A Predictive Model for Phishing Attacks on Mobile Intelligent Agent Systems

Mashako D. Manyama and Okuthe P. Kogeda(✉)

School of Mathematics, Statistics, and Computer Science, University of KwaZulu-Natal, Westville Campus, Durban 4000, Republic of South Africa
KogedaO@ukzn.ac.za

Abstract. Phishing attacks continue to evolve with time and the attackers are always ahead of the existing mitigation plans. The more technology advances, the more sophisticated phishing attacks become. As more people rely on technology to conduct their online businesses, the need for secure Mobile Intelligent Agents (MIAs) systems becomes higher. MIAs are software that execute functions or duties such as managing electronic mail, gathering, and sending out information on behalf of an online user. MIAs play a vital role in carrying out electronic commerce activities whether from business-to-customer, customer-to-customer, or business-to-business. In this paper, we use Decision Tree (DT) to accurately predict the status of a Uniform Resource Locator (URL) and flag those predicted to be phishing. The DT algorithm extract URL features such as the domain name, URL length, host name, page ranking, etc., and feeds them into the model which then makes status prediction. The extracted features are then filtered into the model to improve its future predictions. The proposed model has a prediction accuracy of 91.3% and it is also cost effective as well as easy to use. The other benefit of the proposed solution is its capability to flag phishing URL and prevent a user from launching the web browser thereby protecting their personal information from being stolen by criminals.

Keywords: Agent · Algorithm · Artificial intelligence · Cyber-security · Decision tree · e-commerce · m-commerce · Mobile intelligent agent · Predictive · Prevention · Phishing

1 Introduction

In 2024, the worldwide retail e-commerce sales are estimated to exceed $6.3 trillion (US dollars), and the figure is expected to continue to grow in the coming years [1]. As of 2023, online marketplaces accounted for the largest share of online purchases worldwide. Globally, e-commerce market share accounts for 20.1% of the total retail sales [1]. One of the most contributing factors in the e-commerce growth is the unprecedented usage of mobile devices whereby smartphones account for nearly 80 percent of all retail websites visits worldwide [1]. The usage of mobile devices makes the mobile commerce (m-commerce) much easier for the online customers and it is particularly popular in Asia, with countries like China and South Korea generating more than two-third of their total online sales via mobile devices [1].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14816, pp. 113–128, 2024.
https://doi.org/10.1007/978-3-031-65223-3_8

The research work conducted by [2] reported a potential massive growth opportunity in the digital commerce sector over the next few years particularly in Sub-Saharan Africa whereby the number of Internet users is expected to grow. Such growth is driven mainly by a high number of mobile device users, rising consumer confidence in online transactions, and the expansion of brick-and-mortar retailers into the online sphere by adopting a multi-channel approach [2]. Although the Sub-Saharan Africa (SSA) is the smallest e-commerce region, however, it shows a very strong growth potentials especially since after COVID-19 pandemic that made people to change their shopping behaviour [2].

E-commerce transactions take place using the Internet, which often present an opportunity for online scammers who are always ready to try their luck on unsuspecting e-commerce customers [3, 4]. When performing online transactions, the customers often expose a large amount of their personal information to the merchant or service provider using the Internet, which as a result exposes them to many cyber security attacks. For this reason, a high level of confidentiality and authenticity between the e-commerce stakeholders is always expected [5, 6]. The concept of security and privacy continues to get an enormous amount of attention from the commercial sector since it has got a potential to determine the success of the m-commerce as a new way of shopping [7, 8].

One of the most common cyber security risks to the growth of the m-commerce is phishing attacks aimed at the Mobile Intelligent Agents (MIAs) [9] used to carry out the online business activities on behalf of both the customer and the merchant [10]. The mobile intelligent agents dispatched by the user onto the Internet are the ones interacting with the online shopping system [11], and it is at this moment that they become vulnerable to phishing attacks whilst roaming the Internet [12]. Phishing is a type of cyber-attack used by online scammers to target internet users mainly the e-commerce users with an intention of acquiring personal confidential information through deception [13, 14]. This type of attack involves tracking the potential target by sending spam emails or instant messages with the intention of leading them to a fraudulent website wherein their confidential personal information gets stolen [15]. For example, a phisher may deceive the victim by representing themselves as a particular well-known organization or online shopping outlet despite having no knowledge of the recipient or victim at all [16].

Online businesses across the world continue to be flooded with phishing attacks targeting their employees that are often ill-prepared and under-equipped to process or take necessary actions against such threats [17]. In [18] it is also reported that worldwide organizations are at a higher risk of data breaches with an average monetary loss of over $4.45 million (US dollars) per organization per year. The phishing report [19] titled "Phishing Activities Trends Report 4th Quarter 2022" by an organization called Anti-Phishing Working Group (APWG) reported that the number of global phishing attacks grew slightly in fourth quarter of the year 2022. The organisation observed a total number of 1,350,037 phishing attacks in the fourth quarter from a previous total of 1,270,833 phishing attacks in third quarter of the same year which is a new record high and was the worst quarter that APWG has ever observed.

In this study, we designed and developed a Phishing Predictive Model (PPM) that is used to verify the legitimacy of a URL before launching it on the web browser. We used

the Decision Tree algorithm to train and test our model. To input the URL, we used a mobile application developed in Python and integrated with the decision tree predictive algorithm to return the URL status to the user. Depending on the URL prediction results, the mobile application then allows the user to either launch the verified legitimate URL on the web browser or gets blocked from launching a web browser of a suspected phishing URL. The user is also able to download a list of previously predicted URLs stored in the database.

The rest of this article is structured as follows: Sect. 2 outlines the related work by discussing existing phishing solutions, Sect. 3 outlines the methodology we followed, Sect. 4 present the testing results and evaluation, and lastly Sect. 5 presents the conclusion of the study.

2 Related Works

Various studies have been conducted in the past to investigate ways to prevent phishing attacks aimed at MIA systems. The existing models focus on phishing attacks prediction with some focusing on the Internet in general, online banking, and some on e-commerce systems. As a result, phishing attacks on MIA systems remain one of the most critical areas in cyber security.

There are still other kinds of phishing attacks that not even the security services of various protocols such as Hypertext Transfer Protocol Secure (HTTPS) or Secure Sockets Layer (SSL) are able to prevent [20]. To overcome these security limitations, [20] proposed a phishing detection model which is based on machine learning classifiers and evaluated using different performance metrics. Their phishing detection model is made up of two phases namely, Classification Phase and Phishing Detection Phase. The classification phase's objective is to accurately detect the phishing websites from normal URLs to the phishing URLs. The objective of the feature selection module is to be able to extract all the valid and necessary features so that the classifier can accurately detect the phishing URLs from the attributes as given by the feature selection component. The objective of the phishing detection phase is to detect the legitimate URLs from the phishing URLs given a list of attributes extracted by the feature extraction module during the classification phase. The authors in [20] made use of the five-machine learning algorithms namely, Decision Tree (DT), K-Nearest Neighbour (KNN), Logistics Regression (LR), Random Forest (RF) and Support Vector Machine (SVM) to compare the URL status predictability. The RF algorithm recorded a better phishing detection accuracy of 91.4% as compared to the rest of the other four machine learning algorithms. The similarity between their model and ours is that we both used Decision Tree and our model with an accuracy of 91.30% is closer to their best performing model.

Another study in [21] developed a model to detect phishing websites using the machine learning approach. In their study, they made use of machine learning algorithms such as Random Forest, Decision Tree, Neural Network, and Linear Model to classify data into either phishing or legitimate. The model was able to identify and predict phishing websites from legitimate websites by extracting some unique features from the websites. The dataset used was collected from Miller Smiles archives, PhishTank archive as well as from Google searching operators. The dataset consisted of a total of 2,456

websites and 30 features. The values of attributes used were in the form of integers −1, 0, and 1, whereby the −1 represents phishing, the integer 0 denotes suspicious and the integer 1 denotes legitimate. First, the dataset was processed to ensure data was matured into a desired format before it was split into two datasets by applying the 70% training data and 30% testing data rule. The experiment was carried out using the RStudio installed on Windows 10 after which the four machine learning algorithms (Random Forest, Decision Tree, Neural Network, and Linear Model) were applied on the dataset. The results from the machine learning algorithms were compared in terms of accuracy, True Positive Rate (TPR), True Negative Rate (TNR), Precision, F-Measure, and Error Rate. The RF algorithm recorded the highest prediction accuracy of 95.7% as compared to the other three algorithms. The similarity between their model and ours is that we both used Decision Tree although our model recorded an accuracy of 91.30% which is a bit lower than their best performing model.

The researchers in [22] developed a preventative scheme that uses a specified set of rules on URL behaviour to determine the status of a website based on frequency analysis of extracted phishing features from PhishTank URL data. Support Vector Machine (SVM) was then used to increase the detection power of unknown or suspicious patterns on the URL. After a careful and extensive analysis of comparing the phishing URLs against legitimate URLs, certain heuristics categories were formulated under which classifications were made. Each heuristic category associated with a unique filter was used to formulate detection rules using various combinations of unique filters [22].

In addition, each filter was then mapped with a certain value using the SVM learning system. Each URL is then represented using a vector with either true or false after the identification of all the lexicals in the URL to indicate if it is a phishing or a legitimate URL. The schemes worked according to expectation on smartphones considering that they were also lightweight and taking the memory of the device into account. Although their research was mainly on phishing detection, it is somewhat like ours because it focuses on mobile agents.

The research study in [23] focused on phishing detection using a virtual similarity-based scheme with filtering approaches. The visual schemes compare the visual appearance of suspicious websites with the corresponding legitimate website using various parameters. In their study, they classified the visual similarity-based approaches into HTML Document Object Model (DOM) tree, Cascading Style Sheet (CSS) similarity, pixel-based model, visual feature model, visual perception model, and hybrid model. Three of these models namely, the DOM Tree model, CSS model, and Hybrid model stood out as the best phishing detection approaches since they turn to cover most of what the models are intended to do.

The DOM tree detection model compared the DOM tree websites of suspicious webpage with the legitimate one. The comparison was done to identify the usage of the same personal information (i.e., same username, password, etc.) on multiple websites before issuing warning flag activities on the second website as a suspicious attack. The CSS similarity approach was also effective due to its ability to depict the formatting of a document and set-up the visual appearance of a webpage written in HTML, XHTML, and XML. The authors in [23] used the CSS approach to detect any suspicious-looking features such as fonts, colours, page layout, etc., on any webpage. A combination of

various features from the webpage were analysed by the model by making use of the hybrid approach. The disadvantage of the DOM tree model is that it only compares the new websites with the previously visited websites unlike our model which still analyses the extracted features from any given URL to predict its legitimacy.

The researchers in [24] proposed a Bayesian model to determine the similarity threshold between suspicious websites and legitimate ones. The model is based on visual features such as webpage layout, logos, images, forms, font, background colour, and textual features such as stop words e.g., a, an, the, that, etc. Their model used a naïve Bayes rules-based text classifier to extract texts from the webpage as well as the Earth Mover's Distance (EMD) based image classifier to deal with pixel-level contents after the webpage has been transformed into an image. They used the Bayesian approach during offline training to set the appropriate threshold.

Lastly, they [24] used a Bayesian-based algorithm to aggregate the results from the image and the text classifiers. The model was effective since it presented the researcher with a text classifier using the naïve Bayes rule for phishing detection and its ability to combine the classified results from the text and image classifiers. Although not entirely like our model, we take a step further during our model by not only detecting phishing attacks, but we also prevent the user from accessing any suspicious phishing URL that has been flagged by our model.

The research study in [25] used the artificial neural networks (ANNs), support vector machines (SVMs), decision tree (DTs), and random forest (RF) techniques to develop four phishing detection models for investigating the efficiency of using machine learning to detect phishing domains. They used the uniform resource locators' (URL's) Unified Customer Interface (UCI) phishing domains dataset as a benchmark to evaluate their models. Upon comparing the phishing detection capabilities of the four models, the random forest technique was found to be the most effective algorithm which outperformed the other three techniques.

The authors in [26] proposed the use of Ensemble Learning Methods such as random forest (RF) algorithm and extreme gradient boosting (XBOOST) algorithm for efficient and accurate phishing website detection based on its URL. When comparing the prediction accuracy of the two algorithms, they found that the XBOOST algorithm had the best phishing website detection accuracy of 93.7% whilst the RF had a prediction accuracy of 91.1%.

The researchers in [27] used the Light Gradient Boosting Machine (LightGBM) and URL features such as the domain name to develop a machine-learning-based algorithm that can detect phishing websites and maintain the security of smart systems. They made use of the domain name features due to its capability for multiple domain-name generation algorithms that remain constant. Their model was first used to extract features of the domain name of any given website, including character-level features and other information on the domain name. The extracted features were then filtered to improve the model's accuracy and subsequently used for classification. They [27] found that the detection model which integrates two types of features for training, significantly outperforms the model that uses only a single type of feature.

In this study, we developed a machine learning algorithm using the decision tree (DT) to predict the status of a URL and flag all the suspicious phishing URLs. The developed

phishing prediction and prevention model specifically focuses on MIA systems with a focus on the m-commerce and Internet banking systems as first discussed in [28]. We based our research study on the groundwork that was done in [29] to determine the similarity threshold between the suspicious websites and the legitimate ones as it was first done by researchers in [24]. We make use of the Content-Based Filtering (CBF), Blacklisting, and Whitelisting detection model as first discussed in [30].

3 Methodology

The framework of our model starts with sourcing of URLs dataset from the PhishTank Database. The overall model framework and its various components is shown in Fig. 1.

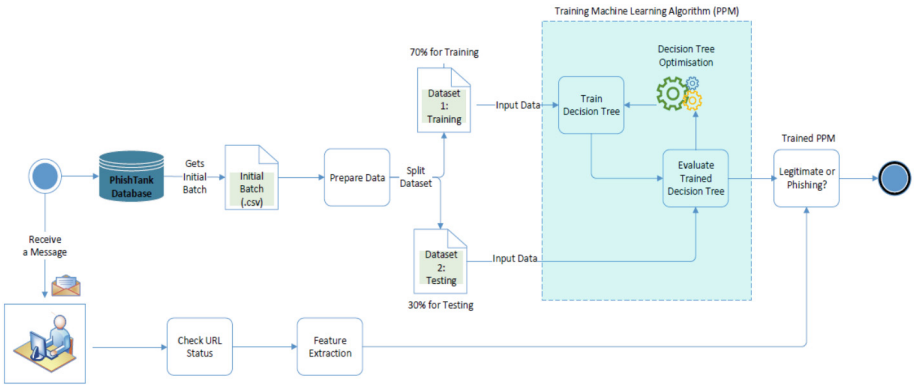

Fig. 1. Phishing Predictive Model (PPM) Framework

Step 1: Dataset Sourcing - the dataset used to train and test the model is sourced from a publicly accessible database on Mendeley website [6]. The dataset was already categorized into phishing and legitimate URLs by the time we sourced it.

Step 2: Dataset Processing - the dataset processing components involves splitting the sourced data into two datasets whereby, one dataset is for training and the other dataset is for testing the trained model. We applied the 70:30 rule to split data into 70% training dataset and 30% testing dataset.

Step 3: Feature Extraction **-** we used Power BI Desktop to extract and explore various data features. Various features were compared with the expected URL status to determine the correlation of such features against the output. This step gave us an indication as to which feature has an influence in predicting URL status and to what extent is the level of influence.

Step 4: Feature Selection **-** during this step, we remove all those features that are relatively discrete and have no correlation between them. We conducted the correlation analysis which is carried out to identify features that either have a strong positive or negative relationship between themselves. Such features cannot be used as inputs when training the machine learning decision tree algorithm.

Step 5: Train PPM **-** the selected features from Step 4 are then used to train the machine learning algorithm component of the PPM. The output of this step is a trained PPM which is later used to predict legitimacy status of any given URL. Once the PPM is fully trained and optimized, it is then integrated with a mobile application that was developed in Python and can predict the status of any given URL.

Step 6: Evaluate PPM **-** the experimental results of the trained and optimized PPM were then analyzed. To determine if the developed model meets the expected objectives, the model was then compared with other available solutions implemented by other researchers.

4 Results and Discussion

4.1 Experimental Hardware and Software Tools

The hardware tools used to implement the PPM model included 8 GB RAM and a 2.40 GHz Processor. The software tools used consists of Windows 10 Pro Operating System and a 64-bit Operating System, Python 3.10, SQL Server version 2019, and Power BI Desktop version 2.117.984.

4.2 Experimental Dataset

The dataset consists of 11,430 URLs obtained from Mendeley database [6]. The data is a consolidated list of known phishing and non-phishing URLs as reported by known industry expert systems such as PhishTank.org and Kaggle.com which are more trusted and reliable. The dataset consists of 87 extracted features and contains exactly 50% phishing and 50% legitimate URLs. The explored data was split into two datasets, namely training dataset and testing dataset. The training dataset consists of labelled data that was used to train the PPM whereas the testing dataset was used to evaluate the PPM. The dataset partitioning is diagrammatically shown in Fig. 2.

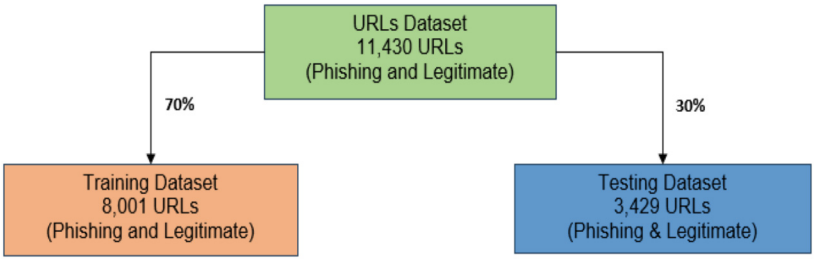

Fig. 2. Dataset Partition

4.3 PPM Performance Indicators

Performance indicators are used to assess the learning of an algorithm, to determine the effectiveness of an algorithm based on metrics using the test datasets. To measure the performance of the PPM, we measured the *accuracy, precision, recall, F-score, Mean Absolute Error (MAE), Mean Squared Error (MSE), and the Root Mean Squared Error (RMSE).* Of the measured indicators, accuracy (as given by Eq. (1)), precision (as given by Eq. (2)), recall (as given by Eq. (3)), and the F-score (as given by Eq. (4)) are the only four indicators used to calculate the confusion matrix:

$$Accuracy(A) = \frac{(TP + TN)}{TP + TN + FP + FN} \tag{1}$$

$$Precision(P) = \frac{TP}{TP + FP} \tag{2}$$

$$Recall(R) = \frac{TP}{TP + FN} \tag{3}$$

$$F1 = \frac{2TP}{2TP + FP + FN} \tag{4}$$

where *TP* represents the URLs that are predicted to be phishing and are indeed found to be phishing, *FP* represents the URLs that are predicted to be phishing while they are legitimate, *TN* represents the URLs that are predicted to be legitimate while they are indeed found to be legitimate, *FN* represents the URLs that are predicted to be legitimate while they are phishing.

The other indicators are measured as follows:

Mean Absolute Error(*MAE*), in the context of machine learning computes the impact or magnitude of the differences between the predicated URL statuses and the actual URL statuses. *MAE* is calculated by Eq. (5) as follows:

$$MAE = \frac{1}{n}\sum_{i=0}^{n-1}|y_i - x_i| \tag{5}$$

where Σ represents the summation value, $y_i$represents the actual URL statuses for the ith observation, $x_i$represents the predicated URL statuses for the ith observation, and $n$represent the number of observations in a dataset.

Mean Squared Error(*MSE*), measures the average squared error between the actual URLs statuses and the predicted URLs statuses. Since PPM is trained to predict the phishing URLs with minimum error, The *Mean Squared Error*(*MSE*) is calculated by Eq. (6):

$$MSE = \frac{\sum_{t\epsilon T}(t_{u,i} - p_{u,i})^2}{\|T\|} \tag{6}$$

where T represent the number of observations in a dataset, $t_{u,i}$ represents the actual URL status, and $p_{u,i}$ represents the predicted URL status.

The last indicator is called *Root Mean Squared Error*(*RMSE*, which is the square root of the *MSE* and is used to plot the difference between the predicted URLs statuses and the actual URLs statuses. The *RMSE* is calculated by Eq. (7):

$$RMSE = \sqrt{\frac{\sum_{t \epsilon T} (t_{u,i} - p_{u,i})^2}{\|T\|}} \tag{7}$$

where T represent the number of observations in a dataset, $t_{u,i}$ represents the actual URL status, and $p_{u,i}$ represents the predicted URL status.

4.4 Experimental Results

The developed mobile application is built to accept a valid URL from a user through a text box field where it can either be typed in or pasted on. Once a valid URL has been captured, the user would then click on the 'Search' button. The welcome page showing both the download and the search buttons is shown in Fig. 3.



Fig. 3. PPM Welcome Page

The PPM is able to save valid URL whose status was verified by the model. The user is also able to download a list of stored URLs from the database, which then automatically get saved on the user's local download folder as shown by the confirmation messgae in Fig. 4.

The mobile application validates each URL that has been received to ensure that only valid URLs, which conform to a certain criteria are accepted. The URL validation message is shown in Fig. 5.

Each URL searched through the mobile app evokes the algorithm component of the PPM system, which then makes URL status predictions. For any URL that is predicted to be 'Not Secure' or phishing, the system then blocks the user from launching the web page of such a URL address and the only option the user has is to exit the status result screen as shown in Fig. 6.

The model is also able to successfully predict a legitimate URL. Once a URL has been predicted to be secure, the user is able to launch the web page by clicking on the 'OPEN URL' button. Alternatlively, the user may opt to exit the confirmiation screen by clicking on the 'EXIT' button. The screen that allows the user to launch the web page or exit confirmation screen is shown in Fig. 7.

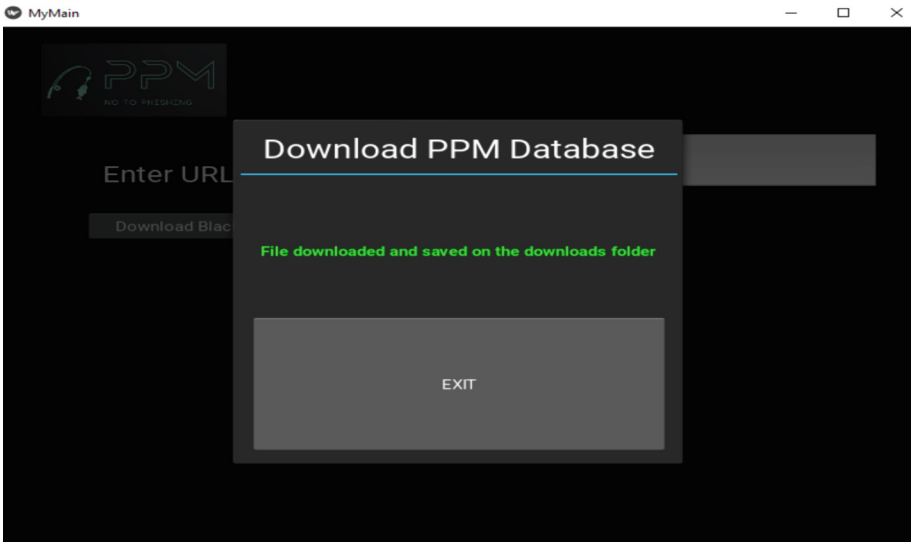

Fig. 4. Downloading URL List

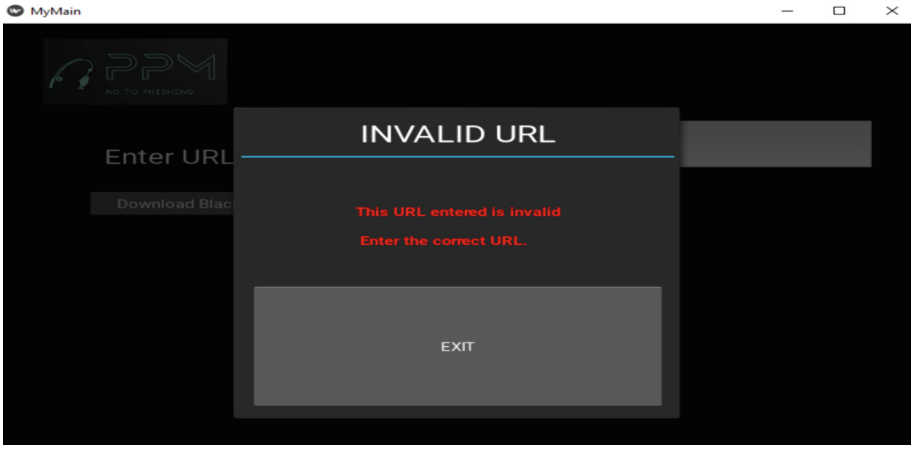

Fig. 5. URL Validation

4.5 Evaluation of PPM

We employed an experimental approach using three different PPMs based on the Decision Tree technique. We then computed the performance matrices of each DT classifier to get their True Positive Ratio (TPR) and True Negative Ratio (TNR) values as shown in Table 1.

To evaluate the performance of the proposed model, we computed their performance indicators, and the results are shown in Table 2.

The comparison results between the three classifiers are shown in Fig. 8.

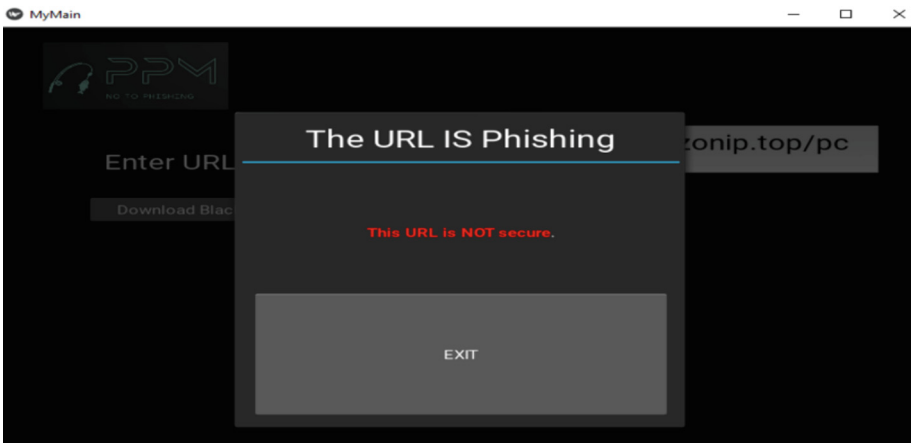

Fig. 6. Predicted Phishing URL

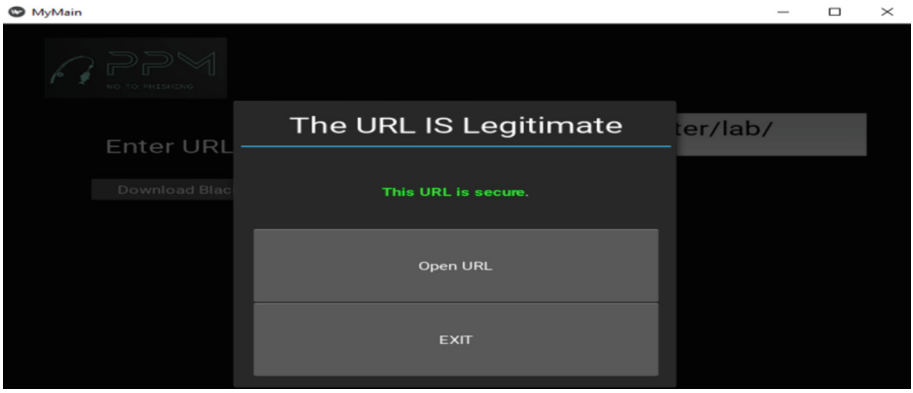

Fig. 7. Predicted Legitimate URL

Selecting the Best PPM: The best PPM is a model that can generalize the testing data very well. The best PPM was selected not only based on its prediction accuracy, but also considering that each of the classifiers used a different set of parameters as shown in Table 1. Based on the PPMs' performance results in Table 2, it would appear as though PPM2 is the best model when looking at its prediction accuracy of 93.2%, and the MSE of 6.8%. However, PPM2 was trained to its full depth which resulted in overfitting of the training data. That means the model would have a higher prediction accuracy during training but have a lower accuracy during testing. To overcome the overfitting effect of the training data, PPM3 was selected as the best model with a prediction accuracy of 91.3%, and the MSE of 8.7%. This is because PPM3 was able to generalize both the training and the testing datasets. Unlike the PPM2 that was trained to its full depth using all features, PPM3 was trained using only the important features and its decision tree was also pruned which made the model to have closer prediction outcomes between training

Table 1. Comparison of DT Classifiers

DT Classifiers	Parameters	TPR	TNR
PPM1	Criterion = gini, Splitter = best, Max_depth = None, min_samples_split = 2, min_samples_leaf = 1, and 87 Features	0.9278	0.9322
PPM2	Criterion = gini, Splitter = best, Max_depth = None, min_samples_split = 2, min_samples_leaf = 1, and 87 Important Features only	0.9278	0.9363
PPM3	Criterion = gini, Splitter = best, Max_depth = 5, min_samples_split = 2, min_samples_leaf = 5, and 50 Important Features only	0.9115	0.9135

Table 2. Evaluation of Phishing Prevention Model (PPM) Results in (%)

Performance Indicator	PPM1	PPM2	PPM3
Accuracy	93.1	93.2	91.3
Precision	93.3	93.7	91.4
Recall	93.0	92.8	91.2
F1-Score	93.1	93.3	91.3
MAE	6.9	6.8	8.7
MSE	6.9	6.8	8.7
RMSE	36.4	26	29.6

and testing. The accuracy scores for both training and testing in five folds for PPM3 shows closer scores between the training and the testing results as shown in Fig. 9.

The comparison between the actual and the predicted URLs statuses for PPM3 classifier is shown in Fig. 10. The graph shows how closely the model was able to make the correct prediction in comparison to the given actual outcome. Wherever the predicted values matched the actual values, only the orange line for the predicted value is visible on the graph as shown in Fig. 10.

Evaluating the Best PPM: The best selected DT classifier, which is PPM3, was then evaluated against existing solutions from studies carried out by other researchers. The evaluation criteria focused on the dataset type that was used by each research study, the machine learning algorithm, the accuracy of the developed model, and lastly the mean squared error. Table 3 shows the comparison between PPM3 and other models developed by other researchers. The researcher's name is listed under the first column called approaches. The dataset used differs from one research to another.

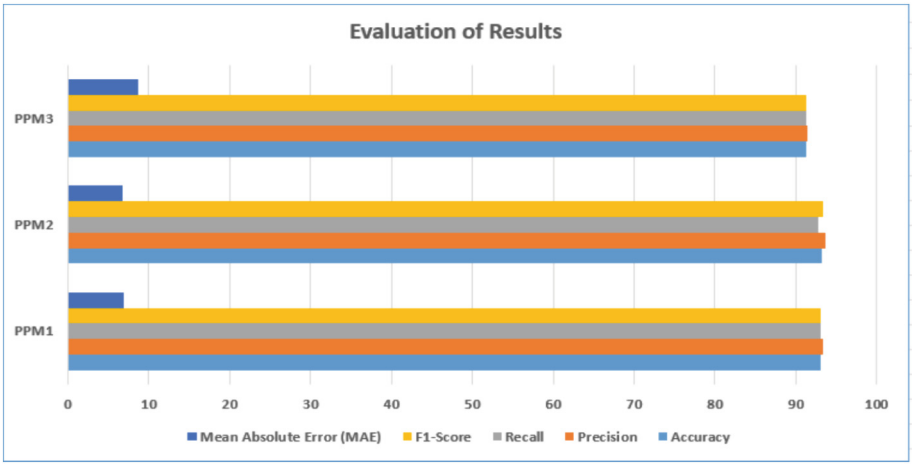

Fig. 8. DT Classifiers Comparison

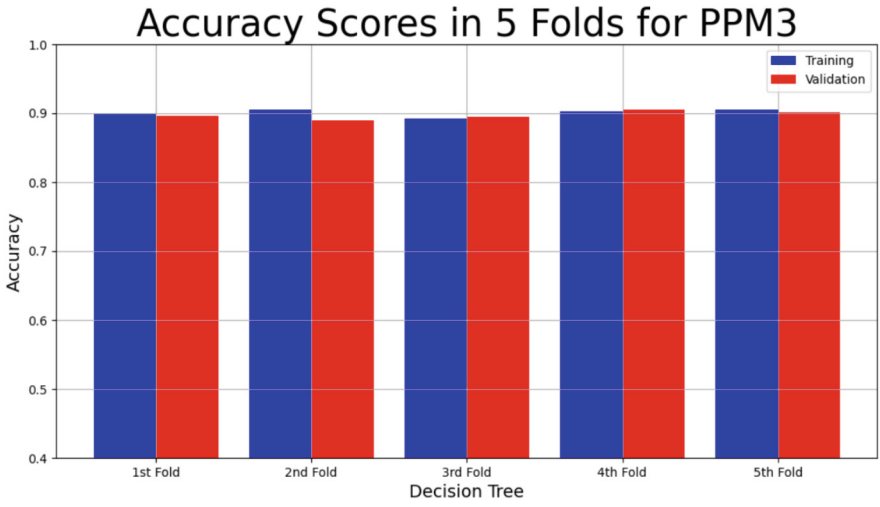

Fig. 9. Accuracy Scores for PPM3

Although PPM3 was selected as our best model amongst the three DT classifiers however, the model developed by [25] stands out as the best approach with an accuracy of 97.3% and error rate of 2.7%. This is because they used 10-fold cross-validation approach to locate a greater performance accuracy dataset amongst the artificial neural network (ANNs), support vector machines (SVMs), decision trees (DTs), and random forest (RF) techniques whilst we used 5-fold cross validation approach and only focused on one machine learning algorithm which is the decision tree (DT). The other reason is because they used URL's UCI phishing domains as their dataset whilst we used the entire URL details which consist of 87 features. Amongst the six researchers we compared our

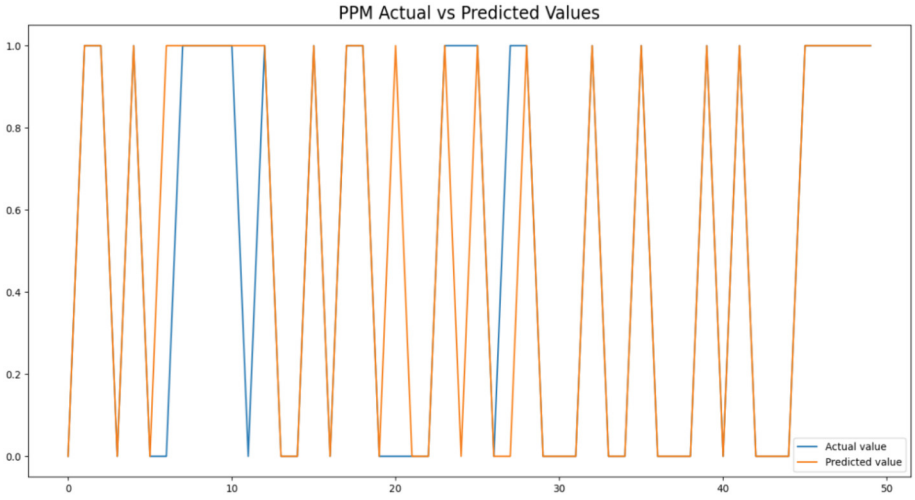

Fig. 10. Actual vs Predicted Values

model with, it is only [20] that our model comes closer to with an accuracy of 91.4% and an error rate of 8.6%. As a result, our study can be improved in the future by employing other machine learning algorithms together with the decision tree and evaluate their prediction results before selecting the best performing model and also by using 10-fold cross-validation as it was done by [25].

Table 3. Comparison of Proposed Model and Other Approaches

Approaches	Dataset Type	Machine Learning Algorithm	Accuracy	MSE
Alnemari and Alshammari [25]	URLs	ANN, SVM, DT, and RF	97.30%	2.70%
Orunsolu et al. [22]	URLs	SVM	96.60%	3.40%
Jalal and Naaz [21]	URLs	DT, RF, NN, and LM	95.70%	4.30%
Zhou et al. [27]	Websites	LightGBM	94.70%	5.30%
Dharani et al. [26]	URLs	RF, and XGBoost	93.70%	6.30%
Naresh et al. [20]	URLs	KNN, LR, RF, and SVM	91.40%	8.60%
Our Model (PPM3)	URLs	DT	91.30%	8.70%

5 Conclusion

In this paper, we designed and developed a predictive model for phishing attacks on MIA systems. The predictive model takes URLs as input and applies the machine learning algorithm to predict the authenticity of a URL and flags any suspicious phishing URL. The machine learning algorithm used is the Decision Tree. The developed model is an online mobile application developed in Python and SQL Server database. The users of the PPM solution can verify the legitimacy of any given URL before launching it on the web browser and can also download a list of previously predicted URLs with their statuses from the database. The developed model helps protect MIA system users from falling victims of phishing attacks and make them aware of already flagged URLs before launching them on the web browser. In this study, the decision tree machine learning algorithm was adopted, and the results were evaluated against other existing phishing algorithms. The developed predictive model can predict URL status with an accuracy of 91.3% and a mean squared error of 8.7%.

Acknowledgments. This research is undertaken in the department of computer science at the University of KwaZulu-Natal (UKZN). The authors would like to extend their special gratitude to the sponsors and the leadership of all the institutions who made it possible to carry out this research.

References

1. Statista, eCommerce Worldwide – Statistics and Facts. https://www.statista.com/topics/871/online-shopping/#editorsPicks. Accessed 28 April 2023
2. Visa Navigate, eCommerce Developments Across Sub Saharan Africa. https://navigate.visa.com/cemea/data-and-insights/sub-saharan-africas-ecommerce-potential/. Accessed 3 March 2023
3. Accounting Learning, eCommerce: What are Intelligent Agents? https://accountlearning.com/what-are-intelligent-agents-features-importance-advantages/. Accessed 8 June 2023
4. Patil, P.: Study on E-commerce security issues and solutions. Int. J. Comput. Sci. Mob. Comput. **6**(1), 100–102 (2017)
5. Niranjanamurthy, M., Chahar, D.: The study of e-commerce security issues and solutions. Int. J. Adv. Res. Comput. Commun. Eng. **2**(7), 1–12 (2013)
6. Mendeley Data: Web Page Phishing Detection. https://data.mendeley.com/datasets/c2gw7fy2j4/3. Accessed 20 July 2023
7. Pivk, A., Gams, M.: Intelligent agents in E-commerce. Electrotechn. Rev. **67**, 251–260 (2000)
8. CISCO, Email Security: What is phishing? https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html. Accessed 13 April 2018
9. Kogeda, O.P., Agbinya, J.I.: Proactive cellular network faults prediction through mobile intelligent agent technology. In: The Proceedings of the 2nd International Conference on Wireless Broadband and Ultra-Wideband Communications, pp. 27–30. Sydney, Australia (2007). ISBN: 978-0-7695-2846-5
10. Banday, M.T., Qadri, J.A.: Phishing - a growing threat to e-commerce, ISSN: 0972–8384, **12**(2), 76–83 (2007)
11. Jansen, W.A.: Intrusion detection with mobile agents. In: Proceeding of the Canadian Information Technology Security. Symposium, pp. 1–14. IPC Science and Technology Press, Ottawa, CA (2000)

12. Goel, D., Jain, A.K.: Mobile phishing attacks and defense mechanisms: state of art and open research challenges. Comput. Secur. **73**(1), 519–544 (2018)
13. Amro, B.: Mobile agent systems, recent security threats, and counter measures. Int. J. Comput. Sci. Issues **11**(2), 146–151 (2014)
14. Cui, Q., Jourdan, G.-V., Bochmann, G. V., Couturier, R., Onut.: Tracking phishing attacks over time. In: Proceedings of the 26th International Conference on World Wide Web. International World Wide Web Conferences Steering Committee, pp. 667–676. Republic and Canton of Geneva, Switzerland (2017)
15. Kumar, A., Roy, S.S., Saxena, S., Rawat, S.S.: Phishing Detection by determining reliability factor using rough set theory. In: Proceedings of International Conference on IEEE, pp. 236–240. Machine Intelligence and Research Advancement, Katra, India (2013)
16. Zhari, C., Hachicha, H., Ghedira, K.: Agent's security during communication in mobile system. Procedia Comput. Scie. **60**(2015), 17–26 (2015)
17. ITWeb. 2017. Phishing Response Trends Phishing response trends | ITWeb. Accessed 29 July 2018
18. The Ponemon Institute, Cost of Data Breach Study. https://www.ponemon.org/research/ponemon-library/security/2017-cost-of-data-breach-study-united-states.html. Accessed 28 July 2018
19. APWG, 4Q 2022 Phishing Activities Trends Report. https://docs.apwg.org/reports/apwg_trends_report_q4_2022. Accessed 15 August 2018
20. Naresh, K.D., et al.: Detection of phishing websites using an efficient machine learning framework. Int J. Eng. Res. Technol. **9**(5), 1–5 (2020)
21. Jalal, K., Naaz, S.: Detection of phishing websites using machine learning approach. In: Proceedings of International Conference on Sustainable Computing in Science, Technology and Management, pp. 1774–1781. Elsevier SSRN, New Delhi, India (2019)
22. Orunsolu, A.A., Alaran, M.A., Adebayo, A.A., Kareem, S.O., Oke, A.: A lightweight anti-phishing technique for mobile phone. Acta Informatica Pragensia, Prague Univ. of Econ. Bus. **6**(2), 114–123 (2017)
23. Gupta, B.B., Jain, A.K.: Phishing detection: analysis of visual similarity based approaches. Secur. Commun. Networks **2017**(4), 1–20 (2017)
24. Zhang, Y., Hong, I., Cranor, L.J.: Cantina: A content-based approach to detecting phishing websites. In: Proceedings of the 16th International World Wide Web, pp. 639–648. Association for Computing Machinery, New York (NY), United States (2007)
25. Alnemari, S., Alshammari, M.: Detecting phishing domains using machine learning. Appl. Sci. **13**(8), 4649 (2023)
26. Dharani, M., Soumya, B., Kimaya, G., Amarsinh, V., Dhanashri, B.: Detection of phishing websites using ensemble machine learning approach. In: ITM WE of Conferences 40, ICACC (03012), pp. 1–5 (2021)
27. Zhou, J.; Cui, H.; Li, X.; Yang, W., Wu, X.: A novel phishing website detection model based on LightGBM and domain name features. Symmetry **15**(1), 180 (2023)
28. Dong, H.L., Kim, H., Na, S.Y.: Prevention schemes against phishing attacks on internet banking systems. Int. J. Adv. Soft Comput. Appl. **6**(1), 1–15 (2014)
29. Padma, U.R., Sarannia, A.: Prevention model for phishing attacks in web applications using linkguard algorithm. Int. J. Innov. Res. Comput. Commun. Eng. **2**(1), 2889–2896 (2014)
30. Shahriar, H., Klintic, T., Clincy, V.: Mobile phishing attacks and mitigation techniques. J. Inf. Secur. **6**(3), 206–212 (2015)