COMPREHENSIVE SECURITY OF SDN CONTROLLERS IN NFVI-BASED 5G NETWORK

Asad Faraz Khan
School of Electrical and Data Engineering
Faculty of Engineering and IT
University Of Technology Sydney
Sydney, Australia
Asadfaraz.khan@student.uts.edu.au

Priyadarsi Nanda
School of Electrical and Data Engineering
Faculty of Engineering and IT
University Of Technology Sydney
Sydney, Australia
priyadarsi.nanda@uts.edu.au

Abstract—**In the present world, Software-Defined Networks (SDN) is the developing technological environment that allows integrated control and splits the control plane from the data plane. It is essential to classify the attacks in SDN-based networks to improve security. Concomitantly, SDN-related networks are vulnerable to numerous attacks especially Distributed Denial of Service (DDoS) attacks which interrupt the data transmission and network data. To resolve this issue, various traditional researchers have attempted to attain attack detection, however, there is a lack in computational cost, accuracy rate, and Packet Delivery Ratio. To overcome the limitations, the proposed hybrid model employs a system creation model for encrypting data using ELGAMAL and ECC algorithms to strengthen data security. Furthermore, the present hybrid model incorporates the wrapper-based approach Sine Cosine hybrid optimization algorithm with Modified Particle Swarm Optimization (SCMPSO) for feature selection which is intended to improve the performance of the classification. Furthermore, it utilizes the XG Boost-Light Gradient-Boosting Machine (GBM) algorithm for attack classification. Accordingly, Extreme Gradient-Boosting (XG Boost) can handle the missing data, and the ensemble nature of XG Boost with multiple Decision trees (DT) combinations makes it challenging to finalize the prediction. To overcome the limitations of the XG Boost algorithm, the proposed model uses Light GBM. Correspondingly, the present method created a dataset using the Mininet tool. The efficacy of the proposed hybrid model is calculated with several evaluation metrics to analyze the performance. The proposed method is intended to contribute to SDN-based network development and is envisioned to contribute to attack detection mechanisms.**

Keywords—Software Defined Network (SDN), Network Function Virtualization Infrastructure (NFVI), 5G Network, XG Boost, Light GBM and Machine Learning (ML).

I. INTRODUCTION

Software-Defined Networks (SDN) are risen as prominent technological fortification which is dignified to bolster network security. It is defined as an evolving technology that revolves around conservative notions of network settings along with decoupled data plane and control plane. SDN brings many benefits like flexibility, programmability and manageability [1]. Simultaneously, control plane is considered as anticipated target of security attacks on opponents due to its characteristics [2]. The data plane is composed of false devices, transferring data packets based on the specified rules. Security susceptibilities in SDN controller could cooperate the network security entirely. DDoS can be mitigated and detected [3]. Moreover, Network Function Virtualization Infrastructure (NFVI) could be considered as cloud infrastructure component. NFV is a conventional technology of 5G network that signifies NFV security importance will improve precisely [4]. Correspondingly, fragile authentication allows the attackers to examine and eavesdrop the traffic [5]. In accordance with security, SDN architecture has its unique security requirements and several lacks in security make the architecture vulnerable to various threats and attacks. Recently, research has been using AI (Artificial Intelligence) based technology for attack and non-attack classification. Advantages with Machine Learning (ML) and Deep Learning (DL) offers several applications in SDN security. The implementation of ML in SDN is a notable aspect of the platform.

Congruently, several conventional models have attempted to undertake attack and non-attack classification. The conventional model has detected network attacks with the help of SDN supported intrusion detection with Long Short-Term Memory (LSTM). The result has shown that the model has identified and classified the attacks with better accuracy [6]. Similarly, the traditional model has created SDN dataset through Mininet emulator and RYU controller to detect various types of DDoS attacks by utilizing classification algorithms for the CIC-DDoS 2019 dataset. The results have shown that the DT has better performance [7]. Contrastingly, the conventional model has employed a data-plane ML solution. The ML solution has evaluated with help of RF, SVM and KNN to detect DDoS attacks in real network traces and the results have shown that the Data plane-ML is faster than the statistical methods [8, 9]. The existing model has used XG Boost and other ML algorithms to enhance the accuracy of the security solutions of the network. The traditional model has attained 91.3% of accuracy in multi-class classification [10]. Accordingly, the conventional models consummated satisfactory results. However, it lacks several limitations such as accuracy, over fitting of data, computational cost and low detection performances.

To resolve these issues, the proposed hybrid model uses certain set of procedures to enhance the performances in detection through classification of attacks in SDN. Initially, the dataset is generated using Mininet tool with the help of Ubuntu. As the Mininet creates virtual network that accomplishes by creating hosts and switches connecting with virtual interfaces. RYU is an SDN controller, which is connected through the 16 switches and 16 hosts. The Mininet helps to connect the virtual interfaces on the switch with each connected part of the host. The switches can control the data where a controller acts as the control plane and open flow switch acts as the data plane. The data gets encrypted using hybrid algorithm of ELGAMAL, and ECC. The encrypted data were secured under authentication to ensure the security of the data. This data is further processed to data pre-processing method. For the feature selection process, the proposed hybrid model uses wrapper-based method of SCMPSO algorithm to select relevant features from the dataset. Therefore, selected data is split into two in the ratio of 80:20 where 80% of data is used for training and 20 is used for testing process. The data were further processed for classification method using hybrid algorithm of XG Boost-Light GBM. After the classification, the testing data is used for the performance calculation in the present hybrid model. Additionally, the proposed model is measured using performance metrics to analyze the classification performance of the proposed hybrid model.

A. *Research Contribution*

The major contribution of the proposed hybrid model as follows,

- To create a dataset using Mininet tool with Ubuntu.
- To employ hybrid algorithm of ELGAMAL and ECC for data authentication.
- To employ the XG Boost-Light GBM algorithm for the classification performance.
- To calculate the efficacy of the proposed hybrid model using performance metrics.

B. *Paper Orgnization*

The flow of the present model is given here: Section II reviews the conventional literature related to anomaly prediction and problem identification. Section III precisely describes the proposed methodology. Furthermore, section IV provides a table and graphical representation of data analysis and results of the proposed model with traditional research. Finally, section V concludes the current model along with future research.

II. LITERATURE SURVERY

This section explains about the analysis of various existing models of SDN and Draft methodology along with other techniques for the prediction on attacks classification system. The existing model has focused on efficiency and possibility of, Distributed Denial of Service (DDoS) attack and mitigation. The prevailing method has examined the DL models, LSTM and Convolutional Neural Network (CNN). It has generated its own dataset for both testing and training. The results have shown that the RNN-LSTM produced 89.63%, Naïve Bayes attained 82.61% and SVM achieved 86.85% of accuracy [11]. Similarly, the conventional method has mitigated DDoS attack in SDN Internet Service Provider (ISP) networks for Internet Control Message Protocol (ICMP) flood attacks and TCP-SYN using ML methods of KNN and XG Boost. It has utilised CAIDA 2007 dataset and the outcome has shown that 98% accuracy when adapted to capacity [12, 13]. Correspondingly, the prevailing model has detected the DDoS attack and classified the normal or traffic in SDN. The prevailing model has applied polynomial SVM to compare the linear SVM by utilising scapy (a packet generation tool and RYU controller). Hence, the dataset has been collected by creating volume-based normal traffic and DDOS attack traffic. According to the results, the polynomial SVM has attained 3% accuracy more and 34% low false alarm rate than linear SVM [14].

Moreover, conventional model has described a modular SDN base architecture with the components which could be enhanced or modified separately, providing flexibility to detect various types of attacks. It also explored ML and DL techniques to resolve which technique has performed better under various attack conditions and types. Thus, it used CICDoS2017 and CICDDoS2019 datasets. The results have shown that the DL models have attained 98% and 95% accuracy rates than ML methods [15, 16]. In the same way, the conventional method has employed the hybrid CNN-LSTM model to detect for classifying the DDoS attack in SDN based networks with the help of custom dataset. The outcome has revealed that the hybrid model attained 99% accuracy [17, 18]. Contrastingly, conventional model has classified the SDN traffic as attack traffic or normal utilising the ML algorithms with Neighbourhood Component Analysis (NCA). The conventional model has utilised public DDoS attack SDN dataset with 23 features. The outcomes of the existing model have shown that the Artificial Neural Network (ANN) and SVM have attained better accuracy. The DT model has attained better results [19, 20].

Concomitantly, the conventional model has employed an effective detection mechanism against DDoS attack in SDN data plane and control plane. For this, the dataset has been generated from the computations and features extraction along with the classifier. The experimental outcomes of the prevailing method have proved that the method has attained better accuracy and less false alarm rate [21, 22]. The conventional model has evaluated experimentally on an entropy-based solution to mitigate and detect DDoS and DoS attacks in the scenarios of IoT utilising a SDN data plane. It developed the application called proof-of-concept at Ryu

SDN controller top which has been detected the DDoS and DoS attacks in terms of entropy values. The results have occurred in three scenarios and attained better accuracy [23, 24]. Similarly, the existing model has proposed to categorise benign traffic from DDoS attack through using ML techniques and has identified attack detections. It has created SDN dataset and the outcomes have shown that hybrid SVC-RF has attained 98.8% of accuracy with low false alarm rate [25].

A. *Problem Identification*

- The conventional attack detection schemes are challenging obstacles because of high false positive rates, high computational costs and low detection performances [26, 27].
- The research with ML methods has to enhance the security solution accuracy and to increase the packet delivery ratio [10]

III. PROPOSED METHOD

The Software-Defined Networking (SDN) is a network architecture approach which is utilized for software-based application programming Interfaces (API) or controllers to transfer with directing traffic on a network and underlying hardware infrastructure. However, the data transmission is vulnerable to malicious attacks which distress the security of SDN based networks. To overcome the issue, several traditional models have focused on attack detection however lacks accuracy, security and computation. To solve this problem, the proposed model employs XG Boost-Light GBM algorithm with attention mechanism based on the classification. The figure. 2 illustrates the flow design of proposed hybrid model.

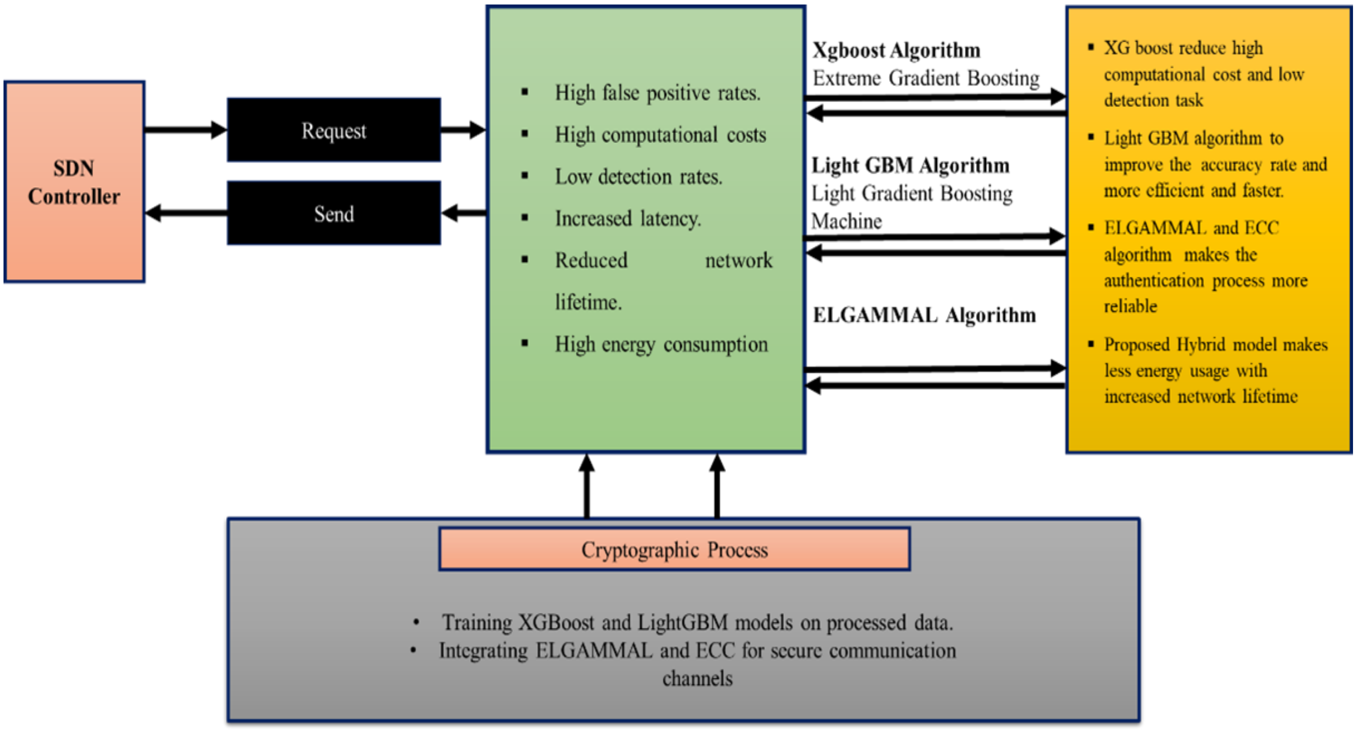


Fig. 1. Comparison of Existing and Proposed Model

Figure. 1 deliberates the comparison performance of proposed model with existing research. The green box represents the existing problems of traditional research which are overcome by the proposed system. The cryptographic process undergoes overcoming the traditional issues to attain better values through proposed model.

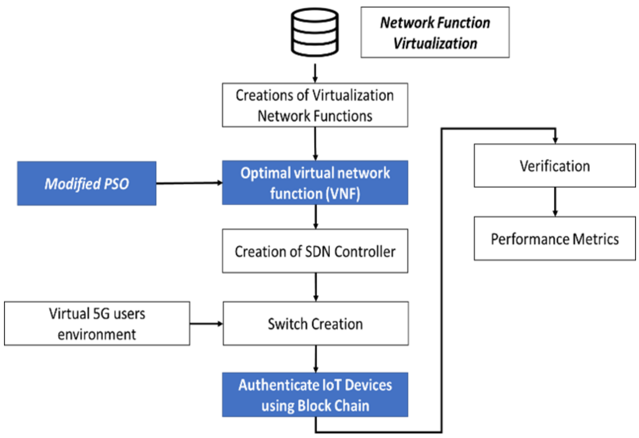


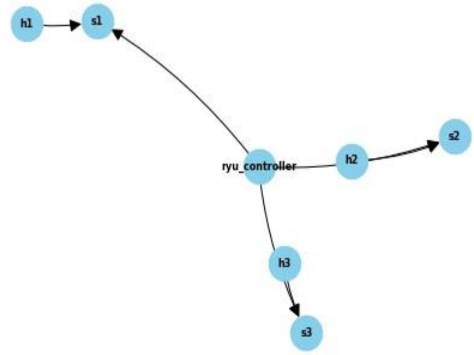
Fig. 2. Comparison of Existing and Proposed Model

The figure. 2 illustrates the overall mechanism of the proposed hybrid model. The dataset is being created for the proposed model classification. Initially, the VNF is created where the switches and hosts are connected. The Modified PSO decides whether the VNF switches whether it is parallel, series, on or off. It creates the SDN controller for 5G user's environment and their security. If the attack is detected in any switch, Modified PSO makes it off to avoid further forwards. Then, it sends an alert to the user with the IP address. The reliable data is passed for authentication process where it is processed with the help of ELGAMMAL and ECC algorithm. It makes the authentication process more reliable and moves for verification. Furthermore, the verified data is used for proposed hybrid model classification. The pseudo code for ELGAMMAL-ECC algorithm is provided below.

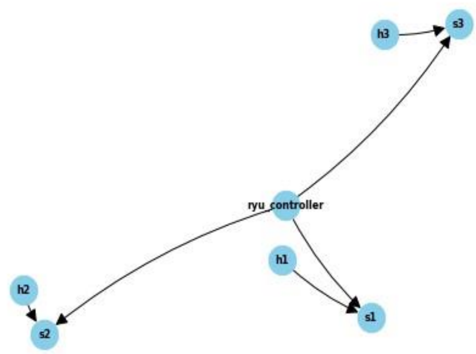
Pseudo code for ELGAMMAL and ECC algorithm
$\boldsymbol{Elliptic\ Curve\ ElGamal\ (EC-EG)\ algorithm}$ $\boldsymbol{Setup. Given\ a\ security\ parameter\ K_i,}$ $\boldsymbol{construct\ an\ elliptic\ curve\ E_i\ defined\ over\ a}$ $\boldsymbol{finite\ field, together\ with\ a\ prime\ p\ and}$ $\boldsymbol{generator\ G_i. KeyGen. Select\ a\ random\ xe}$ $\boldsymbol{F, as\ private\ key, and\ compute}$ $\boldsymbol{Y\ =\ X_i\ G_i. Then, public\ key\ is\ (E_i.p_o.G_i.Y_i).}$ $\boldsymbol{Encrypt. Encrypt\ m\ with\ public\ key\ (E_i.p_o.G_i.Y_i).}$ $\boldsymbol{1. Select\ a\ random\ number\ ke\ F,.}$ $\boldsymbol{2. Compute\ M\ =\ map(m_o), where\ map(m_o)}$ $\boldsymbol{=\ m_o G_i.}$ $\boldsymbol{3. Generate\ ciphertext\ C_o-(R_o,S_o), where\ R}$ $\boldsymbol{-K_i G_i, S_o M-ki}$ $\boldsymbol{Decrypt. Decrypt\ C\ with\ private\ key\ X_i.}$ $\boldsymbol{1. Compute\ MxR_o S_o-xkG_i+M_o+xkG_i.}$ $\boldsymbol{2. Reverse\ through\ m\ =\ map(M).}$ $\boldsymbol{3. Return\ the\ plaintext\ m.}$

A. Data Creation

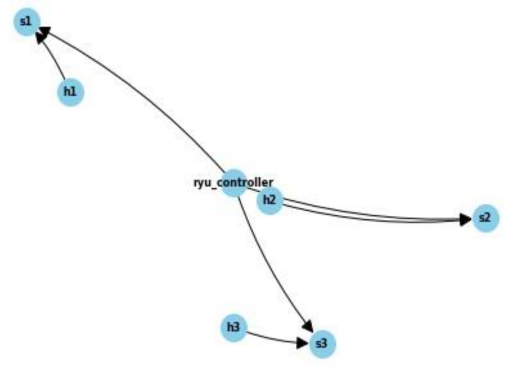
The present model generated a dataset using the Mininet tool with the help of Ubuntu. Mininet is a python-tool for generating SDN based networks. It acts as an emulator of the network which is utilized to visualize the applications and switches of SDN in virtual environment. RYU is an SDN controller that supports open Flow protocol. It uses two controllers called c1 and c2, each has 8 switches and 8 hosts. Controller acts as a sender and host acts as a receiver. If the attack is detected in switch 1, the alert will be sent to the user with IP address. The cryptosystem consists of a decrypting algorithm, encrypting algorithm and well-defined triple text. The current model uses the cryptosystem with the hybrid ELGAMMAL, ECC algorithm to encrypt the data from the switches. These encrypted data are used under authentication to ensure the security of the data and used for dataset creation for the pre-processing. Similarly, figure. 3 represents the SDN controller simulations.



(a)



(b)



(c)

Fig. 3. Simulations of SDN Controller

Figure. 3 illustrates the SDN controller Simulations. It shows the hosts, switches and RYU controller in various nodes topology. The table. 1 Signifies the simulation parameters and its values used in the proposed hybrid model.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulation Area	1000x1000m
Simulation Time	300s
Number of MUs	50
Number of APs	4
Number of Switches	7
Number of Controllers	2
SDN Controller	POX
Flow Type	TCP, UDP
Number of Packets	1500
Flow Timeout	1.5s
Packet Length	1024 bytes
Mobility of MUs	250 m/s
Mobility Model of MU	Random Way Point Model
Interval Time	0.15s
Packet Interval Bit Rate	100 ms
Attack Rate (Per Attacker)	20-1000 pps
Cumulative Attack Packet Rate	1000-1200 Kbps
Protocol Used	IPv6
Delay	10 microseconds
Block Size	4 bytes
Block Header	80 bytes
Transaction Counter	1-9 bytes
Number of Transactions	Variable
Proof Type	Proof of Work
Hash Generation	Blake_256()

B. *Data Pre-Processing*

Pre-processing is a technique of altering the raw data into a suitable data set, which is pre-processed to check the missing values, noisy signals, label encoding, feature scaling and other inconsistencies before applied to the algorithm. Besides, the pre-processing improves the classification performance of the proposed method. To achieve this, the proposed system implemented two significant pre-processing techniques like checking missing values and label encoding. In the process of label encoding, the categorical data values are assigned to numerical labels to enhance the efficiency of the proposed model.

C. *Data Splitting*

In Machine Learning, data splitting is utilized to eradicate the data over fitting. Generally, ML utilizes the data splitting technique to train the present model where the training data is added to the proposed method for equipping the training stage parameters. After the training process, the test set data are measured to calculate the respective model for handling the observations. In the proposed framework, the original data is split into 2 sets, the test and training of 80:20 which indicates eighty percent of the new observations is utilized for the training and the remaining 20 percent of the observations are used for testing. The training set data is employed for training the proposed framework and the testing set data is used to calculate the performance of the respective technique.

D. *Classification- Proposed Hybrid of XG Boost and Light GBM Algorithm*

The present model employs ML based hybrid model, XG Boost-Light GBM algorithm to develop the results of classification. The classification performance takes place in Spyder tool. The security of SDN controllers in 5G network is processed with the proposed hybrid model which is trained in the generated dataset with Mininet Tool. This section exemplifies the algorithms and mechanism of the proposed hybrid model. The following sections illustrate the XG Boost and Light GBM mechanism.

i. Extreme Gradient Boosting (XG Boost)

XG Boost, an ML technique and develops on other models such as Random Forest and Gradient boost. It functions well in complex and huge datasets through using various optimization methods. XG Boost could converge rapidly with lesser steps, more direct to less errors, reduces the computational costs and simplifies calculations to improve the speed. The limitations involved that model training requires more time and resources compared to modest algorithms. In terms of high learning rates or complex models, gradient boosting is prone to the problem of over fitting. Thus, the proposed model was determined to employ the XG Boost algorithm with Light GBM algorithm to enhance the performance of proposed hybrid model

ii. Light Gradient-Boosting Machine Algorithm

The Light GBM algorithm, a gradient boosting ensemble technique which is based on decision trees and used by the Auto ML tool. Light GBM could be used for both regression and classification which is optimized for the high performance along with different distributed systems. Generally, Light GBM is more efficient and faster, making it appropriate for huge datasets whereas XG Boost can perform better only with smaller datasets or while the interpretation is important. Thus, the Light GBM is incorporated with XG Boost to enhance the efficiency of the proposed model.

iii. Proposed Hybrid of XG Boost and Light GBM Algorithm

The ensemble nature of XG Boost with numerous Decision trees (DT) combined, it makes challenging to final prediction. Additionally, it could be computationally intensive when handling huge datasets and complicated models. Furthermore, it finds difficult with imbalanced dataset, and it primarily handles numerical labels. To evade the limitations of the XG Boost algorithm, the proposed model uses the Light GBM algorithm to improve the accuracy rate. Combining the strengths of these algorithms can achieve high accuracy in detecting the attacks. It increases the generalization capability of the proposed ML model and allows for flexibility and customization. Therefore, combining the algorithms can leverage their strengths and could compensate for the weaknesses.

Pseudo code-IV XG Boost-Light GBM

<u>Input: Training Examples</u>

1. $X_{ii} = \text{Value}_{XGBOOST}$ Initialize Weights by XGBOOST Values
2. $S_{hi} := \sum_{i=1}^{n} Y_{ii}.X_{ii} + b_i$ (Y_{i1}, Y_{i2} , $Y_{i3} \ldots\ldots\ldots\ldots.. Y_{in}$) multiplied with their ($X_{i1}, X_{i2}, X_{i3} \ldots\ldots\ldots\ldots.. X_{in}$) for hidden layer node
3. Empricial loss Function $= \sum_{X_{in}}^{Y_{in}} S_{hi}$
4. output hidden $\leftarrow \emptyset(s_{hi})$ output (hidden layer node)
5. $S_{out} := \sum_{i=1}^{n} Y_{ii}.X_{ii} + b_i$
6. Update
7. $D_{it+1}(ii) = \frac{D_{it}(ii)}{z_t} = \{\frac{e^{-\propto t} \text{ if instance ii is correctly classified}}{e^{\propto t} \text{if instance ii is not correctly classified}}$

Where Z_{if} is a normalization factor (chosen so that $\sum_{ii=1}^{m_i} D_{it+1} = 1$

Output the Final hypothesis $H_i(x_i) = \text{sign}(\sum_{t_i-1}^{T} \propto_{it} h_{it}(x_{ii}))$

8. $\text{output}_{predict} \leftarrow \emptyset\left(D_{it+1}(ii)\right)$
9. Compare Error $\left(\text{output}_{predict} - \text{output Actual}\right)$
10. search Error Rate
11. search Error Rate
12. Update network weight
13. $\left(\text{output}_{predict} - \text{output Actual}\right)$

Output Trained Neural Network

IV. EXPERIMENTAL RESULTS

This section provides the experimental and implementation results of the proposed work. Further, we also provide the comparative analysis results of the proposed and existing works respectively that accomplished for ensuring the security in SDN based networks.

A. Exploratory Data Analysis

This section exemplifies the EDA of SDN based dataset utilized in the present model. The EDA is utilized to visualize and understand the data in the generated dataset. The figure. 4 and Figure. 5 represents the system model simulation and data packet flow rate respectively.

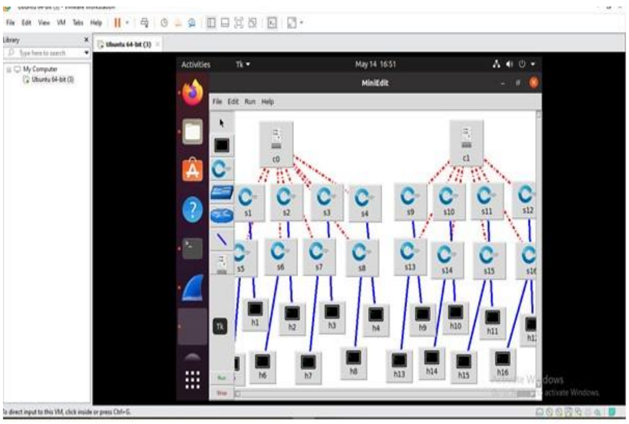


Fig. 4. System model Simulation

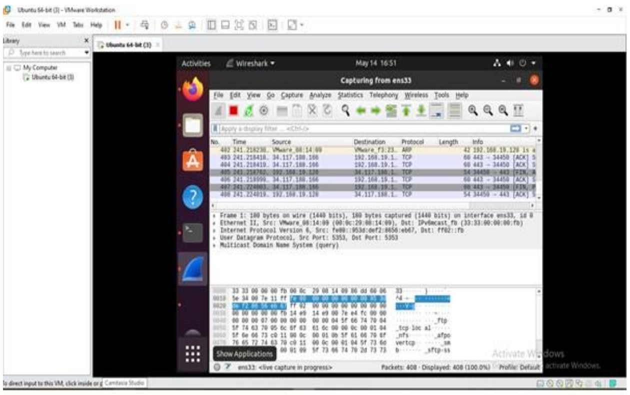


Fig. 5. Data Packet Flow Rate

The figure. 6 exemplifies the attacks in the classification. The blue colour refers to non-attack data whereas orange colour refers to data with attacks.

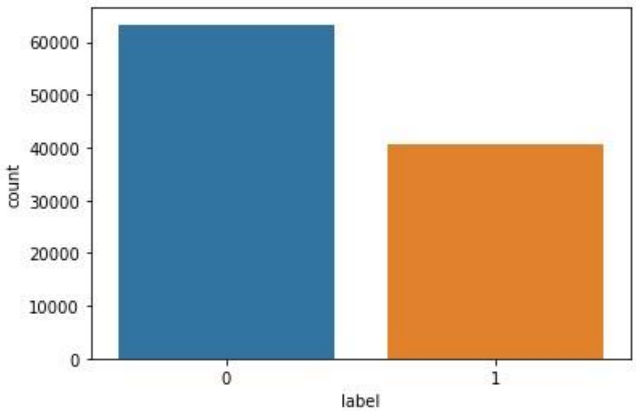


Fig. 6. Attacks predicted in the Present hybrid Model

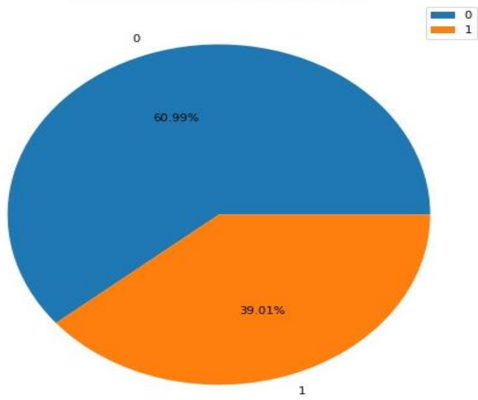


Fig. 7. Pie Chart Distribution of Multi-Class Labels

The figure. 7 shows the pie chart distribution of multi-class labels. Label 1 refers to data with attack whereas, blue color refers to non-attack data. Data with attack has 39.01% and non-attack data has 60.99%.

B. *Performance Metrics*

Performance metrics are primarily used for observing the efficiency of the projected research by utilizing various metrics like recall rate, Precision, Accuracy and F1 score value.

C. *Recal Metric*

Recall is utilized to examine the data percentage which is correctly detected in the respective model. The recall formula is defined in the following equation (14),

$$\text{Recall} = \frac{\text{True\_Pos}}{\text{False\_Neg+True\_Pos}} \tag{14}$$

D. *Accuracy Matric*

The Accuracy is the important metric used to analyze the number of estimates which are approximately correct in the present model. The accuracy formula is illustrated in equation (15),

$$\text{Accu} = \frac{\text{TP+TN}}{\text{TP+FP+TN+FN}} \tag{15}$$

E. *F1 Score Metric*

F1-score is used to analyze the predictions in the present model that are made for positive class. The f1-score formula is mentioned in equation (16),

$$\text{F1 Score} = 2 * \frac{\text{Recall}*\text{Precision}}{\text{Recall+Precision}} \tag{16}$$

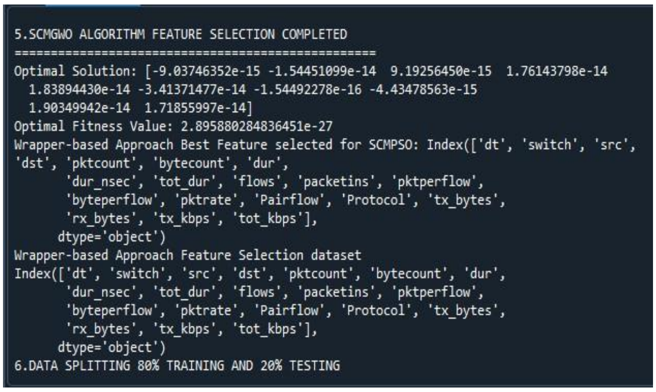
F. *Precision Metric*

The metric precision is indicated as the method's covariance unit of which resulted through suitably predictable cases (True_Pos) to the total group of cases that have been precisely considered (True_Pos + False_Pos). It comprises repeatability and producibility of the capitals. Equation (17) depicts the formula for precision.

$$\text{Precision} = \frac{\text{True\_Pos}}{\text{False\_Pos+True\_Pos}} \tag{17}$$

G. *Performance Analysis*

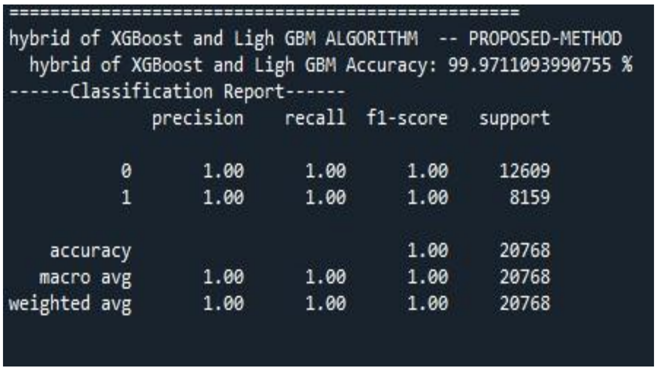
The performance of proposed algorithm is examined utilising evaluation metrics like Recall, Precision, F1-score and Accuracy. Figure. 8 shows the feature selection process in the proposed hybrid model.



```
5.SCMGWO ALGORITHM FEATURE SELECTION COMPLETED
==================================================
Optimal Solution: [-9.03746352e-15 -1.54451099e-14  9.19256450e-15  1.76143798e-14
  1.83894430e-14 -3.41371477e-14 -1.54492278e-16 -4.43478563e-15
  1.90349942e-14  1.71855997e-14]
Optimal Fitness Value: 2.895880284836451e-27
Wrapper-based Approach Best Feature selected for SCMPSO: Index(['dt', 'switch', 'src',
'dst', 'pktcount', 'bytecount', 'dur',
       'dur_nsec', 'tot_dur', 'flows', 'packetins', 'pktperflow',
       'byteperflow', 'pktrate', 'Pairflow', 'Protocol', 'tx_bytes',
       'rx_bytes', 'tx_kbps', 'tot_kbps'],
      dtype='object')
Wrapper-based Approach Feature Selection dataset
Index(['dt', 'switch', 'src', 'dst', 'pktcount', 'bytecount', 'dur',
       'dur_nsec', 'tot_dur', 'flows', 'packetins', 'pktperflow',
       'byteperflow', 'pktrate', 'Pairflow', 'Protocol', 'tx_bytes',
       'rx_bytes', 'tx_kbps', 'tot_kbps'],
      dtype='object')
6.DATA SPLITTING 80% TRAINING AND 20% TESTING
```

Fig. 8. Feature Selection

Figure. 8 signifies feature selection. It shows the optimal fitness value is 2.9. The wrapper based approach is selected for feature selection called Sine Cosine Modified Particle Swarm optimization (SCMPSO). Moreover, the figure. 9 represents the results of classification.



```
================================================
hybrid of XGBoost and Ligh GBM ALGORITHM  -- PROPOSED-METHOD
  hybrid of XGBoost and Ligh GBM Accuracy: 99.9711093990755 %
------Classification Report------
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     12609
           1       1.00      1.00      1.00      8159

    accuracy                           1.00     20768
   macro avg       1.00      1.00      1.00     20768
weighted avg       1.00      1.00      1.00     20768
```

Fig. 9. Classification Result

From figue. 9, it understood that the proosed hybrid model attained efficient results. It attained 100% of accuracy, 100% of precsion 100% of recall and 100% of F1-Score respectively. Similarly, figure. 10 shows the node results.

```
 hybrid of XGBoost and Ligh GBM_specificity: 1.000
cpu_utilization: 1714.9716424216736
Execution Time: 43.34013748168945 seconds
Computational Cost : 0.4334013748168945б
Delay to  192.168.0.60: 0.5 ms
Delay: 2.666432639098635 ms
Throughput: 853.0704201894717 Mbps
 Packet Loss Rate: 2.9041301494689713%
```

Fig. 10. Node Result

Figure. 10 deliberates the node results of proposed hybrid model. It shows that the proposed hybrid model attained execution time of 43.34 seconds, specificity of 1.000, computational cost of 0.43, delay of 2.67 ms, throughput of 853.07 Mbps and packet loss rate is 2.9%.

H. Comparative Analysis

The section exemplifies the comparative analysis of the proposed mechanism with the prevailing approaches depending on performance metrics.

TABLE II. PROPOSED MODEL OUTCOME COMPARISON [28]

Model	Energy Consumption	Throughput
Existing	0.4	0.9542
Proposed	0.32	0.99412

The table deliberates proposed model outcome comparison. It shows the energy consumption and throughput. The present attained 0.32 of energy consumption and 0.99412 of throughput. The table. 3 deliberates the network lifetime.

TABLE III. NETWORK LIFE TIME OF PROPOSED MODEL [28]

Model	Network Lifetime
Existing	32320
Proposed	41000

The table. 3 signifies the Network lifetime. It shows the proposed hybrid model attained 41000 of network lifetime than existing model. The figure. 11 illustrates the performance analysis of proposed hybrid model.

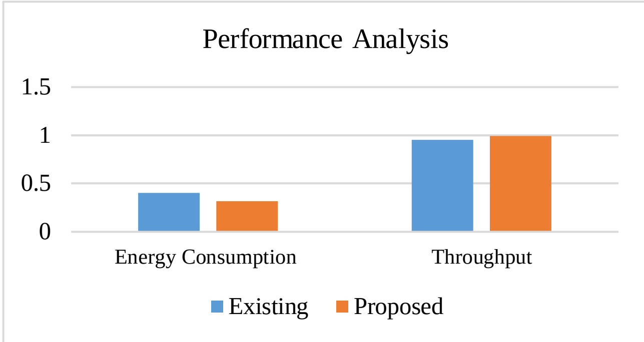


Fig. 11. Performance Analysis of Proposed Hybrid Model

The figure. 11 depicts the performance analysis. It shows that the proposed hybrid model attains 0.08 of energy consumption less than existing model and 0.03992 of throughput more than existing model. It shows the efficacy of the proposed hybrid model. Furthermore, the figure. 12 exemplifies the comparison of proposed model results.

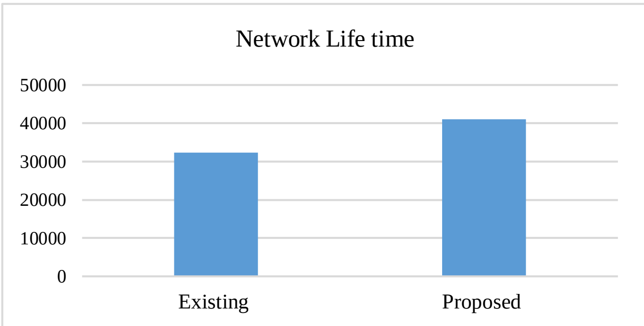


Fig. 12. Comparison of Proposed model's Results

The figure. 12 describes the comparison of Network lifetime with existing model. It attained 8680 more than the existing model which attains only 32320 of lifetime. The table. 4 represents the accuracy comparison with prevailing research.

TABLE IV. ACCURACY COMPARISON WITH EXISTING METHODS [29]

Method	Accuracy
Existing Method	92
Existing Method CNN	91

Existing Method CNN2	90
Proposed Method	97.6

The table. 4 exemplifies that the proposed hybrid model attained 100% of accuracy where other conventional research attained 92%, 91% and 90% of accuracies. Similarly, the figure. 13 represents the accuracy comparison of proposed hybrid model.

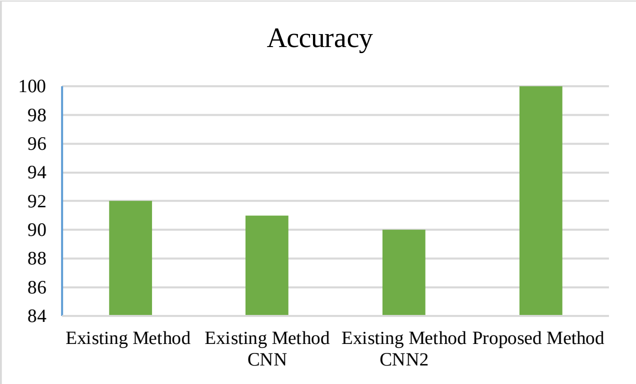


Fig. 13. Accuracy comparison

The figure. 13 shows the accuracy comparison of proposed hybrid model. It attained 8%, 9% and 10% more than conventional models such as existing method, existing CNN and existing CNN2 respectively. Correspondingly, the table. 5 deliberates the recall metric comparison.

TABLE V. COMPARISONS ON RECALL [30]

Model	**Recall**
SVM	0.9
MLP	0.92
Proposed	0.996

The table. 5 depicts the recall metric comparison of the present model. It attained 0.996 of recall which is higher than other prevailing models like SVM and Multi-layer Perceptron (MLP). Similarly, the figure. 14 signifies the recall comparison.

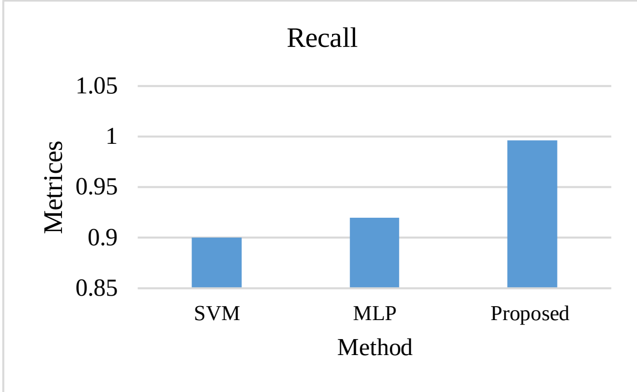


Fig. 14. Recall Comparison with Existing model

The figure. 14 demonstrates the recall comparison of proposed hybrid model. It attained 0.096 and 0.076 recall values more than SVM and MLP models respectively.

V. CONCLUSION

SDN is the emerging technology in the modern world, which provides rapid data and connects hosts in the environment. Consequently, data security is significant for the network environments. The SDN based networks are vulnerable to various attacks like DDoS, numerous research endeavored to attain security in SDN, attack and non-attack classification. However, it lacks accuracy and computation. To overcome this issue, the proposed hybrid model uses ELGAMAL and ECC algorithm for system model creation, wrapper-based method of SCMPSO for feature selection and XG Boost-Light GBM algorithm for attack classification. In the same way, the XG Boost-Light GBM algorithm is used to improve the classification of the proposed hybrid model. Besides, the SDN dataset that has been created was used in the proposed hybrid research for improving the efficiency of the present model. Congruently, the result of the present research is calculated using performance metrics to examine the performance of the present research. From the outcomes, it exemplifies that the proposed hybrid model attained value of accuracy of 100%, recall rate of 100, F1-score of 100 and value of precision of 100. Consistently, the result of the comparative analysis of the respective model signifies the performance of the existing research. The future work includes attack classification on the various attacks can enhance the efficiency and the performance of proposed hybrid model.

REFERENCES

[1] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, M. N. J. C. Sugali, and Security, "DDoS attack detection and mitigation using deep neural network in SDN environment," vol. 138, p. 103661, 2024.

[2] M. Revathi, V. Ramalingam, and B. J. W. P. C. Amutha, "A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework," pp. 1-25, 2021.

[3] S. Ahmad, A. H. J. J. o. N. Mir, and S. Management, "Scalability, consistency, reliability and security in SDN controllers: a survey of diverse SDN controllers," vol. 29, pp. 1-59, 2021.

[4] A. K. Alnaim, A. M. Alwakeel, and E. B. J. S. Fernandez, "Towards a security reference architecture for NFV," vol. 22, no. 10, p. 3750, 2022.

[5] A. Hussein, L. Chadad, N. Adalian, A. Chehab, I. H. Elhajj, and A. J. J. o. C. S. T. Kayssi, "Software-Defined Networking (SDN): the security review," vol. 4, no. 1, pp. 1-66, 2020.

[6] [6] R. Chaganti, W. Suliman, V. Ravi, and A. J. I. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," vol. 14, no. 1, p. 41, 2023.

[7] H. Kousar, M. M. Mulla, P. Shettar, and D. Narayan, "Detection of DDoS attacks in software defined network using decision tree," in *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, 2021, pp. 783-788: IEEE.

[8] R. N. Carvalho, L. R. Costa, J. L. Bordim, E. A. J. C. Alchieri, C. Practice, and Experience, "DataPlane-ML: an integrated attack detection and mitigation solution for software defined networks," vol. 35, no. 19, p. e7434, 2023.

[9] A. J. I. A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," vol. 9, pp. 42236-42264, 2021.

[10] [H. A. Alamri, V. Thayananthan, and J. J. I. J. C. A. Yazdani, "Machine Learning for Securing SDN based 5G network," vol. 174, no. 14, pp. 9-16, 2021.

[11] [J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. J. T. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," vol. 9, no. 1, p. 14, 2021.

[12] N. N. Tuan, P. H. Hung, N. D. Nghia, N. V. Tho, T. V. Phan, and N. H. J. E. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," vol. 9, no. 3, p. 413, 2020.

[13] F. Talpur, I. A. Korejo, A. A. Chandio, A. Ghulam, and S. H. Talpur, "ML-Based Detection of DDoS Attacks Using Evolutionary Algo-Rithms Optimization," 2024.

[14] A. T. Kyaw, M. Z. Oo, and C. S. Khin, "Machine-learning based DDOS attack classifier in software defined network," in 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2020, pp. 431-434: IEEE.

[15] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. J. I. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," vol. 9, pp. 108495-108512, 2021.

[16] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Ddosnet: A deep-learning model for detecting network attacks," in *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2020, pp. 391-396: IEEE.

[17] B. Nugraha and R. N. Murthy, "Deep learning-based slow DDoS attack detection in SDN-based networks," in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2020, pp. 51-56: IEEE.

[18] Y. Al-Dunainawi, B. R. Al-Kaseem, and H. S. J. I. A. Al-Raweshidy, "Optimized Artificial Intelligence Model for DDoS Detection in SDN Environment," 2023.

[19] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert, and R. J. E. Kocaoğlu, "Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking," vol. 10, no. 11, p. 1227, 2021.

[20] R. Anusuya, M. R. Prabhu, C. Prathima, and J. A. J. J. o. S. i. F. S. Kumar, "Detection of TCP, UDP and ICMP DDOS attacks in SDN Using Machine Learning approach," vol. 10, no. 4S, pp. 964-971, 2023.

[21] W. G. Gadallah, H. M. Ibrahim, N. M. J. C. Omar, and Security, "A deep learning technique to detect distributed denial of service attacks in software-defined networks," vol. 137, p. 103588, 2024.

[22] T. E. Ali, Y.-W. Chong, and S. J. A. S. Manickam, "Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN," vol. 13, no. 5, p. 3033, 2023.

[23] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. J. S. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach," vol. 20, no. 3, p. 816, 2020.

[24] J. E. Varghese and B. J. I. A. Muniyal, "An Efficient IDS framework for DDoS attacks in SDN environment," vol. 9, pp. 69680-69699, 2021.

[25] N. Ahuja, G. Singal, D. Mukhopadhyay, N. J. J. o. N. Kumar, and C. Applications, "Automated DDOS attack detection in software defined networking," vol. 187, p. 103108, 2021.

[26] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "A novel machine learning framework for advanced attack detection using sdn," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1-6: IEEE.

[27] M. H. H. Khairi *et al*., "Detection and classification of conflict flows in SDN using machine learning algorithms," vol. 9, pp. 76024-76037, 2021.

[28] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Bloc-sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT," in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, 2020, pp. 499-507: IEEE.

[29] S. Ho, S. Al Jufout, K. Dajani, and M. J. I. O. J. o. t. C. S. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," vol. 2, pp. 14-25, 2021.

[30] P. Gulganwa and S. J. I. J. o. I. T. Jain, "EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach," vol. 14, no. 1, pp. 135-144, 2022.