Wah Academia Journal of Social Sciences
Volume 3, Issue 2, Dec 2024, pp. 165-176
ISSN – E 2958-8731 P 2958-8723
https://doi.org/10.63954/WAJSS.3.2.10.2024

Classification of Malware Using VGGNet-19 Model – An Evaluation for General Understanding

Humza Rana[1]

Abstract

The malware program becomes a disturbance to the user as it grabs the most important files and data of the user. The number of devices attached to the internet is increasing at a high speed which raises the opportunity for the attackers to steal or destroy the user data. Some malicious attackers demand money from the user after hacking the user's most important information. The traditional methods for malware classification including static and dynamic contain some limitations as they consume time in feature extraction. The malware classification needs to be identified in the light of artificial intelligence. The machine learning model is also used by the researcher for classification but now gets old and underperforms in the large dataset to overcome the large dataset issue deep learning algorithms are required which perform efficiently in large datasets. Difference researchers proposed deep learning algorithms for malware detection and achieving the best performance in detection but limited to malware classes. In this paper, the VGGNet-19 model which is also a deep learning model proposed for malware classification is in multiclass. In the VGGNet-19 model, the term VGG stands for Visual Geometric Group which can handle up to 19 layers for its deep network feature. The Malimg dataset contains 9339 samples divided into 25 malware classes. The proposed model is trained on this multiclass malware image dataset, achieving 0.998% performance in training, 0.990% in testing, and 0.990% in overall classification accuracy. The confusion matrix confirms model excellence performance across all classes.

Keywords: Malware Classification, Deep Learning, Machine Learning, Artificial Intelligence

[1] Bahauddin Zakariya University, Multan - Pakistan

Introduction

Malware is a harmful program that is developed to destroy the data, steal the data to get financial benefits, or demand money. With the increase in internet usage, the number of malware attackers also increases for stealing the data (Ahmed, 2023). The use of mobile phones is continuously increasing which may give opportunity to attackers for access the user data without being unaware of users. Malware is now coming in different types which may require a powerful method of classification (Odat, 2022). The main purpose of malware programmers is to disturb people by gaining access to their data. Malicious programs are now becoming an unstoppable problem all over the globe (Alzahrani et. al 2022). The old methods for classifying the malware become slow to detect the modern type of malware with efficiency. An advanced technique is required to tackle this problem. The deep learning model which comes from artificial intelligence can solve this problem efficiently and accurately. This deep learning method also improves time and accurately performs classification (Almotairi et al 2024). Almotairi et al. (2023) propose a deep learning model LSTM for classifying the malware. It used the correlation-based feature selection to select the feature from the dataset and achieve the best results but it does not show the per-class classification of the model on malware. It uses the two-class datasets. The VGG visual geometric group named VGG-19 supports 19 layers which are CNN layers making it stronger for performing classification in this task (Siddhesh, 2024). The ML models are time-consuming in the classification of multiclass malware. The deep learning model is suitable for this task so VGG-19 which is CNN with multiple layers using which takes less time to train and perform accurate classification of malware. The VGG-19 is improved than traditional CNN its depth of the VGG-19 model has also been improved. These multiple layers extract image features more easily and faster than a single CNN model (2020). Different deep learning models were proposed for multiclass malware but time time-consuming and low in accuracy in image datasets. That's why VGG-19 which is an improved version of CNN used in this paper to classify malware accurately. In this paper, the VGGNet-19 model is proposed for classifying the malware. The Malimg dataset used in this experiment contains the twenty-five classes which are multiclass.

- **Problem**
  - The malware image datasets need to be evaluated by the efficient deep learning model so that it classifies the malware images accurately and efficiently.

- The multiclass malware image datasets need to be evaluated by the multiclass model to classify the different and advanced types of malware images.
- The malware gets advanced continuously and comes in different types it is necessary to classify the malware and which variety it's coming from.

❖ **Contribution**

The contribution of this paper is to use the VGG-19 model to classify the malware images correctly which are in multiclass. The model tuning was implemented to improve performance in classification. The proposed model deals with the real-world scenario of malware and improves the classification efficiency. Implement the dropout and batch normalization for handling the overfitting. This research also contributes to cyber security for classifying the advanced types of malware images. This proposed model VGG-19 deals with large datasets and multiclass malware. After this we compare our proposed model with CNN model to determine our model performance in multiclass malware classification of images.

Review of the Literature

Anandhi et al. (2022) proposed the deep learning model dense NET model. It uses two datasets which are the BIG 2015 malware dataset and the Malimg dataset. Their proposed model performance is 99.4% and 96.7% in two class malware families. The model also used the FGSM technique to evaluate the performance it shows 95.5% and 90.5% accuracy. Wei et al. (2022) proposed a model using CNN and Bi-LSTM to perform classification on malicious code. The dataset was taken from virus share container 8 malicious families. The experiment by the CNN-Bi-LSTM shows 0.98% accuracy.

Smitha et al. (2024) proposed deep learning models LSTM and CNN. The genetic algorithm is used to select the suitable features. After the experiment, the proposed model gives 98.5% accuracy in malware detection. The Android-based dataset used in this experiment contains 10,000 apps. These Android apps contain malicious and non-malicious apps. Iqbal et al. (2022) uses the LSTM model to classify malware attacks. The top PE Import 1000 features dataset used in this experiment. The model achieved 99.6% accuracy using the sigmoid function. This model works for malicious and non-malicious files.

Hairil et al (2021) proposed an ANN model for detecting ransomware in transaction coins. The heist dataset is used from the machine learning repository. The dataset contains five classes. After the experiment, their model achieves 97% accuracy performance. Awan et al. (2021) proposed a CNN model with a spatial attention method for classifying the malware named the SACNN model. The Malimg dataset used in this experiment consists of twenty-five malware families. After an experiment from the proposed model, a 97.8% accuracy performance was achieved. James et al. (2022) proposed a visualized-based approach for detecting malware. It consists CNN model and a GAN model named Mal-detect for classify the malware. The MaleVis, Malimg, and Virus Share datasets were used in the experiment. After an experiment, 99.8% and 96.7% accuracy performance were achieved in classification. Xiao et al. (2020) use the VGG-NET 19 model to determine whether the worker wears a mask or not. It is two classes labeled data wear mask, and unmasked. The images datasets 3161 samples of mask and unmasked pictures of workers used. After an experiment from the proposed model, a 97.2% precision score was attained by the model. It needs to be improved in accuracy and optimized the model for identifying the complex scenario. Mitsuhashi et al. (2020) proposed a VGG-NET 19 model for classifying the malware using the class imbalance method. This method of class imbalance technique assigns the malware family to different samples groups like 80, 160, 240 and 320 malware samples by assign a malware family to it. After the experiment from the proposed method 98.8 % accuracy is achieved. By using sampling method 99.7 accuracy performance obtain in 320 samples of malware. The model needs to trained on large dataset for evaluate the model performance.

Pinheiro et al. (2021) proposed a visualization-based deep neural network. The two datasets Microsoft Malware Classification and Malimg datasets used in this experiment. Twelve neural network models were used in the experiment. After an experiment, 99.97% f1 performance was achieved. Schofield et al. (2021) proposed 1DCNN to classify the malware. The Windows API calls datasets contain 8 malware families. After an experiment, a 98.17% accuracy performance by the model was obtained. Joshi et al. (2021) proposed an ANN model for classifying the botnets using a special feature extraction technique fuzzy logic. The CTU-13 dataset was used in the experiment. It contains the two malware classes. After an experiment, a 99.9% accuracy performance was achieved in the model.

Table 1 Existing Model Performance in Malware Classification with Malware Datasets

Author	Model	Dataset	Family	Accuracy
Akhtar (2022)	CNN-LSTM	Kaggle Dataset	Two	0.99%
Kumar (2022)	CNN-BiLSTM	Virus Shares	Eight	0.992%
Jamal (2022)	ANN	IoT Dataset	Nine	0.978%
Mai (2021)	Dec-DCNN	BIG 2015	Nine	0.978%
Qiu (2022)	CNN	Malimg	Twenty-Five	0.99%
Ahmad (2023)	Inception V3	BIG 2015	Nine	0.978%
Alzahrani (2022)	VGG NET 19	Malware Dataset	Five	0.982%

Table 1 shows the different existing deep learning models that were proposed for classifying the malware. Each model is designed to cover malware family classification. It presents the model, datasets, family, and accuracy in a multiclass approach for classifying the different types of malware.

Table 2 Malware Family Covered by researchers with their performance in Family

No	Authors	Families	Accuracy
1	**Viboonsang (2024)**	5-class	0.995%
2	**Ma (2023)**	5-class	0.999%
3	**Wei (2022)**	8-class	0.988%
4	**Alzahrani (2022)**	5-class	0.982%
5	**Awan (2021)**	25-class	0.971%
6	**Alnajim (2023)**	25-class	0.981%
7	**Aslan (2021)**	25-class	0.977%
8	**Jamal (2022)**	9-class	0.971%
9	**Mayhem (2021)**	5-class	0.99%
10	**Chen (2022)**	10-class	0.934%
11	**Sharma (2021)**	4-class	98.2%
12	**Dang (2021)**	20-class	81%

Table 2 presents the authors with covered malware families with the accuracy they achieved in the experiment. It shows the accuracy of the malware family.

Table 3 Strength and Weakness of Existing Models

Models	Strength	Weakness
VGG-19	Deep Network with Multiple Layers to extract image features rather than a single model	High Computational Cost
CNN	CNN is useful for image classification and powerful for extracting image features	High Computation Cost in 3D CNN Network
LSTM	It is very useful for sequential data for classification tasks.	It requires a lot of time for training.
GRU	It is faster than LSTM and uses small memory.	It takes training time and is slow to deal with large datasets.
VGG-16	Deep Network with Multiple layers to take useful image features.	High Computational Cost

Table 3 shows the different type of deep learning models that contains the weakness and strengths of model performance.

Methodology

In this methodology part the proposed model is defined with the complete steps. It defines the data preprocessing and model training steps. All steps of the methodology are defined in pseudo-code form.

Step 1: Load Images from Folders
Step 2: Convert Images into RGB Mode
Step 3: Convert the list of Images & labels into Arrays
Step 4: Let gs_images be training data & gs_labels labeled data
Step 5: Perform Data Splitting in training & label data
Step 6: Perform Label Encoding & Categorical Operation in Labeled Data
Step 7: Load VGG Net 19 Model

```
vgg19 = VGG19(weights='ImageNet', include top=False, input_shape=(224, 224, 3))
for layer in vgg19.layers:
   Layer. Trainable = False
x = Flatten () (vgg19.output)
x = Dense (512, activation='relu') (x)
x = tf.keras.layers.BatchNormalization()(x)
```

```
x = Dropout (0.5) (x)
output = Dense (25, activation='SoftMax') (x)
model = Model (inputs=vgg19.input, outputs=output)
# Compile the model
model. compile(optimizer=tf.keras.optimizers.Adam(learning_rate=0.001),
        loss='categorical_crossentropy',
        metrics=['accuracy'])
# Print the model summary
model.summary()
# Train the model (assuming X_train, Y_train, X_test, Y_test is defined)
history = model. Fit (X_train, Y_train, epochs=25, batch_size=32, validation data=
(X_test, Y_test))
# Evaluate the model
score = model. Evaluate (X_test, Y_test, verbose=0)
```

The above methodology contains the seven steps that define the images fetched from the folder converted into RGB, and a list of array images. After this data is split into training and testing data. The labels encoding and categorical function in labels data. Now load the VGG Net 19 model and add layers of batch normalization and dropout to prevent overfitting. The model parameters are selected after checking the model performance using a different type of parameters that helps to reduce the complexity of the proposed model. Compile and train the model after this evaluate the model performance in classification. The learning rate for the model 0.001 is selected after using different values of learning rate in the training process. After receiving the best result from the proposed model, the parameters listed help to give the best classification task performed by the model.

Table 4 Parameters Used in the Proposed Model

Parameters	Values
Loss	Categorical Cross Entropy
Learning Rate	0.001
Activation Output	SoftMax
Dropout	0.5
Epochs	25

Batch Size	32
Metrics	Accuracy
Verbose	0

Table 4 shows the different model parameters used in the proposed model. Its parameters used in multiclass VGG Net 19 architecture. These parameters are selected after tuning the proposed model during the training phase.

Results & Discussion

In this section, the results are presented from the proposed model. The experiment is taken in core i7 seven generation, 8 GB RAM. The Malimg malware dataset was used in this experiment. The proposed VGG-NET 19 is a multiclass model the results obtained from this model as shown as.

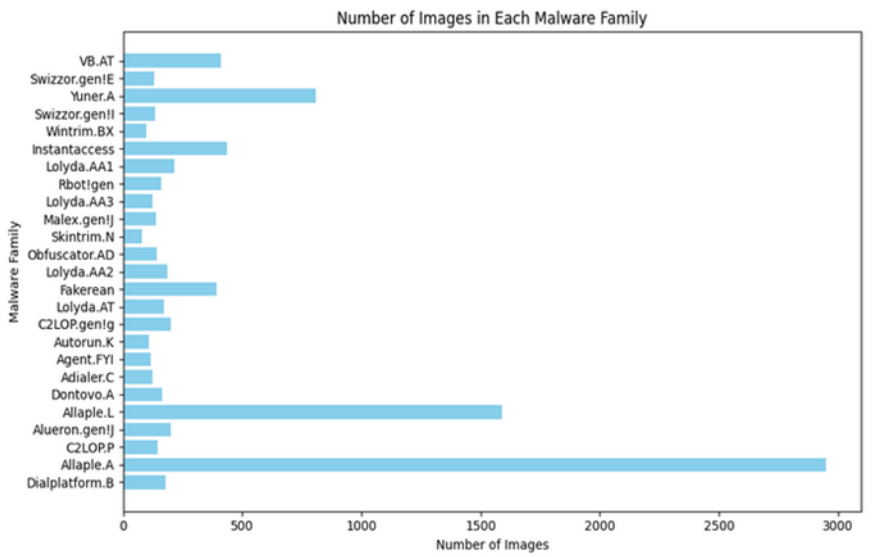

Figure 1 Number of Malware Families in Malimg

Figure 1 contains 25 number of malware families in the data. The quantity of each malware family is present in the dataset.

Table 5 Proposed Model Performance in Dataset

Model	Accuracy	Recall	TPR	F1 score	FPR
VGG NET 19 Model	99.0%	99.0%	1.0	99.0%	0.0
CNN Model	97.1%	97.1%	97.2%	97.0%	0.0

Table 5 shows the proposed model performance which shows the accuracy, recall, f1 score, and accuracy from the model.

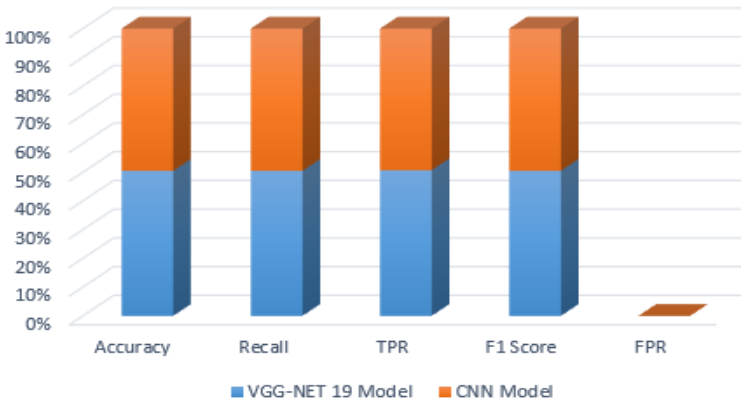

Figure 2 Performance Comparison of Proposed Model with CNN

Figure 2 shows the graphical comparison of the proposed model with the CNN model. It contains the different metrics which evaluate the model performance in each aspect.

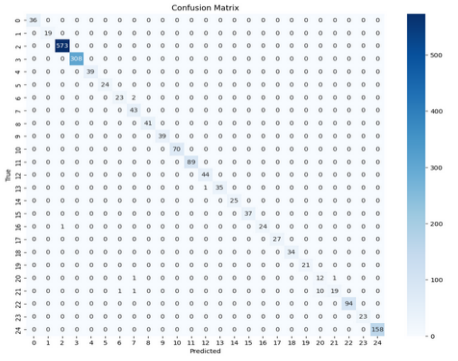

Figure 3 Confusion Matrix from Proposed Model

Figure 3 shows the confusion matrix from the proposed model on the Malimg dataset containing 25 malicious families. This figure presents each class correctly predicted by the proposed model.

The VGG NET 19 model classify each class accurately without miss any class. It shows proposed model performance best due to its depth of network. It extracts the features of images due to the training method of model for perform best classification. The proposed model easily solves the multiclassification malware in the images accurately.

Conclusion

In this paper, the VGG NET 19 model is proposed to classify the malware families. The model is trained using different hyperparameters. The Malimg images dataset was used in this experiment. The dataset contains the 25 number of malware families. After experimenting with the proposed model which is a multiclass model it achieves 99.0% accuracy performance. The model performs best in multiclass malware image classification.

- **Future**

For the advancement in research before training the model the data should be normalized applied feature selection and pass through the process of class balance operation. The big data with multiclass should be implemented in this model. To further evaluate model performance in terms of big data and with the number of malware classes. Different types of feature extraction methods and feature selection methods include PCA, RFE, and fisher score method. The different types of class imbalance methods should improve performance using SMOTE to handle classes.

References

M. Ahmed, N. Afreen, M. Ahmed, M. Sameer, and J. Ahamed, "An inception V3 approach for malware classification using machine learning and transfer learning," Int. J. Intell. Networks, vol. 4, no. September 2022, pp. 11–18, 2023, doi: 10.1016/j.ijin.2022.11.005.

E. Odat, B. Alazzam, and Q. M. Yaseen, "Detecting Malware Families and Subfamilies using Machine Learning Algorithms: An Empirical Study," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 2, pp. 761–765, 2022, doi: 10.14569/IJACSA.2022.0130288.

A.I. A. Alzahrani, M. Ayadi, M. M. Asiri, and A. Al-rasheed, "Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques," pp. 1–20, 2022.

S. Almotairi, M. A. R. Khan, O. Alharbi, Z. Alzaid, Y. M. Hausawi, and J. Almutairi, Detection of Android Malware Using Deep Learning Ensemble with Cheetah-Optimized Feature Selection, vol. 41, no. 5. 2024. doi: 10.17654/0974165824026.

N. S. Sani, M. I. Esa, and B. A. Musawi, "SS symmetry Feature Selection," Symmetry (Basel)., vol. 15, no. 123, pp. 1–21, 2023.

"VGG-Net Architecture Explained. The company Visual Geometry Group... | by Siddhesh Bangar | Medium." https://medium.com/@siddheshb008/vgg-net-architecture-explained-7117931005of (accessed Oct. 30, 2024).

J. Xiao, J. Wang, S. Cao, and B. Li, "Application of a Novel and Improved VGG-19 Network in the Detection of Workers Wearing Masks," J. Phys. Conf. Ser., vol. 1518, no. 1, 2020, doi: 10.1088/1742-6596/1518/1/012041.

V. Anandhi, P. Vinod, V. G. Menon, and K. M. Aditya, "Performance evaluation of deep neural network on malware detection: visual feature approach," Cluster Comput., vol. 3, 2022, doi: 10.1007/s10586-022-03702-3.

L. Wei, F. Xu, N. Zhang, W. Yan, and C. Chai, "Dynamic malicious code detection technology based on deep learning," ICOCN 2022 - 20th Int. Conf. Opt. Commun. Networks, pp. 2022–2024, 2022, doi: 10.1109/ICOCN55511.2022.9901158.

M. Sonia, C. B. N. Lakshmi, S. J. Hussain, M. L. Swarupa, and N. Rajeswaran, "Android Malware Detection Using Genetic Algorithm Based Optimized Feature Selection and Machine Learning," Lect. Notes Electr. Eng., vol. 1106, no. 12, pp. 207–215, 2024, doi: 10.1007/978-981-99-7954-7_19.

S. Iqbal, A. Ullah, S. Adlan, and A. R. Soobhany, "Malware Prediction Using LSTM Networks," Lect. Notes Networks Syst., vol. 350, pp. 583–604, 2022, doi: 10.1007/978-981-16-7618-5_51.

N. Dwi, W. Cahyani, and H. H. Nuha, "Ransomware Detection on Bitcoin Transactions Using Artificial Neural Network Methods," pp. 669–673, 2021.

M. J. Awan et al., "Image-based malware classification using vgg19 network and spatial convolutional attention," Electron., vol. 10, no. 19, 2021, doi: 10.3390/electronics10192444.

O. James, A. Simon, and S. Adebukola, "Mal-Detect: An intelligent visualization approach for malware detection," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 5, pp. 1968–1983, 2022, doi: 10.1016/j.jksuci.2022.02.026.

R. Mitsuhashi and T. Shinagawa, "High-Accuracy Malware Classification with a Malware-Optimized Deep Learning Model," no. August, 2020, [Online]. Available: http://arxiv.org/abs/2004.05258

A.Pinhero et al., "Malware detection employed by visualization and deep neural network," Comput. Secur., vol. 105, p. 102247, 2021, doi: 10.1016/j.cose.2021.102247.

M. Schofield et al., "Convolutional Neural Network for Malware Classification Based on API Call Sequence," pp. 85–98, 2021, doi: 10.5121/csit.2021.110106.

C. Joshi, R. Kumar, and V. Bharti, "A Fuzzy Logic based feature engineering approach for Botnet detection using ANN," J. King Saud Univ. - Comput. Inf. Sci., no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.06.018.

M. S. Akhtar and T. Feng, "Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time," Symmetry (Basel)., vol. 14, no. 11, 2022, doi: 10.3390/sym14112308.

A.I. Journal and M. Kumar, "Scalable Malware Detection System Using Distributed Deep Learning Deep Learning," Cybern. Syst., vol. 0, no. 0, pp. 1–29, 2022, doi: 10.1080/01969722.2022.2068226.

A.Jamal, M. Faisal Hayat, and M. Nasir, "Malware Detection and Classification in IoT Network using ANN," Mehran Univ. Res. J. Eng. Technol., vol. 41, no. 1, pp. 80–91, 2022, doi: 10.22581/muet1982.2201.08.

J. Mai, C. Cao, F. Shi, and X. Chen, "Malware Variant Detection Based on Decomposed Deep Convolutional Network," 2021 IEEE 6th Int. Conf. Big Data Anal. ICBDA 2021, pp. 333–338, 2021, doi: 10.1109/ICBDA51983.2021.9403081.

J. Wang, S. Wang, and Y. Wang, "Malware Classification based on a Light-weight Architecture of CNN : MalShuffleNet," pp. 2–5, 2022.

P. Viboonsang and S. Kosolsombat, "Network Intrusion Detection System Using Machine Learning and Deep Learning," Int. Conf. Cybern. Innov. ICCI 2024, no. February, 2024, doi: 10.1109/ICCI60780.2024.10532673.

W. Ma, C. Gou, and Y. Hou, "Research on Adaptive 1DCNN Network Intrusion Detection Technology Based on BSGM Mixed Sampling," Sensors, vol. 23, no. 13, 2023, doi: 10.3390/s23136206.

A.M. Alnajim, S. Habib, M. Islam, R. Albelaihi, and A. Alabdulatif, "Mitigating the Risks of Malware Attacks with Deep Learning Techniques," Electron., vol. 12, no. 14, 2023, doi: 10.3390/electronics12143166.

O. Aslan and A. A. Yilmaz, "A New Malware Classification Framework Based on Deep Learning Algorithms," IEEE Access, vol. 9, pp. 87936–87951, 2021, doi: 10.1109/ACCESS.2021.3089586.

M. Maithem and G. A. Al-Sultany, "Network intrusion detection system using deep neural networks," J. Phys. Conf. Ser., vol. 1804, no. 1, 2021, doi: 10.1088/1742-6596/1804/1/012138.

Y.-H. Chen, J.-L. Chen, and R.-F. Deng, "Similarity-Based Malware Classification Using Graph Neural Networks," Appl. Sci., vol. 12, no. 21, p. 10837, 2022, doi: 10.3390/app122110837.

A.Sharma and U. Tyagi, "A Hybrid Approach of ANN-GWO Technique for Intrusion Detection," 2021.

D. Dang, F. Di Troia, and C. R. Mar, "Malware Classification Using Long Short-Term Memory Models," pp. 1–16, 2021.

Article Information:

Received	*2-Sept-2024*
Revised	30-Nov-2024
Accepted	5-Dec-2024
Published	15-Dec-2024

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

- **Conflict of Interest**: NIL

- **Funding Sources**: NIL

Correspondence:

Humza Rana

humza.rana99@gmail.com