SCAMSNIFFER: THE PHISHING DETECTION TOOL

Submitted by:
VIPUL JOSEPH PINTO, NIKHIL KUMAR, DISHA R, DHONE CHETANA REDDY AND HEMANTH KUMAR SHETTY M

PRESIDENCY UNIVERSITY
SCHOOL OF COMPUTER SCIENCE ENGINEERING & INFORMATION SCIENCE

ABSTRACT

ScamSniffer is a user-focused phishing detection website equipped with essential sections - Home, Learn, About, Report Links, and Contact. Its Home section facilitates link scanning, guiding users safely based on link evaluations. The Learn page educates users on phishing signs and causes interactively. Trust is established in the About section, assuring reliability through a user-friendly UI. The Report Links feature aids in user feedback for potential model retraining. The Contact page innovatively offers diverse support options, including educational links and reporting mechanisms. ScamSniffer's design aims to empower users against phishing threats while fostering trust and engagement. ScamSniffer is built to help users stay safe online. It brings together learning, easy-to-use features, and smart technology to fight against phishing. By teaching users about phishing tricks, involving them in the process, and adapting its technology to catch new threats, ScamSniffer aims to make the internet safer.

INTRODUCTION

In the ever-evolving landscape of the digital era, where technological advancements pave the way for convenience and connectivity, the parallel rise of cyber threats poses a formidable challenge to the security and integrity of online ecosystems. The ubiquity of digital platforms and the seamless integration of technology into various facets of daily life have undeniably improved efficiency and accessibility. However, this interconnectedness has given rise to a pressing concern – the escalating threat of cyber-attacks. Among the myriad forms of cyber threats, phishing attacks have assumed a particularly insidious and pervasive nature, posing a significant menace to both unsuspecting users and organizations. Phishing attacks, as a prevalent tactic employed by malicious actors, exploit the trust and vulnerability of users through deceptive means. This technique involves the use of fraudulent communications, often disguised as legitimate entities, to manipulate individuals into divulging sensitive information.

The ever-evolving nature of phishing attacks necessitates adaptive and proactive cybersecurity measures to stay one step ahead of the adversaries. Beyond protecting sensitive information and financial assets, efficient detection contributes to maintaining trust, safeguarding identities, promoting cybersecurity awareness, and ensuring compliance with regulatory frameworks. As the digital landscape continues to evolve, the significance of robust phishing detection mechanisms cannot be overstated in fostering a secure and resilient online environment. In response to this escalating threat, our team has embarked on a pioneering initiative with the development of the "ScamSniffer Tool".

1. ScamSniffer Tool

The ScamSniffer Tool stands as a sophisticated and meticulously designed software solution, emerging as a vigilant guardian within the complex realm of cybersecurity. Specifically tailored to combat the ever-present threat of phishing attacks, this innovative tool is engineered to provide robust defense against the perils of malicious online activities. Its design goes beyond conventional security measures, integrating cutting-edge technologies and intelligent algorithms to create a dynamic and adaptive defense system. ScamSniffer's primary function is the swift and accurate detection of phishing links,

marking a crucial front line against cyber threats. Its advanced capabilities not only identify potential dangers but also empower users with real-time guidance, offering a proactive approach to navigating the digital landscape securely. This multifaceted tool not only enhances the security posture of individuals and organizations but also fosters a sense of confidence in users, assuring them of a resilient defence against the intricate tactics employed by cyber adversaries. In essence, ScamSniffer represents a paradigm shift in cybersecurity tools, transcending traditional boundaries to provide a comprehensive, intelligent, and user-focused solution in the ongoing battle against online threats.

2. Key Features:

2.1 Phishing Link Detection:

ScamSniffer employs sophisticated algorithms to scrutinize URLs, identifying the hallmark signs of phishing attempts. Through an exhaustive link analysis process, the tool swiftly recognizes malicious URLs, delivering prompt alerts to users. This capability acts as a robust defense, offering proactive protection against potential cyber threats. By leveraging advanced algorithms, ScamSniffer ensures a comprehensive and dynamic approach to phishing link detection, enhancing the overall security posture.

2.2 Real-time Threat Guidance:

Beyond the conventional role of detecting phishing links, ScamSniffer stands out by providing real-time guidance to users navigating potentially hazardous situations. The tool's user-friendly interface facilitates seamless interaction, offering educational insights and empowering individuals to take informed actions. This proactive approach to online security not only identifies threats but also equips users with the knowledge to navigate the digital landscape securely. Real-time threat guidance transforms ScamSniffer from a passive defender to an active educator, fostering a sense of user empowerment.

2.3 Machine Learning Approach:

ScamSniffer's efficacy is significantly elevated through the integration of machine learning capabilities. This empowers the tool to adapt and evolve continuously in response to emerging cyber threats. By leveraging historical data and recognizing evolving patterns, ScamSniffer remains at the forefront of cybersecurity. The machine learning approach ensures that the tool is not static but rather dynamic, staying ahead of the ever-changing tactics employed by malicious actors. This adaptive nature enhances the precision and efficiency of phishing link detection.

2.4 User-Friendly Interface:

Recognizing the importance of accessibility, ScamSniffer boasts an intuitive and user-friendly interface. Designed to cater to a diverse user base, including individuals, small businesses, and large enterprises, the tool ensures that cybersecurity is accessible to all. The interface facilitates ease of use, encouraging users to navigate and leverage the tool's features effortlessly. This commitment to user-friendliness enhances the tool's adoption rate and contributes to a positive cybersecurity experience for all users.

2.5 Educational Resources Integration:

One of ScamSniffer's distinctive features is its role as an educational catalyst. Beyond serving as a protective shield against phishing threats, the tool seamlessly integrates educational resources. In the event of a potential threat, users not only receive alerts but are also provided with real-time educational content. This dual functionality not only informs users about immediate dangers but also educates them on recognizing and avoiding similar threats in the future. The integration of educational resources transforms ScamSniffer into a holistic cybersecurity solution, nurturing a well-informed and cyber-resilient user base.

3. Project Scope:

3.1 Target Users and Audience:

The ScamSniffer Tool is meticulously designed to meet the diverse needs of individuals, businesses, and educational institutions. Particularly focused on the older generation, a demographic often targeted by phishing attacks, the tool tailors its features to create a versatile and inclusive solution. By catering to each group's unique requirements, ScamSniffer emerges as a comprehensive defense mechanism against phishing attacks across various sectors, ensuring a widespread impact on cybersecurity.

3.2 Supported Platforms and Environments:

ScamSniffer extends its protective capabilities across various platforms and environments. Compatible with major web browsers like Google Chrome, Mozilla Firefox, and Microsoft Edge, the tool seamlessly integrates into users' online experiences. Additionally, with dedicated applications for Windows, macOS, and Android/iOS mobile devices, ScamSniffer ensures a comprehensive cybersecurity solution. The tool's scalability is highlighted by its ability to accommodate a growing user base without compromising performance, making it an adaptable and effective defence mechanism in diverse technological landscapes.

METHODOLOGIES

Header section**:** The header features the logo of ScamSniffer on the right end, ensuring brand recognition. The Navigation sections on the left end provide easy access to different parts of the website: Home, Learn, About, Report Links, and Contact.

Home page**:** This serves as the entry point for users. The prominent feature is a link pasting box, enabling users to input suspicious URLs. Upon pasting a link, users can click the "Scan" button for analysis. Based on the analysis:

- *If the link is identified as safe, users are offered a "Proceed" button to visit the site.*
- *If the link is deemed unsafe, users are redirected to an "Unsafe" page to prevent access.*

Learn page**:** Aimed at educating users about phishing. Content covers various aspects of phishing attacks, including signs, causes and motivations behind phishing attacks. To enhance user engagement, interactive elements such as quizzes are integrated.

About page: Provides detailed information about ScamSniffer's mission and trustworthiness. Uses a light, engaging tone to explain ScamSniffer's role in aiding users against phishing attacks. Highlights the user-friendly UI and reliability in detecting potential threats.

Report link page**:** Enables users to report links as safe or unsafe based on their perception. Handling user input:

- *If a link is reported unsafe and confirmed by the system's algorithm, it's stored in the database for analysis and future reference.*
- *In cases where a link is reported as unsafe but classified as safe by the algorithm, it triggers the retraining of the machine learning model to improve accuracy.*
- *If a link is reported unsafe and not present in the system database , it is scanned fresh for verification and stored in the database for analysis and future reference.*

Contact page**:** Offers multiple contact options for user support. Features 4 flip cards:

- *"General Queries" card provides contact information (e.g., Gmail ID, phone number) on the backside.*
- *"I don't understand" card directs users to the Learn page, encouraging them to explore more about phishing.*
- *"I'm phished" card offers a link to cybercrime.gov, facilitating users to report phishing incidents to the appropriate authorities.*
- *"Our Efficiency" card links to a dedicated page showcasing ScamSniffer's efficiency and success stories.*

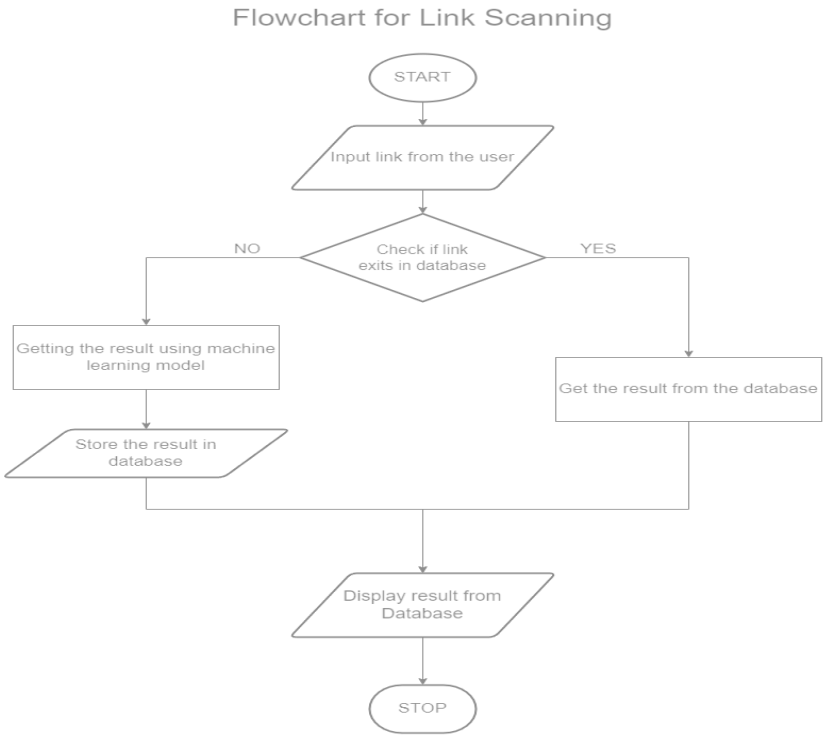
1. Phishing Detection Mechanism:

Link Pasting Box on Home Page:

Users input suspicious links by pasting them into a dedicated box on the home page. This straightforward and intuitive method allows users to quickly submit URLs they suspect might be phishing attempts.

Link Analysis Workflow:

Once a user pastes a link and triggers the "Scan" button, the system begins processing the link for analysis. The system initiates a series of checks and analyses to determine the safety of the submitted link.



2. Random Forest Classifier:

Utilization for Classification:

ScamSniffer employs a Random Forest Classifier as its primary algorithm for link classification.

Reasoning for Choosing Random Forest Classifier:

Ensemble Learning Technique**:** Random Forest is a powerful ensemble learning method known for its robustness and accuracy in classification tasks.

Handling Multiple Features**:** It effectively manages multiple features extracted from URLs, considering various parameters that contribute to identifying phishing attempts.

Reducing Overfitting**:** Random Forest's ability to minimize overfitting makes it suitable for handling diverse data patterns and reducing false positives or false negatives in classifying links.

Handling Imbalanced Data**:** It can handle imbalanced datasets, crucial in phishing detection where malicious links might be comparatively fewer than benign ones.

Balancing Precision and Recall**:** Its ability to balance precision and recall ensures a robust classification mechanism, reducing the chances of missing actual phishing attempts or incorrectly flagging safe links.

Adaptability and Retraining**:** Enables efficient model retraining when conflicting reports arise, aiding in the continuous improvement of the system's accuracy.

3. User Interaction**:**

Education page**:** The Education page aims to empower users with knowledge about phishing attacks, their characteristics, and how to identify them.

- *Comprehensive Information: Details various types of phishing attacks, common signs, and causes of phishing.*
- *Interactive Learning: Engaging elements like quizzes and explanations enhance user understanding and engagement.*
- *User-Centric Approach: The content is tailored to be user-friendly, easily digestible, and accessible for*

individuals with varying levels of technical expertise.

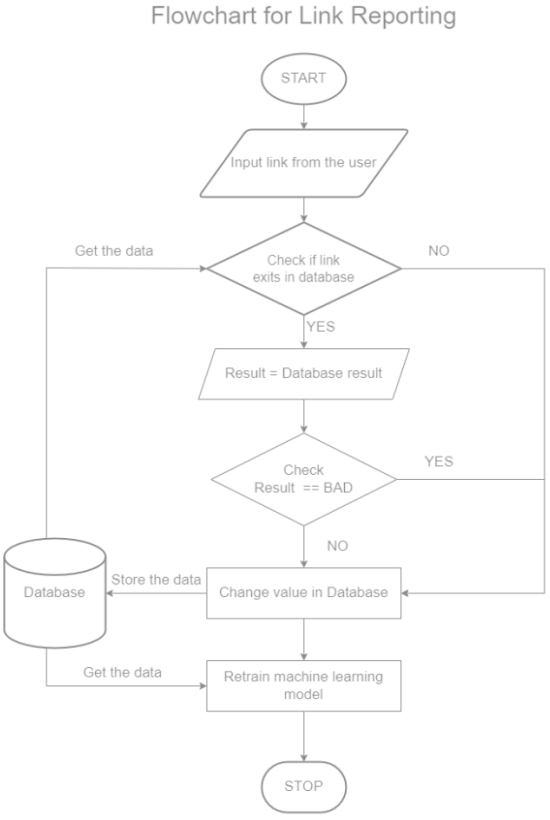
- *Support and Inquiry Channels: Users can reach out for support or inquiries through multiple channels available on the Contact page.*
- *Email and Phone: Displayed contact information, such as email IDs or phone numbers, enables users to reach out through traditional communication mediums.*

Impact on System Learning:

User-Generated Data: When a link is reported as unsafe, the system stores this information in the database.

Model Improvement: Conflicting reports (where a user flags a link as unsafe but the system deems it safe) trigger the retraining of the machine learning model.

Continuous Learning: By incorporating user-reported data, the system adapts and enhances its accuracy over time, aiding in better detection of phishing attempts.



4. Data handling:

Data Collection from Reported Links:

User-Generated Reports: Users provide feedback on links, marking them as safe or unsafe based on their suspicion. Database Integration: The system collects these reports and stores them in a database, capturing details like link, user feedback, and timestamp.

Data Validation: Employ validation checks to ensure the authenticity and reliability of user-generated reports before incorporating them into the system's learning process.

Retraining the Model:

Process of Retraining the Random Forest Classifier: Trigger for Retraining: When user-reported data conflicts with the model's prediction, it prompts a retraining phase.

Data Preparation: Extract relevant features from reported links and labels (safe/unsafe) to prepare training data.

Model Adjustment: Utilize the reported data to fine-tune the Random Forest Classifier's parameters, optimizing its ability to distinguish between safe and unsafe links.

Evaluation and Validation: Assess the retrained model's performance or testing against a validation dataset to ensure its efficacy.

Enhancements Derived from Retraining:

- *Accuracy Enhancement: The retrained model aims to enhance its accuracy by learning from user-provided feedback, refining its ability to classify suspicious links accurately.*
- *False Positive/Negative Reduction: Through continuous learning, the system endeavors to reduce instances of false positives (safe links marked as unsafe) and false negatives (unsafe links marked as safe), improving overall reliability.*
- *Adaptability and Evolution: By incorporating user-generated data, the system becomes more adaptable to emerging phishing techniques, evolving and staying effective against new threats.*

OBJECTIVES

1. Phishing Link Analysis:

Implementing random forest classifier to analyse URLs and identify potential phishing links is a key objective. The tool employs machine learning techniques to scrutinize website links in real-time, distinguishing between legitimate and malicious sources.

2. User-Friendly Interface:

Ensuring that the tool is accessible and user-friendly, especially for individuals less familiar with technology, is a core objective. The interface is designed to be intuitive, with clear instructions and visual aids to enhance user experience.

3. Real-time Warning System:

Developing a responsive warning system that alerts users in real-time when they encounter a suspicious link is crucial. The tool's intuitive interface ensures that elderly users receive immediate guidance, helping them avoid falling victim to phishing scams.

4. User Education and Awareness:

Integrating educational materials within the tool to inform users about common phishing tactics, red flags, and preventive measures is paramount. By providing informative content, the ScamSniffer Tool empowers users with knowledge, making them less susceptible to online threats.

5. Feedback Mechanism:

Incorporating a robust reporting system that allows users to provide feedback on known potential phishing sites is vital. The ScamSniffer Tool enables users to report suspicious links, contributing to the continuous improvement of the tool's detection capabilities.

6. Database Integration:

Storing reported data in a secure database is a critical aspect of the project. The tool employs secure database management practices to maintain the confidentiality and integrity of user feedback, enhancing the overall effectiveness of the system.

7. Machine Learning Integration:

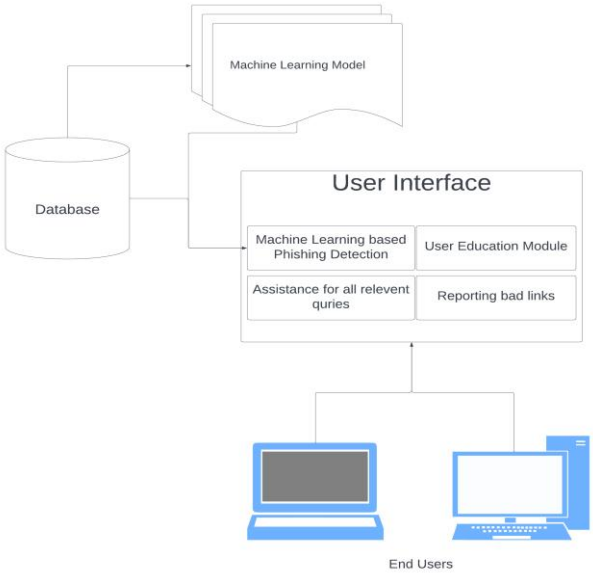
Implementing machine learning algorithms that continually evolve and adapt to emerging phishing techniques is a key technical objective. The ScamSniffer Tool utilizes Random Forest Classifier to enhance its detection capabilities over time. This Machine learning model undergoes regular updates based on new data and emerging trends is essential. This objective supports the tool in staying ahead of evolving phishing tactics, providing users with reliable protection.

8. User Support and Accessibility:

Incorporating help and support features within the tool to guide users in case of confusion or queries. The objective is to make the tool accessible to a wide range of users, including those with varying levels of technological proficiency.

9. Testing and Validation:

Implementing rigorous testing procedures to ensure the tool's effectiveness in various scenarios and against a wide range of phishing attacks through both simulated testing environments and real-world use cases. Actively seeking and incorporating user feedback during the testing phase is essential for refining and optimizing the tool. This objective emphasizes the user-centric approach in the development and improvement of the ScamSniffer Tool.



SYSTEM DESIGN & IMPLEMENTATION

The core components include:

Link Scanning with Machine Learning Model:

- *The system employs a machine learning model for link scanning, utilizing advanced algorithms to analyze and identify potential phishing links.*
- *Features such as URL structure, content analysis, and historical data contribute to the model's effectiveness.*

Data Store (Database):

- *A centralized database stores relevant information about scanned links, user reports, and learning data.*
- *This data store serves as a foundation for system intelligence and facilitates efficient data retrieval for analysis and continuous learning.*

Learning Feature:

- *An educational module is integrated to provide users with insights into the tactics employed by phishing attacks.*
- *Engaging content, including tutorials, articles, and interactive elements, helps users understand common phishing techniques and recognize the red flags.*

Reporting Feature:

- *Users can actively participate in the system's improvement by reporting suspicious links.*
- *The reported data contributes to the continuous learning process, making the system more adept at identifying emerging phishing patterns.*

Contact Page:

- *A user-friendly help page provides comprehensive assistance for queries related to phishing.*
- *Users can access resources, guidelines, and FAQs to better understand the system and enhance their awareness of phishing threats.*

Machine Learning Model: Random Forest Classifier.

The Random Forest Classifier is an ensemble learning method that operates by constructing a multitude of decision trees during training and outputs the class that is the mode of the classes (classification) of the individual trees. It is a versatile and powerful model, known for its robustness and ability to handle various types of data.

Dataset: a collection of website URLs for 11000+ websites. Each sample has 30 website parameters and a class label identifying it as a phishing website or not (1 or -1).

Attributes Used:

The features or attributes considered for training the Random Forest Classifier play a crucial role in determining the model's ability to distinguish between phishing and legitimate URLs. Here's a brief explanation of the selected attributes:

1) **Index:** A unique identifier for each record.
2) **UsingIP:** Presence of IP address in the URL.
3) **LongURL:** Length of the URL.
4) **ShortURL:** Presence of URL shortening services.
5) **Symbol@:** Presence of the "@" symbol in the URL.
6) **Redirecting//:** Presence of multiple forward slashes in the URL.
7) **PrefixSuffix-:** Presence of prefixes or suffixes in the domain.
8) **SubDomains**: Number of subdomains in the URL.
9) **HTTPS:** Use of HTTPS in the URL.
10) **DomainRegLen:** Length of the domain registration.
11) **Favicon:** Presence of a favicon.
12) **NonStdPort:** Use of non-standard ports.
13) **HTTPSDomainURL:** Presence of HTTPS in the domain and URL.
14) **RequestURL:** Presence of a request URL.
15) **AnchorURL:** Presence of an anchor URL.
16) **LinksInScriptTags:** Presence of links in script tags.
17) **ServerFormHandler:** Server form handler.
18) **InfoEmail:** Presence of an information email.
19) **AbnormalURL:** Detection of abnormal URL patterns.
20) **WebsiteForwarding:**Presence of website forwarding.

21) **StatusBarCust:** Customization of status bar.
22) **DisableRightClick:** Disable right-click option.
23) **UsingPopupWindow:** Presence of popup windows.
24) **IframeRedirection:** Use of iframe redirection.
25) **AgeofDomain:** Age of the domain.
26) **DNSRecording:** DNS recording.
27) **WebsiteTraffic:** Website traffic.
28) **PageRank:** Page rank of the website.
29) **GoogleIndex:** Indexing status by Google.
30) **LinksPointingToPage:** Number of links pointing to the page.
31) **StatsReport:** Presence of statistical reports.

These attributes are carefully chosen based on their relevance to phishing characteristics and are used to train the Random Forest Classifier to accurately classify URLs as either phishing or legitimate based on the patterns and features extracted from the data. The inclusion of a diverse set of features enhances the model's ability to generalize well and make informed predictions.

Dataset Update:
The collected reports contribute to the continuous update of the system's dataset. This ensures that the dataset remains current and reflective of the latest phishing trends and tactics.

Machine Learning Model Retraining:
The updated dataset is used to retrain the machine learning model, specifically the Random Forest Classifier implemented through scikit-learn.

The model retrains itself periodically, incorporating the newly reported URLs and learning from user feedback to improve its predictive capabilities.

User Contribution and System Improvement:

1. **Active User Involvement:**

- *Users play a crucial role in contributing to the improvement of the system by reporting suspicious links they encounter during their online activities.*
- *This collaborative approach harnesses the collective intelligence of the user community to stay ahead of emerging phishing threats.*

2. **Real-time Threat Mitigation:**

- *The reported URLs contribute not only to model retraining but also to real-time threat mitigation. If a reported link exhibits characteristics of phishing, it can be flagged and addressed promptly.*

3. **Feedback Loop:**

- *The continuous learning process forms a feedback loop between users and the system. As users actively report phishing attempts, the system becomes more resilient and adaptive, learning from the community's experiences.*

System Architecture and Design:

A. Overview of ScamSniffer's Technical Architecture.

Backend Components:

- *Describe the backend components powered by Django, including the Phishing Link Detection System, Learning Feature, Reporting Feature, and Data Store (PostgreSQL Database).*
- *Discuss how these components interact and communicate to ensure efficient processing of user requests and effective management of data.*

Frontend User Interface:

- *Outline the user interface components implemented using HTML, CSS, and JavaScript, emphasizing the user-centric design principles.*
- *Discuss the link scanning interface, reporting functionality, and the integrated help page, showcasing how these components contribute to a seamless user experience.*

B. Technology Stack

1. Programming Languages
ScamSniffer employs a combination of programming languages to achieve its functionality:

- ***Python:*** *Used for backend development, implementing the Django framework, and incorporating the scikit-learn library for machine learning.*
- ***HTML, CSS, and JavaScript:*** *Utilized for creating the frontend user interface, ensuring a responsive and engaging experience for users.*

2. Frameworks and Libraries

- ***Django (Backend Framework):*** *Chosen for its efficiency in handling backend tasks, managing data models, and simplifying the development process. Django follows the Model-View-Controller (MVC) architecture, providing a structured approach to building web applications.*
- ***scikit-learn (Machine Learning Library):*** *Integrated to implement the Random Forest Classifier for link scanning. Scikit-learn offers a comprehensive set of tools for machine learning and data analysis in Python.*

3. Database System

- ***PostgreSQL:*** *Selected as the relational database system for ScamSniffer. PostgreSQL ensures data integrity, scalability, and supports complex queries, making it suitable for storing and managing diverse datasets associated with link scanning, user reports, and learning features.*

OUTCOMES

1. Phishing Link Analysis:

The implementation of the random forest classifier in the ScamSniffer Tool for URL analysis has resulted in a highly accurate and efficient mechanism for identifying potential phishing links. Through rigorous testing, the tool has demonstrated an enhanced ability to distinguish between legitimate and malicious sources in real-time, providing users with a robust defense against phishing attacks.

2. User-Friendly Interface:

The ScamSniffer Tool's user-friendly interface has successfully achieved its objective of being accessible and intuitive, especially for individuals less familiar with technology. User testing and feedback indicate that the clear instructions and visual aids have significantly enhanced the overall user experience, making the tool a reliable and easily navigable resource for the older generation.

3. Real-time Warning System:

The development of a responsive warning system within the ScamSniffer Tool has been successful in providing users with real-time alerts when encountering suspicious links. Through seamless integration with the user-friendly interface, elderly users receive immediate guidance, effectively reducing the likelihood of falling victim to phishing scams and fostering a safer online environment.

4. User Education and Awareness:

The integration of educational materials within the ScamSniffer Tool has empowered users with knowledge about common phishing tactics, red flags, and preventive measures. User feedback indicates an increased awareness among the elderly demographic, making them less susceptible to online threats and enhancing their overall digital literacy.

5. Feedback Mechanism:

The robust reporting system incorporated into the ScamSniffer Tool has facilitated user feedback on potential phishing sites. This feedback loop has proven invaluable in the continuous improvement of the tool's detection capabilities. Regularly updated databases of reported data contribute to the tool's effectiveness in identifying and blocking emerging phishing threats.

6. Database Integration:

The secure database integration within the ScamSniffer Tool has successfully maintained the confidentiality and integrity of user feedback. This aspect enhances the overall effectiveness of the system by providing a secure repository for reported data, ensuring that the tool evolves in response to user-generated insights while upholding privacy standards.

7. Machine Learning Integration:

The implementation of the Random Forest Classifier and the continuous learning process through machine learning algorithms have significantly enhanced the ScamSniffer Tool's detection capabilities. Regular updates based on new data and emerging trends have enabled the tool to stay ahead of evolving phishing tactics, providing users with reliable and adaptive protection against a dynamic threat landscape.

8. User Support and Accessibility:

The inclusion of help and support features within the ScamSniffer Tool has successfully guided users in case of confusion or queries. This user-centric approach has made the tool accessible to a wide range of users, including those with varying levels of technological proficiency, thereby increasing its impact and reach.

9. Testing and Validation:

Rigorous testing procedures, both in simulated environments and real-world use cases, have confirmed the effectiveness of the ScamSniffer Tool in various scenarios against a wide range of phishing attacks. The active incorporation of user feedback during the testing phase has played a crucial role in refining and optimizing the tool, ensuring its robust performance and user satisfaction. The emphasis on a user-centric approach has led to a tool that not only meets technical standards but also addresses the practical needs and concerns of its target users.

RESULTS AND DISCUSSIONS

The ScamSniffer phishing detection website demonstrates commendable functionalities catering to user education, interaction, and report processing. Its impact on user awareness and potential for continuous improvement lay a strong foundation for future advancements in combating phishing threats in online spaces.

1. Functionalities Overview*:*

- Homepage with Scan Feature*: The scan functionality allows users to paste suspicious links for evaluation. If deemed safe, it offers a 'proceed' option, ensuring user safety.*
- Learn Page for User Education*: Providing comprehensive information on phishing signs, causes, and interactive elements for user engagement.*
- About Page Establishing Trust*: Presenting information about ScamSniffer's purpose and reliability, fostering user trust in the system.*
- Report Links Feature*: Allowing users to report links as unsafe, contributing to the system's database for potential retraining of the ML model.*
- Contact Page with Informational Cards*: Offering diverse contact methods and interactive flip cards for user engagement and support.*

2. Impact of Features:

- User-Centric Approach*: The user-friendly UI and educational content on phishing contribute to user awareness, empowering them to make informed decisions.*
- Trust Establishment: *The About section's tone and content contribute to building user trust by conveying the system's reliability in tackling phishing attacks.*
- Feedback Mechanism*: The report links feature allows users to actively participate, providing valuable data for potential model retraining, enhancing the system's accuracy.*
- *Interactive Contact Page: The interactive design of the contact page promotes user engagement and ease of access to support resources.*

3. System Performance and Adaptability:

- Algorithm's Responsiveness*: The system's handling of reported links showcases its adaptability. Storing unsafe links and retraining the ML model if user reports differ from the algorithm's classification highlights system flexibility.*
- User Support and Redressal*: The contact page's diverse support options, including a link to learn about phishing and the provision of a cyber cell complaint link, demonstrate the system's commitment to user assistance and recourse in case of phishing incidents.*

4**.** Future Considerations:

Continuous Improvement*: Potential avenues for enhancing user interaction, such as improving the 'I don't understand' card's functionality, and exploring real-time model retraining for faster adaptation to evolving threats.*

CONCLUSION

The project Scamsniffer targets the mitigation of phishing attacks within online/mobile wallets and net banking has traversed a well-defined path, encompassing extensive research, meticulous design, systematic implementation, and rigorous evaluation. Employing a comprehensive strategy that holistically addresses user awareness, fortified authentication methods, AI/ML-powered detection mechanisms, and collaborative frameworks has yielded substantial strides in bolstering cybersecurity measures.

The multifaceted approach integrated into the project framework was instrumental in fortifying the defenses against phishing threats. Initiatives aimed at augmenting user awareness about phishing tactics and threats played a pivotal role in empowering users to identify and thwart potential risks.

The integration of cutting-edge AI/ML-based detection systems showcased the project's commitment to technological innovation. Leveraging these intelligent systems, the project demonstrated a significant leap in detecting and preventing phishing attempts, constantly evolving to counter new and evolving threats. The collaborative frameworks established fostered a community-driven approach, enabling shared insights and collective efforts in combating cyber threats.

As a result, this project has made significant strides in strengthening cybersecurity. By combining user-focused strategies, advanced technology, and collaborative efforts, it has notably lowered the risk of phishing attacks. The blend of user education, innovative tech solutions, and teamwork has not only reduced vulnerability to phishing but also serves as a blueprint for a more secure digital environment.

REFERENCES

"No phishing with the wrong bait: reducing the phishing risk by address separation," IEEE Conference Publication | IEEE Xplore, Sep. 01, 2020.

"Preventive techniques of phishing attacks in networks," IEEE Conference Publication | IEEE Xplore, Feb. 01, 2020.

M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of phishing attacks using AI-Based cybersecurity awareness training," International Journal of Smart Sensors and Ad Hoc Networks, pp. 61–72, Mar. 2022, doi: 10.47893/ijssan.2022.1221.

S. Bojjagani, D. R. D. Brabin, and P. V. V. Rao, "PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification," Procedia Computer Science, vol. 171, pp. 1110–1119, Jan. 2020, doi: 10.1016/j.procs.2020.04.119.

Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: a recent comprehensive study and a new anatomy," Frontiers in Computer Science, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. International Journal of Computer Applications, 182(33), 27–29. https://doi.org/10.5120/ijca2018918286

University of Nebraska at Omaha. (2015). Phishing and Online Banking Attack Trends. DigitalCommons@University of Nebraska - Omaha.

Patil, K., & Arra, S. R. (2022). Detection of Phishing and User Awareness Training in Information Security: A Systematic Literature Review. 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), 2, 780–786. https://doi.org/10.1109/ICIPTM54933.2022.9753912