International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(18s) 2026 pp. 1316-1324
https://doi.org/10.70917/ijcisim-2026-4979
Article

A Minority-Aware Deep Learning Framework for Intrusion Detection under Imbalanced Network Traffic

Vikramaditya Sachin Chavan[1], Nikita Patil[2], Reshma Londhe[3], Ashish Yende[4], Vinod Jagannath Kadam[5], Rajnikant Alkunte[6]

[1] Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
Email: vikramadityachavan@gmail.com
[2] Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
Email: patilnikita1975@gmail.com
[3] Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
Email: londhereshma1997@gmail.com
[4] Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
Email: ashishyende2003@gmail.com
[5] Professor, Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
Email: vjkadam@dbatu.ac.in
[6] Assistant Professor, Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
Email: rajnikalkunte@dbatu.ac.in

Abstract: As cyber assaults are on the rise, there is a requirement for a robust and dynamic IDS that efficiently detects harmful activity from network data. However, the class imbalance problem in the network data is a great challenge to the standard IDS. To overcome this problem, FS approaches are used, such as RFE, to minimise the dimensionality of the data and improve the performance of the intrusion detection models. In this paper, a new strategy based on an ensemble method is proposed which leverages the benefits of several classifiers to overcome the issue of class imbalance and improve detection accuracy. The model is tested with the CIC-IDS 2017 dataset which consists of different network traffic scenarios and attack patterns. With the advanced preprocessing and FS methods, the ensemble model has a good performance. Especially, the voting classifier (RF + DT) obtains an excellent accuracy of 99.5%. Based on the results obtained it is shown that the proposed technique is able to solve the problem of imbalanced data without sacrificing high detection performance and therefore is a promising technique to enhance the reliability and efficiency of IDS in real world cyber defence scenario.
Keywords: CIS IDS, cyber security, deep learning (DL), ensemble learning, intrusion detection, network security, Voting Classifier”

1. INTRODUCTION

Communication networks are the backbone of the infrastructure of almost all sectors in the digital era today. Hence, the importance of the security of such systems is more than ever. With the surge in cyberattacks and their complexity, organisations around the world are increasingly focused on protecting their sensitive information and ensuring the integrity of their operations. Amongst all the various types of cyber threats, intrusions in network traffic are the most sinister and challenging to tackle. These are the intrusions that disrupt the security and integrity of communication network by exploiting system vulnerabilities. They are extremely dangerous and difficult to combat since they may remain hidden for extended periods of time. Typically, an intrusion detection system (IDS) is a rule-based or signature-based system that does not necessarily work well for detecting these dynamic attacks. Typically

such systems detect harmful actions based on pre-determined rules or recognized threat signatures. But they can't spot new and undetected hazards that are out of the ordinary. Thus, there is a need for an intelligent and adaptive IDS system [1][2].

As cyberattacks grow in sophistication and dynamism, better IDSs are increasingly needed that are capable of recognising and assessing the new threats. A solution to these problems is proposed by MLM-based techniques which can learn from the data, adapt to new context and gradually improve the detection accuracy [3]. IDS can be used to analyse large amounts of network traffic to detect unusual activities that could indicate intrusion, using ML algorithms. One of the biggest challenges in network traffic analysis is the class imbalance issue, where the majority of network traffic is legitimate, and only a small fraction is malicious. Low detection rates may result from this, especially for uncommon but serious threats like invasions. The network with a larger number of users in certain area is called unbalanced network. Known as unmonitored locations, these can be taken advantage of by attackers. However, cybercriminals can exploit secure areas of the network by infiltrating less monitored areas [4] just as a burglar might target a neighbourhood in which there is weak security.

This imbalance needs to be corrected for intrusion detection systems to work effectively. If there is no monitoring along the entire network, then even low traffic areas can be the target of an assault. Thus, it is crucial to have all components of the network monitored and secured at the same level, both when they are active and when they are not, to provide high security. Recent research has shown that the performance of IDS can be significantly enhanced using powerful ML algorithms, new techniques for class imbalance and feature selection, and become more powerful and resistant to increasingly sophisticated cyber attacks [5][6][7]. The new generation of adaptive IDS is no longer a response to limitations of current IDS but an essential part of the evolution of more secure and resilient network infrastructures.

2. RELATED WORK

The increasing sophistication of cyber-attacks and network incursions has led to a rise in recent focus on IDS and ML / intelligent systems. It is particularly important for sensitive infrastructures, such as UAVs and transport networks, where network communications security is crucial. As the number of cyber attacks is growing, researchers have been working on new IDS strategies that can evolve in anticipation of new kinds of attacks, even in the face of the problems of class imbalance in network traffic. This literature review covers a lot of significant advancements in the area and shows how ML has become a major tool to enhance the capability of IDS and the new approaches to address the inherent challenges.

In transport systems, Bangui and Buhnova [13] provide interesting evaluation of the current progress in incorporation of ML techniques into IDS. Cybersecurity issues and solutions in transportation such as smart cities, ITS and UAVs are discussed. In their work, intelligent systems get highlighted in the handling of the huge volume of data produced by these systems. The assessment focuses on the application of ML techniques including DT, SVM and DL models, which have been found useful for detecting abnormal traffic and intrusion in transport networks. They are making substantial contributions in addressing the need for adaptive systems that can adapt to new attack vectors and network conditions that are constantly changing.

Similarly, Chen et al. [14] propose a spatio-temporal GCN solution to UAV network intrusion detection. UAV networks are used for various applications including surveillance, communication and data collection purposes, and have a decentralised and dynamic structure which makes them vulnerable to cyber-attacks. In this paper, the authors provide a novel approach that takes advantage of spatio-temporal GCNs to describe the interdependence of the network traffic in both space and time. The method takes advantage of the graph structure of the UAV networks and finds complex attack patterns that are not easily detectable by conventional methods. The addition of GCNs could enhance the generalisation and adaptability capabilities, which is extremely important for the security of UAV networks.

Basan et al. [15] provides an intelligent IDS of a group of UAVs and its security for multi-UAV systems for collaborative activities like reconnaissance and monitoring. This study highlights the problems of maintaining the integrity and privacy of communications in such groups, where each UAV could have to share sensitive information with other UAVs. The authors suggest using an intelligent IDS with intelligent intrusion and harmful activity detection based on ML techniques to protect a collaborative network of UAVs. Adaptive approach is suggested to be adaptable to the ever evolving UAV communications that may have varying traffic patterns, which can change rapidly as the mission changes. The proposed IDS is particularly useful in the real-time defence against emerging threats owing to its versatility.

The intrusion detection problem in UAVs is proposed using DRL by Praveena et al. [16]. The authors present an optimum DRL system that enhances the IDS by adaptively learning from the network traffic and dynamically changing network environment. The DRL integration enables the system to learn through time and adaptivate its effectiveness, being able to learn and detect intrusions based on the feedback provided by previous actions. This recommended approach is helpful in scenarios where UAV networks are facing new or unknown threats and the IDS can learn and adapt on a continual basis through the approach. The real-time capability and adaptability of DRL model to new attack patterns is a great advantage for UAV security.

In their study, [17] Whelan et al. investigate the contribution of artificial intelligence to the enhancement of IDS in UAV systems. They review various AI technologies such as ML, DL, and ANN and their applications in UAV network security. In addition, this study seeks to emphasise the potential of AI-based systems to enhance the attack detection and categorisation by learning on the basis of past attack data and adapting to new threats. The authors note that the traditional IDS based on signatures is not applicable for UAVs because it is not able to identify unknown and unique threats. On the other hand, the future of AI models may be more precise and comprehensive in detection. Whelan et al. also discuss the importance of integrating AI methods with real-time data processing to guarantee effective and timely intrusion detection.

DL application for high performance IDS for networked UAVs is discussed by Abu Al-Haija and Al Badawi [18]. The authors propose a DL-based IDS with the CNN model to extract the features from raw network traffic data. The system has been created to deal with the peculiar constraints of UAV networks such mobility, changeable topology, and limited computational resources. The proposed IDS is based on DL model which is trained with large datasets to identify the known attacks, and the new ones. The system is quite successful in identifying a wide range of intrusions including zero-day attacks thanks to its ability to generalise from the training set. The study of Abu Al-Haija and Al Badawi points out the significance of DL to improve the scalability and accuracy of IDS in UAV contexts.

Fotohi et al. [19] introduced a self-adaptive IDS for UAV-to-UAV communications system security that is inspired by the human immune system. The authors propose a biologically-inspired model which changes its methods of detection based on the changing nature of the threats. The system is based on a set of principles that replicate the human immune system behaviour so that it can recognise and respond to potential incursions. This technique is adaptive and the IDS can therefore keep a high detection accuracy even for the attacker that adapts over time. The system could continuously evolve to emerging attacks, and model the immune response to strengthen its resistance to complex and evolving attacks in UAV networks.

He et al. [20] propose a collaborative intrusion detection system for UAV networks based on GANs, employing a distributed federated learning technique with blockchain. The authors integrate the federated learning with GAN to create a decentralized system to train intrusion detection models on multiple UAVs without sharing of sensitive data. This technique can reduce privacy and security problems as each UAV can generate a model independently without providing any information regarding its traffic. The use of GANs can then create synthetic data which can be incorporated into the training data in order for the model to better identify unusual or unique attacks. The use of blockchain enhances the security of the system by making it easier to detect.By using blockchain, the system becomes more secure and transparent in the detection process.

In combination, these studies show the tremendous progress made in IDS for UAVs and transportation networks, especially with respect to ML and DL techniques. Deep reinforcement learning, graph convolutional networks, and GANs are examples of sophisticated algorithms that provide a solid basis for handling the dynamic and ever-changing nature of cyberattacks. Furthermore, the emergence of adaptive and biologically inspired models (BI models), like the immune system based IDS, suggests that it is possible to create IDS systems that can intelligently react to new attacks types. As UAV networks and other vital infrastructures continue to grow, such novel approaches will be of paramount importance to secure and ensure the reliability of networked systems.

3. MATERIALS AND METHODS

To tackle the issue of class imbalance, along with leveraging a combination of advanced FS methods and ensemble learning, we propose a method to enhance the performance of IDS. For high dimensional network traffic data, we will apply FS approaches like as RFE to decrease the feature space and keep the most relevant information. The ensemble technique is used to enhance the detection accuracy and resilience by combining several classifiers such as XGBoost [8] with LSTM [9] and minVGG [12] (1DCNN), AlexNet (1DCNN) and CNN + BiLSTM [10]. Very powerful model for gradient boosting, XGBoost: LSTM model for sequential data analysis, CNN based models (minVGG and AlexNet) for feature extraction, BiLSTM model for capturing forward and backward temporal dependencies. Ensemble method particularly voting classifier with RF and DT will reduce the class imbalance, and the system is more flexible and efficient in real world cyber defence scenarios. Dataset CIC-IDS 2017 [11] will be used to evaluate the system performance for detecting different attack patterns.

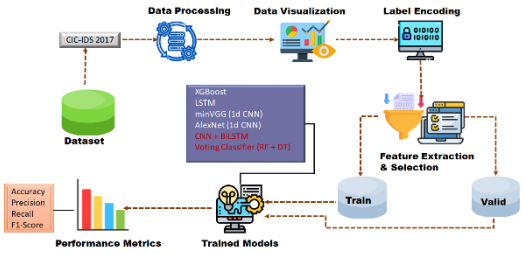


Fig.1 Proposed Architecture

Data is processed and visualised using the dataset for the CIC-IDS 2017 [11]. Label encoding is performed after it is followed by feature extraction and selection. The data set is then split into what is known as a train set and a valid set. Various models such as XGBoost [8], LSTM [9], miniVGG, AlexNet [12], 3dCNN, CNN+BLSTM [10] and VotingClassifier are trained and tested on the dataset. Performance metrics that are used to assess models include accuracy, precision, recall and F1-score.

A) Dataset Collection:

The data used in this study is provided by CIC IDS 2017 [11]. This dataset is the network traffic data used for intrusion detection, emphasizing a study of packet-level features. There are 78 attributes and 17,697 items in the collection with each attribute representing different measurements of network traffic. Feature selection was done and the subset of 10 important characteristics was found to be 'Bwd Packet Length Mean', 'Bwd Packet Length Std', 'Fwd IAT Total', 'Fwd IAT Mean', 'Fwd IAT Min', 'Bwd IAT Std', 'Bwd Packets/s', 'Avg Packet Size', 'Avg Bwd Segment Size', 'Subflow Bwd Packets'. These features capture important aspects of network flow such as packet lengths, inter-arrival periods and flow statistics which are important for effective intrusion detection. The feature set reduction is employed for training the model for better accuracy and efficiency of the detection system.

	Protocol	Flow Duration	Total Fwd Packets	Total Backward Packets	Fwd Packets Length Total	Bwd Packets Length Total	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean	
0	6	4	2	0	12	0	6	6	6.00000	
1	6	1	2	0	12	0	6	6	6.00000	
2	6	3	2	0	12	0	6	6	6.00000	
3	6	1	2	0	12	0	6	6	6.00000	
4	6	609	7	4	484	414	233	0	69.14286	1

5 rows × 78 columns

Fig.2 Dataset Collection Table - CIC-IDS 2017

B) Pre-Processing:

Pre-processing deals with preparing the data for modelling in pre-processing stage. This includes cleaning data, visualising relationships between important data, encoding categorical labels and extracting features to ensure good quality data input to the prediction model.

a) Data Processing: Data cleaning and dealing with missing or duplicate values ensures the accuracy and quality of data. First, we remove those rows where there is missing data so that the data is sound. When duplicate records are found, they are removed and there is no redundancy and each record is unique. The data index of the resulting data set is then reset to correct it after these procedures. Lastly, the category columns will be reviewed for further analysis and a few rows of cleaned data will be shown to verify the changes.

b) Data Visualization: There are 2 types of analysis in standard Visualising data. Then, a count plot is used to visualise the distribution of the target variable, which shows the number of samples for each class label of the dataset. This is helpful for comparing the relative or absolute unbalance between categories. Secondly, a heatmap is built to represent the correlation matrix of the data set. The heatmap shows the associations between the different features, with the colour intensity representing the strength of the correlations, which helps in identifying the strongly associated variables.

c) Label Encoding: This is a technique to encode categorical labels into numerical values. In this case the target variable, 'Label' is changed by assigning an integer value to each of the different categories. This is quite useful for the ML models which are standard, as they require numbers as inputs. The unique integer that represents the Post encoding of the label is the next number.The next number is the Post encoding of the label represented. This will make the dataset more suitable for modelling and preserve the integrity of the original categorical data. The labels thus created are then suitable for further analysis or training.

d) Feature Extraction: Feature extraction is the process of recognising and specifying the main variables that are the input to the model. The data is divided into features (X) and target variable (y). All the columns, except the column 'Label' which is the objective. This is a step to ensure that the data set is properly arranged for future steps in the study. The features are extracting useful properties of the network traffic to be used in the detection procedure.

e) Feature Selection: Feature selection process is used to prune the data by selecting the most relevant variables which can improve the performance of model. RFE is used to test and remove less important features, retaining only the most important features. Hence, 10 features were chosen to optimise the predictions: Flow Duration, Total Fwd Packets, Total Length of Fwd Packets, Flow Bytes/s, Flow Packets/s, Fwd Packet Length Mean, Bwd Packet Length Mean, Average Packet Size, Packet Length Std and FIN Flag Count. These attributes are essential to correctly detect and categorise network traffic, which is the key for the model to be efficient and effective.

C) Training &Testing:

During training and testing the dataset is divided into two parts, one part is used for training the model and the other part is used for testing the model. The testing data is used to evaluate performances on unseen data, and the training data is used to train the model with the goal of predicting the target variable. This method aids in assessing the model's ability to generalise, ensuring that it performs well on new and unknown data and preventing overfitting.

D) Algorithms:

XGBoost: To increase prediction accuracy, particularly when working with big datasets and complex interactions. The boosting technique it uses is suitable for classification tasks dealing with high-dimensional data, and it gradually corrects the defects of previous models, achieving better results.

$$y\hat{}_i = \sum_{k=1}^{K} f_k(x_i), f_k \in F$$

LSTM: Long Short-Term Memory is employed for modelling sequential data and to capture long term dependencies. It [9] is very useful, if one can use past observations to make predictions of the future, in such situations. It works fairly well with assignments that have time-series information or sequences, like forecasting.

$$h_t = o_t \odot tanh(c_t)$$

minVGG (1d CNN): This model [12] is adopted to subsample the spatial features from time series data, called minVGG (1d CNN). It is based on 1D convolutions and well suited for classification tasks where the temporal or sequence features are important for the accuracy.

$$y = f(Softmax(FC(Flatten(Conv1D_n \circ ReLU \circ Conv1D_{n-1} \circ \cdots \circ ReLU \circ Conv1D_1(x)))))$$

AlexNet (1d CNN): Convolutions are used in sequential data to get deep features. It [12] helps in extracting complex patterns from input data and achieves better recognition and classification results particularly when the spatial hierarchy of the input data is important.

$$y_i = f(\sum_j x_{i+j} w_j + b)$$

CNN + BiLSTM: This combines the CNN and the BiLSTM layers to extract spatial and temporal information. It [10] is very powerful for applications that require to understand local pattern and sequence context; hence, it can improve the performance of complex data classification.

$$h_t = LSTM(CNN(X), h_{t-1})$$

Voting Classifier (RF + DT): An Ensemble model where the predictions of both Random Forest and Decision Tree classifiers are combined. When the strengths are combined, there is an improvement in accuracy and resiliency, leading to a more accurate and error-resistant final forecast than if they were used individually.

$$y\hat{} = arg\ arg\ max_c \sum_{i=1}^{N} w_i 1(hi(x) = c)$$

4. RESULTS & DISCUSSION

Accuracy: The accuracy of a test is its capacity to appropriately separate the sick and healthy cases. For us to assess how accurate a test is , we have to know the percentage of true positives and true negatives out of all the instances tested . In mathematics terms, it means:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} (1)$$

Precision: Precision is the ratio of the number of instances or samples that are labeled as positives that are correctly classified as positives. Hence the formula of calculating precision is given as:

$$Precision = \frac{True\ Positive}{True\ Positive\ + False\ Positive} (2)$$

Recall: Recall In ML, recall is a measure of how well a model performs at identifying all the instances of a given class. This is the number of observations that were correctly predicted/actual number of observations (Yes). It gives us information about how well a model is able to find examples of a certain class.

$$Recall = \frac{TP}{TP\ +\ FN} (3)$$

F1-Score: In ML, F1 score is a measure of the accuracy of a ML system. It is a mixture of a model's precision and recall. A measure of the number of accurate predictions made by a model over the entire data set is called accuracy metric.

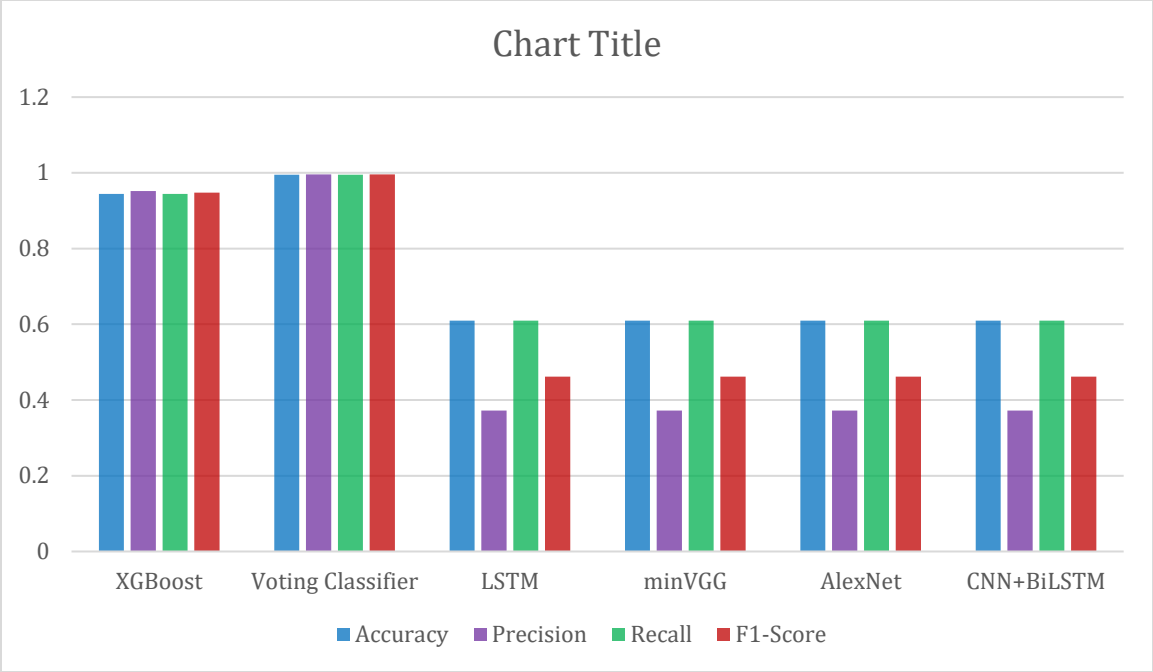
$$F1\ Score = 2 * \frac{Recall\ X\ Precision}{Recall + Precision} * 100(\ SEQ\ "equation"\ \backslash n\ \backslash *\ MERGEFORMAT\ 1)$$

Table(1) shows the performance of each algorithm on accuracy, precision, recall and F1-Score. Voting Classifier achieved at least as good as every algorithm on each of the metrics. The metrics of the other methods are also presented in the tables.

Table.1 Performance Evaluation Metrics

Model	Accuracy	Precision	Recall	F1-Score
XGBoost	0.944	0.952	0.944	0.948
Voting Classifier	**0.995**	**0.996**	**0.995**	**0.996**
LSTM	0.610	0.372	0.610	0.462
minVGG	0.610	0.372	0.610	0.462
AlexNet	0.610	0.372	0.610	0.462
CNN+BiLSTM	0.610	0.372	0.610	0.462

Graph.1 Comparison Graphs



Graph(1) Accuracy in blue, precision in purple, recall in green and F1-Score in red. The Voting Classifier exhibits better performance in all the criteria with the highest scores, compared to the other models. These results are shown in the above graphs.

5. CONCLUSION

In summary, the proposed approach demonstrates the benefits of using advanced feature selection methods and ensemble model to solve the class imbalance issue in network IDS. Ensemble technique utilises the power of several classifiers to greatly boost the detection accuracy. The CIC-IDS 2017 dataset with various network traffic scenarios and attack patterns was used for testing the model. The highest accuracy out of all the tested models was the voting classifier and it was very accurate (99.5%). The result is a high performance that, despite the difficulties arising from a data imbalance, shows how the method recommended here is able to detect intrusions accurately. It is a strong and reliable approach for real-time cyber security applications and can provide possible solutions to the disadvantages of traditional IDS models.

One future research prospect is to further enhance the ensemble model by incorporating more sophisticated algorithms, such as DL algorithms, to achieve higher accuracy and flexibility in detection. Also, real-time data stream analysis can help to adjust an intrusion detection system to new attacks. Further enhancements may involve the integration of additional network traffic characteristics, as well as the investigation of domain-specific optimisations for specific types of attacks to further enhance the model's performance in different network scenarios, leading to greater overall robustness.

REFERENCES

1. R. R. Kumar, A. Tomar, M. Shameem, and M. N. Alam, ‘‘OPTCLOUD: An optimal cloud service selection framework using QoS correlation lens,’’ Comput. Intell. Neurosci., vol. 2022, pp. 1–16, May 2022, doi: 10.1155/2022/2019485.
2. R. R. Kumar, M. Shameem, and C. Kumar, ‘‘A computational frame work for ranking prediction of cloud services under fuzzy environment,’’ Enterprise Inf. Syst., vol. 16, no. 1, pp. 167–187, Jan. 2022, doi: 10.1080/17517575.2021.1889037.
3. M. A. Akbar, M. Shameem, S. Mahmood, A. Alsanad, and A. Gumaei, ‘‘Prioritization based taxonomy of cloud-based outsource software devel opment challenges: Fuzzy AHP analysis,’’ Appl. Soft Comput., vol. 95, Oct. 2020, Art. no. 106557, doi: 10.1016/j.asoc.2020.106557.
4. M.Bakro,S.K.Bisoy,A.K.Patel,andM.A.Naal,‘‘Performanceanalysis of cloud computing encryption algorithms,’’ in Advances in Intelligent Computing and Communication, vol. 202. Cham, Switzerland: Springer, 2021, pp. 357–367.

5. (2030). Cyber Security Market Share, Forecast | Growth Analysis. Accessed: Apr. 23, 2023. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/cyber-securitymarket-101165Benamor
6. S. Lipsa and R. K. Dash, ''A novel dimensionality reduction strategy based on linear regression with a fine-pruned decision tree classifier for detecting DDoS attacks in cloud computing environments,'' in Proc. 1st Int. Symp. Artif. Intell., 2022, pp. 15–25.
7. X. Tan, S. Su, Z. Zuo, X. Guo, and X. Sun, ''Intrusion detection of UAVs based on the deep belief network optimized by PSO,'' Sensors, vol. 19, no. 24, p. 5529, Dec. 2019.
8. Attia, A., Faezipour, M., & Abuzneid, A. (2020, December). Network intrusion detection with XGBoost and deep learning algorithms: an evaluation study. In 2020 international conference on computational science and computational intelligence (CSCI) (pp. 138-143). IEEE.
9. Boukhalfa, A., Abdellaoui, A., Hmina, N., & Chaoui, H. (2020). LSTM deep learning method for network intrusion detection system. International Journal of Electrical and Computer Engineering, 10(3), 3315.
10. P. Sun, P. Liu, Q. Li, C. Liu, X. Lu, R. Hao, and J. Chen, "Dlids: Extracting features using cnn-lstm hybrid network for intrusion detection system," Security and Communication Networks, 2020.
11. R. Panigrahi and S. Borah, "A detailed analysis of CIC IDS 2017 dataset for designing intrusion detection systems," International Journal of Engineering & Technology, vol. 7, no. 3.24, pp. 479–482, 2018.
12. Zhang, X., Chen, J., Zhou, Y., Han, L., & Lin, J. (2019). A multiple-layer representation learning model for network-based attack detection. IEEE Access, 7, 91992-92008.
13. H. Bangui and B. Buhnova, ''Recent advances in machine-learning driven intrusion detection in transportation: Survey,'' Proc. Comput. Sci., vol. 184, pp. 877–886, Aug. 2021.
14. Z.Chen, N.Lyu, K.Chen, Y.Zhang, and, W.Gao, ''UAV network intrusion detection method based on spatio-temporal graph convolutional network,'' J. Beijing Univ. Aeronaut. Astronaut., vol. 47, no. 5, pp. 1068–1076, 2021.
15. E. Basan, M. Lapina, N. Mudruk, and E. Abramov, ''Intelligent intrusion detection system for a groupofUAVs,''inProc.12thInt.Conf.Adv.Swarm Intell., 2021, pp. 230–240.
16. V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea, S. Y. Alyahyan, and M. A. Raza, ''Optimal deep reinforcement learning for intrusion detection in UAVs,'' Comput., Mater. Continua, vol. 70, no. 2, pp. 2639–2653, 2022.
17. J. Whelan, A. Almehmadi, and K. El-Khatib, ''Artificial intelligence for intrusion detection systems in unmanned aerial vehicles,'' Comput. Electr. Eng., vol. 99, Apr. 2022, Art. no. 107784.
18. Q. Abu Al-Haija and A. Al Badawi, ''High-performance intrusion detection system for networked UAVs via deep learning,'' Neural Comput.Appl., vol. 34, no. 13, pp. 10885–10900, Jul. 2022.
19. R.Fotohi, M. Abdan,andS.Ghasemi,''A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks,'' J. Grid Comput., vol. 20, no. 3, p. 22, Sep. 2022.
20. X. He, Q. Chen, L. Tang, W. Wang, and T. Liu, ''CGAN-based collaborative intrusion detection for UAV networks: A blockchain-empowered distributed federated learning approach,'' IEEE Internet Things J., vol. 10, no. 1, pp. 120–132, Jan. 2023.