Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

SI-BBA – A novel phishing website detection based on Swarm intelligence with deep learning

Parvathapuram Pavan Kumar *, T. Jaya, V. Rajendran

Department of ECE, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamilnadu 600117, India

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Uniform Resource Locator (URL)
Internet Protocol (IP)
Swarm Intelligence Binary Bat Algorithm (SI-BBA)
Deep learning (DL)
Bat Algorithm (BA)

ABSTRACT

Websites phishing is one of several defense coercions to Internet Service Provider. Mainly web phishing focused on stealing private information such as username, password, and credit card details too through imitating a legal creature. Deep learning based Neural Networks are extensively used for phishing detection with high accuracy measures and metrics. In this proposed work, an improved version of Binary Bat namely Swarm Intelligence Binary Bat Algorithm is used for designing the neural network which categorize the network URL websites similar to classification approach. It is utilized for the initial moment in this domain of relevance to the preeminent of our understanding. Our experimental results shows that deep learning based Adam optimizer reaches high classification accuracy as 94.8% in phishing websites attack detection based on swarm intelligence technique.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

1. Introduction

Phishing attack is a kind of societalproductionassaultfrequently utilized to embezzle user's information, comprising of login testimonials as well as credit card numbers. This happensonce an aggressor, hidden as a faithindividual, dupes a victim into modifyingemail information, such as instantaneous message, or content message. An attack may leads todestructive outcomes. Adebowale et. al [1] work payed attention on the design as well as development of phishing websites clarification which influenced URL and website related images, frames and text. For that, the author proposed hybrid (Intelligent Phishing Detection System) model which are integrated with CNN based algorithms and LSTM. Bo wei et. al [9] introduced light weight deep learning based model to distinguish the malevolent URL also facilitate in real time, power saving phishing URL detection sensor were used. Lakshmi et. al [17] utilized 30 features to identify malicious web pages. Moreover, deep learning based Adam optimizer method was applied for distinguishing malicious web pages from normal web sites. Finally the performances were compared with other conventional machine learning approaches for finding which algorithm generated best outcomes in detecting phishing websites. [33–35]

1.1. Approaches in phishing URL attack

The methods used in phishing URL attack are as follows:

- Email Phishing- Mainly harasses is throwing by email.
- Spear Phishing- Another two complicated harass comprising in emails are whaling, Smishing and Vishing.
- Angler Phishing-performed hidden as a customer service financial credit on social media, hopeful to accomplish thedispleased consumer.

Several ways to prevent phishing attacks are as follows

- Distinguish what a phishing trick looks like
- Do not click on that specific link
- Should fix the firewalls to prevent the attackers
- Spin the user passwords frequently
- Find free anti-phishing trappings.
- Do not provide user's information to any sites which is not secure
- Pay attention to the updates regarding sites
- Do not get excited by pop-ups.

The illustration of phishing attack efforts are described as follows

* Corresponding author.
E-mail address: ppavankumar432@gmail.com (P. Pavan Kumar).

https://doi.org/10.1016/j.matpr.2021.07.178
2214-7853/
Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

Please cite this article as: P. Pavan Kumar, T. Jaya and V. Rajendran, SI-BBA – A novel phishing website detection based on Swarm intelligence with deep learning, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2021.07.178

- A spoofed email supposedly from the link (myuniversity.edu) is mass-disseminated to as several faculty members as probable.
- The electronic mail declares that the password of user is going to terminate. Instructions are given to go to myuniversity.edu/renewal to renovate their password within a day (24 h).

The categorizing of phishing attack issues along with its solutions were developed by Benavides et. al [8,12] using deep learning based algorithms shown in Fig. 1.

Our work focused on detecting attack in the network environment especially in URL websites and categorizing the same into malicious and legitimate [14]. For that, we are implementing novel approach namely SI_BBA for categorizing the network data into legitimate and malicious which may helpful for several organization using network facilities [29].

1.2. Objectives

The main objective of this proposal is

- To train the neural network using a swarm intelligence approach.
- To develop an algorithm called "A novel SI-BBA (Swarm Intelligence – Binary Bat Algorithm) to predict the phishing websites.
- To enhance the performance level of every deep based optimizer approach, measuring has performed as well as compared.

Ram Basnet et. al [25] introduced novel approach namely heuristic based approach to categorize phishing attack as positive and normal mentioned as negative by means of information existing only in URLs. False Positive Rate, and Error rate are the metrics were evaluated to detect the attack depends on dissimilar features in URL. The Fig. 2 illustrates the general idea about phishing URL attack detection framework using machine learning approaches developed by [25].

2. Related work

Somesha et. al [18] developed several models such as deep based Neural Network, Long short term Memory, CNN for detecting phishing URL websites. These models achieve accuracy as 99.5% for Neural Networks, 99.6% for Long Short Term Memory, and 99.4% for CNN. This proposed model makes the model vigorous to malfunction and enhances the phishing recognition speed. Suleiman Y. Yerima et. al [28] and I Saha et. al [15] introduced deeplearning based CNN approach to obtain high accuracy classification to categorize the authentic websites from phishing websites. Yi et. al [30] recognize the phishing sites by using deep learning structure. First and foremost features designed for phishing websites namely original and interaction features. Aksu et. al [3] Identifying whether the websites are true or fake by using NN, SVM, DT, auto-encoders were utilized as classification approaches. M. N. Alam et. al [19] and Alloghani et. al [4] phishing URL were detected by means of machine learning algorithms [26]. Alam utilized ML approaches like DT and RF in which RF attains greater accuracy in phishing URL detection as 97%. Basit et. al [6] reviewed several techniques such as Deep learning, machine learning, scenario based and hybrid based approach utilized for phishing URL sites detection. Moreover comparisons were performed among all those algorithms. Begum et. al [7] studied several techniques used by various researchers for finding phishing URL websites and pros, cons were discussed for all algorithms. Cuzzocrea et. al [10] To find the websites activities, the author applied machine learning algorithms in order to build model which had ability to differentiate the phishing from legitimate users using indicators. Geetha et. al [13] surveyed several machine learning and deep learning algorithm which helpful to detect the phishing websites consequently that generates secure solutions for cyber security. Ram et. al [25] developed ML algorithm to detect the phishing websites highly effective that attains error rate as 30%, FPR as 20%, and FNR as 50% and Arun kulkarni et. al [5], preeti et. al [22] also applied machine learning approaches for detecting phishing URL websites. Jalil et. al [16] studied many machine learning approaches used by various existing work for identifying phishing attacks in the websites. Rajaram et. al [24] studied several existing works to detect the phishing websites in real time and also non real time using visual based images through CNN approach. Rahman et. al, Soon et. al [23,27] performed comparative study for phishing sites detection among FFNN and DLNN. At last, the evaluation had done which algorithm suitable for phishing sites detection [31,32].

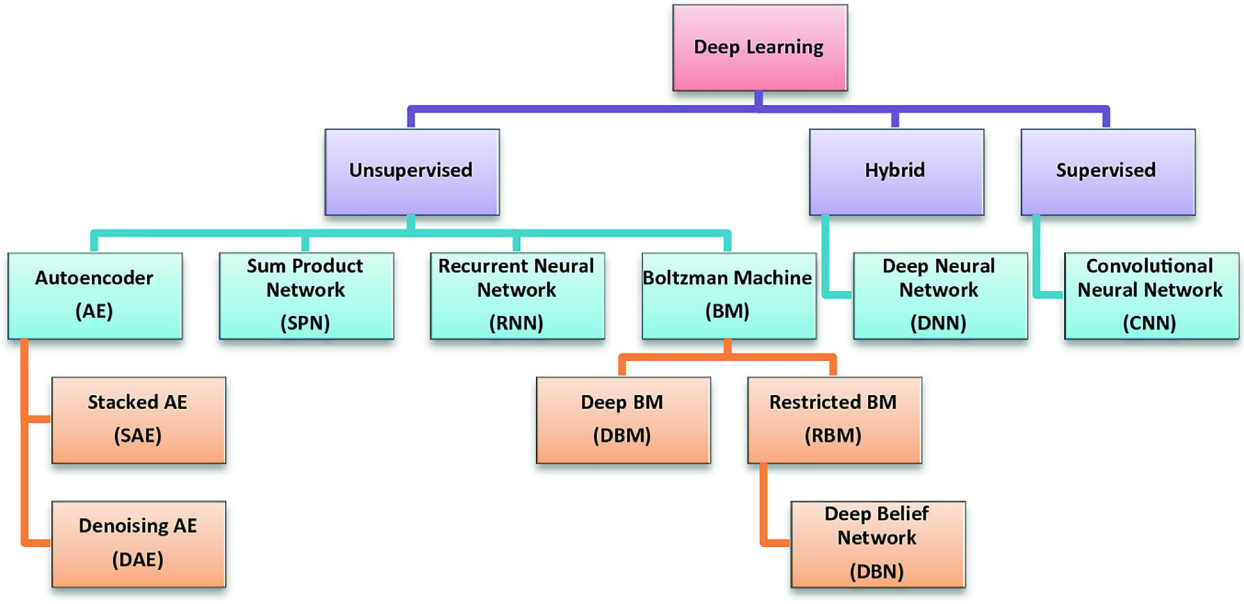

Fig. 1. Phishing detection framework using DL.

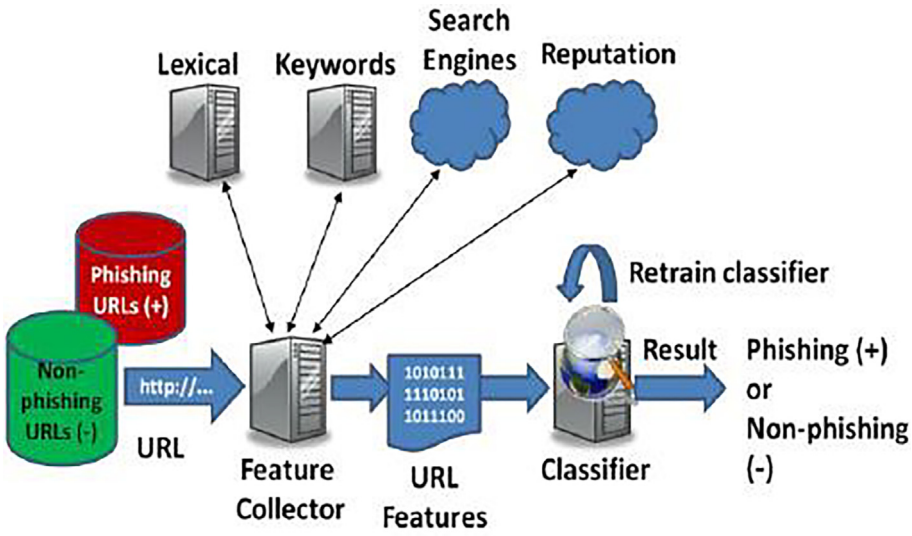

Fig. 2. Phishing websites classification using ML.

3. Flow of proposed method

3.1. Phishing data acquisition

The benchmark dataset phishing.csv is downloaded from the following link https://www.kaggle.com/akashkr/phishing-url-eda-and-modelling/data. Here, we have taken 4898 samples from legitimate websites and phishing websites samples as 6157.

3.2. Preprocessing

The primary processing of data in order to prepare it for primary processing or for further analysis. It eliminates the features that contain missing values or null values.

3.3. 3.3 Feature extraction

The relevant features related to phishing websites URL are extracted through this phase. Here, the features such as URL length, abnormal URL, statistical reports etc are mined for phishing URL detection.

3.4. Proposed SI-BBA algorithm

One of the computational intelligence techniques is swarm intelligence that are utilized to resolve the complex issues with prehistoric persons who are self structured, offered litheness, and sturdiness even once the situations are modifying. Similarly in the case of phishing URL attack detection systems, SI algorithms have been useful for parameter extraction and classification process as a self determining module or else integrated with some other well known predictive models. The Fig. 3 depicts our proposed workflow for phishing websites detection.

3.4.1. BAT algorithm

The Bat-inspired Algorithm (BA) is a *meta*-heuristic algorithm developed in 2010 by Yang [21]. This algorithm is based on the echolocation behavior of micro bats with varying pulse rate of emission along with loudness. In search for a prey, these individuals emit loud sound pulses that help them approximate the difference between an obstacle and its target. The enhanced version of BAT as BBA was developed by Mirjalili et. al [20] in 2013 for optical buffer design. The variants of BA framework from the year 2010 to 2013 is described in Fig. 4.

Deepak Gupta et. al [11] developed an superior version of inventive BBA [2] for distinguishing several kinds of leukocytes. This algorithm was utilized to extract the relevant features from high dimensional white blood cells datas. And finally, the classification algorithms such as Random forest, decision tree, KNN and Logistic Regression were used to classify the WBC dataset for hematological analysis.

One of the applications of BA is classification process to categorize the data into two partitions. Hence, in our work, BAT algorithm is helpful in classifying the network data into phishing attack URL websites and normal one. In our paper, BBA is mainly focused on optimization approach for designing deep learning based neural network method followed by that scheduling takes place. Our model determines the batch size, learning rate, number of neurons in the network and number of epochs. Then finally evaluate the model to validate the outcome based model. The neural network learns the patterns of input data by reading the input dataset and applying different calculations on it. Every trail to be trained from the phishing dataset is called an epoch. So an epoch refers to one cycle through the full training dataset. Usually, training a neural network takes more than a few epochs

3.5. Dense layer

A closelylinked layer provides learning features from all the amalgamation of the features of the previous layer, but a Convolutional layer relies on reliable features with a small repetitive field. Here, we are using the size of dense layer as ten and the number of epochs used for training the data samples as 20.

Classifier- Now our designed CNN based Neural Network model using SI-BBA is suitable for classifying the data samples into phishing attack websites (malignant) and normal (legitimate)

4. Proposed algorithm coding using python language

We are proposing a novel deep learning based Swarm Intelligence-Binary Bat Algorithm for finding the phishing URL websites attack occur in the network surroundings also categorizing the attack websites from normal one.

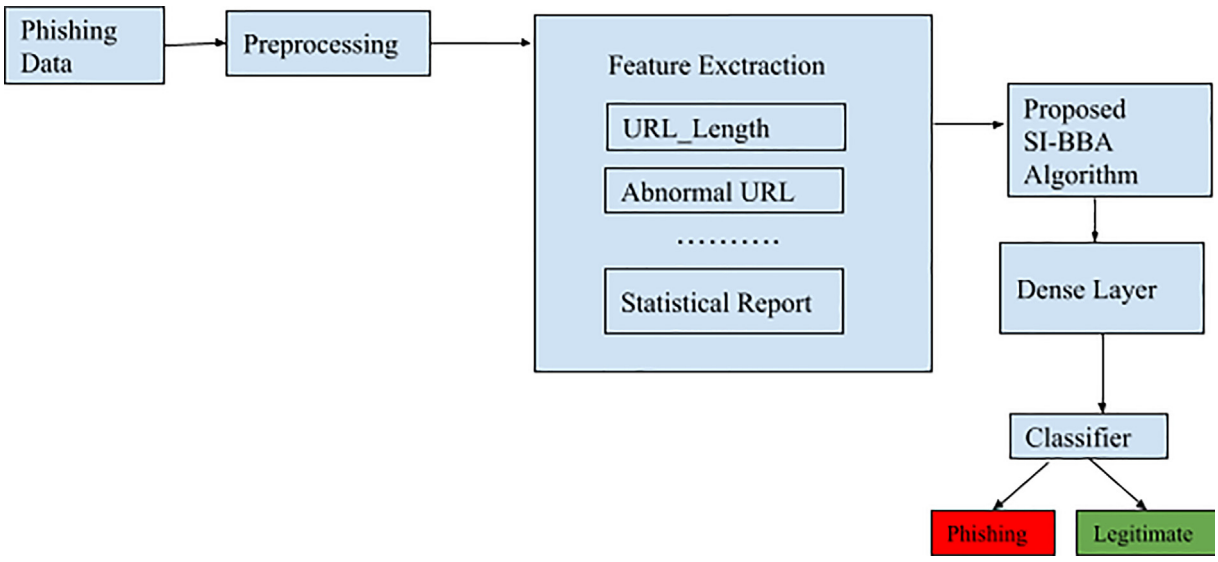

Fig. 3. Proposed method for phishing websites detection.

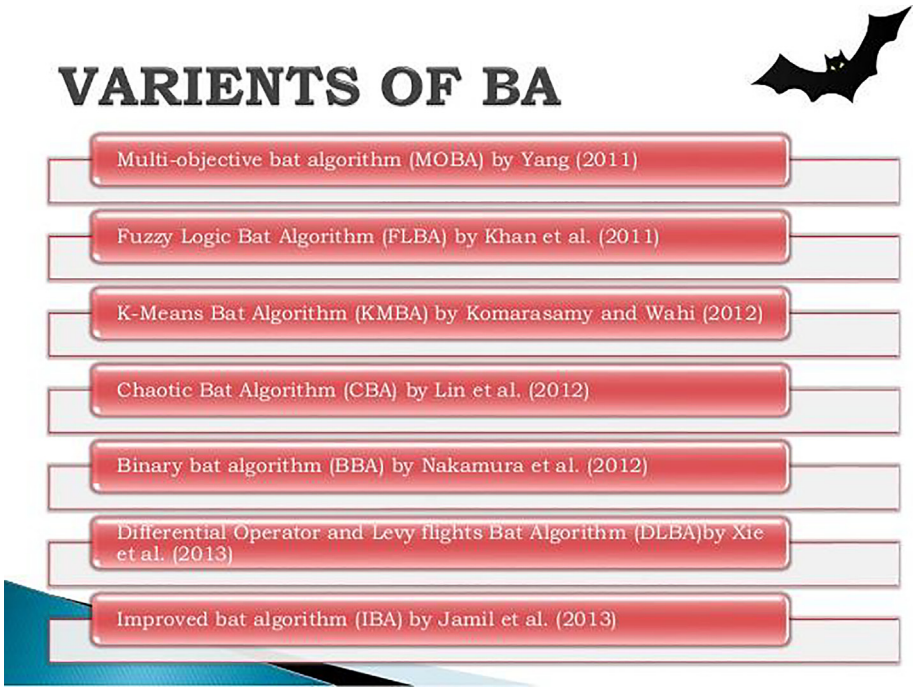

Fig. 4. Varients of BA from 2010 to 2013.

Output: Deep Neural Network model based on hyper-parameter tuning

Step 1: Initialization of models SI-BBA

Step 2: While termination condition not meet

- **Do**

Step 3: Solution = SI-BBA_best_model ();

Step 4: Epoch = pattern_epoch();

Step 5: Batch = pattern_batch ();

Step 6: Learning_rate = pattern_learning_rate ();

Step 7: Num_neurons = pattern_num_neurons ();

Step 8: model.fit = train_eval (Epoch, Batch, Learning_rate, Num_neurons);

Step 9: SI-BBA generate new model (fit)

- **End while**

Step 10: Best = create_model (SI-BBA best_model());

5. Experimental result and analysis

5.1. Features in dataset

The dataset comprises of several features of URL such as user id, IP address, length, port HTTP tokens etcfor detecting and classifying the phishing websites attacks in the network environment.

The features utilized in the datasets for distinguishing attack and normal are described in Fig. 5.

5.2. Dataset classification

The number of samples we have taken for phishing websites detection as 11055. The samples are splitted into training and testing phase samples for evaluate the model characteristics and also better understanding of concerned datas. Here, in our samples we have taken the phishing websites datas are 6157 samples and the legitimate websites as 4898 samples depicted in Fig. 6.

5.3. Summary of data statistics

Here, the data are analyzing statistically which is focused on determining the metrics namely measuring central tendency (count, mean, standard deviation, minimum value, maximum value) for specified features shown in Table 1 as below.

5.4. Central tendency measures

The statistical analysis shows how we are analyzing data via graphical representation. The metrics used for finding central tendency measures are described in Table 2.

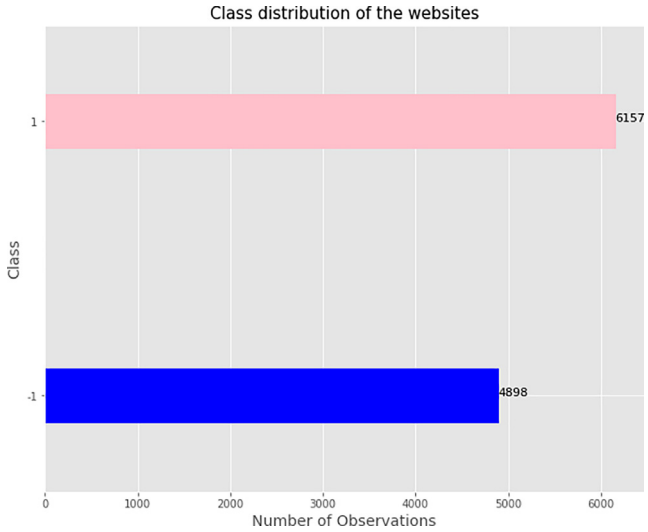

Fig. 6. Phishing URL sample classification.

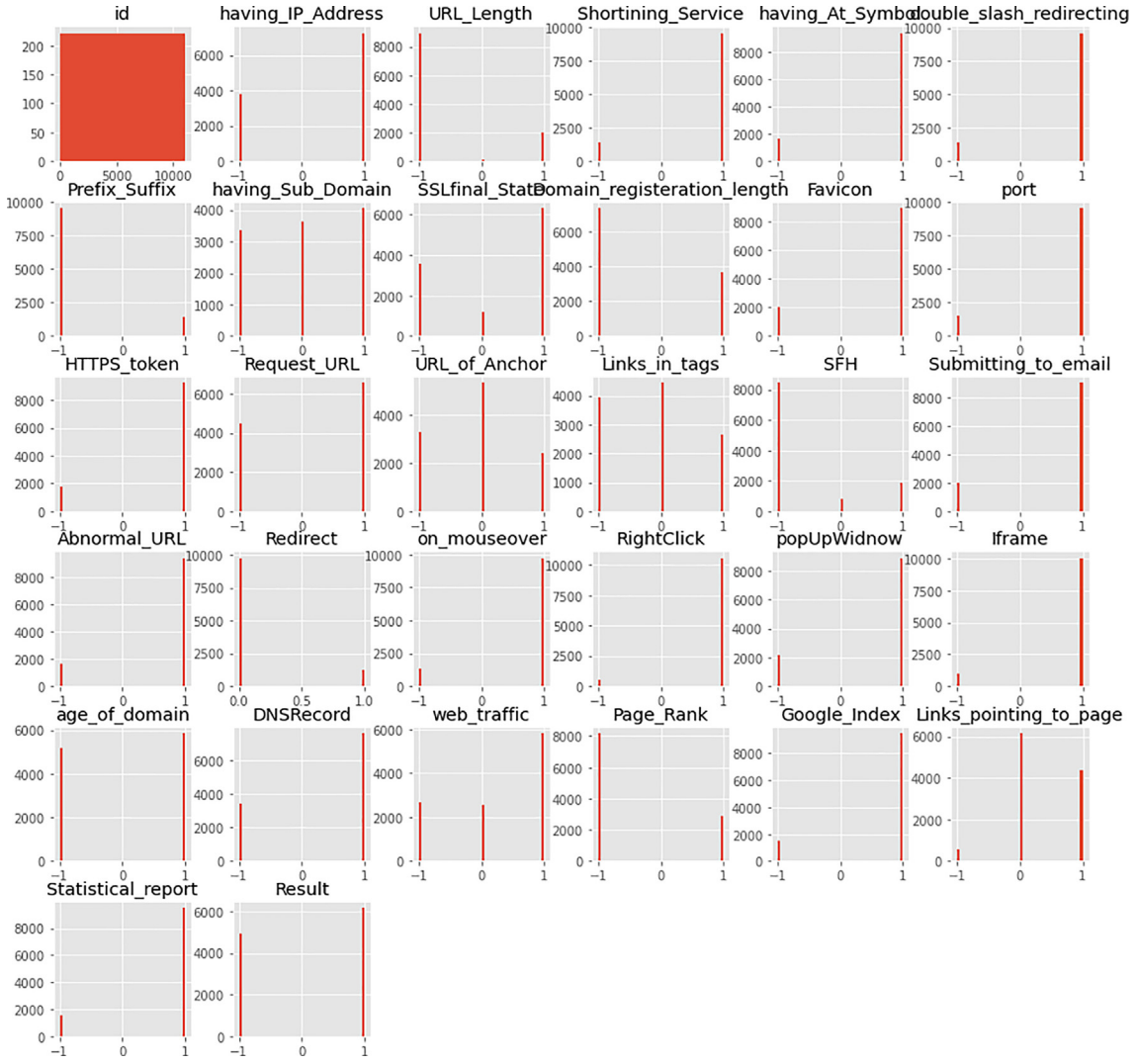

Fig. 5. Features used in our work for phishing URL detection.

Table 1
Features used for phishing detection.

Features	Count	Mean	Std	Min	25%	50%	75%	Max
having_IP_Address	11055.0	0.313795	0.949534	−1.0	−1.0	1.0	1.0	1.0
URL_Length	11055.0	−0.633198	0.766095	−1.0	−1.0	−1.0	−1.0	1.0
Shortining_Service	11055.0	0.738761	0.673998	−1.0	1.0	1.0	1.0	1.0
having_At_Symbol	11055.0	0.700588	0.713598	−1.0	1.0	1.0	1.0	1.0
double_slash_redirecting	11055.0	0.741474	0.671011	−1.0	1.0	1.0	1.0	1.0
Prefix_Suffix	11055.0	−0.734962	0.678139	−1.0	−1.0	−1.0	−1.0	1.0
having_Sub_Domain	11055.0	0.063953	0.817518	−1.0	−1.0	0.0	1.0	1.0
SSLfinal_State	11055.0	0.250927	0.911892	−1.0	−1.0	1.0	1.0	1.0
Domain_registeration_length	11055.0	−0.336771	0.941629	−1.0	−1.0	−1.0	1.0	1.0
Favicon	11055.0	0.628584	0.777777	−1.0	1.0	1.0	1.0	1.0
Port	11055.0	0.728268	0.685324	−1.0	1.0	1.0	1.0	1.0
HTTPS_token	11055.0	0.675079	0.737779	−1.0	1.0	1.0	1.0	1.0
Request_URL	11055.0	0.186793	0.982444	−1.0	−1.0	1.0	1.0	1.0
URL_of_Anchor	11055.0	−0.076526	0.715138	−1.0	−1.0	0.0	0.0	1.0
Links_in_tags	11055.0	−0.118137	0.763973	−1.0	−1.0	0.0	0.0	1.0
SFH	11055.0	−0.595749	0.759143	−1.0	−1.0	−1.0	−1.0	1.0
Submitting_to_email	11055.0	0.635640	0.772021	−1.0	1.0	1.0	1.0	1.0
Abnormal_URL	11055.0	0.705292	0.708949	−1.0	1.0	1.0	1.0	1.0
Redirect	11055.0	0.115694	0.319872	0.0	0.0	0.0	0.0	1.0
on_mouseover	11055.0	0.762099	0.647490	−1.0	1.0	1.0	1.0	1.0
RightClick	11055.0	0.913885	0.405991	−1.0	1.0	1.0	1.0	1.0
popUpWidnow	11055.0	0.613388	0.789818	−1.0	1.0	1.0	1.0	1.0
Iframe	11055.0	0.816915	0.576784	−1.0	1.0	1.0	1.0	1.0
age_of_domain	11055.0	0.061239	0.998168	−1.0	−1.0	1.0	1.0	1.0
DNSRecord	11055.0	0.377114	0.926209	−1.0	−1.0	1.0	1.0	1.0
web_traffic	11055.0	0.287291	0.827733	−1.0	0.0	1.0	1.0	1.0
Page_Rank	11055.0	−0.483673	0.875289	−1.0	−1.0	−1.0	1.0	1.0
Google_Index	11055.0	0.721574	0.692369	−1.0	1.0	1.0	1.0	1.0
Links_pointing_to_page	11055.0	0.344007	0.569944	−1.0	0.0	0.0	1.0	1.0
Statistical_report	11055.0	0.719584	0.694437	−1.0	1.0	1.0	1.0	1.0

Table 2
Central tendency measures, description with formula.

Metrics used in proposed work	Description	Formula
Count	Count data is a statistical data type in which the examination can take only non-negative integers	Count = 0+1+2+3 +4+. . .n
Mean	Average of given dataset	$Mean = \frac{sumofterms}{Numberofterms}$ (or) $\bar{X} = \sum \frac{x_i}{n}$
Std	Measure of dispersion of set of data from its mean value	$\sigma = \frac{\sum_{i=1}^{n}(x_i - \bar{X})}{n-1} \wedge 2$
Min	Finding the minimum value	
Max	Finding the maximum value	

Table 3
Proposed method estimated loss and accuracy.

Deep Learning Model SI BBA	Loss	Accuracy
DL with Adam Optimizer	**0.2024**	**0.9485**

5.5. Proposed method outcomes

The experiment we have done to detect the phishing URL websites through deep learning based Adam optimizer to achieve greater optimization via SI-BBA. The loss and accuracy metrics were evaluated with hyper-parameter settings shown in Table 3 and Fig. 7.

6. Comparison of existing method with proposed algorithm

Table 4 illustrates the comparison of existing work and proposed work in finding the phishing URL detection based on accuracy metrics.

6.1. Test outcomes

Basically, metrics are utilized to observe and evaluate the performance of a model during training as well as testing phase, and do not need to be differentiable. To estimate our novel method performance we take into account the following two performance measures:

6.1.1. Loss

In reality loss is unlike from other metrics in machine learning classification part. Loss function is defined as the function which proves the measure of model performance also utilized to train deep learning approach such as SI-BBA algorithm through several category of optimization typically differentiable in model's features.

6.1.2. Accuracy

Classification Accuracy is possibly very simple metrics which can be defined as number of correct predictions divided by total number of predictions that is multiplied by 100. Here, the classification accuracy is helpful in distinguishing the phishing attack URL from the normal one. In our datasets, 3458 samples are correctly classified from 3648 testing samples hence we achieved the classification accuracy as 94.8%.

Classification accuracy **=** 3458/3648 = 94.8 %

6.2. Comparison of existing DL method

We analyzed three existing work based on deep learning technique for phishing websites detection. In model 1 (SGD, RMS and Adam optimizer), model 2 (SGD, RMSprop and Adam) and model 3 (Adam optimizer) and comparison among every optimizer with every method are shown in Figs. 8–24.

Method-1 with SGD optimizer
Method-1 with RMS optimizer
Method-1 with Adam optimizer

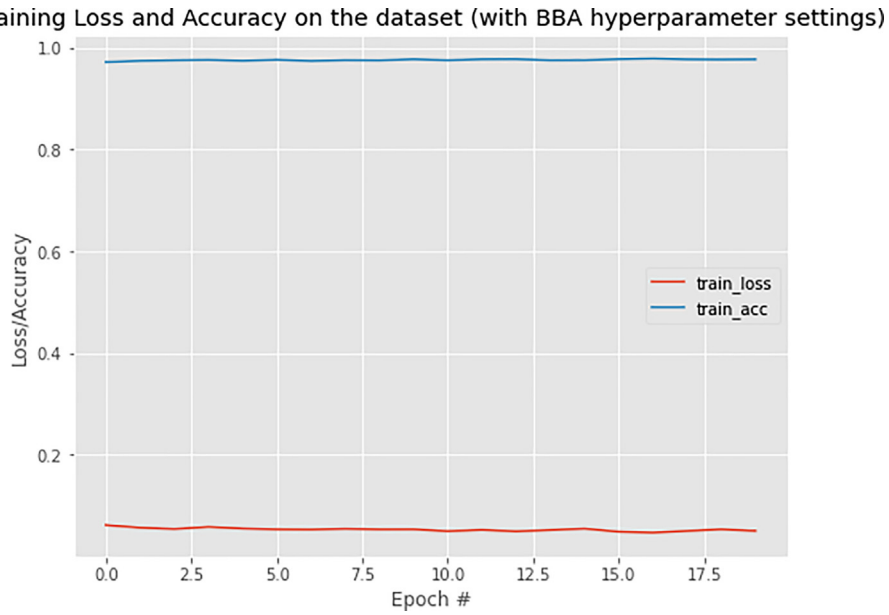

Fig. 7. Training loss and accuracy with hyper-parameter settings.

Table 4
Comparison of existing method and proposed method.

Approaches	Methods		Loss	Accuracy	Accuracy (%)
Existing approach	Method 1	DL with SGD optimizer	0.1148	0.9506	95.06%
		DL with RMSProp Optimizer	0.3335	0.9323	93.23%
		DL with Adam Optimizer	0.1628	0.9427	94.27%
	Method 2	DL with SGD optimizer	0.1586	0.9449	94.49%
		DL with RMSPropOptimizer	0.6313	0.9213	92.13%
		DL with Adam Optimizer	0.2163	0.9473	94.73%
	Method 3	DL with Adam Optimizer	0.1876	0.9455	94.55%
Proposed approach		SI-BBA	0.2024	0.9485	94.85%

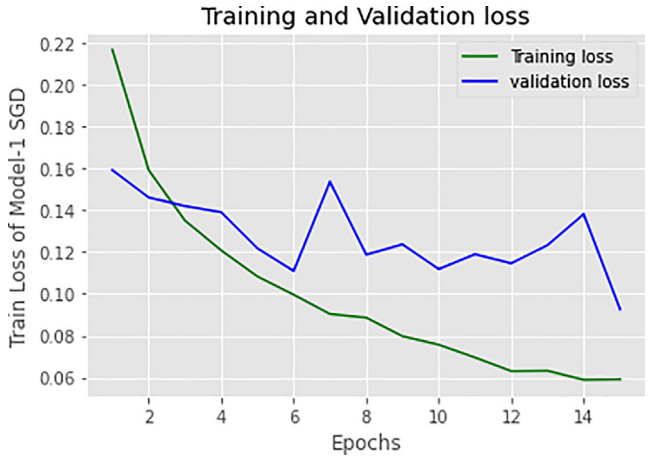

Fig. 8. Loss SGD optimizer-Method 1.

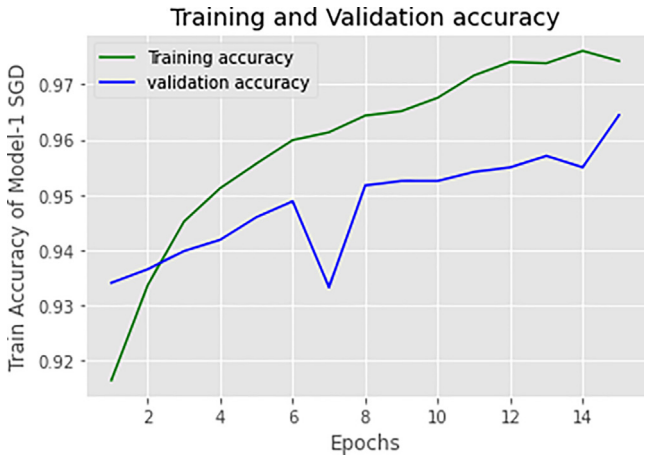

Fig. 9. Accuracy SGD optimizer-Method 1.

6.3. Comparison between optimizer for Model-1

Here comparisons have done between three models in method 1. Among these three in model 1, SGD optimizer achieves greater accuracy.

Method-2 with SGD optimizer
Method-2 with RMS optimizer
Method-2 with Adam optimizer

6.4. Comparison between optimizers for model-2

The comparisons have made among three optimizers based algorithm namely SGD, RMSProp, and Adam to detect the phishing URL websites. Among all, Adam optimizer achieves greater accuracy in detecting phishing web pages or Service provider to the internet.

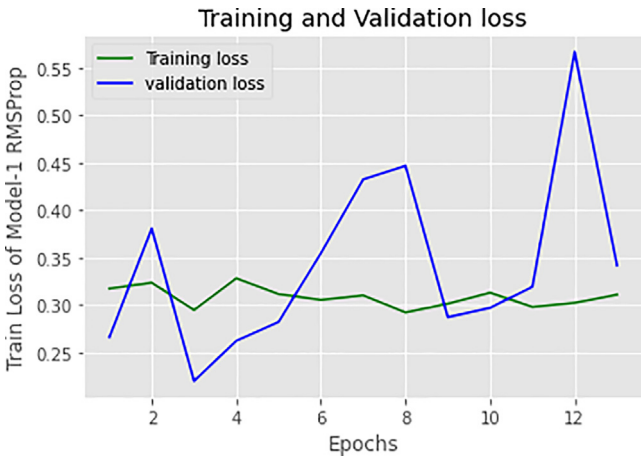

Fig. 10. Loss RMS optimizer-Method 1.

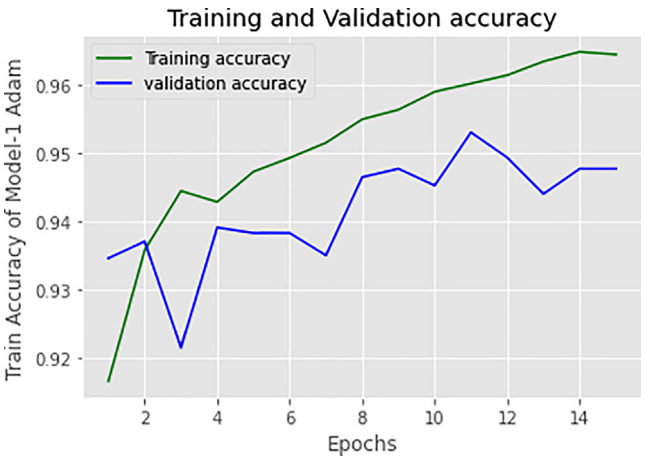

Fig. 13. Accuracy Adam optimizer-Method 1.

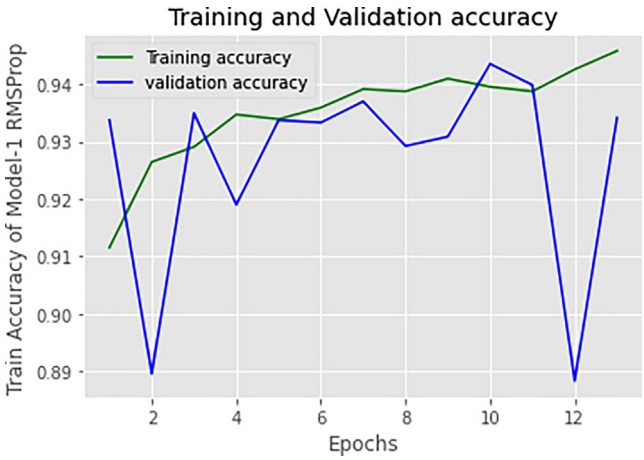

Fig. 11. Accuracy RMS optimizer-Method 1.

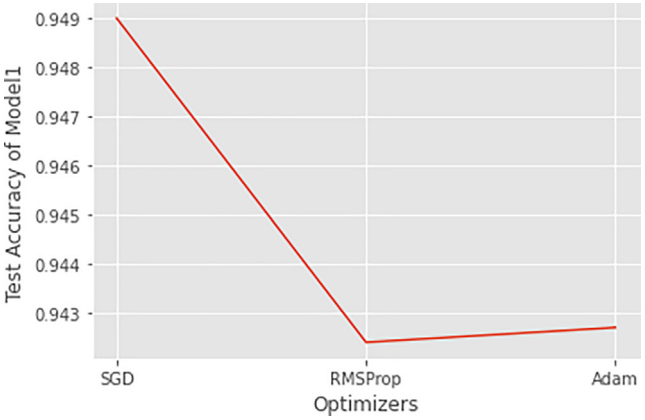

Fig. 14. Comparison among three models in method 1.

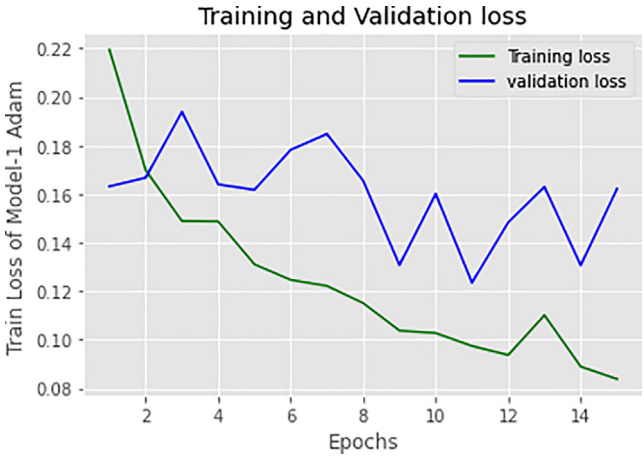

Fig. 12. Loss Adam optimizer-Method 1.

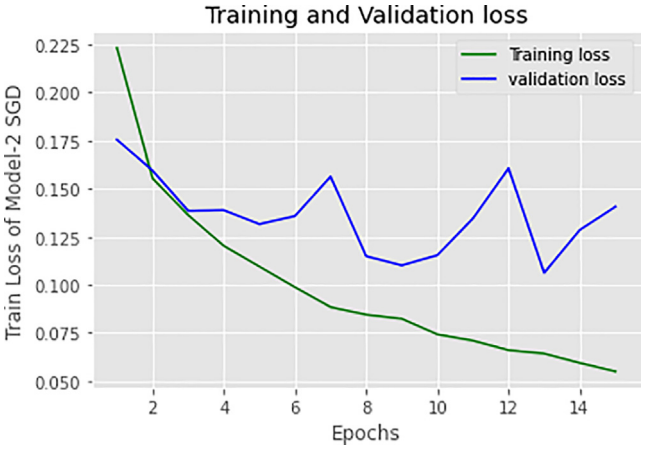

Fig. 15. Loss SGD optimizer-Method 2.

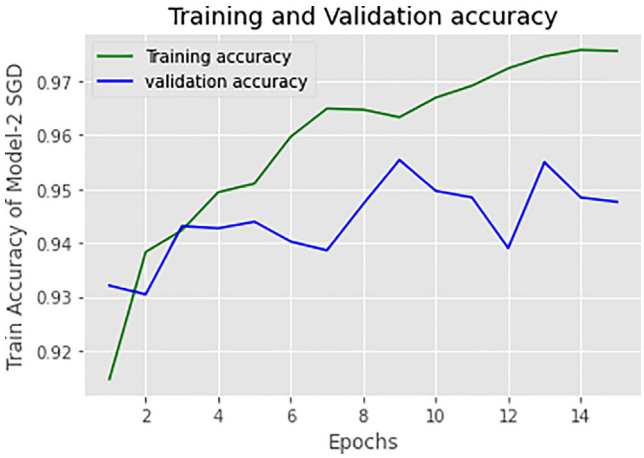

Fig. 16. Accuracy SGD optimizer-Method 2.

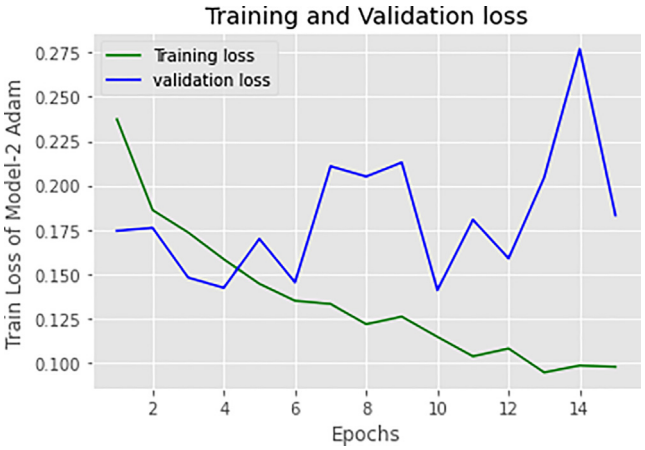

Fig. 19. Loss Adam optimizer-Method 2.

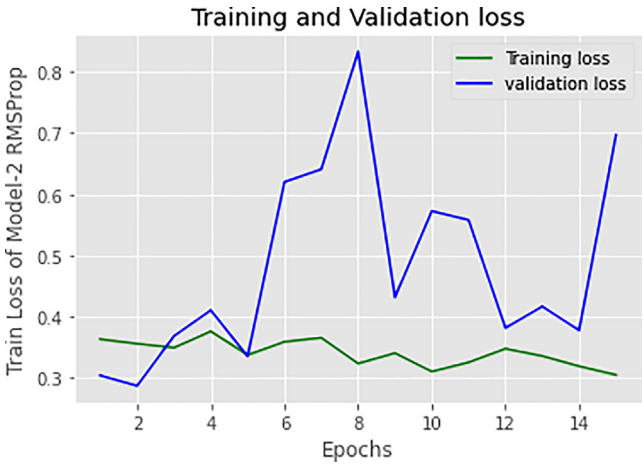

Fig. 17. Loss RMS optimizer-Method 2.

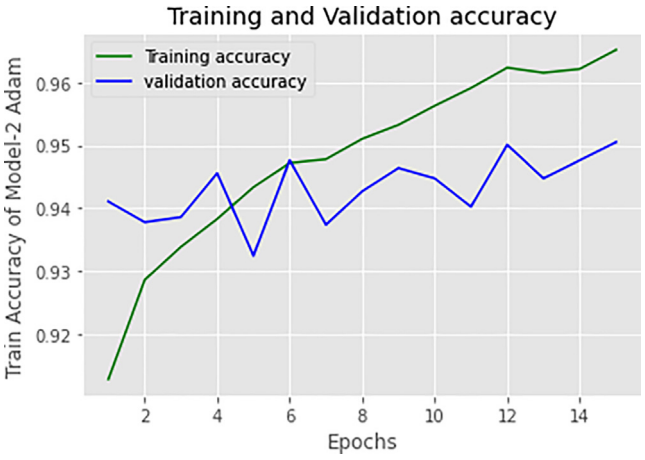

Fig. 20. Accuracy Adam optimizer-Method 2.

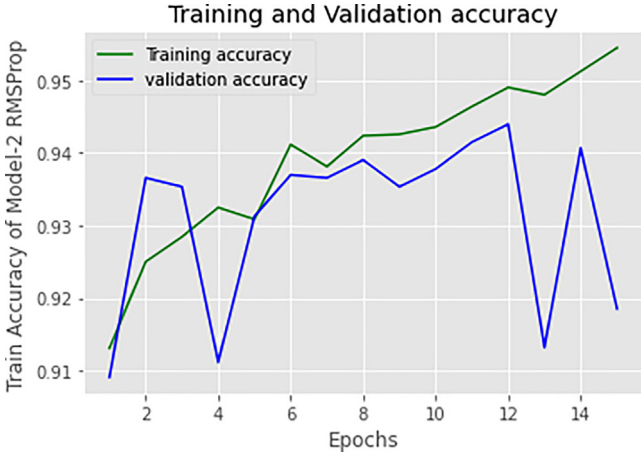

Fig. 18. Accuracy RMS optimizer-Method 2.

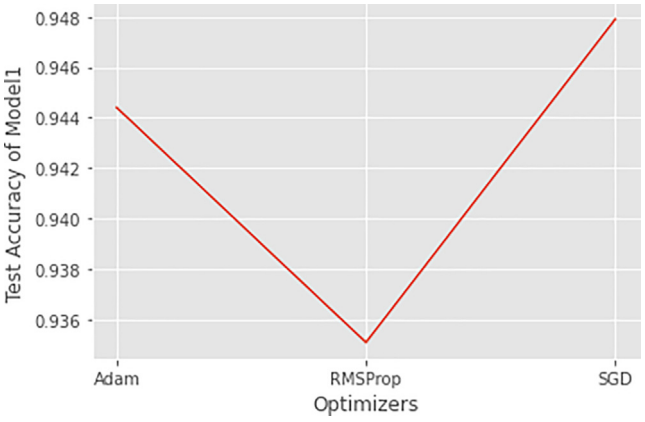

Fig. 21. Comparison graph among optimizers for method 2.

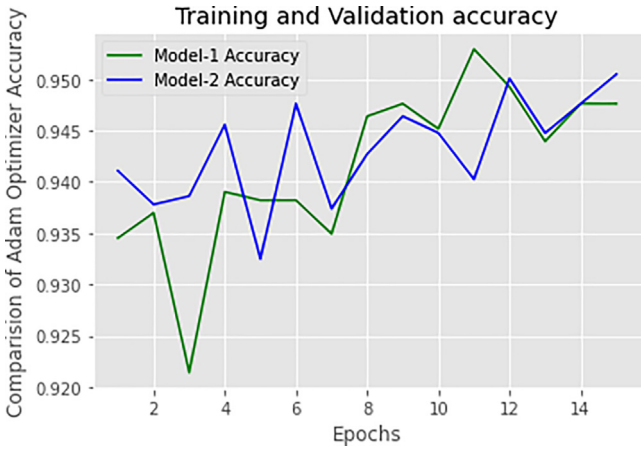

Fig. 22. Comparison graph among Adam optimizer for method 1 and 2.

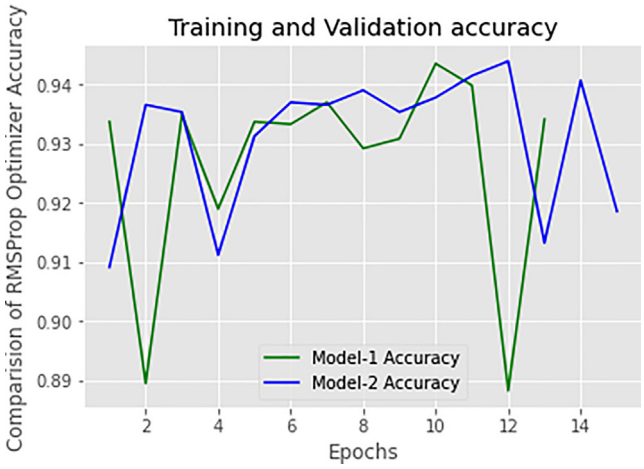

Fig. 23. Comparison graph among RMS optimizer for method 1 and 2.

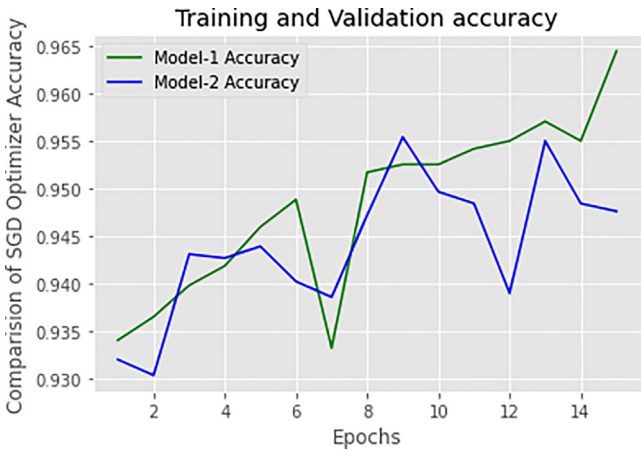

Fig. 24. Comparison graph among SGD optimizer for method 1 and 2.

6.5. Comparison with Adam optimizer for both models

Here the figure depicts the comparison of model 1 and 2 with Adam optimizer for training accuracy and validation accuracy.

6.6. Comparison with RMSprop optimizer for both models

Here the figure depicts the comparison of model 1 and 2 with RMSprop optimizer for training accuracy and validation accuracy.

6.7. Comparison with SGD optimizer for both models

Here the figure depicts the comparison of model 1 and 2 with SGD optimizer for training accuracy and validation accuracy.

7. Conclusion

In this paper we proposed a deep learning model based SI-BBA algorithm for the recognition of phishing websites and also performed classification of phishing websites from legitimate websites. The deep learning based Adam optimizer algorithm achieves the classification accuracy as 94.8% with 0.2 loss value. In future, by adjusting certain key manipulated features such as number of epochs, learning rate and batch size, we will achieve more accuracy so as to mutually consequence in finest optimization will perform by NN model.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Adebowale, M.A., Lwin, K.T. and Hossain, M.A. (2020), "Intelligent phishing detection scheme using deep learning algorithms", Journal of Enterprise Information Management, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JEIM-01-2020-0036.

[2] Adriana-Cristina Enache, Valentin Sgârciu and Alina Petrescu-Ni ¸ta "Intelligent Feature Selection Method rooted in Binary Bat Algorithm for Intrusion Detection", Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium on At: Timisoara, Volume: IEEE, DOI: 10.1109/SACI.2015.7208259.

[3] Aksu D., Turgut Z., Üstebay S., Aydin M.A. (2019) Phishing Analysis of Websites Using Classification Techniques. In: Boyaci A., Ekti A., Aydin M., Yarkan S. (eds) International Telecommunications Conference. Lecture Notes in Electrical Engineering, vol 504. Springer, Singapore. https://doi.org/10.1007/978-981-13-0408-8_21

[4] Alloghani M., Al-Jumeily D., Hussain A., Mustafina J., Baker T., Aljaaf A.J. (2020) Implementation of Machine Learning and Data Mining to Improve Cybersecurity and Limit Vulnerabilities to Cyber Attacks. In: Yang XS., He XS. (eds) Nature-Inspired Computation in Data Mining and Machine Learning. Studies in Computational Intelligence, vol 855. Springer, Cham. https://doi.org/10.1007/978-3-030-28553-1_3

[5] Arun Kulkarni, Leonard L. Brown, "Phishing Websites Detection using Machine Learning", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 7, 2019.

[6] A. Basit, M. Zafar, X. Liu, A.R. Javed, Z. Jalil, K. Kifayat, A comprehensive survey of AI-enabled phishing attacks detection techniques, Telecommunication System 76 (1) (2021) 139–154, https://doi.org/10.1007/s11235-020-00733-2.

[7] A. Begum, S. Badugu, A Study of Malicious URL Detection Using Machine Learning and Heuristic Approaches, in: S. Satapathy, K. Raju, K. Shyamala, D. Krishna, M. Favorskaya (Eds.), Advances in Decision Sciences, Image Processing, Security and Computer Vision. Learning and Analytics in Intelligent Systems, Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-24318-0_68.

[8] Benavides E., Fuertes W., Sanchez S., Sanchez M. (2020) Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review. In: Rocha Á., Pereira R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 152. Springer, Singapore. https://doi.org/10.1007/978-981-13-9155-2_5.

[9] Bo Wei, Rebeen Ali Hamad, Longzhi Yang, Xuan He, Hao Wang, Bin Gao and Wai Lok Woo "A Deep-Learning-Driven Light-Weight Phishing Detection Sensor", Sensors 2019, 19, 4258; doi:10.3390/s19194258.

[10] Cuzzocrea, A., Martinelli, F., &Mercaldo, F. (2018). Applying Machine Learning Techniques to Detect and Analyze Web Phishing Attacks. Proceedings of the 20th International Conference on Information Integration and Web-BasApplications & Services – iiWAS2018. doi:10.1145/3282373.3282422.

[11] Deepak Gupta, Jatin Arora, Utkarsh Agrawal, Ashish Khanna, Victor Hugo C. de Albuquerque, Optimized Binary Bat algorithm for classification of white blood

cells, Measurement, Volume 143, 2019, Pages 180-190, ISSN 0263-2241, https://doi.org/10.1016/j.measurement.2019.01.002.
[12] Eduardo Benavides, Walter Fuertes, Sandra Sanchez and Manuel Sanchez "Classification of Phishing Attack Solutions by Employing Deep Learning Techniques: A Systematic Literature Review", January 2020, Developments and Advances in Defense and Security (pp.51-64), DOI: 10.1007/978-981-13-9155-2_5
[13] R. Geetha, T. Thilagam, A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security, Arch Computat Methods Eng 28 (4) (2021) 2861–2879, https://doi.org/10.1007/s11831-020-09478-2.
[14] https://www.imperva.com/learn/application-security/phishing-attack-scam/.
[15] I. Saha, D. Sarma, R. J. Chakma, M. N. Alam, A. Sultana and S. Hossain, "Phishing Attacks Detection using Deep Learning Approach," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 1180-1185, doi: 10.1109/ICSSIT48917.2020.9214132.
[16] Jalil S., Usman M. (2021) A Review of Phishing URL Detection Using Machine Learning Classifiers. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1251. Springer, Cham. https://doi.org/10.1007/978-3-030-55187-2_47
[17] L. Lakshmi, M.P. Reddy, C. Santhaiah, U.J. Reddy, Smart Phishing Detection in Web Pages using Supervised Deep Learning Classification and Optimization Technique ADAM, Wireless Pers Commun 118 (4) (2021) 3549–3564, https://doi.org/10.1007/s11277-021-08196-7.
[18] M SOMESHA, ALWYN ROSHAN PAIS, ROUTHU SRINIVASA RAO and VIKRAM SINGH RATHOUR "Efficient deep learning techniques for the detection of phishing websites", Sådhanå (2020)45:165 Indian Academy of Sciences https://doi.org/10.1007/s12046-020-01392-4.
[19] M. N. Alam, D. Sarma, F. F. Lima, I. Saha, R. -E. -. Ulfath and S. Hossain, "Phishing Attacks Detection using Machine Learning Approach," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 1173-1179, doi: 10.1109/ICSSIT48917.2020.9214225.
[20] S. Mirjalili, S.M. Mirjalili, X.-S. Yang, Binary bat algorithm, Neural Computing and Applications 25 (3–4) (2013) 663–681, https://doi.org/10.1007/s00521-013-1525-5.
[21] PENG YANG, GUANGZHEN ZHAO , AND PENG ZENG "Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning", IEEE Access, VOLUME 7, 2019, Digital Object Identifier 10.1109/ACCESS.2019.2892066.
[22] Preeti, Nandal R., Joshi K. (2021) Phishing URL Detection Using Machine Learning. In: Hura G., Singh A., Siong Hoe L. (eds) Advances in Communication and Computational Technology. Lecture Notes in Electrical Engineering, vol 668. Springer, Singapore. https://doi.org/10.1007/978-981-15-5341-7_42
[23] S.S.M.M. Rahman, L. Gope, T. Islam, M. Alazab, in: IntAnti-Phish: An Intelligent Anti-Phishing Framework Using Backpropagation Neural Network, Springer, Cham, 2021, https://doi.org/10.1007/978-3-030-57024-8_9.
[24] J. Rajaram, M. Dhasaratham, Scope of Visual-Based Similarity Approach Using Convolutional Neural Network on Phishing Website Detection, in: S. Satapathy, V. Bhateja, B. Janakiramaiah, Y.W. Chen (Eds.), Intelligent System Design. Advances in Intelligent Systems and Computing, Springer, Singapore, 2021, https://doi.org/10.1007/978-981-15-5400-1_45.
[25] Ram B. Basnet, Andrew H. Sung, Quingzhong Liu "LEARNING TO DETECT PHISHING URLs", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.
[26] R.S. Rao, A.R. Pais, Detection of phishing websites using an efficient feature-based machine learning framework, Neural Comput & Applic 31 (8) (2019) 3851–3873, https://doi.org/10.1007/s00521-017-3305-0.
[27] Soon G.K., Chiang L.C., On C.K., Rusli N.M., Fun T.S. (2020) Comparison of Ensemble Simple Feedforward Neural Network and Deep Learning Neural Network on Phishing Detection. In: Alfred R., Lim Y., Haviluddin H., On C. (eds) Computational Science and Technology. Lecture Notes in Electrical Engineering, vol 603. Springer, Singapore. https://doi.org/10.1007/978-981-15-0058-9_57
[28] R. Sridhar, S. Baskar, V.S. Shaisundaram, K. Karunakaran, M. Ruban, S.J.I. Raja, Design and development of material behavior of line follower automated vehicle, MaterialsToday:Proceedings 37 (2021) 2193–2195, https://doi.org/10.1016/j.matpr.2020.07.650.
[29] N.K. Chandramohan, M. Shanmugam, S. Sathiyamurthy, S.T. Prabakaran, S. Saravanakumar, V.S. Shaisundaram, Comparison of chassis frame design of Go-Kart vehicle powered by internal combustion engine and electric motor, Materials Today: Proceedings 37 (2021) 2058–2062.
[30] Suleiman Y. Yerima and Mohammed K. Alzaylaee, "High Accuracy Phishing Detection Based on Convolutional Neural Networks", Third International Conference on Computer Applications & Information Security (ICCAIS 19–21 March, 2020 2020 Riyadh Saudi Arabia.
[31] A. Prabhakaran, K.S. Krishnan, R. Dhinakaran, S. Baskar, V.S. Shaisundaram, Analysis of the efficiency of an automotive alternator by replacing mild steel into aluminum as a material for rotor, Materials Today: Proceedings 37 (2021) 1269–1273.
[32] X.-S. Yang A new metaheuristic bat-inspired algorithm Nature Inspired Cooperative Strategies for Optimization (NICSO 2010) volume 284 of Studies in Computational Intelligence 2010 Springer Berlin Heidelberg 65 74
[33] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, T. Zhu, Web Phishing Detection Using a Deep Learning Framework, Wireless Communications and Mobile Computing 2018 (2018) 1–9, https://doi.org/10.1155/2018/4678746.
[34] Vijayalakshmi.P, Rajendran.V, Arunthathi. S, Pandiselvi Ganesan, D.Ravikumar, (2020). "Performance Analysis of a Balanced-Energy Aware Routing MAC Protocol for Underwater Sensor Networks" Journal of Critical Reviews, Vol 15, No.7, 4577-4586, doi: 10.31838/jcr.07.15.611.
[35] Dr.E.N.Ganesh, Dr. V.Rajendran, Dr. D.Ravikumar, P.Sai Kumar, G.Revathy, P. Harivardhan, "Detection and Route Estimation of Ship Vessels using Linear Filtering and ARMA Model from AIS Data", International Journal of Oceans and Oceanography, Volume 15, No 1, pp. 1-10, ISSN 0973-2667, June 2021.