Comparison of Data Mining Algorithm: PSO-KNN, PSO-RF, and PSO-DT to Measure Attack Detection Accuracy Levels on Intrusion Detection System

by Sularso Budilaksono

Journal of Physics: Conference Series

PAPER • **OPEN ACCESS**

Comparison of Data Mining Algorithm: PSO-KNN, PSO-RF, and PSO-DT to Measure Attack Detection Accuracy Levels on Intrusion Detection System

To cite this article: Sularso Budilaksono *et al* 2020 *J. Phys.: Conf. Ser.* **1471** 012019

View the article online for updates and enhancements.

Comparison of Data Mining Algorithm: PSO-KNN, PSO-RF, and PSO-DT to Measure Attack Detection Accuracy Levels on Intrusion Detection System

Sularso Budilaksono[1], Andri Agung Riyadi[2], Lukman Azhari[3], Dedi Dwi Saputra[4], M. Anno Suwarno[5], I Gede Agus Suwartane[6], Jupriyanto[7], Andika Ramadhan[8], Agus Prasetyo Utomo[9], Achmad Fauzi[10]

[1] University of Persada Indonesia YAI, Jakarta, Indonesia
[2] Master of Computer Science-Postgraduate Program, STMIK Nusa Mandiri, Jakarta, Indonesia
[3], University of Muhammadiyah Tangerang, Indonesia
[4] Master of Computer Science-Postgraduate Program, STMIK Nusa Mandiri, Jakarta, Indonesia
[5] University of Persada Indonesia YAI, Jakarta, Indonesia
[6] University of Persada Indonesia YAI, Jakarta Indonesia
[7] Graduate School Master's Degree Computer Science, STMIK Nusa Mandiri, Jakarta, Indonesia
[8] University of Muhammadiyah Tangerang, Indonesia
[9] University of Stikubank, Semarang, Indonesia
[10] University of Muhammadiyah Tangerang, Indonesia

Abstract. Nowadays, computer networks are widely used to exchange valuable and confidential data information between servers to computers or cellular devices. Access to user control and use of software or hardware as a firewall often experience security problems. Unauthorized access to information through computer networks continues to occur and tends to increase. This study examines the attack detection mechanism by using three data mining algorithms based on particle swarm optimization (PSO), namely PSO-K Nearest Neighbor, PSO-Random Forest, and PSO-Decision Tree in the Canadian Institute for Cybersecurity Dataset (CICIDS2017). The initial experiment showed that the approach using the PSO-RF method was able to produce the highest accuracy of attack detection. Accuracy values generated using the PSO-RF algorithm with a combination of the number of trees and maximal depth = 20 in the CICIDS2017 dataset are intact higher than other proposed algorithms. The highest accuracy of attack detection in the CICIDS2017 dataset is intact, which is 99.76%. In the CICIDS2017 dataset 50% Benign and 50% Attack it turns out that the PSO-RF algorithm with a combination of the number of trees and maximal depth = 20 also gets the highest accuracy value of 99.67%.

Keywords: Intrusion Detection System; Particle Swarm Optimization; K-Nearest Neighbors; Random Forest; Decision Tree

1. Introduction

In the last two decades, the number of internet users in the world is increasing very rapidly. Every day millions of people and hundreds of thousands of institutions to communicate with each other via the internet. In line with these developments, the number of attacks carried out in the network internet continues to increase by the day. Network security tried to protect the network from attacks on the third principle, namely secrecy (confidentiality), integrity, and availability. A network attack is an attempt to break the three essential features (1).

There is software like antivirus, firewalls, data encryption, and user authentication that provides data protection and network from incoming threats, but can not be efficient for all the threats that exist. Multiple studies had been conducted in this field to address this threat. Intrusion Detection Systems (IDS) has been developed to monitor and filter out network activities by identifying attacks and warn network administrators (2). There are two main approaches to the IDS, which are: method of misuse detection and anomaly Friday detection method. Not efficient for all types of threats, but each has strengths and limitations (3). Misuse detection is a method to detect an attack in computer networks by comparing the activities or find a pattern that has been defined earlier as the characteristics of an attack. Misuse detection methods have been efficient to detect known attacks but fail to distinguish the existence of a novel attack (4). By contrast, methods of detection to detect novel anomaly of Friday attacks have been efficient but not so useful in attack detection level already known, so it has high FPR (5). Data mining techniques have been used to obtain useful knowledge from the use of IDS datasets. Full KDD, Corrected KDD99, NSL-KDD, 10% KDD, UNSW-NB15, Caida, ADFA Windows, and UNM are standard IDS datasets used. One of the latest IDS datasets made by the University of New Brunswick's (UNB) Canadian Institute for Cybersecurity (CIC), CICIDS2017 should be analyzed for research (6). The CICIDS dataset 2017 was created using the latest framework that considers organizational policies and conditions using coefficients that can be determined separately for each criterion (7).

Mixed methods have been used as solutions to respond to the challenges of misuse detection and anomaly detection techniques. These methods are used to maximize the capabilities of both techniques (8). Three hybrid methods recommended for use in IDS. They are the misuse detection method followed by the anomaly detection method, the anomaly detection method followed by the misuse detection method or the use of the misuse detection method, and the anomaly detection method simultaneously. The hybrid method in IDS uses many result combinations from training independently on methods of misuse detection and anomaly detection. For example, the hybrid method considers network traffic as an attack if at least one of the two methods classifies it as an attack. In this case, the detection rate will increase, but IDS will still have a high FPR. Conversely, if the hybrid method considers network traffic as an attack, only if both methods are classified as an attack, FPR will be low but will ignore many attacks in network traffic (5). False Positive Rate (FPR) is when a system of IDS detects and classifies benign or normal activities in a computer network into a dangerous attack. The PSO-, PSO-RF, and PSO-DT algorithm methods will be used to measure the accuracy of attack detection in the CICIDS2017 dataset in this study. The algorithm method had never compared or compared using the CICIDS2017 dataset.

2. Study of Literature

IDS is an essential part of protecting information systems in computer networks. The research report written by Anderson (1980) aims to improve computer security audit capabilities and system customer surveillance capabilities. The IDS system has three commonly used approaches, including misuse detection, anomaly detection, and hybrid detection (9). Hybrid detection combines the use of misuse detection and anomaly detection to improve the ability of both methods to detect attacks. There are three ways to implement hybrid methods on IDS, namely the use of the misuse detection method followed by the anomaly detection method, the anomaly detection method followed by misuses detection method or integrating the misuse detection method and the anomaly detection method simultaneously (5).

CICIDS2017 is a dataset made by the University of New Brunswick's (UNB) Canadian Institute for Cybersecurity (CIC). The CICIDS dataset 2017 is created using the latest framework that considers organizational policy and uses coefficients that can be determined separately for each criterion. This dataset consists of around 3.1 million records with more than 80 attributes, where one attribute was used as a label. The attributes in the dataset have seven attack categories and one benign or normal category. The seven categories of attacks in this dataset are Brute Force Attack, Heartble Attack, Botnet, DoS Attack, DDoS Attack, Web Attack, and Infiltration Attack.

Data mining is the application of unique algorithms to extract patterns from data (10). Data mining is about solving problems by analyzing existing data in a database (11). Many techniques and methods

exist to perform various types of data mining tasks. The methods are grouped into three leading data mining paradigms, namely, Predictive Modeling, Discovery, and Deviation Detection. Data mining and Knowledge Discovery in Databases (KDD) are often used interchangeably to explain the process of extracting hidden information in a large database (12). Although it has a different concept, data mining and KDD are related to each other. One of the stages in the whole KDD process is data mining.
The k-Nearest Neighbors (k-NN) classification algorithm method is one of the data mining techniques considered as the ten best data mining techniques. The k-Nearest Neighbors (k-NN) method uses the famous Cicero principle *pares cum paribus facillime congregantur* (feathered birds gather together or the same as sociable) (13). The algorithm is used to compare the accuracy, precision, and recall rates of eight different IDS datasets. Algorithms produce better performance and have higher accuracy, precision, and recall in the NSL-KDD dataset than other datasets (14). Random Forest (RF) is one method used for classification by building many classification trees. Random Forest can improve accuracy due to random selection in generating child knots for each node (node above it) and accumulated classification results from each tree; then the most widely chosen classification results are chosen (15). The Random Forest (RF) algorithm is used to detect four types of attacks on the NSL-KDD dataset, namely DOS, probe, U2R, and R2L. The proposed RF method produces high DR and FAR is low in classifying attack types. In the DOS attack type, RF reaches an accuracy value of 99.67% (16).
Decision Tree (DT) is a classification method that uses a representation of a tree structure which contains alternatives for solving a problem. This tree also shows the factors that influence the alternative results of the decision, along with the estimation of the final results if we make that decision (17). The decision tree (DT) algorithm can produce an accuracy rate of 79% in the NSL-KDD dataset (18).

Particle Swarm Optimization (PSO) is an optimization method that has strong global search capabilities and applicable for dimensional optimization (19). The PSO-k-NN algorithm in the NSL-KDD dataset produces an accuracy of 98.5755%. In the UNSW-NB15 dataset produces an accuracy of 97.9796% (20). Accuracy values using the PSO-based method with a value of k = 5 in the KDDCup99 DOS type attack dataset of 99.91% (21). The average PSO-RF method has an accuracy rate of 96.7810% and FPR of 0.1546% in the KDDCup99 dataset (19). Combined particle swarm optimization (PSO) and decision tree (DT) techniques using the single-objective (SO) and multi-objective (MO) PSO approach used in the KDDCup99 dataset. The MO-DTP algorithm approach produces the lowest FPR value of 0.136% and the highest accuracy rate of 96.65% (19).

3. Methodology

This research uses Knowledge Discovery in Databases (KDD) method consisting of five stages, namely Data Selection, Preprocessing, Transformation, Data Mining, Interpretation, or Evaluation (10). In this study, the authors used the CICIDS2017 dataset as the latest standard dataset for survey and evaluation research in the field of IDS. An analysis was carried out to identify the data further as a preliminary knowledge, and then evaluate the quality of the data. The CICIDS2017 dataset consists of 3.1 million records with 85 attributes, including one attribute used as a label. The attributes in the dataset have seven attack categories and one normal category. The preprocessing process includes removing data duplication, checking inconsistent data, removing features that are less valuable or completely useless, converting all attack type labels to ATTACK labels, and correcting errors in data. There are two types of CICIDS2017 dataset made, namely the whole CICIDS2017 dataset and the CICIDS2017 dataset with a composition of 50% benign and 50% attack. Feature selection is used to determine which features are important and discard features that have low quality and are uncorrelated. Sample needs to be selected for efficiency purposes considering the number of records in the CICIDS2017 dataset. This study took a maximum of 1% of the two types of CICIDS201 dataset used in each sample. The approach models that will be used to compare the results of the accuracy value using the PSO are algorithm approach with k values, PSO-RF with a combination of the number of trees and highest depth each with a value, and PSO-DT with the highest depth value.

4. Discussion

At the classification stage, the approached used was data mining algorithm method to obtain the accuracy of attack detection in the CICIDS2017 dataset. There are two types of datasets used, namely the CICIDS2017 dataset intact and the CICIDS2017 dataset with a composition of 50% benign and 50% attack. The algorithm used is the PSO-algorithm with a value, PSO-RF with a combination of the number of trees and maximal depth each with, and PSO-DT with maximal depth = 5, 10, 15, 20.
The classification phase in the CICIDS2017 dataset intact using the PSO-algorithm with values, PSO-RF with a combination of the number of trees and maximal depth each with, and PSO-DT with maximal depth = 5, 10, 15 and 20.

Table 1. Accuracy, Kappa, Recall, Precision and F-Measure PSO-k-NN values on Dataset CICIDS2017 Whole

k =	PSO- $k-NN$				
	Accuracy (%)	*Kappa*	*Recall* (%)	*Precision* (%)	*F-Measure* (%)
5	97.83	0,932	94.72	94.38	94.55
10	97.38	0,918	94.18	92.75	93.46
15	96.92	0,903	91.99	92.48	92.23
20	96.9	0,902	91.22	93.04	92.12

Table 2. Accuracy, Kappa, Recall, Precision and F-Measure PSO-RF values on Dataset CICIDS2017 Whole

Number of trees and *highest depth =*	PSO-RF				
	Accuracy (%)	*Kappa*	*Recall* (%)	*Precision* (%)	*F-Measure* (%)
5	96.37	0,878	82.02	99.64	89.97
10	99.21	0,975	97.27	98.73	98
15	99.62	0,988	98.64	99.46	99.05
20	99.76	0,993	99.35	99.47	99.41

Table 3. Accuracy, Kappa, Recall, Precision and F-Measure PSO-DT values in Dataset CICIDS2017 Whole

Highest depth =	PSO-DT				
	Accuracy (%)	*Kappa*	*Recall* (%)	*Precision* (%)	*F-Measure* (%)
5	96.59	0,887	84.21	98.4	90.76
10	99.28	0,977	97.74	98.62	98.18
15	99.61	0,988	98.87	99.17	99.02
20	99.65	0,989	99.17	99.05	99.11

The classification stage in the CICIDS dataset2017 with a composition of 50% benign and 50% attack uses the PSO-algorithm with values, PSO-RF with a combination of the number of trees and maximal depth each with, and PSO-DT with highest depth = 5, 10, 15 and 20.

Table 4. Accuracy, Kappa, Recall, Precision and F-Measure PSO-k-NN values on the CICIDS2017 50% Benign and 50% Attack

k =	PSO- $k-NN$				
	Accuracy (%)	*Kappa*	*Recall* (%)	*Precision* (%)	*F-Measure* (%)
5	96,89	0,938	97,06	96,71	96,89
10	96,5	0,93	97,3	95,75	96,52
15	95,03	0,901	96,04	94,12	95,07
20	95,15	0,903	95,92	94,45	95,18

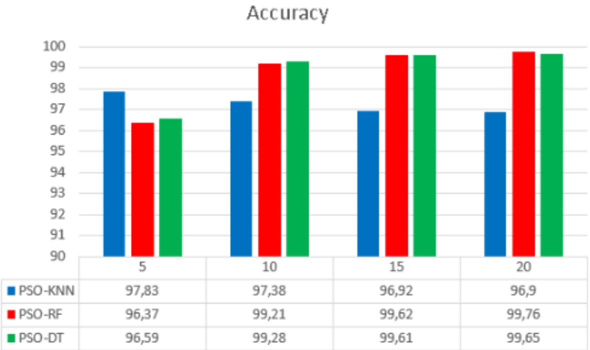
Table 5. Accuracy, Kappa, Recall, Precision and F-Measure PSO-RF values on the CICIDS2017 50% Benign and 50% Attack

Number of trees and *highest depth* =	PSO-RF				
	Accuracy (%)	*Kappa*	*Recall* (%)	*Precision* (%)	*F-Measure* (%)
5	95.21	0,904	97	93.63	95.29
10	98.5	0,97	98.74	98.27	98.5
15	99.61	0,992	99.64	99.58	99.61
20	99.67	0,993	99.7	99.64	99.67

Table 6. Accuracy, Kappa, Recall, Precision, and F-Measure PSO-DT values on the CICIDS2017 Dataset 50% Benign and 50% Attack

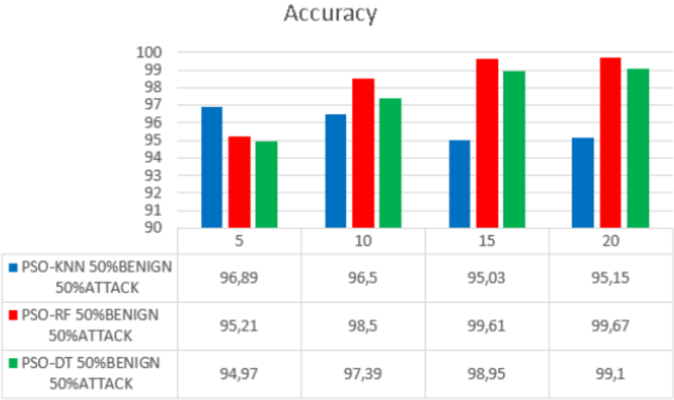
Highest depth =	PSO-DT				
	Accuracy (%)	*Kappa*	*Recall* (%)	*Precision* (%)	*F-Measure* (%)
5	94.97	0,899	95.32	94.64	94.98
10	97.39	0,948	97.48	97.31	97.39
15	98.95	0,979	98.86	99.04	98.95
20	99.1	0,982	99.22	98.98	99.1

The results of this study are displayed in graphical form in Figure 3 and Figure 4 with the accuracy of each algorithm used in two types of datasets CICIDS 2017 with k values as the number of trees and maximal depth set at values 5, 10, 15 and 20. For k = 5, the k-NN PSO algorithm is the best in the CICIDS2017 dataset intact with 97.83% accuracy or the CICIDS2017 dataset with a combination of 50% Benign and 50% Attack with an accuracy of 96.89%. At k = 10, k = 15 and k = 20, the PSO-RF algorithm is the best in the CICIDS2017 dataset intact with 99.21% accuracy up to 99.76% or the CICIDS2017 dataset with a combination of 50% Benign and 50% Attack with accuracy 98.5% to 99.67%.



	5	10	15	20
🟦 PSO-KNN	97,83	97,38	96,92	96,9
🟥 PSO-RF	96,37	99,21	99,62	99,76
🟩 PSO-DT	96,59	99,28	99,61	99,65

Figure 1. Comparison of Accuracy Levels of each Algorithm in the CICIDS2017 dataset Whole



	5	10	15	20
🟦 PSO-KNN 50%BENIGN 50%ATTACK	96,89	96,5	95,03	95,15
🟥 PSO-RF 50%BENIGN 50%ATTACK	95,21	98,5	99,61	99,67
🟩 PSO-DT 50%BENIGN 50%ATTACK	94,97	97,39	98,95	99,1

Figure 2. Comparison of Accuracy Levels of each Algorithm on the CICIDS2017 50% Benign and 50% Attack

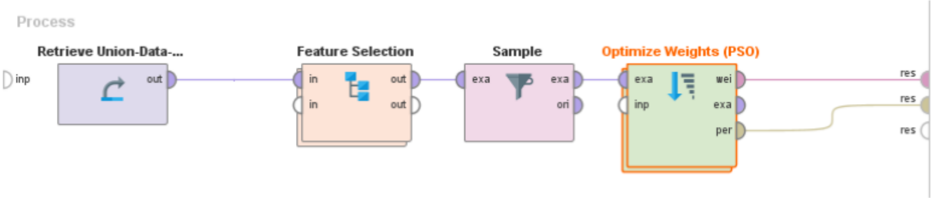


Figure 3. Classification Modelling using Rapid Miner

5. Conclusion

Based on data processing using the PSO-RF algorithm with a combination of the number of trees and maximal depth = 20 on the complete data, the accuracy value is higher than the other proposed algorithms. The highest value of attack detection accuracy in the whole data is 99.76%.
Based on data with a composition of 50% Benign and 50% Attack it turns out that the PSO-RF algorithm with a combination of the number of trees and maximal depth = 20 also gets the highest accuracy value that is equal to 99.67%.

References

[1]. Kahate A. 2013, Cryptography and Network Security, Third Edition New Delhi: McGraw Hill Education(India) Privated Limited

[2]. Chung YY,&NW. 2012, A hybrid network intrusion detection system using simplified swarm optimization (SSO): Applied Soft Computing 12, 3014–3022

[3]. Lin WC, KSW, &TCF.2015, CANN: An intrusion detection system based on combining cluster centers and nearest neighbors.: Knowledge-Based Systems

]4]. Zhang J, LH, GQ, WH, &LY. 2014, Detecting anomalies from big network traffic data using an adaptive detection approach: Information Sciences

[5]. Kim, G., Lee, S., & Kim, S. 2014, A novel hybrid intrusion detection method integrating anomaly detection with misuse detection: Expert Systems with Applications, 1690-1700;

[6]. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. 2018,A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In 4th International Conference on Information Systems Security and Privacy; p. 108-116.

[7]. Gharib, A., Lashkari, A. H., Sharafaldin, I., & Ghorbani, A. A.2016, An Evaluation Framework for Intrusion Detection Dataset. In International Conference on Information Science and Security (ICISS)

[8]. , O., Topallar, M., Anarim, E., & Ciliz, M. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer network: Expert Systems with Applications, 713-722.; 2005.

[9]. Mchugh J., Allen, J. H., & Christie A..2000, The Role of Intrusion Detection Systems: IEEE Software , 42-51.

[10]. Gama J. 2010, Knowledge Discovery from Data Streams New York: Chapman and Hall/CRC

[11]. Witten, I. H., Frank, E., & Hall, M. A. 2011, Data Mining: Practical Machine Learning Tools and Technique San Francisco: Morgan Kaufmann Publishers Inc.

[12]. Agushinta, D., & Irfan, M. 2008, Perancangan Aplikasi Data Mining Untuk Memrediksi Permintaan Customer Pada Perusahaan Persewaan Mobil. In Seminar Ilmiah Nasional Komputer dan Sistem Intelijen,; p. 206-213.

[13]. Mucherino, A., Papajorgji, P. J., & Pardalos, P. M.2009, K-Nearest Neighbor Classification: Data Mining in Agriculture, 83-106.

[14]. Hamid, Y., Balasaraswathi, V. R., Journaux, L., & Sugumaran, M.2018, Benchmark Datasets for Network Intrusion Detection: A Review. International Journal of Network Security.

[15]. Zainal, A., Maarof, M. A., Shamsuddin, S. M., & Abraham, A. Ensemble of One-Class Classifiers for Network Intrusion Detection System. In The Fourth International Conference on Information Assurance and Security; p. 180-185.

[16]. Farnaaz, N., & Jabbar, M. A. 2008, Random Forest Modeling for Network Intrusion Detection System. : Procedia Computer Science, 213-217.; 2016.

[17]. Tsang, S., Kao, B., Yip, K. Y., Ho, W.-S., & Lee, S. D. 2009, Decision Trees for Uncertain Data. In IEEE 25th International Conference on Data Engineering;. p. 441-444.

[18]. Befekadu A.. 2018, Enhancing the Performance of Network Intrusion Detection System by Combining Naïve Bayes, Decision Tree and K-Nearest Neighbors Algorithms. International Journal of Computer Applications.: p. 48-53.

[19]. Malik, A. J., Shahzad, W., Khan, F. A. 2012, Network intrusion detection using hybrid binary PSO and random forests algorithm.: Security and Communication Networks, 1-15;

[20]. Khan, A., & Nigam, A. 2018;, Analysis of Machine Learning Techniques for Intrusion Detection. International Journal of Innovative Research in Computer and Communication Engineering.: p. 5482-5492.

[21]. Syarif, A. R., & Gata, W.2017, Intrusion Detection System Using Hybrid Binary Pso And K-Nearest Neighborhood Algorithm.. In 11th International Conference on Information & Communication Technology and System (ICTS);. p. 181-186.

[22]. Wu SX.2010, The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing. p. 1-35.

Comparison of Data Mining Algorithm: PSO-KNN, PSO-RF, and PSO-DT to Measure Attack Detection Accuracy Levels on Intrusion Detection System

ORIGINALITY REPORT

19%	13%	14%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	infor.seaninstitute.org Internet Source	1%
2	Enggar Tyastiwi Munawaroh, Rani Irma Handayani, Euis Widanengsih. "The Implementation of K-Means Algorithm for Cluster Majoring to New Students in SMKN 2 of South Tangerang", SinkrOn, 2019 Publication	1%
3	infonomics-society.org Internet Source	1%
4	coek.info Internet Source	1%
5	doaj.org Internet Source	1%
6	Novi Trisman Hadi, Siti Rochimah. "Enhancing Software Defect Prediction Using Principle Component Analysis and Self-Organizing Map", 2018 Electrical Power, Electronics,	1%

	Communications, Controls and Informatics Seminar (EECCIS), 2018 Publication	
7	Antonio Mucherino. "k-Nearest Neighbor Classification", Springer Optimization and Its Applications, 2009 Publication	1 %
8	Rajendra Patil, Harsha Dudeja, Chirag Modi. "Designing an Efficient Security Framework for Detecting Intrusions in Virtual Network of Cloud Computing", Computers & Security, 2019 Publication	1 %
9	Zhang, Enlai, Liang Hou, Chao Shen, Yingliang Shi, and Yaxiang Zhang. "Sound quality prediction of vehicle interior noise and mathematical modeling using a back propagation neural network (BPNN) based on particle swarm optimization (PSO)", Measurement Science and Technology, 2016. Publication	1 %
10	china.iopscience.iop.org Internet Source	1 %
11	techscience.com Internet Source	1 %
12	A Lopes, ML Nogueira D Genta, V da Costa Miranda, RV Mendonza Lopez, F Marino	1 %

	Carvalho, J Paula Carvalho. "94 Histopathological response on clinicoradiological presentation and prognosis of patients with advanced high grade serous ovarian carcinoma treated with neoadjuvant chemotherapy", E-Poster discussions, 2019 Publication	
13	www.mdpi.com Internet Source	1 %
14	download.atlantis-press.com Internet Source	<1 %
15	www.science.gov Internet Source	<1 %
16	onlinelibrary.wiley.com Internet Source	<1 %
17	R McWeeny. "The Diamagnetic Anisotropy of Large Aromatic Systems Parts I and II", Proceedings of the Physical Society. Section A, 1951 Publication	<1 %
18	Dela Youlina Putri, Rachmadita Andreswari, Muhammad Azani Hasibuan. "Analysis of Students Graduation Target Based on Academic Data Record Using C4.5 Algorithm Case Study: Information Systems Students of Telkom University", 2018 6th International	<1 %

	Conference on Cyber and IT Service Management (CITSM), 2018 Publication	
19	piyanit.nl Internet Source	<1 %
20	"Big Data and Security", Springer Science and Business Media LLC, 2020 Publication	<1 %
21	Fang Deng, Jie Chen, Yanyong Wang, Kun Gong. "Measurement and calibration method for an optical encoder based on adaptive differential evolution-Fourier neural networks", Measurement Science and Technology, 2013 Publication	<1 %
22	Yao, Yu, Lei Guo, Hao Guo, Ge Yu, Fu-xiang Gao, and Xiao-jun Tong. "Pulse quarantine strategy of internet worm propagation: Modeling and analysis", Computers & Electrical Engineering, 2012. Publication	<1 %
23	cybersecurity.springeropen.com Internet Source	<1 %
24	www.ijitee.org Internet Source	<1 %
25	Bernhard Schölkopf, John C. Platt, John Shawe-Taylor, Alex J. Smola, Robert C.	<1 %

	Williamson. "Estimating the Support of a High-Dimensional Distribution", Neural Computation, 2001 Publication	
26	Imtiaz Ullah, Qusay H. Mahmoud. "A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks", 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019 Publication	<1 %
27	Kaniz Farhana, Maqsudur Rahman, Md. Tofael Ahmed. "An intrusion detection system for packet and flow based networks using deep neural network approach", International Journal of Electrical and Computer Engineering (IJECE), 2020 Publication	<1 %
28	Wei Chen, Shiyu Li, Peixiang Lu, Dongxiang Wang. "High Performance Large Mode-Area Ytterbium-doped Photonic Crystal Fiber for Fiber Lasers", Journal of Physics: Conference Series, 2011 Publication	<1 %
29	acikbilim.yok.gov.tr Internet Source	<1 %
30	link.springer.com Internet Source	<1 %

31	repository.nwu.ac.za Internet Source	<1 %
32	www.ijera.com Internet Source	<1 %
33	www.springerprofessional.de Internet Source	<1 %
34	Raniyah Wazirali. "Intrusion Detection System Using FKNN and Improved PSO", Computers, Materials & Continua, 2021 Publication	<1 %
35	Arif Jamal Malik, Farrukh Aslam Khan. "A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection", Cluster Computing, 2017 Publication	<1 %
36	S. Varuna, P. Natesan. "An integration of k-means clustering and naïve bayes classifier for Intrusion Detection", 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 2015 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off

Exclude bibliography On