MULTI-OBJECTIVE FIREFLY OPTIMIZATION ALGORITHM FOR PHISHING ATTACK DETECTION USING ARTIFICIAL NEURAL NETWORK MODEL

Bharathkumar J[1], Athiban S[2], Malcom vijay josephraj D[3], GOPALAKRISHNAN B[4]

Bachelor of Engineering, Electronics and Communication Engineering, BannariAmman Institute of Technology, Erode, India

Bachelor of Engineering, Electronics and Communication Engineering, BannariAmman Institute of Technology, Erode, India

Bachelor of Engineering, Electronics and Communication Engineering, BannariAmman Institute of Technology, Erode, India

ABSTRACT

Phishing attacks exert a significant influence on the internet, yielding financial setbacks, identity misappropriation and data infringements. They undermine trust in online dealings and impair email sender credibility. These assaults frequently propagate malware and filch login particulars, resulting in compromised websites and services. Phishing incidents diminish productivity in enterprises and have the potential to disseminate disinformation. The defence against phishing depletes substantial resources and exerts a global economic impact. In a nutshell, phishing attacks wield extensive ramifications on individuals, entities, and the broader internet ecosystem. There are various evolutionary algorithms introduced to provide the solutions. Multi Objective firefly optimization algorithm combines multiple objectives to enhance performance of a detection model. It draws inspiration from the collective behaviour of fireflies. The algorithm aims to strike a balance between reducing both false positives and false negatives, all the while striving to attain a diverse set of objectives, such as Accuracy, Recall, precision and F1-score. This will ultimately enhance the overall effectiveness of the detection process. The proposed algorithm offers a robust countermeasure against evolving and adaptable phishing strategies, displaying remarkable resistance to attacks of varying degrees of complexity.

1.INTRODUCTION

Phishing attacks exert a significant influence on the internet, yielding financial setbacks, identity misappropriation and data infringements. They undermine trust in online dealings and impair email sender credibility. These assaults frequently propagate malware and filch login particulars, resulting in compromised websites and services. Phishing incidents diminish productivity in enterprises and have the potential to disseminate disinformation. The defence against phishing depletes substantial resources and exerts a global economic impact. In a nutshell, phishing attacks wield extensive ramifications on individuals, entities, and the broader internet ecosystem. There are various evolutionary algorithms introduced to provide the solutions. Multi Objective firefly optimization algorithm combines multiple objectives to enhance performance of a detection model. It draws inspiration from the collective behaviour of fireflies. The algorithm aims to strikea balance between reducing both false positives and false negatives, all the while striving to attain a diverse set of objectives, such as Accuracy, Recall, precision and F1-score. This will ultimately enhance the overall effectiveness of the detection process. The proposed algorithm offers a robust countermeasure against evolving and adaptable phishing strategies, displaying remarkable resistance to attacks of varying degrees of complexity.

1.1 BACKGROUND OF THE PROJECT

Malicious actors have invested significant efforts in crafting websites that are highly convincing and appear authentic. This often involves impersonating reputable organizations, such as Microsoft. The aim of bad actors who mimic trustworthy websites is to trick end users into providing their credentials. Hence, deceptive URL tactics serve as a smokescreen for incursions aimed at harvesting sensitive data.When executed effectively, Phishing attack can lead to the theft of usernames, passwords, credit card information, and other confidential data. Some of the most common tactics involve coercing users into logging into their banking or email accounts. In the absence of robust safeguards, both individuals and enterprises are vulnerable to falling victim to such schemes. Phishing attack can be employed through various means and frequently initiates with an email. Deceptive URL tactics involve the creation of a hostile website alongside the act of phishing. Perpetrators utilize methods of social engineering to entice the target into clicking the link and visiting the malevolent site. The link to this site is often embedded within a deceitful email. Attackers employ a variety of strategies to concoct enticing URLs, including misspelling company names or original URLs. For instance, they might use "goggle.com" instead of "google.com," incorporating visually similar characters from different alphabets. Take, for example, "wikipedia.org" and "wikipadia.org," where the "e" and the "a" are visually distinct characters in subdomains resembling the actual domain name. They might opt for "paypal.accounts.com" instead of "accounts.paypal.com," with the second domain being controlled by PayPal but having no authority over the first alternative top-level domain (TLD). Another approach is "paypal.io" as opposed to "paypal.com." Many prominent companies seek domain registration under well-known TLDs like ".com," ".net," and ".org," but there is an extensive array of available TLDs.

2. LITERATURE SURVEY

Butt et al(2023) proposed that cloud-based software pertains to the request accessibility of a personal computing device resources, especially, information storage and computational capability, not with the customer's direct involvement. Email correspondence serve as a common means to transmit and obtain data for people or organizations.Credit histories, financial information, and other private information are routinely shared online. Scams and fraudconstitute a fraudulent stratagem employed by cybercriminals to illicitly obtain sensitive data from users, often masquerading as trusted sources. The sender can manipulate a phished email to deceive you into divulging confidential information. The primary concern here is email-based phishing attacks during the exchange of electronic communications. The attacker dispatches unsolicited data through by email and procures your details upon opening and peruse the message. The past few years, this is emerged as significant issue in light of all internet users. Thatstudy employs varying reputable and deceptive data volumes, identifies updated emails, andA employs diverse attributes and formulas in light of categorization.Reworked datasets are established later evaluating acurrent methodology.The email attack classification employing NB, LSTM, and SVM classifiers attains the greatest levels accuracy, namely 99.62%, 97%, and 98%, respectively [8].

Joshi et al (2023) proposed thatthe security of blockchain has emerged as a matter of apprehension due to the recent advancements in the domain. Amongthat greatest prevalent Among online assaults, in which that wrongdoer deceives into the miningincorporating malevolentblot into that link beneath authentic pretences, aiming as to elude being discovered as well possibly wreak havoc on all of the chain of. Present efforts in recognition encompass the protocol for consensus; nevertheless, thatproves ineffective when a legitimate miningendeavorsas to append a brand-new blockchain block. Policies of zero trust have begun to gain traction in this sphere as they guarantee comprehensive identification of phishing endeavors. Nonetheless, their deployment remains a work in progress, entailing a substantial timeframe. A more precise approach to Machine learning models is used in phishing detection to leverage precise qualities to fully automate the process of categorizing anendeavouras an attempt at phishing or as benign one. That article spotlights various examples which hold the potential to yield secure outcomes and aid in the eradication of blockchain phishing attempts [14].

Abdulrahman et al (2023) proposed that the COVID-19 pandemic compels individuals to adhere to the "telecommute" arrangement. The internet also serves as a potent avenue for social interactions. The substantial reliance of the populace on digital media exposes vulnerabilities to deception. Phishing stands as a type of *online criminal activity utilized for pilfering user passwords related to internet banking, electronic commerce, virtual educational institutions, online marketplaces, and other digital domains. Fraudsters fabricate counterfeit websites mirroring authentic ones and dispatch unsolicited emails to users. When a digital user accesses these counterfeit webpages via unsolicited emails, malefactors abscond with their login credentials. Hence, it is imperative to detect these fraudulent web resources before they inflict harm upon unsuspecting sufferers. Motivated by the eternal-evolving nature usingPhishing attacks websites, this essay assesses that state of detection of phishing attacks and seeks as to scrutinize methodologies primarily oriented toward the identification and prevention of phishing attempts, as opposed to mere mitigation. In this instance, we present acomprehensive a summary of the most efficacious approaches to detecting phishing attacks, emphasizing profound understanding techniques.*

Almutairy et al (2023) proposed that the extensive application Phasor Measurement Units (PMUs) stands as a pivotal contribution towards enhancement of the force grid surveillance. PMUs serve as virtual instruments delivering synchronized phasor readings, temporally synchronized with the GPS, or Global Positioning System. Theabsence cryptographic protection within traditional GPS devices incorporated within PMUs renders those susceptible as to Global Positioning System GSAs, or spoofing attacks, which lead to thedevice losing synchronization, consequently inducing a phase alteration in all measurements acquired by the impacted PMU.

Altamimi et al (2023) demonstrated that Cybersecurity grapples with an immense challenge concerning the preservation of the integrity and privacy of users' sensitive info, like passwords and PIN codes. Every day, Billions of people are impacted by counterfeit log in screens that request confidential info. Multiple methods in fact employed as to deceive person into visiting website, including Phishing attacks emails, enticing click the adverts manipulation, SQL injection, malware, and session interception, between-the-peopleattacks, cross-site scripting and denial of service attacks. Phishing or web spoofing constitutes a deceptive computerized scheme if the assailant creates a malevolent replica an authentic website to solicit people's personal data, like that passwords [5].

3.OBJECTIVE AND METHODOLOGY

3.1 Proposed work

The objective of the multi-objective firefly optimization algorithm for phishing attack detection using an artificial neural network (ANN) model is to enhance the performance of the phishing attack detection system by optimizing multiple conflicting objectives simultaneously.

- ***Maximizing Detection Accuracy:*** *The algorithm aims to maximize the accuracy of the phishing attack detection system, ensuring that legitimate websites are accurately identified and distinguished from phishing websites.*

- ***Minimizing False Positives:*** *False positives occur when legitimate websites are incorrectly classified as phishing websites. Minimizing false positives helps improve the reliability of the detection system and reducesthe likelihood of blocking legitimate users.*

- ***Minimizing False Negatives:*** *False negatives occur when phishing websites are incorrectly classified as legitimate. Minimizing false negatives is crucial for ensuring that potential security threats are detected and mitigated effectively.*

By optimizing these multiple objectives simultaneously, the multi-objective firefly optimization algorithm seeks to find a balance between detection accuracy, false positive rate, and false negative rate, ultimately improving the overall performance and robustness of the phishing attack detection system based on the artificial neural network model.

3.2 Objectives of the Proposed Work

Improving Phishing Detection Accuracy:

The primary objective of our project is to enhance the accuracy of phishing attack detection methods. Phishing attacks continue to evolve in sophistication, making them increasingly challenging to detect using traditional techniques. By developing advanced algorithms and methodologies, we aim to significantly improve the accuracy of phishing detection systems, thereby reducing the risk of successful phishing attacks and safeguarding users' sensitive information.

Integration of Multi-Objective Firefly Optimization Algorithm (MOFOA):

We seek to integrate the Multi-Objective Firefly Optimization Algorithm (MOFOA) into our phishing detection framework. MOFOA offers powerful optimization capabilities that can be leveraged to fine-tune the parameters of machine learning models, such as Artificial Neural Networks (ANNs), for improved performance in detecting phishing attacks. By integrating MOFOA into our framework, we aim to enhance the effectiveness and efficiency of our phishing detection system.

Utilization of Artificial Neural Network (ANN) Models:

We aim to utilize Artificial Neural Network (ANN) models as the core component of our phishing detection system. ANNs have demonstrated remarkable capabilities in capturing complex patterns and relationships in data, making them well-suited for tasks such as phishing attack detection. By leveraging ANN models, we seek to develop a sophisticated and robust detection system capable of accurately distinguishing between legitimate and phishing websites.

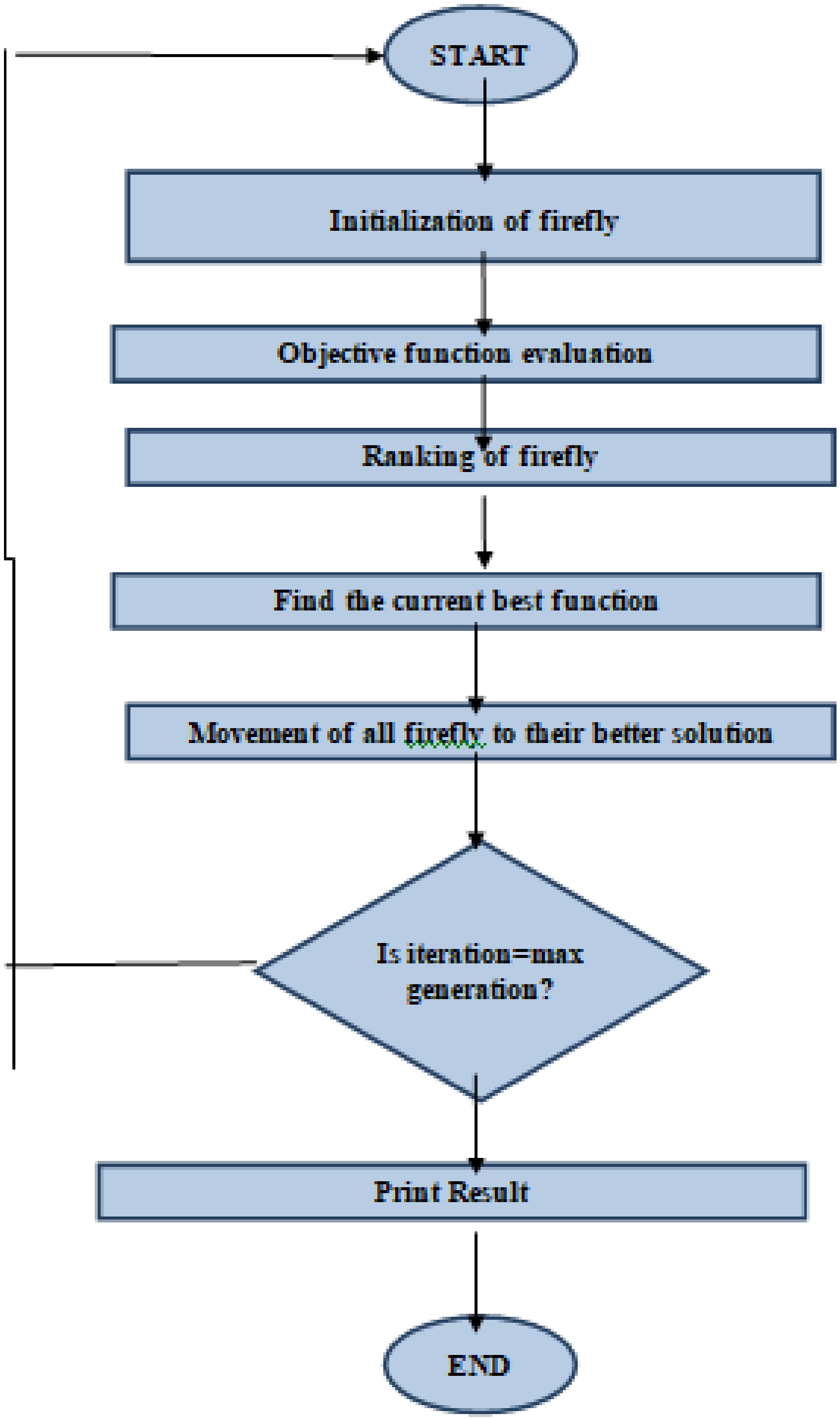
***Evaluation of Detection Robustness**:*

We endeavor to evaluate the robustness of our phishing detection system against various types of phishing attacks, including sophisticated and evolving tactics employed by attackers. Robustness is a critical aspect of any cybersecurity system, as it determines the system's ability to withstand and adapt to changing threat landscapes. By rigorously evaluating the robustness of our detection system, we aim to identify vulnerabilities and weaknesses that could be exploited by attackers, thereby enhancing the overall resilience of the system.

3.3 *METHODOLOGY OF THE PROPOSED WORK*

We have taken four different datasets from ICSX URL, UCI repository, Kaggle repository and Mendeley. Gather a diverse dataset containing samples of both legitimate and phishing websites.Preprocess the dataset to handle missing values, normalize features, and remove outliers to ensure data quality. We gathered a comprehensive dataset that included instances of both legal and phishing websites for the data collection and preparation phase. This dataset was carefully preprocessed to guarantee that it was suitable for our study and of high quality. To improve the robustness of our analysis, we eliminated outliers, corrected missing values, and normalized features. We tried to create a strong basis for our analysis and model building by carefully selecting and honing the dataset. During the information assortment stage, we fastidiously obtained a different dataset that included many real sites as well as instances of known phishing sites. This dataset was fundamental for preparing and assessing our phishing identification model. We used different sources including freely accessible datasets, storehouses, and information bases committed to online protection examination to guarantee an exhaustive portrayal of both real and malignant web substances.

3.3 BLOCK DIAGRAM


START
Initialization of firefly
Objective function evaluation
Ranking of firefly
Find the current best function
Movement of all firefly to their better solution
Is iteration=max generation?
Print Result
END

3.4.SPECIFICATION & TECHNIQUES

3.4.1 ANN MODEL

Artificial neural networks (ANNs) are computer algorithms that draw inspiration from the biological structure of the human brain to mimic its information processing. ANNs accumulate their understanding by recognizing patterns and connections within data, and theyacquire knowledge through learning experiences, as opposed to being explicitly programmed. ANNs consist of numerous individual components, which artificial neurons are interconnected with coefficients (referred to as weights) that make up the neural architecture. These components are also commonly referred to as processing elements (PE) since their primary function is to handle and process information.

An ANN comprises three tiers, the hidden layer, the input layer and the output layer. Connections must be established between nodes in input layer and those in hidden layer, as well as between each node in hidden layer and those in output layer. The input layer is responsible for receiving data from the network. The hidden layer takes in the unprocessed information from the input layer and carries out data processing. Subsequently, the resultant value is relayed to the output layer, which also engages in processing the information fromthe hidden layer to produce the final output.

The output of the model is evaluated from the output metrics. The metrics consists of parameters like accuracy, precision, recall and F1 score.

3.4.2 PERFORMANCE METRICS

Performance metrics serve to assess how well the model aligns with a specific criterion. These metrics are applied to test datasets following standard procedures of feature engineering, feature selection, model implementation, and category output generation. Diverse machine learning algorithms are appraised using a range of performance evaluators. This paper evaluates the proposed model using performance metrics such Accuracy,Recall, precision and F1-score.

PRECISION

Precision is defined as the proportion of accurate predictions relative to the total number of predictions generated by model. In more straightforward terms, it can be described as the relationship between true positives and the overall count of values that were predicted correctly.It will be calculated by using the equation (6.1).

$$Precision=\frac{TP}{TP+FP}$$

RECALL

Recall can be defined as the model's ability to correctly identify the proportion of predictions. It is the ratio between the number of positive values correctly categorized as positive and the sum of both true positives and false negatives.It will be calculated by using the equation (6.2).

$$Recall=\frac{TP}{TP+FN}$$

F1 SCORE

The term F-Measure is synonymous with the F1 score, which is a metric that combines recall and precision values with appropriate weighting. F1 Score is considered, particularly when addressing imbalanced classification scenarios, prioritizing it over accuracy. To compute the score, F1 Score takes into consideration false positives and false negatives.It will be calculated by using the equation (6.3).

$$F1\ score = \frac{2 * recall * precision}{recall + precision}$$

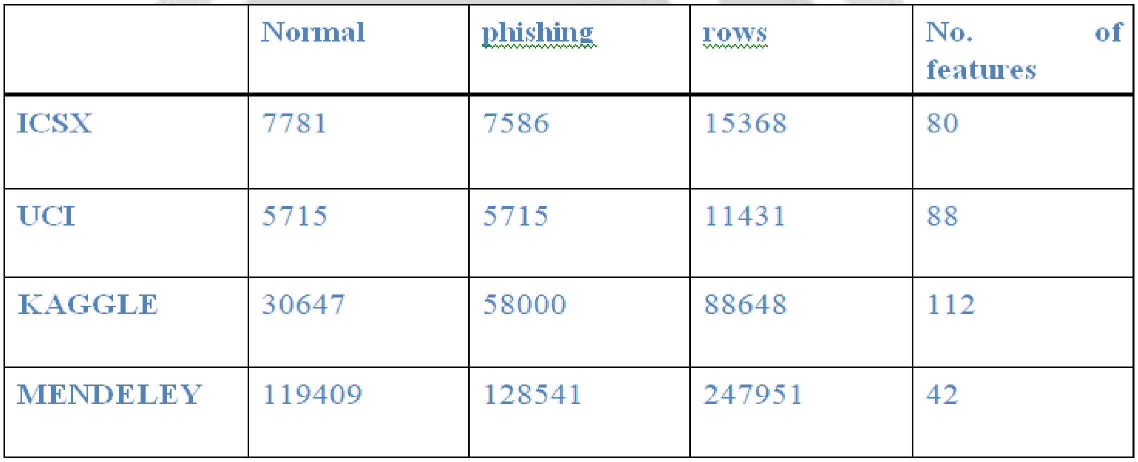
ACCURACY

Accuracy serves as the evaluation metric for classification models, computed as the ratio of correctly predicted actual outcomes to all other predictions. In essence, it represents the percentage of correct predictions. Enhanced model accuracy not only aids in minimizing time and cost but also becomes crucial. In scenarios where datasets are uniform with identical false negatives and positives, alternative parameters are taken into account when appraising the model.It will be calculated by using the equation (6.4).

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

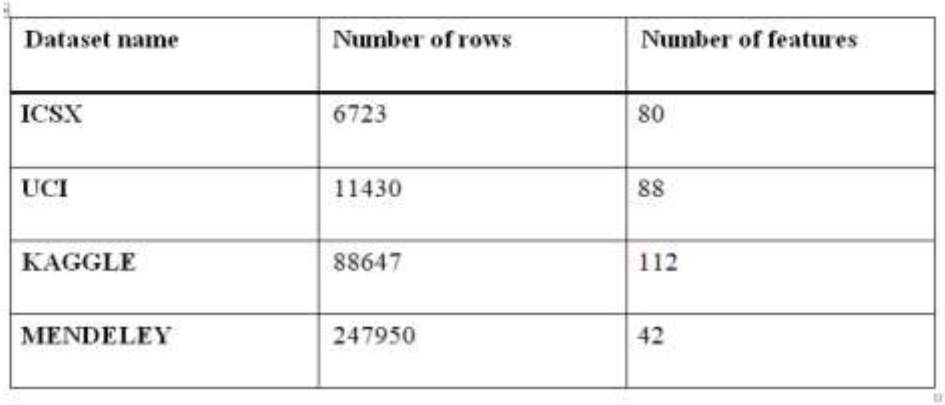
4.RESULT AND DISSCUSION

The description of dataset before pre-processing is given and the description of dataset after pre-processing is given in the table.



	Normal	phishing	rows	No. of features
ICSX	7781	7586	15368	80
UCI	5715	5715	11431	88
KAGGLE	30647	58000	88648	112
MENDELEY	119409	128541	247951	42

4.1 Dataset before Pre-processing



Dataset name	Number of rows	Number of features
ICSX	6723	80
UCI	11430	88
KAGGLE	88647	112
MENDELEY	247950	42

4.2 Dataset after Pre-processing

4.1 Result of Ann Model With 2 Layers

The result of the different datasets with 2 layers is shown in the table 4.3 and their evaluation is given in the figure 4.1.

Dataset name	Accuracy	Recall	Precision	F1 score
ICSX	91.34	91.73	90.81	91.14
UCI	71.50	71.49	71.91	71.36
Kaggle	66.76	52.22	75.12	44.51
Mendeley	80.51	80.30	80.87	80.36

4.3 Performance of 2 layers

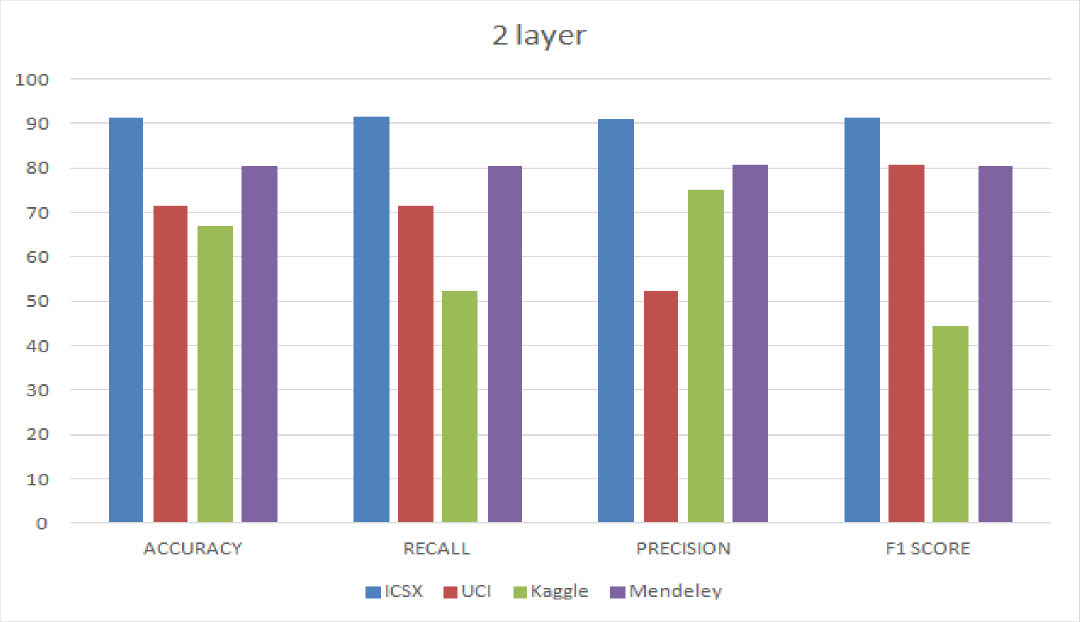


Figure 4.1 Performance graph for 2 layers

4.2 Result of ANN Model With 4 Layers

The result of the different datasets with 4 layers is shown in the table and their evaluation is given in the figure.

Dataset name	Accuracy	Recall	Precision	F1 score
ICSX	93.42	93.88	92.91	93.26
UCI	49.94	50.00	24.97	33.30
Kaggle	68.35	64.85	58.43	57.67
Mendeley	87.89	88.64	87.58	87.71

4.4 Performance of 4 layers

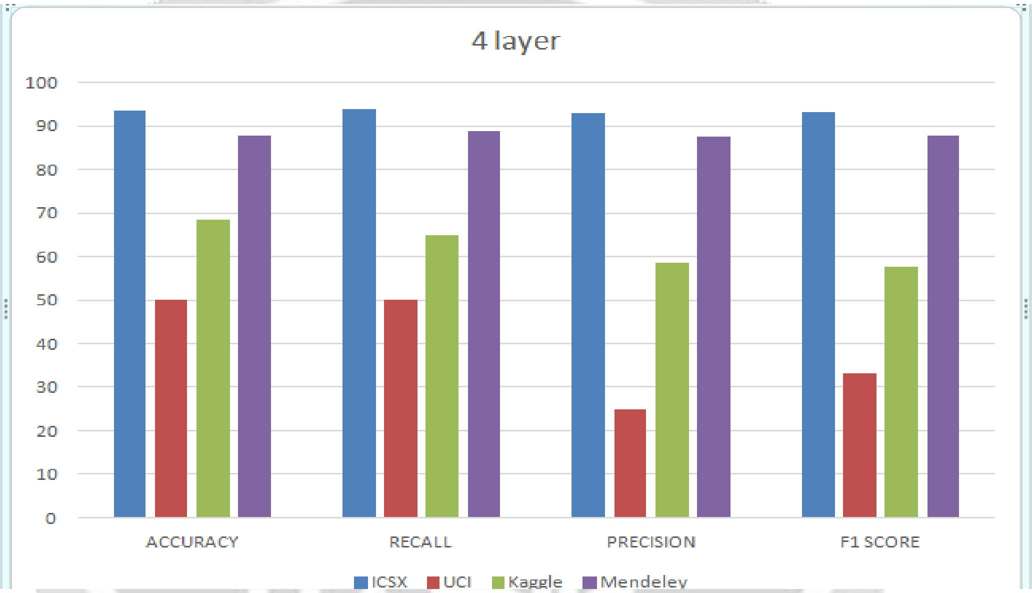


Figure 4.2 Performance graph for 4 layers

4.3 Result of ICSX Dataset

	Accuracy	Precision	Recall	F1-score	Total no. of features	Reduced features	Training Time(sec)
Full dataset+ANN	93.42	92.91	93.88	93.26	80	80	12.88
FFA+ANN	95.43	95.59	95.35	95.42	80	32	8.56
MOFFA+ANN	91.45	91.48	91.47	91.45	80	13	6.13

4.5 Performance of ICSX dataset

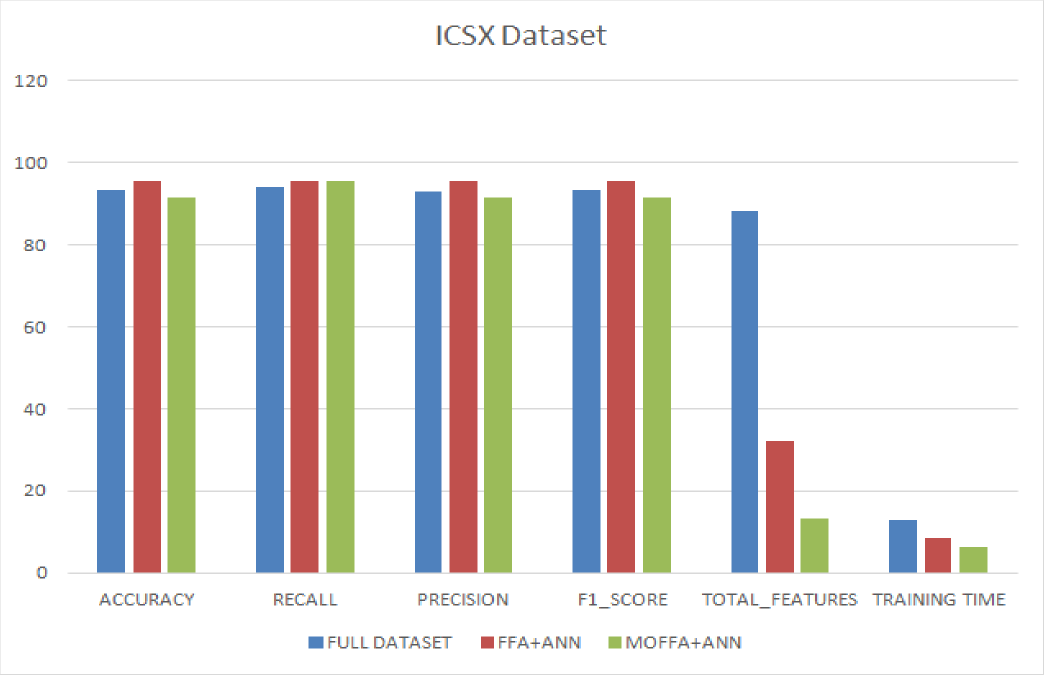


Figure 4.3 Performance graph of ICSX dataset

4.4 Result of UCI Dataset

	Accuracy	Precision	Recall	F1-score	Total No. of features	Reduced features	Training Time(sec)
Dataset+ANN	49.94	24.97	50	33.30	88	88	11.51
FFA+ANN	75.90	81.89	75.87	74.70	88	34	10.02
MOFFA+ANN	80.64	80.80	80.64	80.62	88	19	8.62

4.6 Performance of UCI dataset

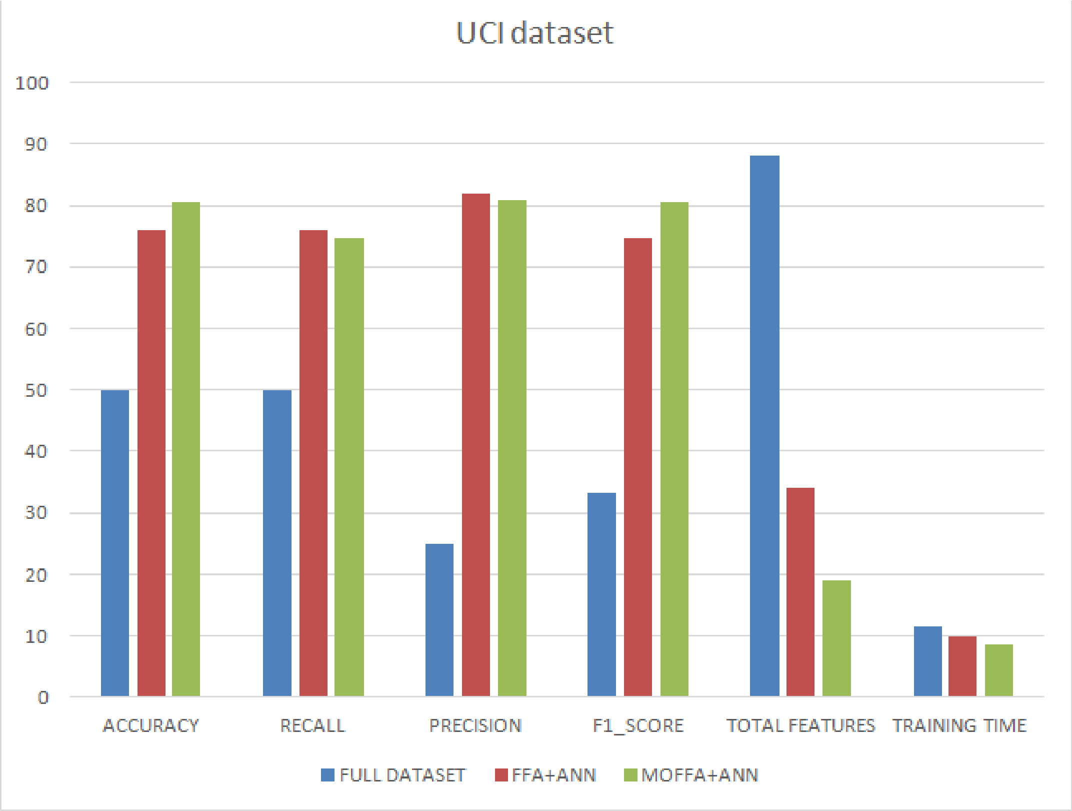


Figure 4.4 Performance graph of UCI dataset

4.5 Result of Kaggle Dataset

	Accuracy	Precision	Recall	F1-score	Total No. of features	Reduced features	Training Time(sec)
Dataset+ANN	68.35	58.43	64.85	57.67	112	112	44.47
FFA+ANN	71.05	59.43	75.25	57.79	112	41	43.10
MOFFA+ANN	66.32	51.64	71.64	43.42	112	19	39.28

4.7 Performance of Kaggle dataset

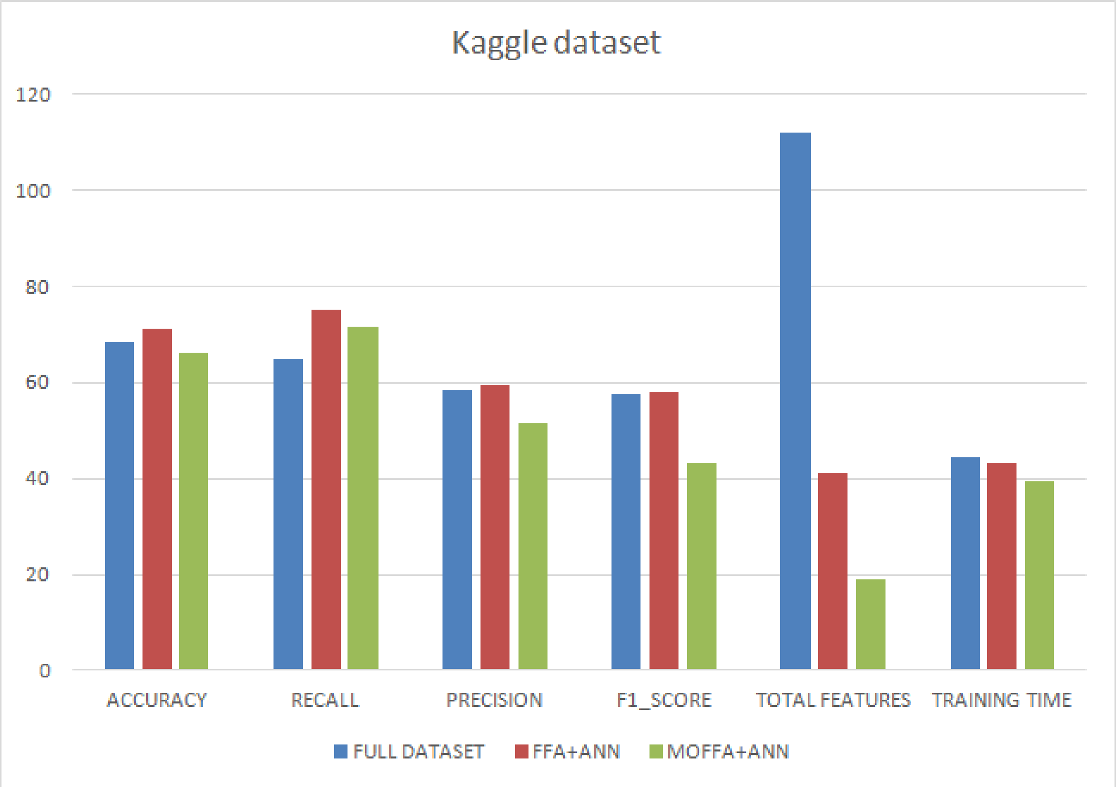


Figure 4.5 Performance graph of Kaggle dataset

4.6 Result of Mendeley Dataset

	Accuracy	Precision	Recall	F1-score	Total No. of features	Reduced features	Training Time(sec)
Dataset+ANN	87.89	87.58	88.64	87.71	42	42	143.38
FFA+ANN	84.76	84.54	85.26	84.63	42	15	123.65
MOFFA+ANN	77.00	76.61	78.13	76.57	42	11	119.99

4.8 Performance of Mendeley dataset

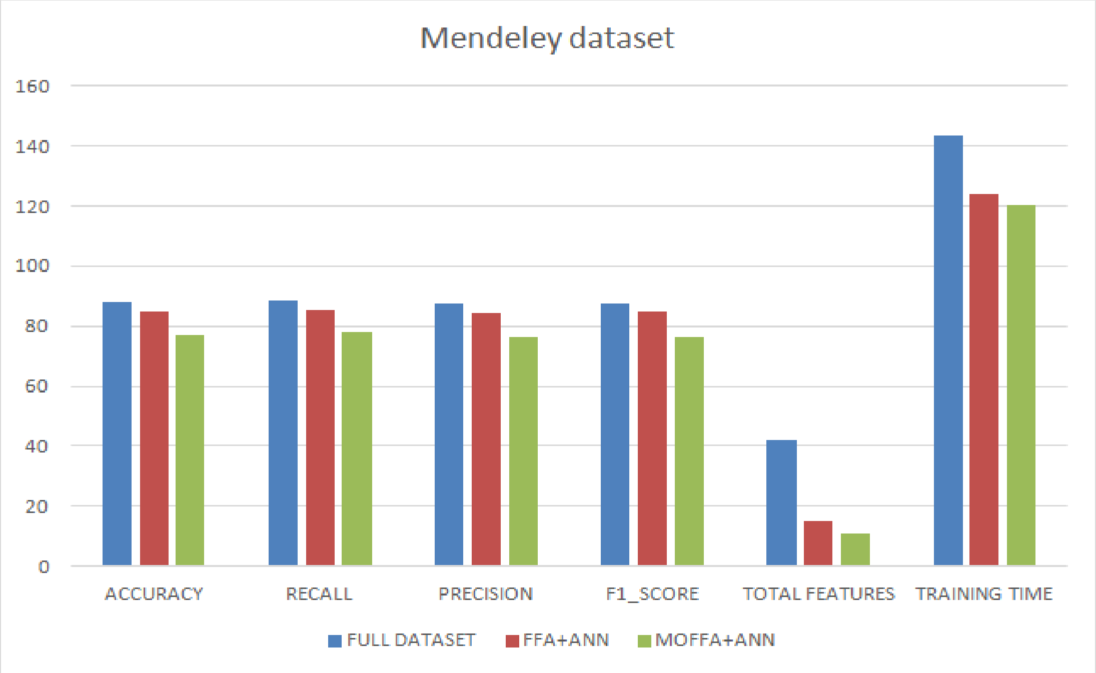


Figure 4.6 Performance graph of Mendeley

The inference from the results will be as follows:

- *The ICSX dataset gives an accuracy of 91.45%, precision of 91.48%, recall of 91.47%, and F1-score of 91.45% with only 13 features for the multi-objective firefly optimization algorithm, which is closely equal to the results of the firefly algorithm with 32 features. The training time will also be reduced to 2 seconds.*
- *The UCI dataset gives an accuracy of 80.64%, precision of 80.80%, recall of 80.64%, and F1-score of 80.62% with only 19 features for the multi-objective firefly optimization algorithm, which is slightly more than the results of the firefly algorithm with 34 features. The training time will also be reduced by almost 2 seconds.*
- *The Mendeley dataset gives an accuracy of 77%, precision of 76.61%, recall of 78.13%, and F1-score of 76.57% with only 11 features for the multi-objective firefly optimization algorithm, which is slightly less than the results of the firefly algorithm with 15 features. The training time will also be reduced to 3 seconds.*

5.CONCLUSION

The proposed multi objective firefly optimization algorithm using ANN models predicts the phishing attack in the internet has been implemented in the four different datasets. ANN model does the data pre-processing and produces a better result in terms of metrics like Accuracy,Recall, Precision and F1 score. From the results, the ICSX dataset gives almost equal results for both MOFA and FFA. The UCI dataset's result for MOFA is slightly greater than the result for FFA. Kaggle and Mendeley's result for MOFA is slightly less than the result for FFA.Accuracy can be increased by increasing the number of layers in ANN model. Overall the proposed method got the efficient output with least number of features in feature extraction method with multi objective fitness equation.

The Multi-Objective Firefly Optimization Algorithm (MOFOA) with an Artificial Neural Network (ANN) model for the detection of phishing attacks. Our investigation into this innovative approach has yielded several significant findings and insights into the realm of cybersecurity.

Through empirical evaluation using real-world datasets, we have demonstrated the effectiveness of the MOFOA-ANN framework in enhancing phishing detection accuracy while mitigating false positives. The results indicate that our approach outperforms traditional methods and showcases promising potential for practical application in real-world scenarios.

Our study underscores the importance of leveraging advanced optimization techniques and machine learning algorithms to combat the growing threat of phishing attacks. By harnessing the collective intelligence of MOFOA and the learning capabilities of ANN, we have developed a robust framework capable of adapting to evolving attack vectors and identifying previously unseen phishing attempts with high precision.

However, while our findings are encouraging, several avenues for further research and development remain open. Future endeavors could focus on enhancing the interpretability of the model outputs, exploring adaptive learning mechanisms for dynamic threat detection, and evaluating the generalization capabilities of the proposed framework across diverse domains.

Additionally, the integration of user feedback mechanisms, privacy-preserving techniques, and real-time detection capabilities represents exciting directions for future exploration in the field of cybersecurity.

The effectiveness of integrating the Multi-Objective Firefly Optimization Algorithm (MOFOA) with an Artificial Neural Network (ANN) model for phishing attack detection. Through extensive experimentation and evaluation, several key findings have emerged. The integration of MOFOA with the ANN model has led to a significant improvement in phishing attack detection accuracy compared to traditional methods.

By leveraging the optimization capabilities of MOFOA, the ANN model has been able to adapt and evolve, resulting in more robust and effective detection performance. Additionally, our approach has shown promise in reducing false-positive rates, thereby minimizing the risk of erroneously flagging legitimate websites as phishing attempts. This improvement is crucial for enhancing the usability and reliability of phishing detection systems in real-world scenarios. Moreover, the MOFOA-ANN framework exhibits robustness and scalability, making it suitable for deployment in diverse environments and handling large-scale datasets. Its ability to adapt to evolving threat landscapes and varying patterns of phishing attacks positions it as a valuable asset in the cybersecurity arsenal.

However, there remain several avenues for further exploration and enhancement. Future work includes the investigation of hybrid approaches combining MOFOA-ANN with other machine learning techniques, enhanced feature engineering tailored for phishing detection, real-time detection and response mechanisms, integration with user awareness training programs, evaluation in dynamic and adversarial environments, scalability and deployment considerations, and continuous improvement and evaluation mechanisms. By pursuing these avenues, we aim to further enhance the efficacy, robustness, and usability of the MOFOA-ANN framework, ultimately contributing to the advancement of cybersecurity practices and the protection of online users and organizations against phishing attacks.

For the upcoming future works, the proposed model's accuracy can be increased with different multi objective fitness functions and also by using the Ensemble learning model.

6.REFERENCE:

1. *Abdul Samad, S. R., Balasubaramanian, S., Al-Kaabi, A. S., Sharma, B., Chowdhury, S., Mehbodniya, A,Bostani, A. (2023). Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection. Electronics, Vol.12, No.7 pp 1642.*

2. *Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., Ramachandran, V. (2021). Enterprise Credential Spear-phishing attack detection. Computers &amp; Electrical Engineering, Vol.94, pp 107363.*

3. *Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. IEEE access, Vol.8, pp 142532-142542.*

4. *Alshammari, G., Alshammari, M., Almurayziq, T. S., Alshammari, A.,Alsaffar, M. (2023). Hybrid Phishing Detection Based on Automated Feature Selection Using the Chaotic Dragonfly Algorithm. Electronics, Vol.12, No.13 pp 2823.*

5. *Altamimi, A. B., Ahmed, M., Khan, W., Alsaffar, M., Ahmad, A., Khan, Z. H., &amp; Alreshidi, A. (2023). PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using Machine Learning. IEEE Access.*

6. *Barlow, L., Bendiab, G., Shiaeles, S., Savage, N. (2020, October). A novel approach to detect phishing attacks using binary visualisation and machine learning. In 2020 IEEE World Congress on Services (SERVICES) (pp 177-182). IEEE.*

7. *Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Nuñez-Agurto, D., &amp; Rodríguez-Galán, G. (2023). A Phishing-Attack-Detection Model Using Natural Language Processing and Deep Learning. Applied Sciences, Vol.13, No.9 pp 5275.*

8. Butt, U. A., Amin, R., Aldabbas, H., *Mohan, S., Alouffi, B., and amp; Ahmadian, A (2023). 'Cloud*-based email *phishing attack using machine and deep learning algorithm'*, Complex and amp; Intelligent Systems, Vol.9, No.3 pp 3043-3070.

9. *Chaudhari, S., Kamthe, A., Kudmethe, M., Barapatre, N., &amp; Bahenwar, S. (2020). Detection of SMS Fraudulent using ANN Algorithm. Annals of the Romanian Society for Cell Biology, pp 190-197.*

10. *Elamathi, M. U,Aruna, M. A. (2023). An Effective Secure Mechanism for Phishing Attacks Using Machine Learning Approach. Journal of Pharmaceutical Negative Results, pp.2724-2732.*