Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

ANRAD: Adaptive Network Risk and Anomaly Detection for Risk-Based Network Breach Identification

Ravi N, Kanishk Raja V G, Ajith Kumaran S, Naveen S S, Karthik M, Sarathi L

Department of Information Technology, PSG Polytechnic College Coimbatore, Tamil Nadu, India

Abstract: Because network traffic is constantly growing, it can be difficult to identify unusual and possibly harmful activity. In this research, a risk-oriented system called ANRAD (Adaptive Network Risk and Anomaly Detection) is proposed. It integrates anomaly detection based on Isolation Forest, network vulnerability indicators, and traffic deviation. In order to categorize network behavior into various risk levels, these elements are combined to provide a Security Risk Score. The framework obtains an accuracy of 83.34%, precision of 77.92%, recall of 43.63%, and F1-score of 55.94% when tested on the CICIDS2017 dataset. The findings demonstrate that while attack-family analysis identifies regions in need of more development, combining several network-behavior indicators offers a cohesive strategy for network risk assessment.

Keywords - Network Security, Intrusion Detection, Anomaly Detection, Isolation Forest, Risk Assessment, CICIDS2017, Network Traffic Analysis.

I. INTRODUCTION

Effective network security monitoring has become more crucial due to the quick growth of computer networks, cloud services, Internet-connected technologies, and digital infrastructure. Large amounts of diverse traffic are constantly produced by modern networks, making it challenging to manually spot unusual activity and any security concerns. As a result, intrusion detection systems, or IDSs, are frequently employed to keep an eye on network activity and spot traffic patterns linked to suspicious or malicious activities.

Conventional intrusion detection systems mostly use signature-based methods, which match network activity to previously recognized attack patterns. Their reliance on predetermined signatures may restrict their capacity to identify novel or altered attack behaviors, notwithstanding their effectiveness for recognized threats. Because machine-learning-based intrusion detection techniques may find connections between network features and security incidents and learn traffic patterns from past data, they have drawn a lot of interest.

Supervised machine-learning techniques can deliver strong classification results when there is an adequate amount of labeled training data. Nevertheless, their success relies heavily on the quality and representativeness of that training data. A model that is trained on particular types of attacks might not perform as effectively when faced with different traffic patterns or new, unseen attack methods. This highlights the necessity for methods that can detect anomalies in typical network behavior without relying solely on predefined attack signatures.

Anomaly-based detection tackles this issue by modeling typical network behavior and pinpointing observations that significantly deviate from the defined baseline. Among unsupervised techniques for anomaly detection, Isolation Forest has been extensively researched due to its ability to pinpoint anomalous observations through random partitioning and its general efficacy in isolating atypical observations with fewer partitioning steps. However, an anomaly score by itself may not accurately reflect the operational risk associated with a network flow. A statistically unusual flow does not necessarily equate to a security threat, while certain network characteristics may offer additional insights into suspicious behavior.

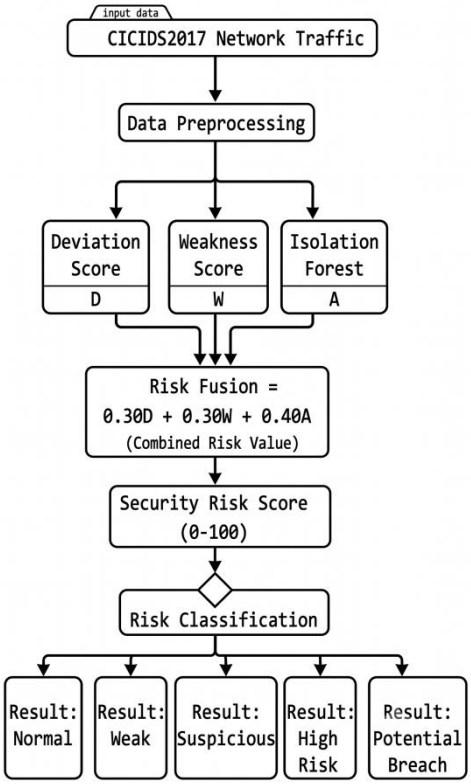
To overcome this limitation, this study introduces ANRAD (Adaptive Network Risk and Anomaly Detection), a risk-focused framework that integrates three supporting types of evidence: divergence from typical network activity, characteristics of network vulnerabilities, and anomaly detection. These elements are combined to produce an ongoing Security Risk Score (SRS) instead of depending solely on a binary classification of benign or malicious. The

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

conceptual architecture of the suggested framework is shown in

Fig. 1 — Proposed ANRAD Conceptual Architecture.



The CICIDS2017 dataset has been used to evaluate the proposed framework where it contains various attacking categories and benign traffic where it also includes denial of service, distribution of denial of service, brutal force, web attacks, botnet, infiltration, Heartbleed traffic and port scanning. The Canadian Institute for Cybersecurity developed this dataset to use this as a benchmark for the research related to detection of intrusion.

This research was done mainly to find out whether the combination of network weakness indicators, anomaly detection without supervision will be able to give an useful risk related representation of the network traffic. The study also further finds out ANRAD against an Isolation Forest baseline and determines the performance in various attack families.

II. LITERATURE REVIEW

The evolution of the Detection system for intrusion started from the traditional signature based techniques to anomaly based and machine learning approaches. The signature based detection systems are very useful for the known attacks with only limited capacity against the modified threats or the unnoticed ones. This limitation is well addressed by the machine learning techniques utilizing the various patterns from the network traffic.

Supervised learning methods such as Decision Trees, Random Forest, and Support Vector Machines have demonstrated high detection performance when labelled attack data are available. However, their performance depends strongly on the quality and diversity of the training dataset. This limits their ability to generalize to new attack patterns.

The learning methods with supervision such as Support Vector Machines, Random Forest, Decision Trees, have shown a very high performance in detection with the help of the labeled attack data. However, the diversity and quality of the training dataset plays a major role on their performance. So the ability of creating new attack methods is limited due to this.

Unsupervised anomaly-detection methods provide an alternative by modelling normal traffic and identifying significant deviations. Isolation Forest, introduced by Liu et al. [2], detects anomalies by recursively partitioning observations and isolating unusual samples with fewer splits. It has therefore been widely applied to network anomaly detection. The CICIDS2017 dataset introduced by Sharafaldinet al. [1] provides benign and diverse attack traffic and has been widely used for evaluating intrusion-detection methods. However, many existing approaches focus primarily on classifying traffic as benign or malicious rather than representing the degree of security risk associated with individual network flows.

Based on this gap, ANRAD combines statistical deviation, network weakness indicators, and Isolation Forest anomaly detection to produce a continuous Security Risk Score. This provides a risk-oriented representation that complements conventional binary intrusion classification. The CICIDS2017 dataset was selected for evaluating the proposed framework because it contains both benign traffic and multiple attack scenarios. According to the dataset description, normal traffic was generated on Monday, while different attack scenarios were conducted during the subsequent days [1]. The dataset contains flow-level network features generated using CICFlowMeter.

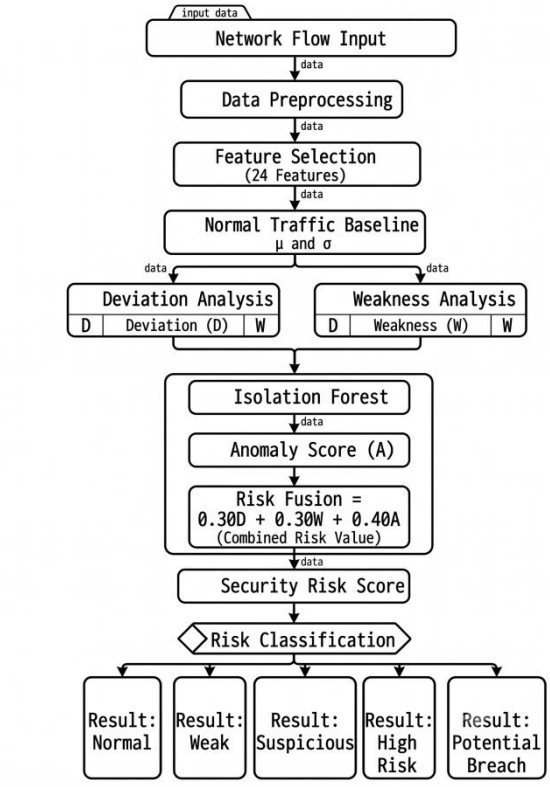
III. PROPOSED METHODOLOGY

The proposed ANRAD framework is designed to analyse network-flow records and transform multiple behavioural indicators into a unified Security Risk Score. The methodology consists of data preprocessing,normal-baseline construction, deviation analysis, weakness analysis, anomaly detection, risk fusion, and risk classification. The overall processing sequence of the framework is presented in **Fig. 2.**

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

Fig. 2 - ANRAD Processing Methodology.



A. Dataset and Data Preparation

The CICIDS2017 dataset was selected for evaluating the proposed framework because it contains both benign traffic and multiple attack scenarios. According to the dataset description, normal traffic was generated on Monday, while different attack scenarios were conducted during the subsequent days [1]. The dataset contains flow-level network features generated using CICFlowMeter.

There are about eight CSV files in the Machine Learning CSV collection that has been utilized in this research relating to various traffic periods. These files are having benign traffic and also Bot, PortScan, brute-force, DoS, infiltration, web attack, and Heartbleed traffic. The pattern of distribution of the traffic utilized in this study is given in the **Table II.**

Table II. Distribution of CICIDS2017 Traffic Used in the Study

Traffic Type	Records
Benign	22,73,097
Attack	5,57,646
Total	**28,30,743**

During the stage of preprocessing there was involvement of removal of unnecessary whitespaces, loading of records of the network flow, selection of the relevant attributes of network flow, invalid numerical values handling etc. Before further processing, the missing and infinite values were removed. About 24 features of network flow were chosen for the analysis of ANRAD. There was representation of packet stats, direction of traffic, TCP flags, flow characteristics, information of window, and characteristics of activity. The features selected are summarized in **Table III.**

Table III. Selected Network-Flow Features

Category	Features
Flow	Duration, Bytes/s, Packets/s
Packets	Fwd/Bwd Packets, Packet Length
Timing	Flow IAT Mean, Flow IAT Std
Flags	SYN, RST, ACK
Direction	Down/Up Ratio
TCP	Initial Window Sizes
Activity	Active Mean, Idle Mean

B. Normal Traffic Baseline

To determine the significance of how a network flow differs from the expected network behavior a normal traffic baseline is required. For a normal reference, the traffic data from CICIDS2017 on Monday was used since it has benign traffic with no attack circumstances present on the subsequent days [1].

There are about 529,918 records originally present in the Monday dataset. About 529,481 records were retained for the baseline construction after the removal of records having numerical values that were invalid. The mean and standard deviation for every selected feature were obtained from the cleaned normal traffic.

For a feature i, the mean is calculated as

$$\mu_i = \frac{1}{N}\sum_{j=1}^{N} x_{ji}$$

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

and its standard deviation is calculated as

$$\sigma_i = \sqrt{\frac{1}{N}\sum_{j=1}^{N}(x_{ji} - \mu_i)^2}.$$

The corresponding network feature's expected behaviour are demonstrated from this statistical parameters and are subsequently utilized by the deviation component of ANRAD.

C. Deviation Score

The difference between a normal baseline and its corresponding observed network flow feature is represented by the Deviation Score. The standardized absolute deviation for each selected feature is calculated as

$$d_i = \frac{|\, x_i - \mu_i \,|}{\sigma_i + \epsilon},$$

Where μ_i denotes the normal mean, $x_i$denotes the observed feature value, $\epsilon$is a small constant introduced to prevent division by zero and σ_i denotes the normal standard deviation.

The individual feature deviations are aggregated and normalized to produce the overall Deviation Score D, where

$$0 \leq D \leq 1.$$

A higher value of Dindicates greater deviation from the established normal traffic profile.

D. Weakness Score

The network characteristics indicating abnormal communication behaviour is represented through the Weakness Score. The weakness component focuses on selected characteristics of network communication whereas the deviation component measures the statistical distance from the normal baseline.

The weakness indicators that were implemented include, downstream-to-upstream traffic relationships, forward and backward packet-related imbalance, RST behaviour, and TCP SYN. The combination of these indicators were normalized and so obtained a Weakness Score W, where

$$0 \leq W \leq 1.$$

An additional evidence is provided by the Weakness Score which can be combined with the deviation and anomaly components. It does not independently define a flow as malicious.

E. Anomaly Score

Using the Isolation Forest, a third component of ANRAD- an unsupervised anomaly score is generated. Using split values and randomly selected features the Isolation Forest operates by repeatedly partitioning the observations. The isolation of anomalous observations generally happens with fewer partitions because they differ from the majority of observations [2], [3].

The Isolation Forest output is transformed into a normalized Anomaly Score A, where

$$0 \leq A \leq 1.$$

A larger value of Arepresents stronger evidence that the corresponding network flow exhibits anomalous characteristics.

F. Risk Fusion

With regards to the behaviour of the network flow, various forms of evidence is provided by the three components. The selected network behaviour characteristics are represented by the Weakness Score, the statistics difference from a normal behaviour is denoted by the Deviation Score, and the output of the unsupervised anomaly detector is denoted by the Anomaly Score.

The following weighted risk-fusion equation combines these components:

$$R = 0.30D + 0.30W + 0.40A$$

A weight of 0.40 is assigned to the anomaly component and the weakness and deviation components are assigned 0.30 weights each respectively. The resulting risk value is converted into a Security Risk Score using

$$SRS = 100R$$

Thus, the final score lies between 0 and 100. The score is subsequently mapped into risk categories to provide an interpretable representation of the detected network condition. The classification ranges are presented in **Table IV**.

Table IV. Security Risk Score Classification

SRS	Risk Level
0–24	Normal
25–49	Weak
50–69	Suspicious
70–84	High Risk
85–100	Potential Breach

G. ANRAD Detection Procedure

Before calculating the three ANRAD components the whole processing sequence begins with a network-flow record and applies the selected preprocessing operations. The resulting values are combined using the proposed risk

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

equation, and the final score is mapped to its corresponding risk category.

The complete algorithm is presented as **Algorithm 1**.

Algorithm 1: ANRAD Risk Detection Procedure

Input:

Network flow X
Normal baseline parameters μ and σ
Trained Isolation Forest model

Output:

Security Risk Score SRS
Risk category

1. Preprocess the input network flow.
2. Select the required network-flow features.
3. Calculate deviation from the normal baseline.
4. Aggregate and normalize the deviation to obtain D.
5. Calculate network weakness indicators.
6. Normalize the weakness indicators to obtain W.
7. Apply Isolation Forest and obtain A.
8. Calculate R = 0.30D + 0.30W + 0.40A.
9. Calculate SRS = 100R.
10. Assign the corresponding risk category.
11. Return SRS and risk category.

IV. RESULTS AND DISCUSSION

A. Experimental Evaluation

The prepared CICIDS2017 traffic data was used to evaluate the proposed ANRAD framework. The evaluation considered accuracy, precision, recall, F1-score, specificity, false-positive rate, and receiver operating characteristic area under the curve (ROC-AUC).

To examine whether the integration of deviation and weakness information provided additional value beyond the anomaly detector, an Isolation Forest-only configuration was also evaluated as a baseline.

The resulting performance of ANRAD is presented in **Table V**.

Table V. Overall Performance of ANRAD

Metric	ANRAD
Accuracy	**83.34%**
Precision	**77.92%**
Recall	**43.63%**
F1-Score	**55.94%**
Specificity	**96.04%**
False Positive Rate	**3.96%**
ROC-AUC	**0.7688**

An accuracy of **83.34%** and a precision of **77.92%** was achieved from the proposed framework. The framework correctly identified a large proportion of benign traffic under the evaluated configuration which is proved by the specificity of **96.04%**. About **3.96%** is the false-positive rate.

The current configuration did not detect all attack traffic and it is indicated through the recall value which is **43.63%.** Consequently, the results should be interpreted as evidence of the behaviour of the proposed risk framework under the selected experimental configuration rather than as evidence of complete intrusion detection.

B. Comparison With Isolation Forest

The performance comparison between the Isolation Forest baseline and the complete ANRAD framework is presented in **Table VI**.

Table VI. Comparison Between Isolation Forest and ANRAD

Metric	Isolation Forest	ANRAD
Accuracy	82.45%	**83.34%**
Precision	73.39%	**77.92%**
Recall	43.30%	**43.63%**
F1-Score	54.47%	**55.94%**
Specificity	94.98%	**96.04%**
ROC-AUC	0.7609	**0.7688**

After incorporating the additional ANRAD components the results showed some minimal changes. There was an increase in accuracy from **82.45%** for the Isolation Forest configuration to **83.34%** for ANRAD, while precision increased from **73.39%** to **77.92%**. The F1-score also increased from **54.47%** to **55.94%**.

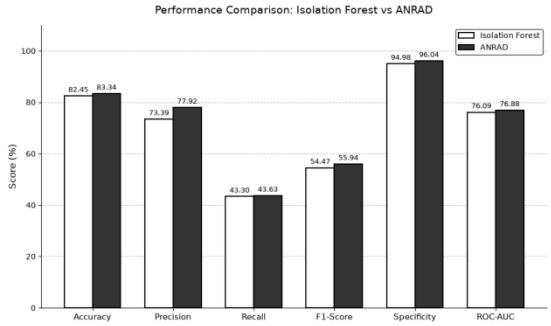
The difference in recall was comparatively small, increasing from **43.30% to 43.65%.** There was an indication that the additional components did not substantially increase the number of detected attack records in the evaluated configuration. Nevertheless, the combined framework provides a broader representation of network behaviour by incorporating statistical deviation and weakness characteristics along with the anomaly score.

The quantitative comparison will be visually represented in **Fig. 3**, which will contain the performance metrics of the two configurations.

Fig. 3. Performance comparison between Isolation Forest and ANRAD.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026



C. Attack-Family Evaluation

The detection results were analysed across different attack families for further examination of the behaviour of ANRAD. The resulting performance is presented in **Table VII**.

Table VII. Attack-Family Evaluation of ANRAD

Attack Family	Recall	F1-Score
DDoS	63.66%	76.61%
PortScan	0.18%	0.35%
Web Attacks	0.73%	0.93%
Infiltration	61.11%	3.33%

The performance of ANRAD was not uniform across all attack families which was demonstrated through the results produced. The F1-score of 76.61% and recall score of 63.66% caused by the DDoS traffic indicated stronger detection for this pattern of traffic upon comparison.

In contrast, a substantially lower recall and F1-score values was produced by the PortScan and Web Attack traffic. This shows that the risk-fusion configuration and selected features may not adequately represent the characteristics of these attack families.

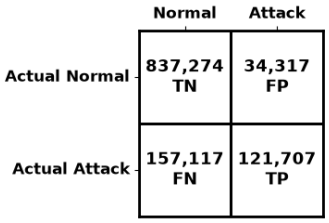
The importance of evaluating multiple metrics simultaneously is demonstrated by the infiltration results. Although the recall reached 61.11%, the F1-score was only 3.33%, indicating a substantial precision limitation for this attack family.

There is an indication from the results that before ANRAD could be considered suitable for uniform detection across different attack categories, a further investigation of thresholds, attack-specific features, and temporal characteristics is required.

D. Confusion Matrix Analysis

The confusion matrix provides a direct representation of the true-positive, true-negative, false-positive, and false-negative classifications produced by the final ANRAD configuration. The final confusion matrix will be presented in **Fig. 4**.

Fig. 4. Confusion matrix of the final ANRAD evaluation.



E. Ablation Analysis

To investigate the contribution of the individual components of ANRAD, an ablation analysis is used. The analysis considers configurations based on Deviation, Weakness, and Anomaly components individually and in combination.

The complete configuration is represented by

D+W+A

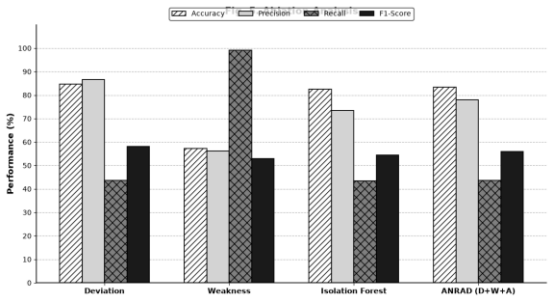
The ablation results are presented in **Table VIII**.

Table VIII. Ablation Analysis of ANRAD Components

Configuration	Threshold	Accuracy	Precision	Recall	F1-Score
Deviation	1	84.71%	86.62 %	43.67 %	58.06%
Weakness	0.3	57.19%	56.06 %	99.12 %	52.89%
Isolation Forest	0.75	82.45%	73.39 %	43.30 %	54.47%
ANRAD (D+W+A)	**70**	**83.34 %**	**77.92 %**	**43.63 %**	**55.94%**

The corresponding component-wise comparison will be illustrated in **Fig. 5**.

Fig. 5. Ablation analysis of the ANRAD components.



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

V. FUTURE WORK

For future development of the proposed framework, there are several directions provided from the current results. The incorporation of temporal behaviour into the risk-assessment process is one important direction. Network attacks frequently generate sequences of related flows rather than isolated observations. Additional information for incident-level assessment can be obtained by Incorporating temporal persistence and repeated risk observations.

Adaptive optimization of the weights used in the risk-fusion equation in another direction. The current implementation uses fixed weights of 0.30, 0.30, and 0.40 for deviation, weakness, and anomaly components, respectively. Data-driven or validation-based methods for selecting these weights can be utilized for future work.

There is a need for improved feature representations which is indicated by the attack-family results. A substantially lower detection performance than DDoS traffic is noted in the PortScan and Web Attack traffic. To improve sensitivity to these traffic patterns, future studies can investigate additional flow features and attack-specific characteristics.

An another important direction is Cross-dataset evaluation. For evaluating the generalization of the proposed framework beyond CICIDS2017, testing ANRAD on additional intrusion-detection datasets should be strongly considered.

Finally, ANRAD can be extended into a real-time network monitoring system in which incoming network flows are continuously processed and assigned risk scores. An explainable output layer could also categorize the major factors contributing to a particular risk score, enabling security analysts to better understand why a flow was classified as suspicious or high risk.

VI. CONCLUSION

This paper presented ANRAD, a risk-oriented network anomaly-detection framework that combines statistical deviation, network weakness indicators, and unsupervised anomaly detection. By Combining the Deviation Score, Weakness Score, and Isolation Forest Anomaly Score using a weighted fusion mechanism the framework generates a Security Risk Score.

The proposed framework was evaluated using the CICIDS2017 dataset and achieved an accuracy of 83.36%, precision of 78.01%, recall of 43.65%, F1-score of 55.98%, specificity of 96.06%, and ROC-AUC of 0.7692. Comparison with an Isolation Forest baseline showed modest improvements in several aggregate performance measures.

Considerable variation in detection performance was noted in the attack family analysis. DDoS traffic, in particular, produced substantially stronger results than Web Attack traffic and PortScan. These findings demonstrate that the current ANRAD configuration should be noted as a risk-oriented anomaly-detection framework instead of a universal replacement for attack-specific or supervised intrusion-detection models.

Overall, the results demonstrate the feasibility of combining multiple behavioural indicators into a unified network-risk representation. The involvement of temporal analysis, adaptive weight optimization, improved attack-specific features, and evaluation on additional datasets will be helpful in strengthening the framework and give a more comprehensive assessment of its generalization capability.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to **PSG Polytechnic College, Coimbatore**, for providing the academic environment and facilities required to carry out this research work. The authors also thank the faculty guide, **Mr. N. Ravi,** for their guidance and support during the development and testing of ANRAD and evaluation of the proposed framework.

The authors acknowledge the **Canadian Institute for Cybersecurity, University of New Brunswick**, for providing the CICIDS2017 dataset used in this research.

REFERENCES

[1] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in *Proc. 4th Int. Conf. Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108–116.

[2] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation Forest,” in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, 2008, pp. 413–422.

[3] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation-Based Anomaly Detection,” *ACM Trans. Knowledge Discovery from Data*, vol. 6, no. 1, pp. 1–39, 2012.

[4] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward a Reliable Intrusion Detection Benchmark Dataset,” *Software Networking*, vol. 2017, no. 1, pp. 177–200, 2017.

[5] F. Pedregosa *et al.*, “Scikit-learn: Machine Learning in Python,” *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[6] G. Engelen, V. Rimmer, and W. Joosen, “Troubleshooting an Intrusion Detection Dataset: The CICIDS2017 Case Study,” in *Proc. IEEE Security and Privacy Workshops (SPW)*, 2021

(This work is licensed under a Creative Commons Attribution 4.0 International License.)