International Journal of Multidisciplinary Global Research
Vol. 01 (04), Oct-Dec 2024, pp. 86-99.
Online ISSN: 3107-4197

The Hacker Eye

NILESH KHODIFAD*
Parul Institute of Engineering and Technology, Parul University
Vadodara (Gujarat) - 391760, India
nkhodifad@gmail.com

SUMERSING DAYARAM PATIL
Parul Institute of Engineering and Technology, Parul University
Vadodara (Gujarat) - 391760, India
sumerpatil75@gmail.com

AKRUTI PANDWAL
Parul Institute of Engineering and Technology, Parul University
Vadodara (Gujarat) - 391760, India
akrutiladdha@gmail.com

SYED IBAD ALI
Parul Institute of Engineering and Technology, Parul University
Vadodara (Gujarat) - 391760, India
ibad85@gmail.com

KUSH BHUSHANWAR
Parul Institute of Engineering and Technology, Parul University
Vadodara (Gujarat) - 391760, India
kush.bhushanwar@gmail.com

BHAVESH ATULBAHI VAGHELA
Parul Institute of Engineering and Technology, Parul University
Vadodara (Gujarat) - 391760, India
vaghelabhavesh404@gmail.com

Abstract

As the hacker eye is a concept of significant risk to internet safety, the hacker eye tries to deprive gullible consumers of private information. Phishing websites are the threat that researchers are trying to fight, and various techniques for detecting phishing websites have been developed, such as machine learning algorithms. It is possible to train a machine learning system to distinguish between legal and fraudulent websites by analyzing their patterns and traits. Once identified and blocked, these algorithms can be used to find and prey on phishing Web sites while users are still unscathed. A

* Corresponding Author.

machine learning approach to detecting Hacker Eye website phishing websites is feature extraction, where, through a set of features regarding a website, such as URL structure, domain age, and content, the ideas around these features are used to identify such websites. The other approach involves using deep learning algorithms to autonomously extract characteristics and detect complex patterns in the data collected from the company's website. There is hope for phishing website detection algorithms based on machine learning as these methods can achieve accuracies that are on par with or better than rule-based approaches. However, with further research and development, these techniques could become a powerful weapon in anyone's arsenal when fighting against online phishing attacks.

Keywords: AdaBoost, Gradient Boosting, Hybrid Module Evaluation, Random Forest, SVM, Voting classifier, XGBoost.

1. Introduction

Websites attempting to steal sensitive information, such as login passwords, credit card numbers, and personal identity data, are detected and flagged by the Hacker Eye website detection process. These fraudulent websites use exact replicas of legitimate ones. The sophistication of phishing assaults has increased over time, and attackers often use tactics such as social engineering and fake login screens to trick users into giving up their sensitive information. Hacker Eye websites also may employ URL spoofing to trick the user into thinking they are on a legitimate.

The standard type of cybercrime is phishing, where the attacker poses as one and sends fraudulent emails and messages to steal sensitive information through their phishing attacks. The most effective defense against phishing assaults is the ability to filter and prevent phishing websites. Hacker Eye identifies and flags websites that trick consumers using various technologies and tactics. Attackers also use one common technique to create websites similar to the appearance of genuine sites like banks or e-commerce sites. These are often hosted on compromised servers or by domain names that are close copies of the authentic sites (J. Shad and S. Sharma, 2018).

One way to combat this problem is to improve machine learning algorithms that can analyze website metadata, content, and other features to detect Hacker Eye phishing sites is one way to combat this problem. We can train these algorithms on datasets of known Hacker Eye websites to learn the common patterns and various characteristics of Hacker Eye websites. Some machine learning models may also be fed with real-time indicators to find and mark suspicious sites as they appear.

Another solution to phishing website detection is reputation-based systems, which keep lists of known malicious websites. These systems can use a score of sources of information like blocklists, user reports, and threat intelligence feeds to identify and block phishing sites. Some web browsers also use reputation-based systems to warn users when a new site is accessed, known as phishing. Other techniques that can work in Hacker Eye detection include behavioral analysis, utilizing which unusual or suspicious activities on a website may be detected (Y. Sonmez, 2018).

For instance, these techniques may look for deviations from normal user behavior, such as a spike of user login credentials or a high spate of redirects to other sites. The Hacker Eye websites can be detected and blocked as part of an effective cyber security scheme. Organizations can protect their users and keep sensitive information from falling into the hands of attackers by using a blend of machine learning algorithms, reputation-based systems, and behavioral analysis techniques. It makes it bright to watch the latest phishing threat trends and detection methods (T. Peng, 2018).

1.1. *Problem Statement*

There's currently an exponential proliferation of phishing websites, which utilize the availability of resources offered via digital platforms. Unfortunately, traditional detection based on predetermined rules has not been sufficient due to its increasing sophistication by cyber criminals. Thus, creating a more adaptable, proactive, and responsive phish website identification approach in real-time is challenging.

1.2. *Objectives*

The main aim is to leverage Machine Learning and develop a reliable Hacker Eye website detection system. The project will train models with massive datasets to get high classification accuracies and distinguish between legitimate and phishing websites.

2. Literature Review

2.1. *Introduction to Phishing and Detection Challenges*

Because phishers construct phony websites to steal vital information like passwords, credit card data, and personal details, they pose a serious threat to users. Over time, the attacks have evolved, making detection more complex. Traditional rule-based systems are typically inefficient in processing phishing techniques' flexible and changing nature (M. Karabatak, 2018).

Many recent studies reveal that machine learning (ML) is a more robust mechanism for phishing detection based on applying ML techniques to recognize the fine-grained structure of website features, characterizing possible phishing sites (S. Parekh, 2018).

2.2. *Feature Selection and Data Representation*

Several research efforts have appeared to attempt to discover the critical features distinguishing phishing websites from legitimate ones. Some commonly used features are as follows: URL length, domain age, the presence of memorable characters, and SSL certificate details. For example, (Shaikh, 2024) analyzes the lexical features of URLs and integrates them alongside content-based attributes like HTML structure and JavaScript behavior. Feature extraction is a key step in building a strong phishing

detection model, and feature engineering often makes or breaks the model (Ali, 2024).

2.3. *Machine Learning Algorithms for Phishing Detection*

Phishing detection has applied several machine learning algorithms, which have had varying success. In the comparative research, the authors (Shaikh, Mohammad Shahnawaz, 2024) tested several ensemble learning approaches, such as AdaBoost and XGBoost, decision trees, support vector machines (SVM), and random forests.

Ensemble methods always perform better than individual classifiers because they can reduce errors by combining a set of weak learners. Another study applied deep learning techniques and showed that deep learning networks can capture more complex patterns in phishing websites than traditional algorithms (Mungale, 2024).

2.4. *Evaluation Metrics and Model Performance*

Evaluating the performance of phishing detection algorithms is vital since it is difficult to assess their efficacy in real-world scenarios. The F1 score, ROC-AUC curve analysis, accuracy, precision, and recall are typical metrics in the literature. While pinpoint precision is critical, maintaining a healthy ratio of false positives to false negatives is paramount (Sheikh, M.S., 2024). A high false positive rate can create trust problems, and a high false negative rate permits phishing attacks to bypass detection (Preeti Chopkar, 2024).

2.5. *Recent Advances and Future Directions*

With the advances in natural language processing (NLP) and graph-based models, recent work in phishing detection has been combining machine learning and graph-based models. Detecting phishing using NLP will attempt to analyze suspicious textual content inside websites, while graph-based models can determine malicious network links (Himanshu Kitey, 2024).

In addition, the promise of hybrid approaches involving multiple machine learning models (stacking, voting) in detecting images with resolution ambiguity has also resulted in higher detection rates. Future research could be based on a real-time phishing detection approach using adaptive learning systems and exploring reinforcement learning in ever-changing attack scenarios (Mohammad Shahnawaz Shaikh, 2016).

2.6. *Ethical Hacking: An Impact on Society*

Ethical hacking is carried out by testing the weaknesses & vulnerabilities in the system or a computer network. A word to explain how to trick a network in the right way. It's a good thing the ethical hacker is doing it. It's become popular in our mind that if we think of someone as a hacker, he should be immoral, fanatic, criminal, and unethical (Ali, Syed Ibad, 2025).

Some hackers have caused serious harm to some organizations by stealing critical consumer data. In particular, government organizations have harmed sensitive information, including social security numbers. That is why hackers are not gaining a good reputation. Many organizations try to reduce the probability of such conditions by employing ethical hackers to be in touch with their systems and computer networks (Ali, Syed Ibad, and Mohammad Shahnawaz Shaikh, 2025).

3. Methodology

The methodology for this Phishing Website Detection Using Machine Learning project is divided into several key steps, each focusing on building a robust system for identifying phishing websites using various machine learning algorithms. Below is an overview of the methodology.

3.1. *Data Collection and Preprocessing*

3.1.1. *Data Collection*

- The dataset, containing phishing and legitimate website information, was sourced from a trusted platform (Kaggle).
- The raw data was inspected and cleaned by handling missing values and removing unnecessary columns.

3.1.2. *Feature Selection*

- Relevant features that could help identify phishing websites were selected, including URL structure, domain-related attributes, and website content features.
- Unwanted columns were removed to reduce noise and improve model performance enumerate environment (S. Singh, 2024).

3.1.3. *Data Splitting*

- The training set comprised 80% of the dataset, whereas the testing set comprised 20%.
- It ensures the model can generalize well on unseen data. The features were stored separately (X for features, y for the target labels).

3.2. *Model Implementation*

Several machine learning algorithms were tried to find phishing websites. These include:

(1) **Random Forest Classifier**: An ensemble learning method that builds several decision trees and makes predictions using majority voting. It is known for working well on large data sets and not overfitting.\item command.

(2) **AdaBoost Classifier**: It is a boosting algorithm that sequentially builds models, correcting errors of previous models and attending to the most misclassified instances for that final performance.
(3) **XGBoost Classifier**: An optimized gradient boosting algorithm for speed and accuracy. The regularization techniques XGBoost uses to prevent overfitting means that it is used very widely.
(4) **Support Vector Classifier (SVC)**: It is a linear kernel-based classifier that tries to find the hyperplane that separates the data more effectively between legitimate and phishing websites.
(5) **Gradient Boosting Classifier**: A different boosting algorithm to build a set of models iteratively to correct the errors made by preceding models. It can be used primarily for classification problems, but we must ensure it does not overfit.
(6) **Stacking Classifier**: An ensemble method trains several base classifiers (Random Forest, XGBooster) to create predictions and merge them in their meta type for the final classification step.
(7) **Voting Classifier**: This method aggregates the predictions given by several classifiers and makes the final decision by applying majority voting (M. S. Shaikh, K. Bhushanwar, 2024).

3.3. *Model Evaluation*

Each model was assessed using independent performance metrics such as F1 score, recall, accuracy, and precision. The model's ability to distinguish between phishing and genuine websites is evaluated statistically. Confusion matrices were also used, which displayed the number of false positives and true negatives and each model's performance relative to the others (Mohammad Shahnawaz Shaikh, 2016).

3.4. *Model Comparison*

Models were compared by the precision and capacity of both phishing and legitimate websites. Random Forest, XGBoost, and ensemble-based models such as Stacking and Voting Classifiers performed the best with the highest accuracy and balanced performance for both classes (Mohammad Shahnawaz Shaikh, 2019).

3.5. *Model Saving*

Then, Models were trained and evaluated, and the model was saved using joblib for future use. It enables the deployment of the models for real-time phishing website detection without re-training.

4. Proposed Work

4.1. *Implementation Constraints*

4.1.1. *Regular Compliances*

- **Data Privacy**: Data processing must adhere to all relevant data protection rules and regulations, including the General Data Protection Regulation (GDPR) for EU consumers.
- **Security Standards**: Securing user data and ensuring the integrity of analysis on files and URLs.
- **Transparency**: They should be transparent about how they collect data, analyze, and deal with user-submitted files and URLs (Mohammad Shahnawaz Shaikh, 2019).
- **Model Integration**:
    - **Classification Algorithms**: The implementations will be done on multiple classification algorithms, including:
        - Random Forest classifier
        - AdaBoost classifier
        - XGBoost classifier
        - Support Vector Classifier
        - Gradient Boost classifier
        - Stacking Classifier
        - Voting classifier

4.1.2. *Evaluation and Validation:*

- **Evaluation Metrics**: Determine the model's efficacy by examining its F1 score, recall, accuracy, and precision.
- **Validation**: Besides validating the model on the test datasets, I evaluate its generalizability and potential to perform better on unknown data.
- **Functionality**: For the input URL, the trained model will predict the classification for the website and will specialize in predicting sites, such as phishing and legitimate websites.

4.2. *Technologies Stack*

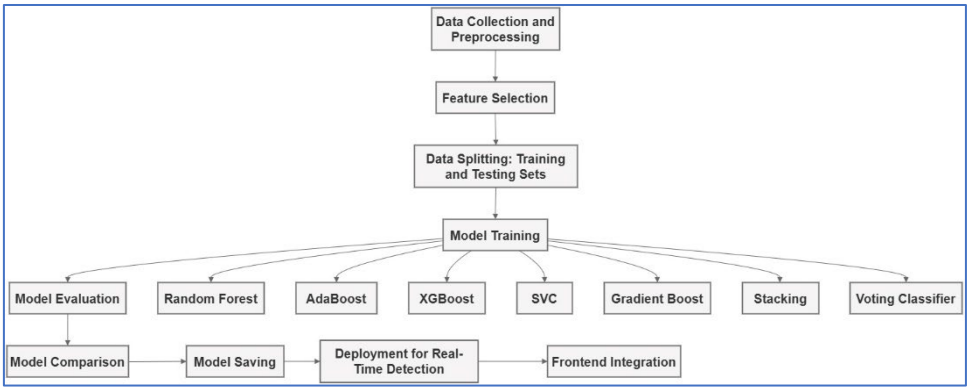
- **Frontend**: Integration with Google Sign for JavaScript APIs. 2. Backend: Handling authentication requests and storing user data in MongoDB database using Machine learning with Python.

4.3. *Design Consideration and Standards*

- **Security**: Security is of the essence, considering HackerEye is a service looking at potentially malicious files and URLs. Based on the industry's best practices for security, the platform should follow encryption of data in transit and at rest, have a secure authentication mechanism, have regular security audits, and adhere to security standards measured by OWASP (Open Web Application Security Project) guidelines.
- **Scalability**: HackerEye needs to process many requests for file and URL analysis. So, we can imagine its architecture is designed to address scalability issues like distribution of computing, load balancing, and dynamic resource allocation to match demand.
- **Performance**: By providing timely results, users expect when they are submitting files or URLs to be analyzed. So likely, HackerEye's design emphasizes performance optimization techniques such as efficient algorithms for analysis, caching to avoid getting the same analysis again and again, and optimizing database queries.
- **Reliability**: To keep our users' trust, our product, HackerEye, must be highly top-notch. This design effort involves designing for redundancy, fault tolerance, and disaster recovery strategies so that the platform remains available and responsive even during hardware failures or network outages.
- **Data Privacy and Compliance**: Depending on what data HackerEye handles, it's almost certainly such as PII and confidential files. Thus, the platform has to meet strict data privacy laws like GDPR and have substantial data handling policies regarding user privacy and law enforcement.
- **User Experience (UX)**: HackerEye has to have a user-friendly interface to attract and retain users. Intuitive navigation, precise feedback on the analysis results, and responsive design to support cross-device cross-screen size access are considerations in the design.
- **Interoperability**: Perhaps HackerEye will be an integral system that, for example, could connect to external systems and tools, such as antivirus engines, threat intelligence platforms, and security information and event management (SIEMs). Interoperability design requires a consistent use of standardized protocols & APIs to allow systems to communicate freely with each other.
- **Monitoring and Analytics**: HackerEye may have much going on underneath a user-friendly UI to ensure the platform's health, performance, and security. Real-time monitoring of system metrics, logging user activities, and

analyzing usage patterns to identify (Md. Shahnawaz Shaikh, Ankita Choudhry, 2016).

Fig. 1. Proposed Haker Eye Work Flow Chart.



5. Result and Discussion (Result Analysis)

Concerning accuracy, precision, recall, F1 score, and number of confusion matrix components, table 1 summarizes the performance of several machine learning classifiers used for phishing website detection. With 83% accuracy and balanced precision for the phishing and genuine classifications (0.76 and 0.88, respectively), we discovered that Random Forest and AdaBoost classifiers produced comparable results. F1 scores were intermediate (0.81 and 0.78), with reputable websites showing high recall (0.87) and phishing websites showing very significantly lower recall (0.73). They have 137 false positives and 286 false negatives, 887 true negatives, and 770 real positives in their confusion matrices.

Table 1. Number of parameters in the experimentation†.

Classifier	Accuracy	Precision	Recall	F1-Score	True Positives (TP)	True Negatives (TN)	False Positives (FP)	False Negatives (FN)
Random Forest	83	0.76/ 0.88	0.87/ 0.73	0.81/ 0.78	770	887	137	286
AdaBoost	83	0.76/ 0.88	0.87/ 0.73	0.81/ 0.78	770	887	137	286
XGBoost	83	0.76/ 0.88	0.87/ 0.73	0.81/ 0.78	794	926	98	262
SVC	78	0.71/ 0.92	0.87/ 0.63	0.81/ 0.75	663	968	56	393

† Column Headings: "Accuracy in Percentage; Precesion (Class 0/Class 1); Recall (Class 0/Class 1); F1-Score (Class 0 / Class 1); True Positives (TP); True Negatives (TN); False Positives (FP); False Negatives (FN)."

Overall accuracy (83%) was similar for the XGBoost classifier, and it was slightly better in reducing the false negatives (262) as well as the false positives (98), indicating the classifier's ability in both precision and recall. Its robust gradient-boosting approach iteratively minimizes classification errors and will behave accordingly.

At 78% accuracy, we obtained a lower accuracy with the Support Vector Classifier (SVC). Its precision for phishing websites was high (0.92). However, its recall for the same class was low (0.63), meaning a more significant number of false negatives. The conclusion of this trade-off was the lower F1 scores (0.81 for legitimate websites, 0.75 for phishing websites) presented in the confusion matrix where we did see such a large amount of false negatives (393), which were higher than the other models.

Overall, ensemble-based models such as Random Forest, AdaBoost, and XGBoost performed well as they could aggregate predictions by combining predictions from different learners, thus significantly reducing errors made. However, this choice of the classifier may vary based on particular use case priorities, i.e., choose the least false negatives or increase the recall.

6. Advantages of the Hacker Eye

Machine learning techniques, as proposed in "The Hacker Eye," have several benefits when used to identify phishing websites:

- **Exceptional Detection Precision**: Machine learning techniques such as XGBoost, Gradient Boosting, Random Forest, SVM, and AdaBoost have shown remarkable accuracy in distinguishing legitimate websites from fraudulent ones. To reliably detect fraudulent sites, these algorithms use massive datasets to spot minor trends and outliers.
- **Streamlining and Expandability**: A machine learning-based system, in contrast to a rule-based one, may learn and adjust to new phishing techniques automatically, without the need for regular human intervention. Because of its flexibility, it can scale to manage many websites effectively.
- **Advanced algorithms**: They can identify and block phishing websites in real-time, limiting end-users danger. This real-time protection ensures that consumers are not compromised. This preventative security measure dramatically lessens the likelihood of consumers being swindled by phishing attempts.
- **All-Inclusive Feature Analysis**: By using deep learning methods, automated feature extraction is made possible, allowing for the analysis of intricate properties, including domain age, website content, and URL structure. This thorough investigation improves the system's capacity to identify even complex phishing endeavors.
- **Affordable Choice**: Machine learning models, once trained, seldom need updating and use fewer resources while running than conventional systems. Because of their affordability, businesses of all sizes may consider them.

- **Flexibility in the Face of Changing Dangers**: Phishing methods change often. Adapting and improving over time, machine learning models (especially those employing ensemble approaches, such as Voting Classifiers) can sustainably guard against new threats.

7. Social Welfare of the Hacker Eye

Implementing "The Hacker Eye" approach will make the internet a safer place for everyone, from people to businesses:

- **Stronger Online Protection**: These methods lessen the chances of identity theft and financial fraud by efficiently identifying and blocking phishing websites, which protect sensitive personal and financial information.
- **Providing Users with Power**: By using automatic phishing detection systems, users may confidently use the internet, knowing that possible risks are being actively reduced.
- **Preserving At-Risk Communities**: These developments are advantageous to gullible customers, often the principal targets of phishing attempts. Users with less technological expertise or who are elderly are more likely to not fall for these methods.
- **Reduction in Attacks**: Businesses may gain and keep their consumers' confidence by reducing the likelihood of phishing attacks, making for a safer and more dependable online marketplace.
- **Saving Money**: Businesses lose billions of dollars yearly due to phishing assaults. Everyone, from people to governments, stands to gain economically from the widespread use of detection systems powered by machine learning, which may significantly mitigate these harms.
- **Cyber Security Progress**: Progress in cybersecurity is propelled by the development and implementation of sophisticated phishing detection tools, which encourages more study and innovation in the sector.

8. Future Enhancements

While current approaches are encouraging, there is much space for development in the area of phishing website detection:

- **Integration with the cryptocurrency blockchain**: When paired with machine learning models, its immutability and decentralization make it an ideal tool for detecting and blocking website phishing attempts.
- **Incorporating Behavioral Analytics**: Future systems may examine user activity patterns to spot phishing attempts. For instance, alarms might be sent in real-time in response to suspicious login attempts or navigational habits.
- **The robustness and worldwide** applicability of models may be improved by increasing the diversity of datasets to include a broader range of phishing and genuine websites from various languages and locations.

- **More Trust in the System**: Organizations and end-users will better understand why a website is marked as phishing if models are developed to provide clear and easy-to-grasp outcomes.
- **Methods for Hybrid Detection**: By integrating machine learning with more conventional rule-based techniques, we may build hybrid systems that are more effective and dependable than either method alone.
- **Phishing assaults** are becoming more common on mobile devices and Internet of Things (IoT) platforms. Thus, it's essential to tailor detection methods to these settings to ensure complete security.
- **Simulation of AI-Powered Phishing Assaults**: By simulating phishing assaults, cybersecurity frameworks may be further strengthened via staff training and testing the robustness of detection systems.
- Networks for sharing threat information across businesses may improve collective security systems and provide timely reactions to developing phishing operations. Real-time threat intelligence sharing is essential.

9. Conclusion

In conclusion, HackerEye is a pivotal resource in the cybersecurity landscape, offering unparalleled malware detection and analysis capabilities. Hacker Eye is the most used website to detect which URLs or files are safe to access. Its platform covers millions of data points across over 70+ antivirus engines and other security tools, giving you a comprehensive view of possible threats. The website's user-friendly interface and extensive API support facilitate seamless integration into existing security workflows for individuals and organizations. HackerEye commitment to transparency and collaboration, evidenced by its partnerships with leading cybersecurity firms and continuous improvement initiatives, underscores its importance as a trusted ally in the fight against cyber threats. Hence, by using this application, we know that URLs are unsafe, so we must go through the unknown links carefully. HackerEye remains at the forefront as the cybersecurity landscape evolves, continuously adapting and expanding its capabilities to meet the ever-changing challenges posed by malicious actors. With its robust infrastructure and unwavering dedication to cybersecurity excellence, HackerEye is an indispensable asset in safeguarding digital ecosystems worldwide.

10. References

Ali, S. I. (2024). AI Applications and Digital Twin Technology Have the Ability to Completely Transform the Future. In S. Ponnusamy et al. (Eds.), Harnessing AI and Digital Twin Technologies in Businesses (pp. 26–39). IGI Global. https://doi.org/10.4018/979-8-3693-3234-4.ch003

Ali, S. I., & Shaikh, M. S. (2025). The Ethical Dilemma of Using (Generative) AI to Science and Research. In L. Gaur (Ed.), Responsible Implementations of

Generative AI for Multidisciplinary Use (pp. 249–264). IGI Global. https://doi.org/10.4018/979-8-3693-9173-0.ch009

Ali, S. I., et al. (2025). The Era of Metaverse and Generative Artificial Intelligence. In L. Gaur (Ed.), Responsible Implementations of Generative AI for Multidisciplinary Use (pp. 29–44). IGI Global. https://doi.org/10.4018/979-8-3693-9173-0.ch002

Himanshu Kitey, Chandankhede, P., Jajulwar, K., Shaikh, M. S., & Fatinge, P. M. (2024). Solar Poour Generation Technique and its Challenges - A Comprehensive Review. Grenze International Journal of Engineering and Technology, 10(1), 122.

Karabatak, M., & Mustafa, T. (2018). Performance comparison of classifiers on reduced phishing website dataset. In 6th International Symposium on Digital Forensic and Security (ISDFS 2018) (pp. 1–5).

Md. Shahnawaz Shaikh, Choudhry, A., & Wadhwani, R. (2016). Analysis of Digital Image Filters in Frequency Domain. International Journal of Computer Applications, 140(6), 12–19. https://doi.org/10.5120/ijca2016909330

Md. Shahnawaz Shaikh, & Gupta, K. (2014). A Review of Spectrum Sensing Techniques for Cognitive Radio. International Journal of Computer Applications, 94(8), 1–5. https://doi.org/10.5120/16360-5781

Md. Shahnawaz Shaikh, & Gupta, K. (2014). Analysis of Cognitive Radio Spectrum Sensing Techniques. International Journal of Computer Applications, 102(12), 1–7. https://doi.org/10.5120/17864-8805

Md. Shahnawaz Shaikh. (2016). Li-Fi - An Emerging Wireless Communication Technology. International Journal of Advanced Electronics & Communication Systems, 5(1), 10758.

Md. Shahnawaz Shaikh. (2019). Cognitive Radio Spectrum Sensing with OFDM: An Investigation. International Journal on Emerging Trends in Technology (IJETT), 6(2).

Mungale, S. G. (2024). Safeguard Wrist: Empowering Women's Safety. In S. Ponnusamy et al. (Eds.), Wearable Devices, Surveillance Systems, and AI for Women's Wellbeing (pp. 192–205). IGI Global. https://doi.org/10.4018/979-8-3693-3406-5.ch012

Peng, T., Harris, I., & Sawa, Y. (2018). Detecting Phishing Attacks Using Natural Language Processing and Machine Learning. In Proceedings of the 12th IEEE International Conference on Semantic Computing (ICSC 2018) (pp. 300–301).

Preeti Chopkar, Wanjari, M., Jumle, P., Chandankhede, P., Mungale, S., & Shaikh, M. S. (2024). A Comprehensive Review on Cotton Leaf Disease Detection using Machine Learning Method. Grenze International Journal of Engineering and Technology.

Shaikh, M. S. (2024). AI-Based Advanced Surveillance Approach for Women's Safety. In S. Ponnusamy et al. (Eds.), Wearable Devices, Surveillance Systems, and AI for Women's Wellbeing (pp. 13–25). IGI Global. https://doi.org/10.4018/979-8-3693-3406-5.ch002

Shaikh, M. S. (2024). Harnessing Logistic Industries and Warehouses With Autonomous Carebot for Security and Protection: A Smart Protection Approach.

In S. Ponnusamy et al. (Eds.), Harnessing AI and Digital Twin Technologies in Businesses (pp. 239–257). IGI Global. https://doi.org/10.4018/979-8-3693-3234-4.ch017

Shaikh, M. S. (2024). Harnessing Logistic Industries Using Autonomous Carebot for Smart Surveillance, Protection, and Security. In F. AlTurjman (Ed.), The Smart IoT Blueprint: Engineering a Connected Future (pp. 20). Springer. https://doi.org/10.1007/978-3-031-63103-0_20

Shad, J., & Sharma, S. (2018). A Novel Machine Learning Approach to Detect Phishing Websites. Jaypee Institute of Information Technology, 425–430.

Singh, S., Shaikh, M. S., Sheikh, A., Dhargave, S., & Mungale, S. (2024). Advanced Security and Protection for Logistic Industries and Warehouse Using Autonomous Carebot. In 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET) (pp. 1–7). https://doi.org/10.1109/ACROSET62108.2024.10743701

Sonmez, Y., Tuncer, T., Gokal, H., & Avci, E. (2018). Phishing Websites Features Classification Based on Extreme Learning Machine. In 6th International Symposium on Digital Forensic and Security (ISDFS 2018) (pp. 1–5).