Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.015859
Article

Tech Science Press

A Smart Comparative Analysis for Secure Electronic Websites

Sobia Wassan[1], Chen Xi[1,*], Nz Jhanjhi[2] and Hassan Raza[3]

[1]Nanjing University Business School, Nanjing, 210000, China
[2]School of Computer Science and Engineering SCE, Taylor's University, Subang Jaya, 47500, Malaysia
[3]Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Islamabad, 57000, Pakistan
*Corresponding Author: Chen Xi. Email: chenx@nju.edu.cn
Received: 11 December 2020; Accepted: 16 April 2021

Abstract: Online banking is an ideal method for conducting financial transactions such as e-commerce, e-banking, and e-payments. The growing popularity of online payment services and payroll systems, however, has opened new pathways for hackers to steal consumers' information and money, a risk which poses significant danger to the users of e-commerce and e-banking websites. This study uses the selection method of the entire e-commerce and e-banking website dataset (Chi-Squared, Gini index, and main learning algorithm). The results of the analysis suggest the identification and comparison of machine learning and deep learning algorithm performance on binary category labels (legal, fraudulent) between similar datasets, and understanding which function plays a vital role in predicting safe e-banking and e-commerce website datasets. The e-commerce and e-banking website dataset was compiled from the UCI machine learning library. We obtained 11,056 entries based on 30 unique website attributes. We used the machine learning algorithms support vector machine (SVM), k-nearest neighbors, random forest (RF), decision tree (DT), and the multilayer perceptron (MLP) deep learning algorithm to analyze the datasets of e-commerce and e-banking websites and found the best algorithms based on accuracy, precision, recall, and F1-measure. MLP had the highest precision at 97%. With this procedure we can now accurately test websites to assist in the early prediction of secure e-banking e-commerce transactions.

Keywords: Malicious; attack; secure; e-banking and e-commerce website; phishing; trust; privacy; machine and deep learning

1 Introduction

Malware websites are designed to look the same as the legitimate sites they intend to mimic. These fake websites have noticeable hyperlinks used to scam their victims, and they link to sites that appear similar to legitimate sites to fool users into trusting the site. Researchers have identified a rapid escalation in the number of malicious phishing websites in the past year, which lead victims to fake pages that request confidential information such as bank statements, credit card numbers, and passwords. These cyber threats are a broad-based social engineering attack that has caused serious problems in today's e-commerce and e-banking business [1].

Malicious actors involved in phishing—its name derived from catching fish—invite users, for example, via message or email, to take advantage of an opportunity, which is a scam [2]. Phishing scams have cost businesses tens of billions of dollars and can damage brand image and consumer trust as well [3].

Abdelhamid et al. [4] explained phishing detection approaches using different classification and data mining techniques; phishing approaches impact the performance of websites, which has a direct impact on customers and their reviews. Through text mining, authors can gain essential information from the dataset. Researchers could use this data mining method in several fields, such as retail business, consumer research, and decision-making analysis. The objective is to verify the possible usage of advanced data mining tools to identify complicated problems or malicious scams. Classification methods for such cases of online fraud include spelling mistakes, long URL suffixes, prefixes, and customization. These attributes can be obtained from different sites as well as smartphone apps.

Decision trees are beneficial for data analysis and machine learning because they decompose complex data into more manageable parts. They are commonly used in predictive analysis, data classification, and regression [5]. Each tree produces a category estimate in the random forest, and the most polled category is our model prediction; the trees guard each other against mistakes. Whereas individual trees can be incorrect, some are correct, and trees might migrate to the right track. K-nearest neighbors (KNN) algorithm is for nonparametric and lazy learning. The distribution of the analytical effects has no perception. In other words, the configuration of a model is specified by a dataset. This can be helpful as most real-world databases do not conform to statistical assumptions [6]. A support vector machine (SVM) is a supervised machine learning algorithm used for classification or regression. However, it is mainly used for classification problems [7].

This study compares the output of various machine learning and deep learning algorithms on binary class labels (valid, malfeasance) from the same datasets and identifies features that play a vital role in predicting secure e-commerce and e-banking websites. We used SVM, KNN, RF, DT machine learning algorithms, and a deep learning algorithm, multilayer perceptron (MLP). For this study, we used the selection method of the entire e-commerce and e-banking website dataset (Chi-Squared, Gini index, and main learning algorithm). We analyzed an e-banking and e-commerce website dataset based on these parameters, selecting the optimal algorithm based on precision, accuracy, recall, and F1-score. Our experimental results were used to evaluate the best accuracy of the MLP, which was 97%.

We now turn to our evaluation of the websites in the early phase to enable early forecasts for secure e-commerce and e-banking transactions.

The remainder of the article is structured as follows: Section 2 discusses related work and Section 3 outlines the methodology and data collection. Predictive methods are discussed in Section 4. Section 5 presents results and discussion and Section 6 is a final discussion of the article. Conclusions are addressed in Section 7.

2 Literature Review

The use of malicious software, or malware, is an illegal attempt to breach secure digital ecosystems to access personal information such as names, passwords, and bank account numbers. The e-banking and e-commerce sectors are more concerned with identity fraud than any other industry. Using software for phishing website analysis will help customers determine the reputation of a service they wish to use. A research tool accumulates and evaluates website parameters using different algorithms [8].

The banking industry uses the latest networking mechanisms, and it faces data security and privacy issues. Jain et al. [9] present a detailed analysis of e-banking activities, including e-banking issues and challenges, privacy, and other security threats, and their possible mitigation approaches.

E-commerce has also come to play a crucial role in fulfilling customer demand. With operating system (OS) support, e-commerce applications cannot function on the internet. Online business managers are usually careless and know nothing about possible cyber threats due to a lack of security knowledge [10].

Malicious websites are designed to perform illegal activities such as a number of different types of cyber-attacks. Latif et al. [11] describe various features of legal, suspect, and phishing attacks. Features input to WEKA built-in data mining techniques are used to compute and verify the proposed algorithm's performance. The proposed methodology in Latif et al. [11] can be used to evaluate a website's trustworthiness while making payments.

The fundamental forms of banking fraud from the digital world are identified. The authors suggest a scientific model that explains the mechanism of electronic banking crime. The proposed model was established on the classic Lotka-Volterra logistic growth model and the Holling-Tanner dynamic model. Unfortunately, it is impossible to investigate this problem based on real facts while cyber challenges are locked [12].

The study explores the consequences of electronic banking services on electronic trust using an electronic safety system. Findings show that an electronic bank service has an overall effect on the e-trust mechanism. This study aimed to develop an e-banking model from a security perspective [13].

While the volume of payments being made over the internet is increasing at a furious pace, cyber-attack techniques are likewise proliferating. A survey report analyzed the digital e-payment system and its prospects. It briefly addresses fraudulent transaction rates that will become benchmarks for implementing a reliable e-payment system [14].

This article discusses the implementation of electronic banking in Colombia. The empirical study, based on the UTAUT2 model, gathered data from around the world, assuming that the factors that build confidence in e-banking are essential [15].

Sarkar et al. [16] discusses the use of encryption key privacy preservation watermarking to protect e-banking records, citing a method in which a picture was split into eight fragments for the embedding of sensitive information. Eight characters are required for eight consecutive lines to form the block key [16].

Alghazo et al. [17] presents a theoretical framework based on e-banking surveys in Saudi Arabia, India, and Pakistan. In this study the evaluation was focused on customer behaviors. Based on 1,045 credit card operators and 91 online payment sites, the findings of this analysis indicated the difference between bank preferences and user feedback.

Privacy and accessibility are also essential issues in e-banking. Companies have invested extensively in the security and user interface of their websites. Alarifi et al. [18] suggests a formal evaluation model for a comprehensive examination of the accessibility and protection of internal and external e-banking properties. The author uses the proposed model to test five central banks to show the inadequacy of current models. The assessment shows several flaws in the identification of missing and incorrectly configured security and privacy functions. The purpose is to allow other researchers to build on their observations and extend their work.

Generally, these methods are based on multiple characteristics derived from many sites. These same functions can distinguish malicious attacks from real attacks. If the website algorithm's architecture is compatible with clearly specified rules, the website is declared a malware scam. This article provides a detailed study of security attacks, manipulation, and the latest machine learning methods for detecting malicious attacks [19].

From the perspective of individual consumers over the past two decades, the main goal has been to classify Russia's best e-banking platforms. Banks use digital IT technology to build strategic advantages

and use some solutions to leverage banking services to benefit customers. The groups listed are categorized into three groups: financial, technological, and anti-crisis [20].

Trust has never been a critical factor in e-commerce research. To maintain an understanding of the application of e-banking, in this study, the author addresses incorporating trust into total addressable marketing (TAM). Directly and indirectly, the two essential factors of legitimacy and reputation of trust affect the attitude toward the internet banking industry's applications and behavioral motives [21]. This research distinguishes from the same datasets between performance comparisons of several machine learning and deep learning algorithms on binary target classes (valid, malfeasance) and to understand which feature plays an essential role in predicting secure websites for e-commerce and e-banking.

Kok et al. [22] proposes that malware will prevent access to the target service before paying for it. For encrypted ransomware identification before any encryption, in this article, the author recommends using the drug detection algorithm (PEDA) [22].

Saeed et al. [23] shed light on the fact that malware may encrypt all data to prevent users from accessing sensitive data and information. The smart phones with the least resources requires additional processing power and resources, and conventional protection measures are no longer allowed. Author analyzed the effect of malware on the internet of things (IoT).

Smart cities use ICTs to improve their residents' quality of life by paving the way for urban infrastructure to strengthen, upgrade the transportation sector, and manage transport. The report has established and predictable multiple security and data protection threats related to different computer security issues, challenges, and recommendations, including potential guidance. It identifies cyber-threats based on new research [24].

The study of data defense to promote cyber-technologies has grown immensely. The purpose of this analysis is presented in Humayun et al. [25] to recognize and examine common errors in cybersecurity. Researchers have found primary errors such as rejection of service, phishing, and malware. According to previous work by Humayun et al. [25] primary errors, targeted/victimized applications, mitigation strategies, and infrastructures need to be established.

3 Methodology and Data Collection

The fundamental purpose of this analysis is to classify features that separate legitimate and malicious websites. Some analysis may also be conducted using different Python algorithms to classify certain features to discover more variations in the website's groups. Fig. 1 displays our research methods. The dataset of e-banking and e-commerce websites was obtained from the UCI machine learning library. We collected 11,056 entries based on 30 attributes, as shown in Fig. 2. We then used SVM, KNN, RF, Decision Tree, and Multilayer Perceptron MLP.

4 Predictive Methods

4.1 Decision Tree Classifier

A decision tree (DT) can be customized for classification and estimation. The expansion of a decision tree works with conditions such as "if," "this," and "then" strokes. Decision Tree is simple to understand, and accessible to a large dataset. DT also provides an optimum solution to each step without agreeing on an optimum solution at the final stage. Decision Tree classifier is a tree-based algorithm. The root has the highest nodes, decision procedures represent classes, and leaf nodes display the results. The tree is recursively split.

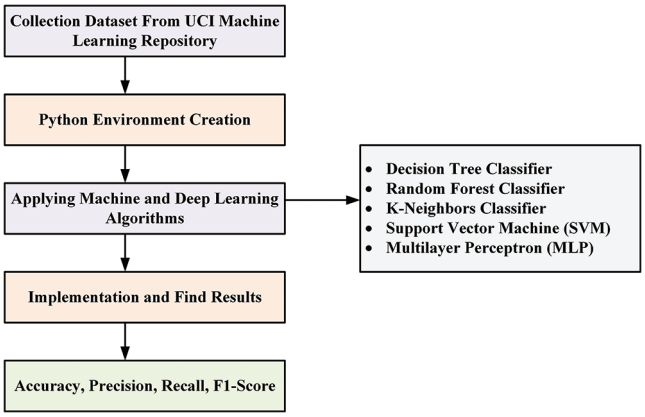

Figure 1: Process diagram for stable e-commerce and e-banking sites

1	having_IP	URL_Leng	Shortining	having_At	double_sl	Prefix_Su	having_Su	SSLfinal_S	Domain_r	Favicon	port	HTTPS_tol	Request_l	URL_of_A	Links_in_t	SFH	Submittin	Abnormal
2	-1	1	1	1	-1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	-1	-1
3	1	1	1	1	1	-1	0	1	-1	1	1	-1	1	0	-1	-1	1	1
4	1	0	1	1	1	-1	-1	-1	-1	1	1	-1	1	0	-1	-1	-1	-1
5	1	0	1	1	1	-1	-1	-1	1	1	1	-1	-1	0	0	-1	1	1
6	1	0	-1	1	1	-1	1	1	-1	1	1	1	1	0	0	-1	1	1
7	-1	0	-1	1	-1	-1	1	1	-1	1	1	-1	1	0	0	-1	-1	-1
8	1	0	-1	1	1	-1	-1	-1	1	1	1	1	-1	-1	0	-1	-1	-1
9	1	0	1	1	1	-1	-1	-1	1	1	1	-1	-1	0	-1	-1	1	1
10	1	0	-1	1	1	-1	1	1	-1	1	1	-1	1	0	1	-1	1	1
11	1	1	-1	1	1	-1	-1	1	-1	1	1	1	1	0	1	-1	1	1
12	1	1	1	1	1	-1	0	1	1	1	1	1	-1	0	0	-1	-1	-1
13	1	1	-1	1	1	-1	1	-1	-1	1	1	1	1	-1	-1	-1	-1	-1
14	-1	1	-1	1	-1	-1	0	0	1	1	1	-1	-1	-1	1	-1	1	1
15	1	1	-1	1	1	-1	0	-1	1	1	1	1	-1	-1	-1	-1	1	1
16	1	1	-1	1	1	1	-1	1	-1	1	1	-1	1	0	1	1	1	1
17	1	-1	-1	-1	1	-1	0	0	1	1	1	1	-1	-1	0	-1	1	1
18	1	-1	-1	1	1	-1	1	1	-1	1	1	-1	1	0	-1	-1	-1	-1
19	1	-1	1	1	1	-1	-1	0	1	1	-1	1	1	0	-1	-1	-1	-1
20	1	1	1	1	1	-1	-1	1	1	1	1	-1	-1	0	-1	-1	-1	-1

Figure 2: Screenshot of the sample dataset of e-commerce and e-banking websites

4.2 Random Forest Classifier

Random forests are a robust machine learning algorithm that can be used for various tasks, including regression and classification. This is an ensemble method, which means that the random forest model consists of many small decision trees, called deciders, each of which produces its own predictions. The random forest model combines estimator predictions to produce more accurate predictions. As long as they do not move the same way, the trees protect each other from producing errors. While individual decision trees may produce errors, the majority of the group will be correct, thus moving the overall outcome in the right direction.

4.3 K-Neighbors Classifier

KNN is a nonparametric, lazy algorithm; that is to say, no assumptions are made about the fundamental distribution of data. The dataset specifies the configuration of the model. It helps ensure that all datasets in the real world are inconsistent with statistics and empirical assumptions. A lazy algorithm requires no training datasets. However, while preparation for KNN is relatively fast, testing is slow and expensive and can require much data storage.

4.4 Support Vector Machine (SVM)

SVMs are also supervised learning models with similar machine learning algorithms that estimate the knowledge used for regression and describes machine learning. The algorithm constructs a model of training examples consisting of a sequence of courses, each categorized with a paired group and allowing for an anti-contingent classification model. The model portrays examples as space points, determined to guarantee that only a certain distance separates class examples. Previously, instances were traced at the same location and calculated as belonging to a time-based division. The algorithm aims to locate a hyperplane with a distinct category of datasets in an N-dimensional region (i.e., N features).

4.5 Multilayer Perceptron (MLP)

An MLP is a backpropagation CNN. It has more than one layer; the sensor input nodes and sensor output layer decide the signal. For these two layers, the junk in each hidden layer is the MLP computing system. MLP is a linear classifier algorithm to partition straight-line data into two sections. When MLP has such a nonlinear vector activation in each hidden layer, graph theory implies that any layer may be lower than the activation function of two layers. Fig. 3 demonstrates the MLP structure, where the activation function contains 36 features and three invisible layers. The product is binary, indicating that a website is either safe or not. MLP depends on learning techniques with backpropagation. Errors on the output node z with such an instance point are computed as:

$$e_z(x) = b_z(x) - y_z(x)\,, \tag{1}$$

where b is an expectation and y is the estimated value.

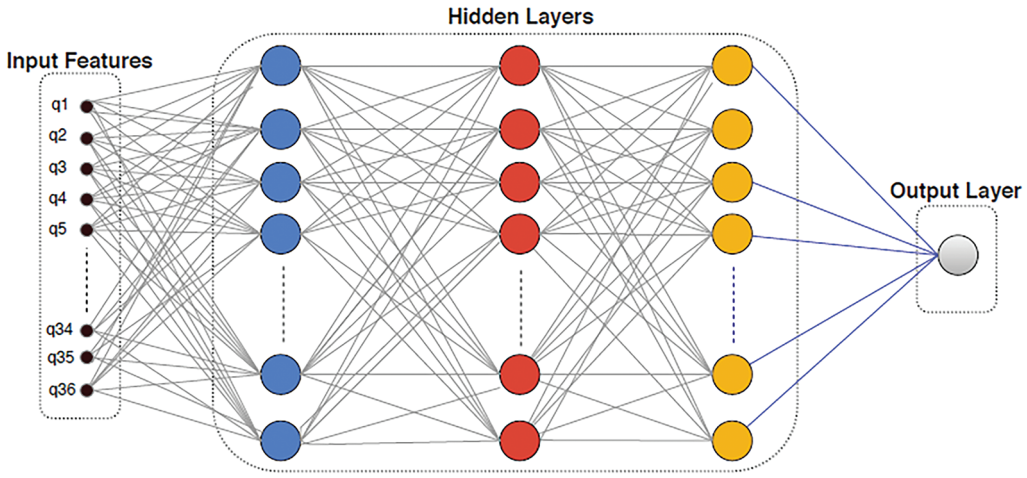

Figure 3: MLP architecture of a neural network used to protect e-banking and e-commerce websites

The backpropagation weight is changed to reduce performance layer error when there is an absolute simultaneous error,

$$\in (x) \; = \frac{1}{2}\sum_{z} e_z^2(x). \tag{2}$$

The gated recurrent unit (rectified linear) is a feature of activation. ReLU is computed as

$$y = n^{+} = max(0, n), \tag{3}$$

where x appears to be the input of the perceptron.

The hyperbolic tangent and logistic equation both use a kernel function, but ReLU is significantly better, so high-profit margin x does not lack regression problems. Once these optimization algorithms are adjusted to hyperparameters, ReLU can be obtained. Both parameters for which this model is designed are accumulated utilizing hyperparameter tuning. “Epoch” is a commonly used term in computer programs.

5 Results and Discussion

We conducted a review focused on the security issues of e-commerce and e-banking webpages with the combination of the various machine learning algorithms discussed above. We estimated recall, precision, accuracy, and F-score for computing different algorithm performance to determine an algorithm for secure analysis.

5.1 Calculated Results of Machine Learning Algorithms

The DT algorithm was 91% accurate. The macro average and weighted average ratios for recall, precision, and F-score were the same, at 91%. The decision tree representation of the classifier of the decision tree can be seen in Fig. 4.

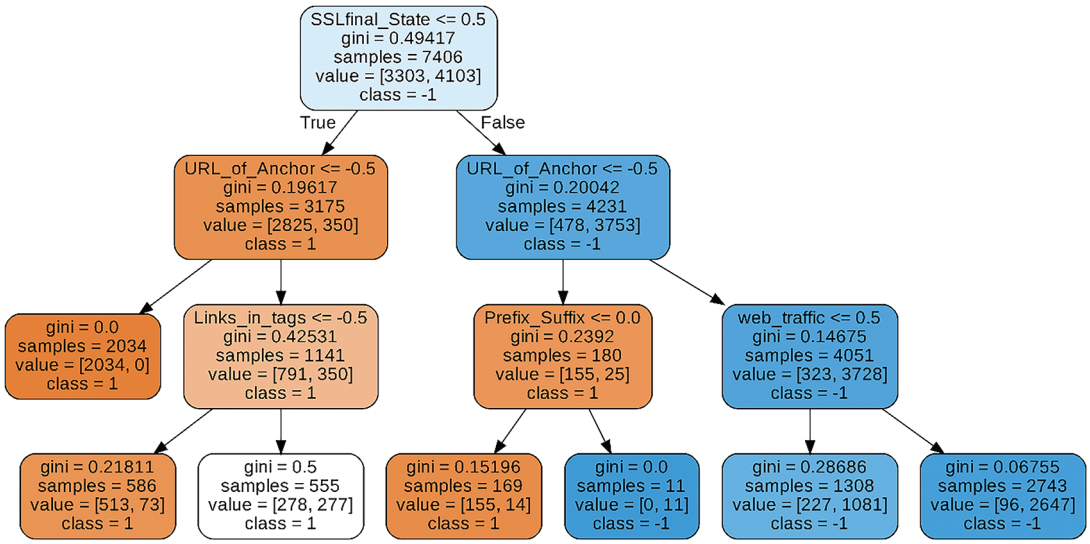

Figure 4: The decision tree visualization of the decision tree algorithm

The RF algorithm was 93% accurate. Precision, recall, and F-score were 93%, 92%, and 91%, respectively. The precision weighted ratio for F1 was 93%.

KNN was 94% accurate. The macro average ratios for precision, recall, and F-score were 93%, 94%, and 94%, respectively, and the corresponding ratios of the weighted average were the same, at 94%.

SVM was 95% accurate. The ratios of the macro average for precision, recall, and F-score were all 95%, as were the weighted average ratios.

MLP was the most accurate of all algorithms tested, at 97%. The macro average ratios for precision, recall, and F-score were 97%, 96%, and 97%, respectively, and the corresponding ratios of the weighted average were the same, at 97%.

MLP had the highest accuracy, 97%, *because* it was the most accurate to scrutinize secure e-commerce and e-banking websites, as shown in Tab. 1.

Table 1: The statistical evaluated the different ML and DL algorithms

Decision Tree			
	(Precision)	(Recall)	(F1-Score)
–1	(0.89)	(0.91)	(0.90)
+1	0.93	(0.91)	(0.92)
Accuracy			(0.91)
Macro average	(0.91)	(0.91)	(0.91)
Weighted average	(0.91)	(0.91)	(0.91)
Random Forest			
	Precision	Recall	F1-Score
–1	(0.95)	(0.88)	(0.91)
+1	(0.91)	(0.96)	(0.94)
Accuracy			(0.86)
Macro average	(0.93)	(0.92)	(0.92)
Weighted average	(0.93)	(0.93)	(0.93)
K-Neighbor Algorithm			
	Precision	Recall	F1-Score
–1	(0.90)	(0.96)	(0.93)
+1	(0.97)	(0.92)	(0.94)
Accuracy			0.94
Macro average	(0.93)	(0.94)	(0.94)
Weighted average	(0.94)	0.94	(0.94)
Support Vector Machine (SVM)			
	Precision	Recall	F1-Score
–1	(0.96)	(0.92)	(0.94)
+1	(0.94)	(0.97)	(0.96)
Accuracy			(0.95)
Macro average	(0.95)	(0.95)	(0.95)
Weighted average	(0.95)	(0.95)	(0.95)

Table 1 (continued).

Decision Tree			
Multilayer Perceptron (MLP)			
	Precision	Recall	F1-Score
–1	(0.97)	(0.95)	(0.96)
+1	(0.96)	(0.98)	(0.97)
Accuracy			(0.97)
Macro average	(0.97)	(0.96)	(0.97)
Weighted average	(0.97)	(0.97)	(0.97)

5.2 Precision-Recall Curve

Precision-recall is a strong indicator of prediction performance when classes are significantly different. Accuracy measures the importance of results in processing details; therefore, recall measures whether the results are correct. The precision-recall curve suggests a balance between accuracy and the recall of numerous thresholds. A large area under the arc provides high precision and a high level of recall. High accuracy leads to a low rate of false positives and high recall at a low false-negative rate. Accuracy results indicate that the classifier produces the correct results (good performance) and produces positive results (high recall). Fig. 5 shows a graphical representation of the high-precision curves of various machine learning methods. We evaluated that MLP had the highest precision-recall graph, and average precision equaled 0.95. However, the accuracy of the decision tree algorithm was low.

Fig. 6 displays the confusion matrix for the design process of SVM, KNN, RF, and DT.

6 Discussion

We compared machine learning algorithms and one deep learning algorithm on a dataset of e-commerce and e-banking websites with different attributes and two classes. We concluded from this comparison that, if we developed a webpage in a real-time environment to detect the websites, we could use the deep learning algorithm as back-end support. Our analysis also showed that the MLP belonging to the deep learning family has the highest accuracy related to deep learning algorithms.

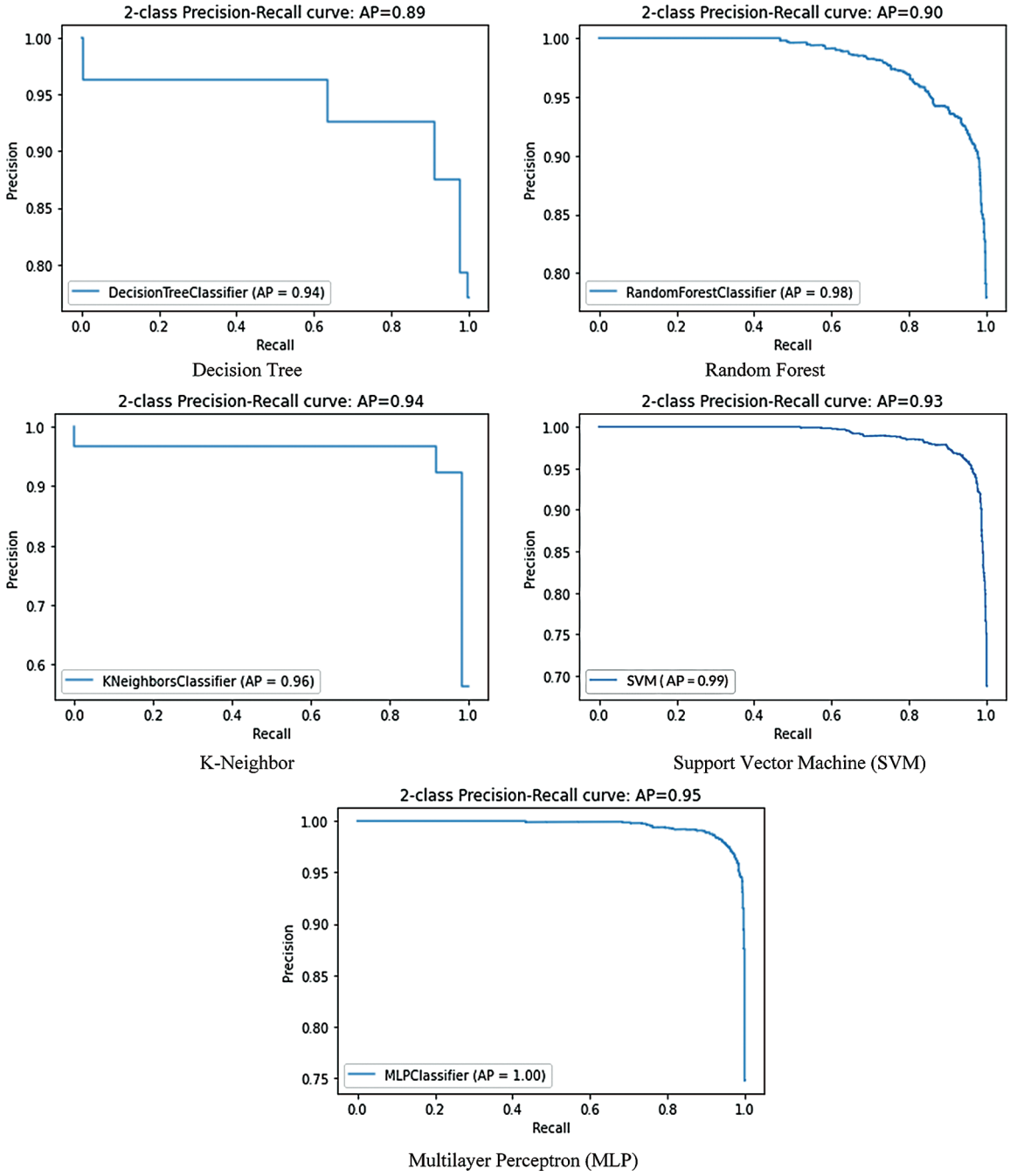

Figure 5: Display precision, recall curve with different DL and ml algorithm

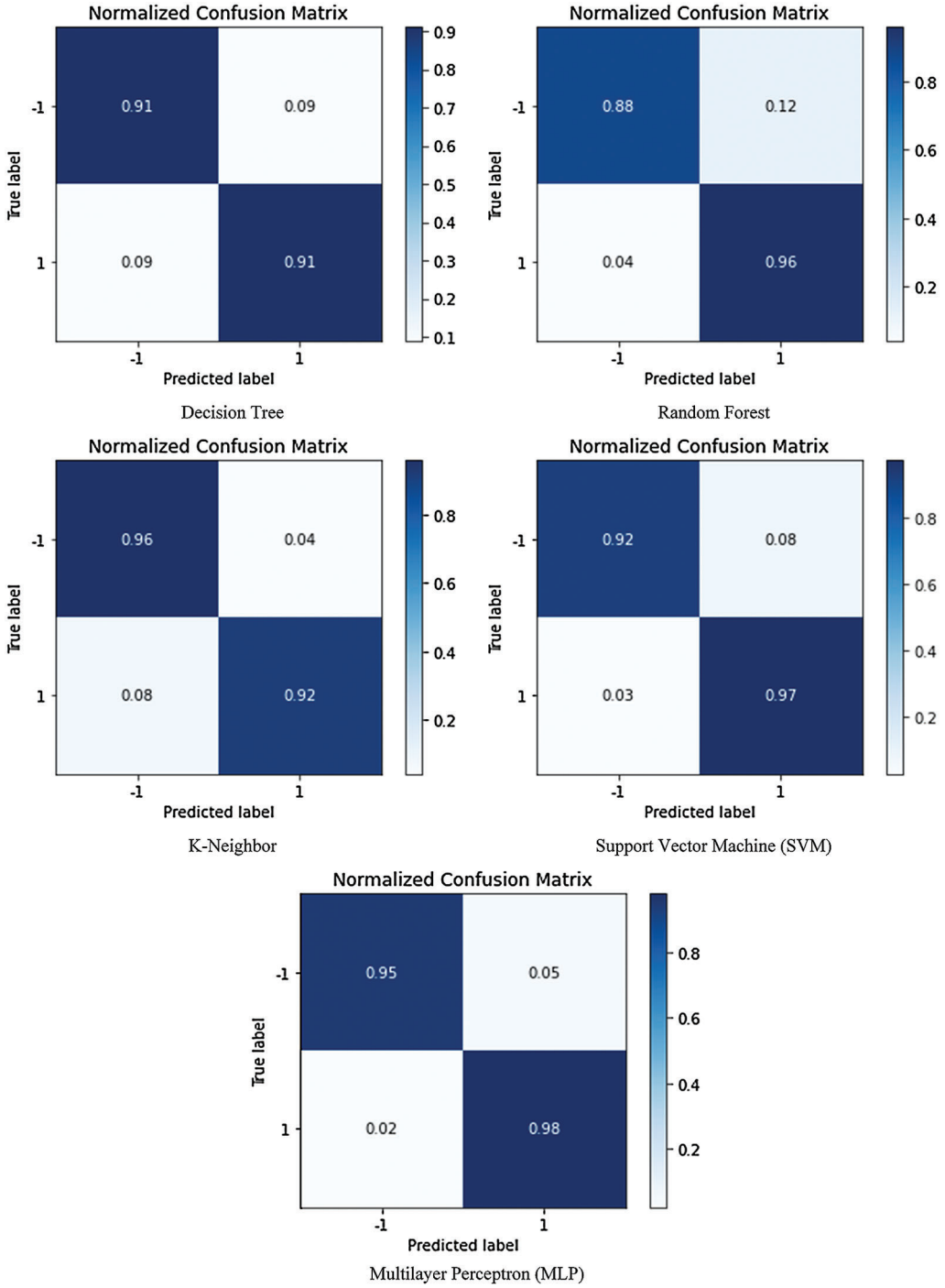

Figure 6: The graphical representation of the confusion matrix of the different ML and DL algorithm

7 Conclusion

Online service in the Pakistani banking sector gives access to a plan for the use of digital technologies to advance organizational performance and service superiority to attract and engage customers. Using ATMs in Pakistani banking networks provides banks with opportunities to gain customers' overall enthusiasm to implement a more profitable service. This research enables bankers to perform efficient tracking. Banks should focus on essential features of trust, time, and effective handling of ATMs and other services. They can extend their ATM commitment to craft a lasting relationship with regular customers. We compared various machine learning and deep learning methods on binary-type labels (legitimate, scam) on the same dataset. We evaluated e-banking and e-commerce websites' datasets based on all these methodologies and discovered the optimum solution based on accuracy, precision, recall, and F1-measure and found that MLP had the best accuracy, at 97%, this helps pre scanning of the web to provide security against fraud.

8 Future Work

In the future, we will build a website or network on which we can deploy this idea for secure e-commerce and e-banking websites. We can do more practice on data set features in deep learning methods, preferably more accurate than machine learning methods.

Funding Statement: The work was supported in part by the National Natural Science Foundation of China under Grant Nos. 71771118, 72071104 and 71471083, by the Ministry of Education Humanities and Social Sciences Foundation of China under Grant No.18YJCZH146, and by the Key Project of Jiangsu Social Science Foundation under Grant No. 20GLA007.

Conflict of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. R. Ibrahim and A. H. Hadi, "Phishing websites prediction using classification techniques," in *Proc. 2017 Int. Conf. on New Trends in Computing Sciences (ICTCS)*, Amman, Jordan: IEEE, pp. 133–137, 2017.

[2] M. Kayatan and D. Hanbay, "Effective classification of phishing web pages based on new rules by using extreme learning machines," *Bilgisayar Bilimleri*, vol. 2, no. 1, pp. 15–36, 2017.

[3] W. Ali, "Phishing website detection based on supervised machine learning with wrapper features selection," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 9, pp. 72–78, 2017.

[4] N. Abdelhamid, A. Ayesh and F. Thabtah, "Phishing detection based associative classification data mining," *Expert Systems with Applications*, vol. 41, no. 13, pp. 5948–5959, 2014.

[5] D. S. Campo, G. L. Xia, Z. Dimitrova, Y. Lin, J. C. Forbi *et al.,* "Accurate genetic detection of hepatitis C virus transmissions in outbreak settings," *Journal of Infectious Diseases*, vol. 213, no. 6, pp. 957–965, 2016.

[6] M. Ali, A. Yopp, P. Gopal, M. S. Beg, H. Zhu *et al.,* "A variant in PNPLA3 associated with fibrosis progression but not hepatocellular carcinoma in patients with hepatitis C virus infection," *Clinical Gastroenterology and Hepatology*, vol. 14, no. 2, pp. 295–300, 2016.

[7] V. V. Chirikov, F. T. Shaya, E. Onukwugha, C. D. Mullins, S. Dosreis *et al.,* "Tree-based claims algorithm for measuring pretreatment quality of care in Medicare disabled hepatitis C patients," *Medical Care*, vol. 55, no. 12, pp. 104–112, 2017.

[8] S. J. Pai, R. Gokuldas, R. Kakkadan, S. Hegde and M. S. Suvarna, "Phishing website analyzer to secure e-banking and e-commerce websites," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 2, no. 5, pp. 510–520, 2020.

[9] A. Jain and A. Sarupria, "Security and privacy model for analyzing the consumer awareness with regards to electronic banking services in Udaipur city," *International Journal of New Technology and Research (IJNTR)*, vol. 6, no. 6, pp. 34–44, 2020.

[10] R. I. Royel, M. H. Sharif, R. Risha, T. Bhuiyan, M. M. Hassan *et al.,* "A risk based analysis on linux hosted E-commerce sites in Bangladesh," in *Proc. 2020 Int. Conf. on Cyber Security and Computer Science*, Dhaka, Bangladesh: Springer, pp. 140–151, 2020.

[11] R. M. A. Latif, M. Umer, T. Tariq, M. Farhan, O. Rizwan *et al.,* "A smart methodology for analyzing secure e-banking and e-commerce websites," in *Proc. 2019 16th Int. Bhurban Conf. on Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan: IEEE, pp. 589–596, 2019.

[12] O. Syniavska, N. Dekhtyar, O. Deyneka, T. Zhukova and O. Syniavska, "Security of e-banking systems: Modelling the process of counteracting e-banking fraud," in *SHS Web of Conf.*, Odessa, Ukraine: EDP Sciences, vol. 65, pp. 03004–03009, 2016.

[13] M. N. Esfahani, "E-bank services: Analyzing the effect of e-bank service on e-trust with e-security approach," *European Research Studies Journal*, vol. 22, no. 1, pp. 158–166, 2019.

[14] J. Yomas and C. Kiran, "Critical analysis on the evolution in the e-payment system, security risk, threats and vulnerability," *Communications on Applied Electronics*, vol. 7, no. 23, pp. 21–29, 2018.

[15] J. A. Sánchez-Torres, A. V. Sandoval and J. A. S. Alzate, "E-banking in Colombia: Factors favouring its acceptance, online trust and government support," *International Journal of Bank Marketing*, vol. 36, no. 1, pp. 170–183, 2018.

[16] A. Sarkar and S. Karforma, "Image steganography using password based encryption technique to secure e-banking data," *International Journal of Applied Engineering Research*, vol. 13, no. 22, pp. 15477–15483, 2018.

[17] J. M. Alghazo, Z. Kazmi and G. Latif, "Cyber security analysis of internet banking in emerging countries: User and bank perspectives," in *Proc. 2017 4th IEEE Int. Conf. on Engineering Technologies and Applied Sciences (ICETAS)*, Salmabad, Bahrain: IEEE, pp. 1–6, 2017.

[18] A. Alarifi, M. Alsaleh and N. Alomar, "A model for evaluating the security and usability of e-banking platforms," *Computing*, vol. 99, no. 5, pp. 519–535, 2017.

[19] A. K. Jain and B. Gupta, "Comparative analysis of features based machine learning approaches for phishing detection," in *Proc. 2016 3rd Int. Conf. on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India: IEEE, pp. 2125–2130, 2016.

[20] W. Chmielarz and M. Zborowski, "Comparative analysis of electronic banking websites in Poland in 2014 and 2015," in *Information Technology for Management*, 1st ed., vol. 243. Lodz, Poland: Springer, pp. 147–161, 2016.

[21] K. B. Mansour, "An analysis of business' acceptance of internet banking: An integration of e-trust to the TAM," *Journal of Business and Industrial Marketing*, vol. 31, no. 8, pp. 982–994, 2016.

[22] S. Kok, A. Azween and N. Jhanjhi, "Evaluation metric for crypto-ransomware detection using machine learning," *Journal of Information Security and Applications*, vol. 55, no. 2, pp. 102646–102660, 2020.

[23] S. Saeed, N. Jhanjhi, M. Naqvi, M. Humayun and S. Ahmed, "Ransomware: A framework for security challenges in internet of things," in *Proc. 2020 2nd Int. Conf. on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia: IEEE, pp. 1–6, 2020.

[24] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber security issues and challenges for smart cities: A survey," in *Proc. 2019 13th Int. Conf. on Mathematics, Actuarial Science*, Karachi, Pakistan: Computer Science and Statistics (MACS), pp. 1–7, 2019.

[25] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3171–3189, 2020.