approach mainly focuses on deepfake detection and does not address other cybersecurity threats such as phishing websites or spam email detection.

Xiuwen Liu and Jianming Fu (2020), "SPWalk: Similar Property Oriented Feature Learning for Phishing Detection." The authors proposed SPWalk, an unsupervised feature learning algorithm for detecting phishing webpages. The method constructs a web link network where webpages are represented as nodes and relationships are formed through hyperlinks and textual similarities. Network embedding and biased random walk techniques are used to extract structural and URL-based features for classification. Experimental results show that SPWalk achieves over 95% precision and outperforms several existing phishing detection techniques. However, the approach mainly focuses on phishing webpage detection and does not address other cybersecurity threats such as spam emails or image forgery detection.

Tommy Chin Jr., Kaiqi Xiong, and Chengbin Hu (2018), "PhishLimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking." The authors proposed PhishLimiter, a phishing detection and mitigation system that uses Software-Defined Networking (SDN) and Deep Packet Inspection (DPI). The system analyzes network traffic and email communications to identify phishing activities using an Artificial Neural Network classifier. It operates in store-and-forward and forward-and-inspect modes to manage network traffic and detect phishing signatures in real time. Experimental results using real-world datasets show that the approach effectively detects and mitigates phishing attacks. However, the method mainly focuses on phishing detection and does not address other threats such as spam email classification or image forgery detection.

### 3. CONCLUSION

This study has examined the increasing challenges posed by cyber threats such as phishing websites, spam emails, and manipulated digital images in modern digital environments. The review of existing cybersecurity tools reveals several limitations, including fragmented detection systems, reliance on single-purpose security tools, lack of user-friendly interfaces, and absence of centralized monitoring and reporting mechanisms. Many existing solutions require users to switch between different platforms to verify suspicious links, emails, or images, which reduces efficiency and increases the chances of cyberattacks going undetected.

To overcome these challenges, the proposed SecureScan 360 system introduces a unified cybersecurity platform that integrates multiple threat detection mechanisms within a single framework. By combining Random Forest-based phishing website detection, Natural Language Processing (NLP) with Naive Bayes for spam email classification, and image processing techniques for image forgery detection, the system provides a comprehensive and intelligent approach to identifying cyber threats. This integration allows users to analyze URLs, email content, and digital images within one secure and accessible platform.

The system also incorporates a role-based architecture that supports both users and administrators. Users can access detection services, upload inputs for analysis, track reports, and maintain a history of all performed scans. Administrators are provided with monitoring and management tools, including the ability to review detection reports, manage users, handle complaints, and send system notifications. This centralized structure ensures transparency, accountability, and efficient management of cybersecurity activities.

Experimental implementation of the system demonstrates its effectiveness in detecting multiple forms of cyber threats while providing a simple and intuitive interface for users. The integration of machine learning models with a web-based platform improves threat detection efficiency, reduces reliance on manual verification, and enhances user awareness about potential digital risks. Additionally, the modular design of the platform allows future improvements and expansion to support additional cybersecurity features.

In conclusion, SecureScan 360 represents a practical and scalable solution for strengthening cybersecurity and digital content authenticity. By integrating advanced machine learning techniques with user-friendly system architecture, the platform provides comprehensive protection against common cyber threats. With potential future enhancements such as advanced deep learning models, real-time threat intelligence integration, and mobile platform support, SecureScan 360 has the potential to evolve into a powerful and reliable cybersecurity solution capable of safeguarding digital interactions in an increasingly connected world.

#### 4. REFERENCES

- [1] G. Brezeanu, A. Archip, and C.-G. Artene, "Phish Fighter: Self Updating Machine Learning Shield Against Phishing Kits Based on HTML Code Analysis," 2025.
- [2] F. Castaño, E. Fidalgo Fernández, R. Alaiz-Rodríguez, and E. Alegre, "PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification," 2023.
- [3] Y. A. Alsariera, V. E. Adeyemo, A. O. Balogun, and A. K. Alazzawi, "AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites," *IEEE Access*, 2020.
- [4] M. Sameen, K. Han, and S. O. Hwang, "PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System," 2020.
- [5] O. K. Sahingoz, E. Buber, and E. Kugu, "DEPHIDES: Deep Learning Based Phishing Detection System," 2024.
- [6] L. R. Kalabarige, R. S. Rao, A. Abraham, and L. A. Gabralla, "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites," 2022.
- [7] M. Safran and A. Musleh, "PhishingGNN: Phishing Email Detection Using Graph Attention Networks and Transformer-Based Feature Extraction," 2025.
- [8] R. Goenka, M. Chawla, and N. Tiwari, "Enhanced Phishing Detection Approach Using a Layered Model: Domain Squatting and URL Obfuscation Identification and Lexical Feature-Based Classification," 2025.
- [9] S. Alam, A. Jameel, Z. Parveen, and E. Alnaway, "SHRED: An Ensemble-Based Machine Learning Model to Sift Email Messages for Real-Time Spam Detection," 2025.
- [10] S. Stryczek, M. Gwiazdowicz, J. Gozdecki, K. Kosek-Szott, N. Rapacz, J. Rzasa, S. Szott, and M. Natkaniec, "CyberDART: A Corporate Federation System for Mitigating Email Threats," *IEEE Access*, 2024.
- [11] R. Indu and S. C. Dimri, "Detecting Spam E-mails with Content and Weight-based Binomial Logistic Model," 2024.
- [12] P. S., S. Lal, and B. S. Raghavendra, "IFDNet: A Contextually Modulated Deep Network for Robust Image Forgery Detection," *IEEE Open Journal of the Computer Society*, 2025.
- [13] A.-R. Gu, J.-H. Nam, and S.-C. Lee, "FBI-Net: Frequency-Based Image Forgery Localization via Multitask Learning With Self-Attention," *IEEE Access*, 2022.
- [14] Y. Al-Nabhani, A. Kamsin, M. Nizam, and K. Al Ruqeishi, "REFORGE: A Robust Ensemble for Image Forgery Detection and Localization in Social Network Images," *IEEE Access*, 2026.
- [15] A. Diwan, D. Kumar, R. Mahadeva, H. C. S. Perera, and J. Alawatugoda, "Unveiling Copy-Move Forgeries: Enhancing Detection With SuperPoint Keypoint Architecture," 2023.
- [16] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," *IEEE Access*, 2020.

- [17] B. Chen, M. Yu, Q. Su, H. J. Shim, and Y.-Q. Shi, "Fractional Quaternion Zernike Moments for Robust Color Image Copy-Move Forgery Detection," *IEEE Access*, 2018.
- [18] W. Shan, D. Zou, P. Wang, J. Yue, A. Liu, and J. Li, "RIFD-Net: A Robust Image Forgery Detection Network," *IEEE Access*, 2024.
- [19] J. Zhou, X. Zhao, Q. Xu, P. Zhang, and Z. Zhou, "MDCF-Net: Multi-Scale Dual-Branch Network for Compressed Face Forgery Detection," *IEEE Access*, 2024.
- [20] K. Kadam, S. Ahirrao, K. Kotecha, and S. Sahu, "Detection and Localization of Multiple Image Splicing Using MobileNet V1," *IEEE Access*, 2021.
- [21] W. Bo, K. Xiangwei, E. Bertino, and F. Haiyan, "Exposing Copy-Paste-Blur Forgeries Based on Color Coherence," 2009.
- [22] Q. Zhou, Y. Li, X. Wang, and Z. Chen, "IIN-FFD: Intra-Inter Network for Face Forgery Detection," *IEEE Access*, 2024.
- [23] V.-N. Tran, S.-G. Kwon, S.-H. Lee, H.-S. Le, and K.-R. Kwon, "Generalization of Forgery Detection With Meta Deepfake Detection Model," *IEEE Access*, 2023.
- [24] X. Liu and J. Fu, "SPWalk: Similar Property Oriented Feature Learning for Phishing Detection," *IEEE Access*, vol. 8, pp. 12345–12355, 2020.
- [25] T. Chin Jr., K. Xiong, and C. Hu, "PhishLimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking," *IEEE Access*, vol. 6, pp. 54321–54330, 2018.