

An enhanced classification framework for intrusions detection system using intelligent exoplanet atmospheric retrieval algorithm

Slamet^{1,2}, Izzeldin Ibrahim Mohamed Abdelaziz²

¹Department of Information System, Faculty of Technology and Informatics, Universitas Dinamika, Surabaya, Indonesia

²Faculty of Electrical and Electronics Engineering, Universiti Malaysia Pahang, Pahang, Malaysia

Article Info

Article history:

Received Oct 29, 2021

Revised Jan 12, 2022

Accepted Mar 2, 2022

Keywords:

Classification

False alert

INARA

Intrusion

ABSTRACT

Currently, many companies use data mining for various implementations. One form of implementation is intrusion detection system (IDS). In IDS, the main problem for nuisance network administrators in detecting attacks is false alerts. Regardless of the methods implemented by this system, eliminating false alerts is still a huge problem. To describe data traffic passing through the network, a database of the network security layer (NSL) knowledge discovery in database (KDD) dataset is used. The massive traffic of data sent over the network contains excessive and duplicated amounts of information. This causes the classifier to be biased, reduce classification accuracy, and increase false alert. To that end, we proposed a model that significantly improve the accuracy of the intrusion detection system by eliminating false alerts, whether they are false negative or false positive negative alerts. The results show that the proposed intelligent exoplanet atmospheric retrieval (INARA) algorithm has improved accuracy and is able to detect new attack types efficiently.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Slamet

Department of Information System, Faculty of Technology and Informatics, Universitas Dinamika

Jl. Kedung Baruk 98 Surabaya, 60298, Indonesia

Email: slamet@dinamika.ac.id

1. INTRODUCTION

Human life today is inseparable from the important role of information and communication technology. The use of the internet and computer networks is increasing rapidly because of the human need to obtain information and to keep businesses running. In terms of technology, especially related to security technology, it also has a history of technological development. Starting with passive security defense systems such as firewalls, which later developed into active security defense systems such as intrusion detection technology. Attacks often occur quickly and are almost difficult to recognize in large data traffic on the network. Most of today's products of network security are manually operated by security experts. This operation causes unknown attacks not only difficult to detect, but the detection rate and timeliness is also a big problem.

In this regard, realizing the adaptive operation of the intrusion detection system (IDS) becomes an urgent and necessary need by combining data mining and intelligence technology. This intrusion detection classifies normal events and abnormal events massively from the data in the network so that the type of attack can be found. For this reason, most researchers examine their IDS systems to improve the IDS accuracy and reduce false warning.

In general, intrusion detection technology is distributed in two types: anomaly detection and misuse detection [1]. Misuse detection or signature detection aims to determine the intrusion pattern by known attacks and completing the detection task by assessing the pattern of intrusion. The disadvantage of misuse detection is detect only known attacks in advance. Misuse detections have false alerts when the normal packet pattern matches the attack pattern or signature [2]. The challenge in implementing this IDS is difficult to distinguish normal and abnormal traffic or precised to the existing range of detection knowledge and failed to detect attacks outside of existing knowledge.

The second type of IDS is anomaly detection. This detection does not refer to specific behavior such as detection criteria but refers to the using of resources or user behavior in determining whether they have been attacked. Anomaly detection implementations are relatively robust and successfully detect extraneous attacks, and are not limited by known attack modes. The common weakness of this IDS is rating of false detection, particularly in a multi-user environment. This is also due to the structure of network, parameters of system, changing of working conditions, and other elements of this detection system.

2. RELATED WORKS

Currently, there has been a lot of research models on effective intrusion detection classification. As the following examples, in [3], a hybrid intrusion detection system that combines anomaly and misuse detection is proposed. Some intrusion detection system have applied other learning algorithms, such as genetic algorithms, artificial neural networks, and support vector machines (SVM) [4]–[7]. Research by Ali [8] the honeybee framework used to increase IDS detection rate by an overall rate of 99.1%. Research by Dhakar and Tiwari [9] a hybrid intrusion detection system achieved an accuracy of 99.96%. Chen *et al.* [10] presented a graphical feature generation approach and achieved an accuracy of 98.54%. Shawe and Abbas [11] introduced a standard for increasing accuracy using singular value decomposition (SVD) enhancement by reducing data, and the classification algorithms used is back propagation neural network (BPNN) with an accuracy of 94,34%. Studies in [12]–[17] have higher detection rates and false alarm rates, also integrated of classification and clustering reached better results. In [18] and [19], analysis of fuzzy cluster is used to classify data and achieved better results. In [20]–[22] uses neighborhood algorithms for classification. The literature by Ibrahim and Ouaddane [23] uses the data dimension reduction method to analyze data features.

3. METHODOLOGY

False alerts in intrusion detection and lowering IDS detection rates are a challenge for network administrators. The main objective is to minimize the warning level caused by classification bias. This bias is caused by duplicated or redundant instances and differences in attacks distribution across classes in the data set. To that end, we introduce an enhanced model to reduce false warning rates and increase classification accuracy using intelligent exoplanet atmospheric retrieval (INARA) algorithm. INARA algorithm is a meta learning technique designed to improve the classification performance of J-48 [1].

The proposed model is carried out in five steps. Firstly, is the preprocessing step. Output of this step is pre-processed data. The second step is to clean data from duplicate data. Output of this phase is a removed set of duplicated data set. The third step is the classification process used to compare the performance of the most popular classification algorithms in machine learning. The fourth step enhances the best classifier from third stage using INARA algorithm. The fifth step is the evaluation stage. We implemented the enhanced classifier from the fourth step to the pre-processed data set and clean data sets [24]. The structure model of this research is shown in Figure 1. We used RapidMiner tools in conducting our experiments. The input data set is the network security layer (NSL) knowledge discovery in database (KDD) (494021 instances and 23 classes (22 attacks and normal)).

3.1. Pre-processing stage (data preparation)

Some of the work carried out at this stage is: i) implemented a numeric filter to a nominal attribute in an attribute with a symbolic value, ii) implemented rename face value filter, iii) implemented remove unused class value filters.

3.2. Cleaning data stage

In cleaning up redundant instance data, a duplicate removal filter is implemented. The rename face value filter has been applied to non-duplicated data sets, further removing obsolete class value filters. The result of this step is a clean data set.

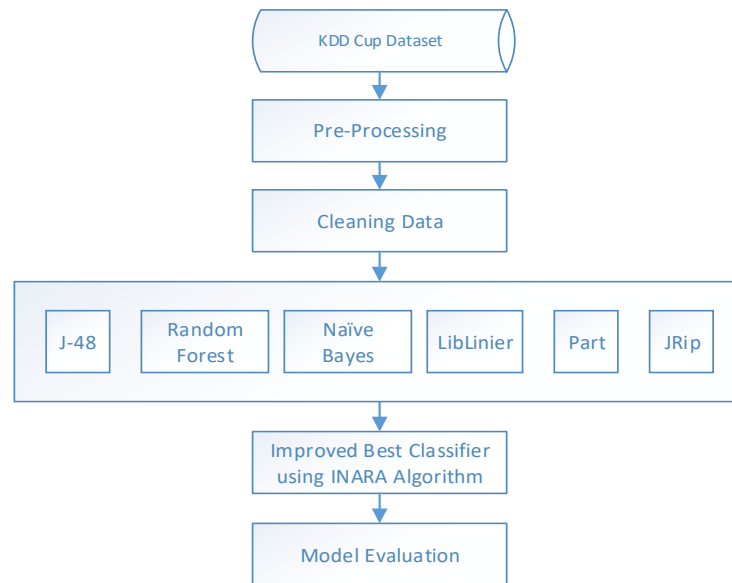


Figure 1. Model structure

3.3. Classification stage

In this stage, it has been implemented some of the most famous classification algorithms, including tree algorithms (J-48 and random forest), Bayes algorithms (Naive Bayes), functions (liblinear), and rule algorithms (part and Jrip). All these algorithms performed multilevel 10-fold cross-validation. In this last stage, selected the best classifier with the lowest false warning and highest accuracy after comparing accuracy of all classifiers.

3.4. Improved best classifier stage

To enhance the best classifier, INARA algorithm is used. The result is an improved classifier. This classifier is used to classify the data being tested.

3.5. Evaluation stage

In this phase, pre-processing stage data is used as input data. The improved classifier from the previous step were applied to examine the data. Evaluated the performance of the improved classifier on the tested data, regarding the results for each class of false positive warning and false negative warnings. It also relates to overall accuracy and false alert rates.

3.6. Performance measurement

General criteria for evaluating the efficiency model are accuracy, precision, false positive rate, true positive rate, and overall, of false warning. The evaluation parameters are shown in Table 1.

Table 1. Confusion matrix evaluation

Actual class	Classified class	
	Normal	Attack
Normal	TN	FP
Attack	FN	TP

Where: True positive (TP): means attack instances are classified as attacks.

True negative (TN): means normal instances classified as normal.

False positive (FP): means normal instances classified as attacks.

False negative (FN): means attack instances classified as normal.

Referring to those terms, true positive rate (TPR) is used to describe the correct number of instances classified to the right class.

4. RESULTS AND DISCUSSION

4.1. Pre-processing stage (data preparation)

The input used consists of 494021 instances and 23 classes consist of 3 nominal features and 38 numeric features. The data set is taken from NSL KDD data set. This first data set consists of preprocessing data with 23 classes and the second data set consists of 5 classes from the tested data. Output of this stage is two datasets of 494021 instances consist of 7 nominal features and 34 numeric features.

4.2. Elimination duplication stage

Input in this stage is data from pre-processing step. All duplicate instances were removed so that the data set was reduced to 70% and obtained a proper data set of 145586 instances which were spreaded into 5 classes, see Table 2.

Table 2. Distribution of instances in the clean data set

Normal	DOS	U2R	R2L	Probe	Total
87832	54572	52	999	2131	145586

4.3. Classification stage

Clean data from the previous stage is classified using the best classifier in all classifiers environment. The results are shown in Figure 2, where accuracy of J-48 classifier achieved 99.80%, random forest 99.50%, part 95.50%, Jrip 99.70%, liblinear 97.48%, and Naïve Bayes 90,78%. Meanwhile, the false alarms from J-48 classifier were 0.07%, random forest 0.08%, part 0.12%, Jrip 0.09%, liblinear 0.10%, and Naïve Bayes at 0.15%, as shown in Figure 2.

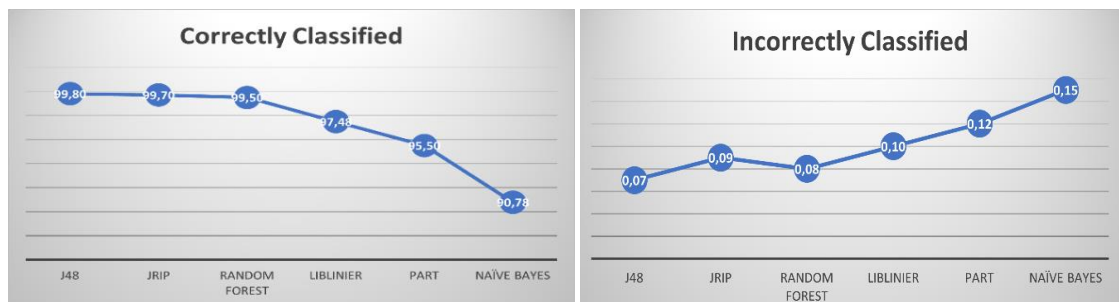


Figure 2. Accuracy of classifier false alert percentage on classification stage

4.4. Enhanced best classifier stage

In this stage, we used INARA Algorithm (the meta learning algorithm by the multi-class classifier to increase J-48). In the experiment conducted, the accuracy was 99.96% and the false alarm rate was 0.05% which was better than the J-48, see Figure 3.

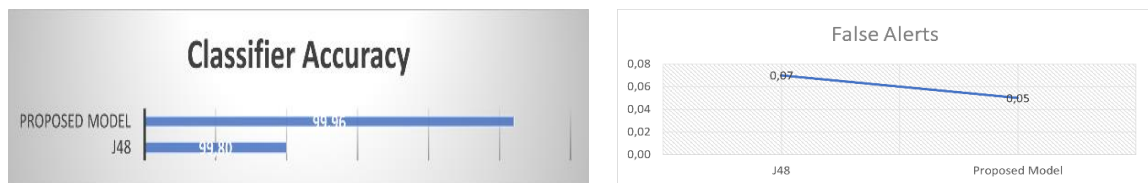


Figure 3. Accuracy and false alert comparison for J-48 and proposed model

4.5. Evaluation stage

In the evaluation stage, we implemented an improved classifier by integrating multi class classifier and J-48. This improved classifier examined data set from: pre-processing stage, remove duplication stage, and the origin data set. The 10-fold cross-validation test method is used to provide more accurate results than

the data split method, where the number of false alerts and the tested data has changed along with the change in the ratio of the separated data.

The proposed model achieved an improved detection rates for all classes, the lowest false alarm rate of 0.01% and the highest accuracy of 99.99% which is better than other models discussed. We surveyed various models used to improve IDS performance. Khraisat *et al.* [25] used an adjusted dataset in a smaller number of instances, but its model has a high false positive warning. Research by Siamese [12] models achieve the best accuracy using split mode to test the data. So, we compared the proposed model with the Siamese model using a 10-fold cross-validation for more accuracy.

The proposed model achieved the lowest false warning and the best detection rate for all classes on the test data set from the preprocessing stage. While the overall accuracy is 99.99% and false warnings are 0.01%, see Figure 5.

We tested the model on clean data from the pre-processing phase and removed duplicates. The test results show that the proposed model achieved lower false alerts and better accuracy in all classes, see Figure 4. The overall accuracy is 99.95% and false alerts are 0.05%, while the accuracy of Siamese is 99.88% and false warning of 0.12%.

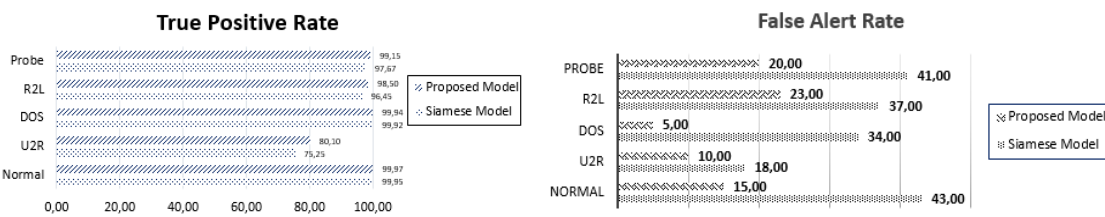


Figure 4. True positive and false alert rate (all class) on clean data

Figure 5 shows that proposed model reduces false warning and increases the rating of detection for the normal class and the DOS class. In addition, it increases the detection rate of other models from 60% to 77% of the U2R class has the lowest illustration of data set. Additionally, it increases the R2L class and probe class despite lower instance counts in each class in the original data set. The proposed model reduces false warning and improved accuracy of detection for normal classes shown in Figure 6. See Figure 7 for the DOS category which has six styles of attacks (smurf, land, pod, teardrop back, and neptune).

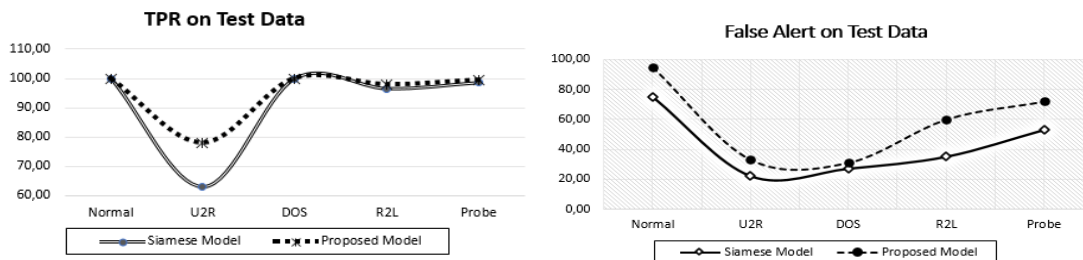


Figure 5. True positive and false alert rate on test data

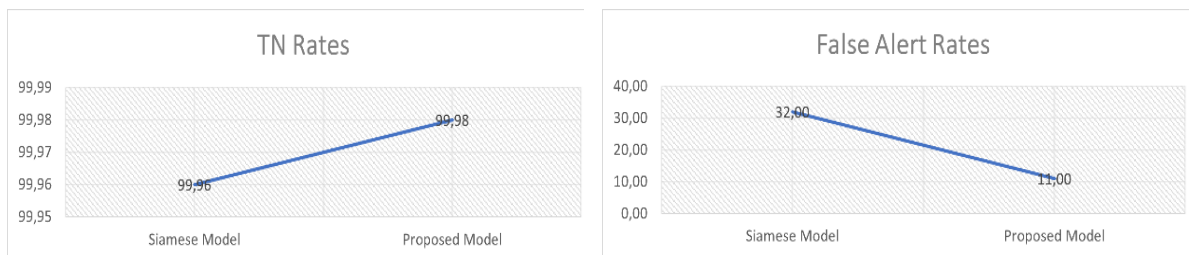


Figure 6. True negative and false alert rate for 10% KDD cup

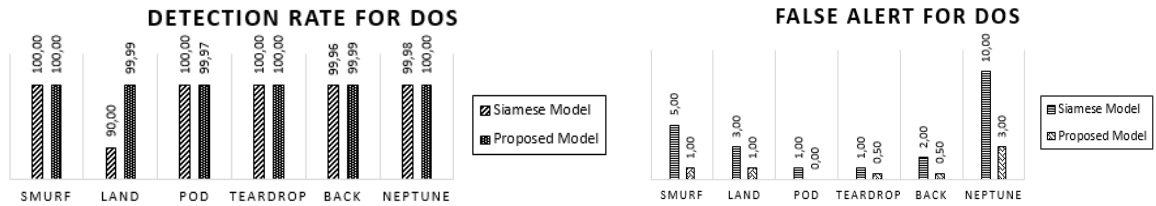


Figure 7. Detection rate and false alert for DOS category

The data set of the DOS category has the highest representation and good training for its attacks, so most classifiers get a good detection rate. Figure 7 shows that the increased accuracy of the proposed model was obtained zero false warnings on attacks, despite having the lowest number of occurrences in detecting 4 types of attacks (back, teardrop, smurf, and ground). The proposed model is better than Siamese model which only detects 2 attacks (pod and teardrop). An increase in the accuracy of the total detection rate was also obtained in the probe category with four styles of attacks (Ipsweep, Nmap, Portsweep, and Satan). For inspection, see Figure 8.

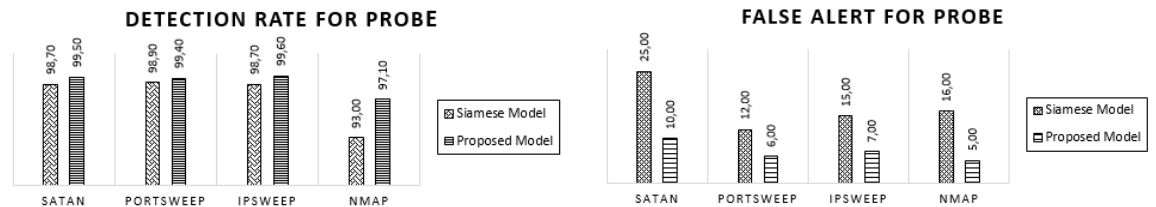


Figure 8. Detection rate and false alert for probe category

Figure 8 shows that the proposed model increases rating of detection for all attacks even though probe category representation is lower, while the least number of instances is obtained in the Nmap attack. There are eight styles of attacks in R2L category, consist of: warezclient, warezmaster, spy, phf, multihop, imap, guess_password, and ftp_write. This category has a lower representation of the data set than the number of instances in most attacks. The proposed model can increase the rating of detection by detecting seven styles of attacks, whereas Siamese can only detect four styles, see Figure 9.

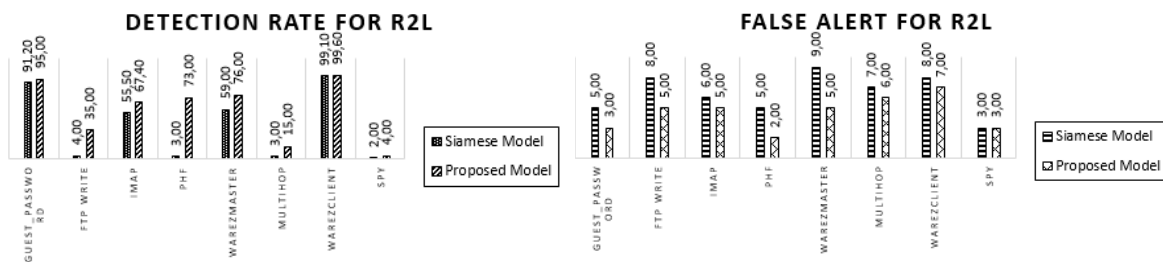


Figure 9. Detection rate and false alert for R2L category

In the guess_password attack, the proposed model can improve the overall detection rate, as shown in Figure 9. In addition, three styles of attacks (ftp_write of 37.5%, phf of 75%, and multihop of 14.5%) could be detected by the proposed model, whereas the Siamese model failed to detect any of the three styles of attacks. In the U2R category with four attack styles (perl, rootkit, loadmodule, and buffer_overflow), the proposed model can increase rating of detection by detecting new attacks, which the Siamese model was unsuccessful to do, see Figure 10.

The Siamese model failed to detect U2R attacks, while the proposed model was able to detect three new attacks (buffer with a percentage of 80%, loadmodule with a percentage of 20% and Perl with a percentage of 50%), as shown in Figures 10. Finally, the experimental results show that the proposed model achieved the lowest false warning and the best rating in detection. In addition, it also successfully detected five new attacks. Figure 11 show comparisons with other models in the related work section.

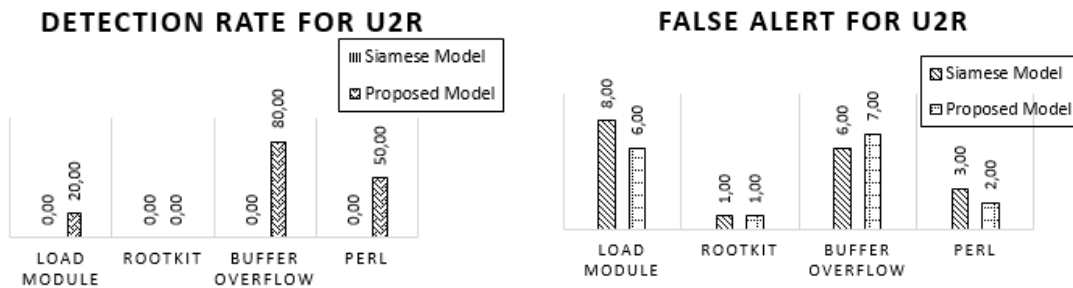


Figure 10. Detection rate and false alert for U2R category

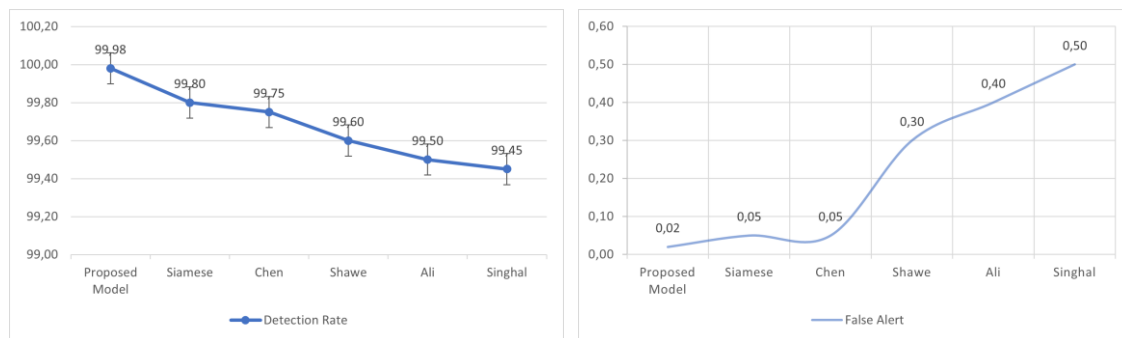


Figure 11. Detection rate and false alert of overall model

5. CONCLUSION

This paper proposed an enhanced model for elimination false warning and increase accuracy of IDS by selecting the best classifier. Improved detection was achieved by proposed model for all classes especially for classes with the least representation in a data set such as U2R. False positive warnings have also been minimized, thus preventing four styles of attacks (smurf, land, teardrop, and back) in the DOS category. In addition, three new attacks (multihop, phf, and ftp_write) in the R2L category. On the other hand, there are two new attacks (loadmodule and Perl) in the U2R category were successfully detected by the proposed model, although the number of attacks was lower. In the end, the best overall accuracy of 99.98% with the lowest false alert rate of 0.02% was achieved by proposed model.

ACKNOWLEDGEMENTS

The authors are grateful to the Universitas Dinamika, Surabaya, Indonesia and Universiti Malaysia Pahang, Malaysia for supporting this research.





REFERENCES

- [1] Slamet, I. I. Mohamed, and F. Samsuri, "Campus Hybrid Intrusion Detection System Using SNORT and C4.5 Algorithm," in *Lecture Notes in Electrical Engineering*, vol. 632, pp. 591–603, March 2020, doi: 10.1007/978-981-15-2317-5_50. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-15-2317-5_50.
- [2] S. K. Wagh, V. Pachghare, and S. Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques," *Int. J. Comput. Appl.*, vol. 78, no. 16, pp. 30–37, 2013.
- [3] M. Panda, A. Abraham, and M. R. Patra, "A hybrid intelligent approach for network intrusion detection," *Procedia Eng.*, vol. 30, pp. 1–9, 2012, doi: 10.1016/j.proeng.2012.01.827.
- [4] Slamet and I. I. Mohamed, "Network Intrusions Classification Using Data Mining Approaches," *J. Theor. Appl. Inf. Technol.*, vol.





- 99, no. 7, pp. 1679–1692, 2021.
- [5] H. Chen, S. Hu, R. Hua, and X. Zhao, “Improved naive Bayes classification algorithm for traffic risk management,” *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, pp. 1–12, 2021, doi: 10.1186/s13634-021-00742-6.
 - [6] W. Park and S. Ahn, “Performance Comparison and Detection Analysis in Snort and Suricata Environment,” *Wirel. Pers. Commun.*, vol. 94, pp. 241–252, 2017, doi: 10.1007/s11277-016-3209-9.
 - [7] E. A. Shams and A. Rizaner, “A novel support vector machine based intrusion detection system for mobile ad hoc networks,” *Wirel. Networks J. Mob. Commun. Comput. Inf.*, vol. 24, pp. 1821–1829, 2018, doi: 10.1007/s11276-016-1439-0.
 - [8] G. A. Ali, “Enhancing Intrusion Detection System (IDS) by Using Honeybee Concepts and Framework,” in *International Conference on Information Technology*, 2015, pp. 297–302, doi: 10.15849/icit.2015.0044.
 - [9] M. Dhakar and A. Tiwari, “A novel data mining based hybrid intrusion detection framework,” *J. Inf. Comput. Sci.*, vol. 9, no. 1, pp. 37–48, 2014.
 - [10] S. Chen, Z. Zuo, Z. P. Huang, and X. J. Guo, “A graphical feature generation approach for intrusion detection,” in *MATEC Web of Conferences*, vol. 44, p. 02041, March 2016, doi: 10.1051/mateconf/20164402041.
 - [11] R. T. Shawe and S. H. Abbas, “Using An Improved Data Reduction Method in Intrusion Detection System,” *Int. J. Eng. Res. Adv. Technol.*, vol. 3, no. 1, pp. 1–20, January 2017.
 - [12] H. Jmila, I. M. Khedher, G. Blanc, and M. A. El Yacoubi, “Siamese Network Based Feature Learning for Improved Intrusion Detection,” *Lect. Notes Comput. Sci.*, vol. 11953, pp. 377–389, 2019, doi: 10.1007/978-3-030-36708-4_31.
 - [13] M. F. Umer, M. Sher, and Y. Bi, “Flow-based intrusion detection: Techniques and challenges,” *Comput. Secur.*, vol. 70, pp. 238–254, September 2017, doi: 10.1016/j.cose.2017.05.009.
 - [14] B. M. Susanto, “Naaive Bayes Decision Tree Hybrid Approach for Intrusion Detection System,” *Bulletin of Electrical Engineering and Informatics*, vol. 2, no. 3, pp. 225–232, September 2013, doi: 10.12928/eei.v2i3.208.
 - [15] J. Pirgazi, M. Alimoradi, T. E. Abharian, and M. H. Olyae, “An Efficient hybrid filter-wrapper metaheuristic-based gene selection method for high dimensional datasets,” *Sci. Rep.*, vol. 9, no. 1, pp. 1–15, 2019, doi: 10.1038/s41598-019-54987-1.
 - [16] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, “K-Means Clustering and Naive Bayes Classification for Intrusion Detection,” *J. IT Asia*, vol. 4, no. 1, pp. 13–25, 2014, doi: 10.33736/jita.45.2014.
 - [17] M. Mazini, B. Shirazi, and I. Mahdavi, “Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms,” *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 31, no. 4, pp. 541–553, October 2019, doi: 10.1016/j.jksuci.2018.03.011.
 - [18] L. Liu, B. Xu, X. Zhang, and X. Wu, “An intrusion detection method for internet of things based on suppressed fuzzy clustering,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2018, no. 1, pp. 1–7, 2018, doi: 10.1186/s13638-018-1128-z.
 - [19] N. Koryshev, I. Hodashinsky, and A. Shelupanov, “Building a fuzzy classifier based on whale optimization algorithm to detect network intrusions,” *Symmetry*, vol. 13, no. 7, p. 1211, 2021, doi: 10.3390/sym13071211.
 - [20] R. Wazirali, “Intrusion detection system using FKNN and improved PSO,” *Comput. Mater. Contin.*, vol. 67, no. 2, pp. 1429–1445, 2021, doi: 10.32604/cmc.2021.014172.
 - [21] B. B. Rao and K. Swathi, “Fast kNN Classifiers for Network Intrusion Detection System,” *Indian J. Sci. Technol.*, vol. 10, no. 14, pp. 1–10, 2017, doi: 10.17485/ijst/2017/v10i14/93690.
 - [22] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, “A new intrusion detection system based on KNN classification algorithm in wireless sensor network,” *J. Electr. Comput. Eng.*, vol. 2014, 2014, doi: 10.1155/2014/240217.
 - [23] K. Ibrahim and O. Ouaddane, “Management of intrusion detection systems based-KDD99: Analysis with LDA and PCA,” *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2017, pp. 1–6, doi: 10.1109/WINCOM.2017.8238171.
 - [24] Canadian Institute for Cybersecurity, “NSL-KDD dataset,” [Online]. Available: <http://www.unb.ca/cic/datasets/nsl.html> [accessed Jun. 01, 2021].
 - [25] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, “Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine,” *Electronics*, vol. 9, no. 1, p. 173, 2020, doi: 10.3390/electronics9010173.

BIOGRAPHIES OF AUTHORS



Slamet     is a Ph.D candidate at the Department of Electrical and Electronic Engineering, Universiti Malaysia Pahang, his interest is in networking and security. He has 10 years of experience as a Network Engineer and 13 years in Teaching at the Department of Information System, Universitas Dinamika, Surabaya, Indonesia. His research areas include data mining, network security, computer networking, network traffic measurement, information security management system, and IT risk management. He can be contacted at email: slamet@dinamika.ac.id.



Izzeldin Ibrahim Mohamed Abdelaziz     is Senior Lecturer in Faculty of Electrical and Electronics Engineering, Universiti Malaysia Pahang, Malaysia. He has more than fifteen years of experience in teaching and published more than thirty papers in International Journals and also presented in various national and international conferences. His research areas include data mining, network security, computer networking, network traffic measurement and analysis, network management and traffic engineering, FPGA programming, micro controller, embedded system design, microcontroller programming, electronics and communication engineering, and digital signal processing. He can be contacted at email: izzeldin@ump.edu.my.