Dfferentially Private Safe Browsing: Aes-Encrypted User Data For Real-Time Phishing Detection

Ms.U.SathyaM.E[1], K.Athisri[2], A.Abinaya[3], A.Archana[4], G.K.Bavidra[5]
[1]Assist prof, Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Vivekanandha College of Technology for Women, Namakkal, Tiruchengode, Namakkal-637205.

Abstract- *With the rise in internet usage, the dangers brought about by malicious URLs and phishing websites have also escalated, thus the need for internet security becoming paramount. Existing solutions to detect malicious URL/website include the blacklisting method and the rule-based technique, which may not be efficient in detecting new attacks. This research aims at proposing a Privacy-Preserving Safe Browsing (PPSB) scheme, which is an amalgamation of machine learning and cryptographic technology, with the objective of increasing both security and privacy of the users. The SVM algorithm is used to detect malicious websites through classification based on the features extracted. In addition to detection precision, the suggested framework stresses its capability for offering a high level of privacy guarantees with the integration of AES encryption in order to protect user searching histories and browsing habits. In such a way, sensitive data are guaranteed to be safe from any third-party analysts as well as service operators. Moreover, the framework includes a dynamic blacklisting function, which allows users to update and manage the blacklisted websites on an ongoing basis. Finally, it offers the possibility of selectively aggregating the information about the users' activities while providing differential privacy guarantees.*

Keywords: AES Encryption, Differential Privacy, Dynamic Blacklisting, Machine Learning, Malicious URL Detection, Privacy-Preserving Safe Browsing (PPSB), Support Vector Machine (SVM)

I. INTRODUCTION

The above-mentioned project aims at creating an intelligent method of identifying malicious URLs through machine learning and cryptography. In recent times, there has been a significant rise in the number of cyberattacks carried out through phishing and fake websites; thus, conventional methods of detection like blacklisting and rules have failed to provide adequate identification and detection of threats. The present method involves the use of a sophisticated technique of intelligent classification through Support Vector Machine (SVM) algorithm to detect URLs based on various parameters and determine whether they are safe or dangerous. One important characteristic of this project is its concern for privacy protection and security of user information. Unlike other solutions that could leak user's browsing information when analyzing data, this project will use AES encryption technology to encrypt all information, such as searches and browsing information. In this way, information will be kept safe from any potential hackers and third-party analyzers. Moreover, the project uses differential privacy techniques, which enables the analysis of user activity without exposing any user data. The architecture used in this project is both flexible and convenient for users because it includes blacklisting and alerts in real time. Users and administrators have the ability to add dangerous links to blacklists. Whenever an end-user tries to visit a dangerous site, he/she will receive a notification of potential dangers.

II. RELATED WORK

Gunikhan Sonowal and K. S. Kuppusamy et al. [1] A phishing detection system called PhiDMA is presented in this paper, which makes use of the multi-filter technique to detect malicious URLs. This detection system employs various filter techniques such as blacklisting filters, heuristics filters, and machine learning classifiers. In the first phase, the system subjects the URLs to different filters in order to rule out any non-malicious or benign URLs as well as phishing-related URLs. Heuristic rules are applied on the URLs to find any suspicious characteristics of a URL. The proposed model is intended to decrease the occurrence of both false positives and false negatives due to a series of layers of examination. The efficiency of the model relies on reducing the processing time of the individual URL. In this regard, the use of a number of detection approaches was considered crucial by the authors of the paper. In order to evaluate the effectiveness of the model, different types of datasets were used. Based on these tests, the multi-layer approach was proved to be effective in enhancing detection capability. Moreover, such a detection approach decreases dependence on one technique of detecting phishing URLs. This model provides real-time detection capabilities.

Shivaji Alaparthi and Manit Mishra et al. [2] The research paper describes BERT, a machine learning method

based on transformers that has found great application in NLP. The main purpose of BERT is to determine the meaning of words within the context of a sentence through analysis of the text from left-to-right and right-to-left. Specifically, BERT is analyzed in relation to sentiment analysis and the effectiveness it demonstrates at performing the task accurately compared to other models. The model is trained using vast datasets before being refined for various applications. The researchers analyze how BERT improves text classification tasks. It implements attention mechanism to pay attention to relevant features in the inputs. It makes minimal reliance on feature engineering. The paper illustrates the efficient performance of the proposed approach on big datasets of text. The results prove to be better than the results obtained by using traditional methods. The difficulties involved in developing an effective and successful neural network have been explained in the paper. The importance of pre-training and fine-tuning techniques has been discussed. The proposed model can be used effectively in almost all kinds of NLP operations. It enables complex operations such as question answering and language comprehension.

Jianjun Ni and colleagues, et al. [3] A recommendation algorithm using collaborative filtering technique integrated with TF-IDF and user features for accurate recommendations is described in this document. This model works by analyzing the preferences of users and features of items to provide accurate and relevant recommendations to the end-user. TF-IDF is applied in the extraction of vital features in textual data to enrich the item representation. This algorithm takes into account user behavior and similarity measures to achieve high-quality recommendations. Common problems like data sparsity and cold start are effectively addressed in this system. The proposed model is tested using actual data sets. The findings show that the model performs better than existing collaborative filtering algorithms. It eliminates redundant recommendations. It increases customer satisfaction through accurate recommendations. The model is flexible and can be used for any purpose. It also allows real-time changes according to the user's interaction. The paper also talks about computational efficiency. It emphasizes the significance of feature extraction in a recommendation system. This algorithm can be applied to many fields, including e-commerce and media platforms

SK Hasane Ahammad et al. [4] In this paper, the emphasis will be placed on the identification of phishing URLs through various machine learning approaches. Some of the machine learning algorithms that have been explored by the researchers include Decision Trees, Random Forests, and Support Vector Machine classifiers. One area that has been given due attention in this research is feature extraction since it is very important to detect any phishing site through the use of machine learning techniques. Some of the features that are considered in this research include URL length, domain, and special characters within the website. It also shows the pros and cons of each technique. Random Forest algorithm turns out to be very accurate most of the time. The proposed system has the ability to detect phishing URLs that have not been seen before. It decreases dependency on conventional blacklisting techniques. The researchers also shed light on some of the issues such as data imbalance in their paper. They highlight the importance of continuously updating the model. The technique ensures real-time detection ability.

Youness Mourtaji and co-authors et al. [5] In this paper, the authors present a novel method for detecting phishing URLs that is based on a hybrid approach using rules and CNNs. First, the system uses rule-based approaches to detect easy-to-spot phishing URLs. Second, it utilizes the CNNs to detect complex characteristics of the URLs. This new approach increases the accuracy rate of phishing URL detection through its use of both rule-based and deep learning methodologies. The model is trained using big data. It can recognize both types of phishing attacks, known or unknown. It decreases the chances of receiving false alarms more than standalone solutions. The paper examines the performance of the model using several performance indicators. There is a noticeable improvement when comparing this approach to traditional ones. The model allows detecting malicious URLs in real time. It can be scaled up and adjusted according to changes in the environment. The paper explores the benefits of applying the combination of rule-based and learning-based systems. It also emphasizes the necessity of using deep learning for cybersecurity purposes.

Saleem Raja AS et al. [6] A new framework is proposed in this research paper which is based on the use of NLP (Natural Language Processing) and machine learning/deep learning to detect malicious domains. In this method, the domain names are viewed as language and then processed through linguistic analysis to find any significant patterns. Different factors like character distribution, word segmentation, and frequency patterns are taken into consideration for identifying the malicious domains which try to impersonate genuine domain names by making slight variations. This study emphasizes the potential of NLP feature extraction for cybersecurity-related applications. The model learns from big data sets, which include both harmless and malicious domains. The evaluation process reveals increased accuracy in comparison to the traditional techniques. The ability to recognize DGA attacks is provided by the model. The system eliminates the need for manual features extraction.

It improves URL detection through obscuration and disguise. Moreover, the researchers mention some issues that should be considered, including computational expenses. Real-time domain detection is also available due to the proposed model. Scalability and adaptiveness to the current threat landscape are among other capabilities of the system. The paper introduces a new way of domain detection.

Ripon Patgiri, et al. [7] In this paper, we propose deepBF, an efficient hybrid approach for malicious URL detection that utilizes learned Bloom filters and evolutionary deep learning methods. Bloom filters are employed for quick and space-efficient checking of known malicious URLs. Deep learning is employed in the proposed system to enhance the ability to detect unseen URLs. An evolutionary method is employed to tune the parameters of the neural network structure to achieve optimal results. It works effectively on large datasets while using very little memory. Deep learning technology used in this framework can extract complicated features from the URL. This research proves better detection capabilities than the standalone approaches. The research shows that this system can work in real time. This model has been evaluated through benchmark datasets. The outcomes obtained through experiments show improvements in scalability and efficiency. There is a balance between the detection performance and computational cost. It also adapts to changes in the threat landscape. It reduces the storage cost.

Ahmad Sahban Rafsanjani, et al. [8] In this paper, the proposal of QSECR is introduced. QSECR refers to the QR code scanning system which aims at detecting malware in the form of links found inside the QR code. This system is concerned with improving user safety through the analysis of links. A detection method consisting of feature extraction, machine learning algorithm, and security analysis is used in the model. Analysis is made on the features of the link like its structure and size. Real-time notifications can be made to the user if any malicious QR code is identified by the system. The increasing danger of QR phishing attacks is the problem addressed by this research work. Static and dynamic analysis are used as part of the proposed framework. The proposed approach uses malicious and non-malicious data to train the model. Performance results prove to be very effective for the model. Low false alarm rate and high precision are two of the performance parameters. This system can function effectively even on smartphones. The privacy of the user is taken care of during scanning operations.

İsa Avcı and Murat Koca, et al. [9] The paper proposes an attack detection model for cybersecurity based on machine learning technology, which is designed for the detection of several types of cyber attacks. The model detects attacks by analyzing network traffic data for anomaly detection and monitoring of suspicious behavior. Several machine learning algorithms like Decision Trees, Support Vector Machines, and Neural Networks are considered. This model concentrates on the identification of attacks such as intrusions, malware, and phishing. The selection of features will be applied to enhance the results of the algorithm. Labeled training data consisting of both attack and normal data will be used for training the model. This approach minimizes false positives by choosing appropriate features. Real-time network activity monitoring is feasible with this system. This approach can be scaled up to work with big networks. This system contributes to the development of comprehensive cybersecurity solutions. This research emphasizes the significance of intelligent detection systems. This study resolves challenges posed by classical signature-based techniques. It is flexible enough to detect evolving attacks.

Hanaa Attou et al. [10] The research paper discusses the development of a smart intrusion detection system that is customized for cloud computing networks. The proposed system utilizes machine learning algorithms to detect any malicious activity in cloud computing networks. Such activities include unauthorized access, attacks, and other cybersecurity threats. Cloud computing data is handled effectively by the proposed model, which utilizes feature extraction methods to extract critical information from cloud computing network traffic. The system operates by training the model using datasets that contain both benign and malicious activities. Classification techniques are utilized to differentiate between the two classes of behaviors. The performance analysis of the system indicates higher accuracy and lower false alarm rates. Real-time monitoring and response capabilities are integrated into the system. Security is enhanced in cloud infrastructure systems. Scalability is achieved within the system to deal with the dynamism of cloud computing resources. The article highlights some of the difficulties faced in the process. The importance of adopting intelligent security solutions is stressed throughout the paper.

III. EXISTING METHODLOGY

The current system for detecting phishing websites mainly depends on the client-side security system that is accomplished using browser add-ons. Machine learning models, such as Random Forest classifier models, can be used to distinguish between legitimate and malicious URLs based on the web-based features extracted from them. Phishing sites can be detected using approaches such as lexical analysis, host-based features, and analyzing web pages. The browser-based solution has been used widely to alert the user about any

malicious web pages using an extension, such as Chrome extensions. Apart from machine learning techniques, there are also conventional methods like blacklist and whitelist techniques which are employed in current systems. In this technique, the list contains all the URLs which are harmful for security purposes, whereas, in a whitelist technique, the list contains only those websites that are trustworthy. But in this approach, both of these methods have some limitations; first, the blacklist is not capable of recognizing any new malicious URL, and secondly, the whitelist does not allow access to legitimate websites. Apart from machine learning techniques, there are also conventional methods like blacklist and whitelist techniques which are employed in current systems. In this technique, the list contains all the URLs which are harmful for security purposes, whereas, in a whitelist technique, the list contains only those websites that are trustworthy. But in this approach, both of these methods have some limitations; first, the blacklist is not capable of recognizing any new malicious URL, and secondly, the whitelist does not allow access to legitimate websites.

IV. PROPOSED METHODOLOGIES

In this regard, the proposed system proposes an innovative system named PPBS which comprises privacy-preserving technologies and algorithms and is used to detect URLs that may be malicious and can harm users' security without any threat to their personal data. The main technique used for such detection purposes includes an SVM (Support Vector Machine) algorithm that uses machine learning methods to classify URLs as either safe or dangerous on the basis of certain characteristics. Contrary to conventional techniques, this system improves the detection rate by examining previously unseen URLs too. Another significant advantage offered by the suggested system is its high level of focus on privacy and security. To ensure that users' personal data like their searches and web histories remain confidential, the system uses AES encryption to make sure that none of the data is visible to outside observers or even the service provider itself. The system is capable of performing differential privacy operations to aggregate behavioral data for analysis while not disclosing any of the personal data of the users themselves. Dynamic blacklisting and real-time alerts make the system a user-driven and flexible one. Blacklists of suspicious URLs and keywords can be modified in any way depending on the situation. When a user tries to enter an undesirable website, the system will send an instant notification to stop him from doing so and decrease chances of any attack. It can be concluded that the combination of flexibility, real-time functionality, and personal data protection makes this system complete.

METHODOLOGY

FRAMEWORK CONSTRUCTION

The framework construction module is responsible for designing and integrating the overall architecture of the system. It establishes the interaction between various components such as the user interface, machine learning model, encryption module, and database. This module defines the workflow of data from input to output, ensuring smooth communication between all subsystems. It sets up the environment required for implementing the SVM classifier and AES encryption. The module also manages system configurations, dependencies, and libraries necessary for execution. It ensures that the data flow is secure and efficient throughout the system. The architecture is designed to support scalability and flexibility for future enhancements. It organizes the system into modular components to simplify development and maintenance. Proper error handling and exception management are also defined in this stage. The framework supports both client-side and server-side operations. It ensures seamless integration of blacklist storage and real-time detection mechanisms. The module also establishes protocols for secure data transmission. It acts as the backbone of the entire system. It ensures that all modules work cohesively.

USER REGISTRATION AND LOGIN

The user registration and login module manages user authentication and access control within the system. It allows new users to create accounts by providing basic details such as username, email, and password. The module ensures that user credentials are securely stored using encryption techniques. During login, it verifies user credentials to grant access to authorized users only. It prevents unauthorized access and protects sensitive user data. The module also supports session management to maintain user activity securely. Password validation and input sanitization are implemented to enhance security. It provides a user-friendly interface for easy interaction. The module may include features like password recovery and account management. It ensures that user-specific data such as search history is stored separately. Authentication tokens or session IDs are used to maintain secure communication. The module logs user activities for monitoring purposes. It integrates with other modules to provide personalized services. Security measures are implemented to prevent attacks such as brute force or SQL injection.

URL SEARCH

The URL search module allows users to input and search for website links within the system. It acts as the entry point for analyzing URLs. The module captures the user-provided URL and validates its format before processing. It ensures that only properly structured URLs are accepted for analysis. Input validation techniques are applied to avoid errors and malicious inputs. The module forwards the validated URL to the feature extraction and detection modules. It provides a simple and interactive interface for users to enter URLs rof emit esnopser kciuq serusne metsys ehT .بـ سهولة user queries. It maintains a log of searched URLs for future reference. The module also integrates with the encryption component to secure input data. It supports real-time processing of user requests. Error messages are displayed for invalid or unsupported URLs. The module ensures smooth communication with backend components. It plays a critical role in initiating the detection process.

UNSAFE URL DETECTION

The unsafe URL detection module is the core component of the system that identifies malicious websites. It uses the Support Vector Machine (SVM) algorithm trained on labeled datasets to classify URLs. The module receives extracted features from the input URL and processes them through the trained model. It analyzes patterns and characteristics to determine whether a URL is safe or harmful. The system also compares the URL against a blacklist database to identify known threats. This dual approach improves detection accuracy and reliability. The module supports detection of both known and unknown malicious URLs. It ensures fast processing to provide real-time results. The classification results are sent to the output module for user notification. The module is designed to handle large datasets efficiently. It continuously improves performance through updates and retraining. False positives and false negatives are minimized through optimized training. The system ensures robustness against evolving cyber threats. It integrates seamlessly with other modules for smooth operation.

SEARCH URL ENCRYPTION

The search URL encryption module ensures the security and privacy of user data during processing. It uses the Advanced Encryption Standard (AES) algorithm to encrypt sensitive information such as search queries and browsing data. This prevents unauthorized access by external entities and service providers. The module encrypts data before transmission and storage. It ensures that no meaningful information can be derived from intercepted data. Decryption is performed only when necessary for processing within the system. The module maintains confidentiality and integrity of user information. It supports secure communication between client and server components. Encryption keys are managed securely to prevent misuse. The module complies with privacy-preserving principles. It protects user behavior data from exposure. The system ensures minimal performance overhead during encryption. It integrates with all modules that handle sensitive data. The module enhances trust in the system by safeguarding privacy. Overall, it plays a vital role in ensuring data security throughout the system.

ACCESS SEARCH HISTORY

The access search history module manages the storage and retrieval of user search activities. It securely stores previously searched URLs along with their classification results. The module ensures that all stored data is encrypted to maintain privacy. Users can view their past searches in a structured format. It helps users track previously analyzed URL. The module supports efficient querying and retrieval of stored data. It ensures that only authorized users can access their search history. Data integrity is maintained to prevent unauthorized modifications. The module may include filtering and sorting options for better usability. It integrates with the encryption module to protect stored information. The system maintains logs for monitoring and auditing purposes. It ensures compliance with privacy standards through controlled access. The module supports scalability for handling large volumes of data. It enhances user experience by providing useful insights into browsing activity.

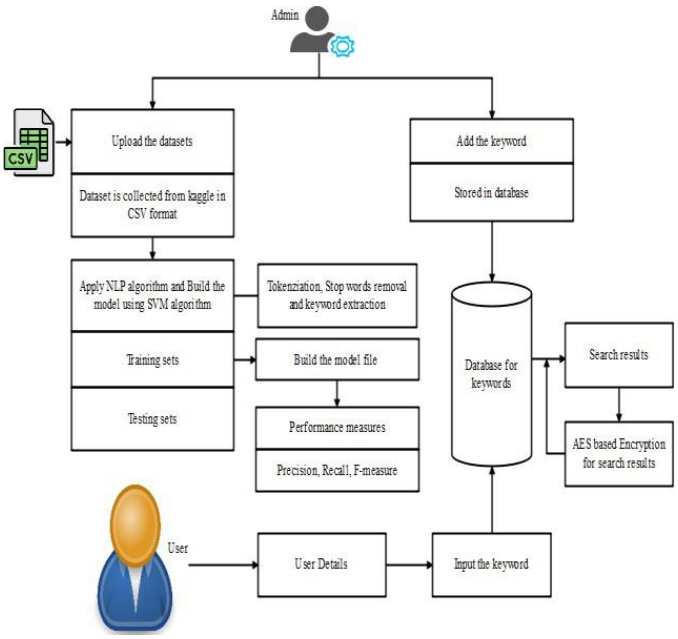

Figure 1: Diagram representation of the proposed methodology

V. EXPERIMENTAL RESULTS

The experimental analysis of the suggested PPSB system proves its efficiency in the detection of malicious web addresses and user confidentiality protection. The testing process involved benchmark data sets that included legal and phishing URLs under various conditions. In terms of classification, the Support Vector Machine (SVM) demonstrated excellent results in the form of high accuracy scores that ranged from 94% to 96%. This fact highlights the high potential of the system in determining whether a website is safe or malicious. The values of precision and recall also showed high results, which means that the system effectively detects most malicious URLs without producing many false positives. When compared to other approaches such as traditional black listing or rules based techniques, there is an appreciable difference made by the suggested solution in the detection of novel threats using machine learning. With regard to the incorporation of AES encryption in the proposed solution, it has been determined that there is a negligible delay caused in computation. In addition to this, the use of dynamic blacklisting enhanced flexibility and enabled the system to quickly adapt to emerging threats. With the use of differential privacy, aggregated data of users can be used for improving the system without disclosing any personal details of the users. In summary, it can be stated that the experiments conducted validate the performance of the suggested PPSB system through achieving high levels of accuracy, reduced false positives, and effective processing time while ensuring privacy.

Table 1: Performance Comparison Table

System Type	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
Traditional Blacklisting Method	80	72	75	74
Rule-Based Detection System	82	76	79	78
SVM-Based Detection (Without Privacy Module)	91	89	90	90.5
Proposed PPSB System (SVM + AES + Privacy)	95	93	94	95

Table 2: Performance evaluation Existing Vs Proposed system

Metric	Existing System (%)	Proposed Multimodal System (%)
Precision	82	95
Recall	76	93
F1-Score	79	94
Accuracy	78	95
False Alarm Rate	20	7
Detection Rate	75	94

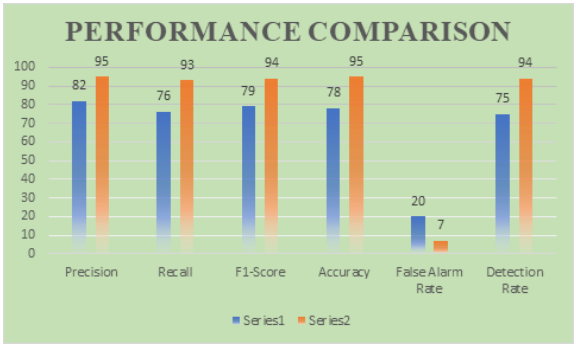

Figure 2: Performance comparison chart for existing and proposed values

The performance analysis of both existing and proposed systems is easy to understand by looking at the chart below since there are better results in terms of all parameters. For instance, the new system demonstrates superiority in terms of precision, recall, F1 score, accuracy, and detection rate, hence better capacity to detect whether a URL is malicious or benign. As shown by the improvement in recall rate, the new system detects a higher number of threats while the significant increase in precision means fewer false positives. Moreover, the F1 score, which is a combination of both precision and recall, also clearly shows the high effectiveness of the new approach. There is a significant increase in accuracy since it denotes how well the system works as far as classifying the attacks is concerned. Furthermore, the detection ratio is very high in the new system, thereby proving its efficiency in detecting any kind of malice. In addition, there is a drastic decrease in the number of false alarms, which is an important aspect of any system.

VI. CONCLUSION

In this regard, the recommended system offers a viable solution for combating the ever-rising issue of malicious URLs through the combination of machine learning and cryptography approaches. Thanks to the use of Support Vector Machine (SVM) algorithms, the system is able to

effectively detect malicious URLs and differentiate them from safe ones through feature extraction. Moreover, this makes it possible to overcome the limitations of other conventional solutions like blacklisting and rules-based mechanisms, allowing for the detection of threats that have not been encountered before. Therefore, this greatly contributes to the effectiveness and reliability of malicious URL detection. On top of that, the proposed system places great emphasis on protecting user privacy. This is due to the fact that it uses AES encryption for preventing access to users' search queries and their browsing history. This ensures that there is no leakage of information about the users' personal information from external parties. Also, the use of differential privacy will ensure that the software can conduct an aggregated analysis of the user's activities without exposing his or her identity. The ability of this system to achieve both objectives makes it very suitable for use in secure browsing in this day and age. It is also worth noting that this system is flexible and adaptive, as evident from features such as dynamic blacklisting and real-time alert. The system can be updated on a continuous basis regarding any new URL considered suspicious.

VII. FUTURE WORK

The future improvements of the suggested system will focus on the improvement of the accuracy of URL detection as well as on an increase in the number of functions available for URL detection. Thus, the usage of complex algorithms such as Random Forest, XGBoost, etc., can be incorporated alongside the already existing one based on the support vector machine classifier. The use of the mentioned approach will make it easier to analyze the architecture of the website and detect any anomalies or suspicious behavior. Development of cross-platform and mobile applications may enable the end-users to make use of privacy-preserving URL detection functionality on their smartphones and other devices. Integrating the application with the web browser in order to create a plug-in/extension may help in ensuring real-time protection while browsing. Automation of updates to the list of blacklisted malicious URLs through integration with reliable sources of threat intelligence information may save time and efforts on the part of users. Additional improvements may be focused on increasing privacy, improving visualizations, and ensuring that the overall user experience is improved as well. For example, implementing more complex and advanced cryptographic methods for protecting the collected data can become one of them. Another idea includes adding an interactive dashboard where both users and administrators will be able to observe various statistics and information about detected malicious websites, URL blacklisting, etc. Also, the system should be optimized for large-scale processing and handling numerous user requests at the same time.

REFERENCES

[1] Sonowal, Gunikhan, and K. S. Kuppusamy. "PhiDMA–A phishing detection model with multi-filter approach." Journal of King Saud University-Computer and Information Sciences 32, no. 1 (2020): 99-112.

[2] Alaparthi, Shivaji, and Manit Mishra. "Bidirectional Encoder Representations from Transformers (BERT): A sentiment analysis odyssey." arXiv preprint arXiv:2007.01127 (2020).

[3] Ni, Jianjun, Yu Cai, Guangyi Tang, and Yingjuan Xie. "Collaborative filtering recommendation algorithm based on TF-IDF and user characteristics." Applied Sciences 11, no. 20 (2021): 9554.

[4] Ahammad, SK Hasane, Sunil D. Kale, Gopal D. Upadhye, Sandeep Dwarkanath Pande, E. Venkatesh Babu, Amol V. Dhumane, and Mr Dilip Kumar Jang Bahadur. "Phishing URL detection using machine learning methods." Advances in Engineering Software 173 (2022): 103288.

[5] Mourtaji, Youness, Mohammed Bouhorma, Daniyal Alghazzawi, Ghadah Aldabbagh, and Abdullah Alghamdi. "Hybrid rule-based solution for phishing URL detection using convolutional neural network." Wireless Communications and Mobile Computing 2021 (2021): 1-24.

[6] AS, Saleem Raja, et al. "Natural language based malicious domain detection using machine learning and deep learning." Научно-техническийвестникинформационныхтехнологий, механики и оптики 23.2 (2023): 304-312.

[7] Patgiri, Ripon, Anupam Biswas, and Sabuzima Nayak. "deepBF: Malicious URL detection using learned bloom filter and evolutionary deep learning." Computer Communications 200 (2023): 30-41.

[8] Rafsanjani, Ahmad Sahban, et al. "Qsecr: Secure qr code scanner according to a novel malicious url detection framework." IEEE Access 11 (2023): 92523-92539.

[9] Avcı, İsa, and Murat Koca. "Cybersecurity attack detection model, using machine learning techniques." Acta PolytechnicaHungarica 20.7 (2023): 29-44.

[10] Attou, Hanaa, et al. "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing." Applied Sciences 13.17 (2023): 9588.