A Dimensionality Reduction Approach for Machine Learning Based IoT Botnet Detection

By Susanto Susanto

WORD COUNT	3521	TIME SUBMITTED	02-AUG-2021 07:00AM
		PAPER ID	75124154

A Dimensionality Reduction Approach for Machine Learning Based IoT Botnet Detection

Susanto
Faculty of Computer Universitas Bina Insan/ Faculty of Engineering
Universitas Sriwijaya
Lubuklinggau, Indonesia
susanto@univbinainsan.ac.id

Deris Stiawan*
Computer Engineering Department, Faculty of Computer Science
Universitas Sriwijaya
Palembang, Indonesia
deris@unsri.ac.id

M. Agus Syamsul Arifin
Faculty of Computer Universitas Bina Insan/ Faculty of Engineering
Universitas Sriwijaya
Lubuklinggau, Indonesia
mas.arifin@univbinainsan.ac.id

Juli Rejito
Department of Computer Science, Faculty of Math. and Natural Sciences
Universitas Padjadjaran
juli.rejito@unpad.ac.id

Mohd. Yazid Idris
School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia
yazid@utm.my

Rahmat Budiarto
College of Computer Science and IT, AlBaha University
Albaha, Saudi Arabia
rahmat@bu.edu.sa

***Abstract*— The use of Internet of Thing (IoT) technology in industry or daily lives are improving massively. This improvement attracts hackers to perform cyber attack which one of them is botnet. One of the botnet threat is disrupting network and denial service to IoT devices. Therefore, a reliable detection system to keep the security is required urgently. One of the detection method which has been widely used by previous research works is machine learning. However, performance problem on machine learning needs more attention, especially for data with high scalability. In this paper, we conduct experiments on random projection dimensionality reduction approach to boost the machine learning performance to detect botnet IoT. Experiment results show random projection method combined with decision tree is able to detect IoT botnet within 8.44 seconds with accuracy of 100% and very low false positive rate (close to 0).**

Keywords—dimensionality reduction, random projection, botnet IoT, machine learning

I. Introduction

The use of IoT applications and services are improving massively. Many organizations are compete in developing IoT devices, from smartwatch, whole smart grid network, autonomous vehicle, smart manufacturing to smart mining. As IoT system consists of high numbers of devices and is applicable anywhere, it attra potential hackers to launch cyber attack and data stealth. One of the attack is distributed denial of service (DDoS) botnet basis in IoT network [1],[2]. Botnet IoT is able to exploit device's vulnera ity by taking over IoT device control [3], then it may cause network disruption and denial of services to the IoT devices [4]. Therefore, botnet is considered as serious threat in cyber crime [5].

Authors in [6] predict and detect attack threat using machine learning technique. Detection methods with machine learning are proven effective, eventhough it does not mean without limitation [7]. The detection performance can be improved by using dimens lity reduction [8]. Dimensionality reduction is solid technique in machine learning which used to solve problem effectively in various applications [9]. The use of dimensionality reduction method gives and advantage on machine learning implementation. One of the advantage is the ability to boost the performance because the dataset can be reduced less than original dimension [10].

This research work contributes towards the development of workflow for detection system with machine learning. The proposed detection system uses random projection to reduce dimension and combinied with different classification algorithms, i.e.: k-Nearest Neighbor (k-NN), decision tree (DT), random forest (RF), adaboost (AD), and gradient boosting (GB). The main contribution of this research works include:

1. Representation of dimensional reduction with effective features, using random projection dimensional reduction approach.
2. Efficient approach for dimensionality reduction and compare to different classification algorithms, i.e.: k-NN, DT, RF, AD, and GB
3. Evaluation of classification system performance through comparison of combination matrix through measusuring accuracy, sensitivity, specificity, false positive rate (FPR), false negative rate (FNR), precision, and execution time

The composition of this paper is as follows. In Section 2, we present various works on the use of dimensionality reduction approach on machine learning. In Section 3, we present the research methodology, which consists of dataset used, explanation about random projection approach and classification methods, also performance measurement. Section 4 presents results and discussion also comparison with the existing similar works. Section 5 provides summary and future work on dimensionality reduction approach.

II. Related Work

Application of dimensionality reduction method in boosting performance of machine learning especially for botnet IoT detection has been widely used in previous researches. Bahsi et al. [11] perform feature reduction using Fisher's score, so it could minimize computation complexity of decision tree classification on machine learning to detect IoT botnet which compared to k-NN. Then Nomm and Bahsi [12] introduce autonomous learning model which has high accuracy to detect IoT botnet with feature reduction, then it could perform detail analysis with feature ability which discriminative and comparison of detection performance. The authors use entropy method, variance, and Hopkins for trial feature reduction, while process evaluation uses one

class SVM and isolation forest. Next, Alqahtani et al [13] implement feature selection using Fisher score which plays effective role in dimensionality reduction while minimizes class distance and maximizes between class distance as well as improves extreme gradient model with genetic based. The work improves extreme gradient for classification and genetic algorithm to select optimal parameter XGBoost value and improves minority class accuracy without impacting whole accuracy of other class in detecting botnet IoT attack. Moreover, Desai et al. [14] perform feature reduction using Principal Component Analysis (PCA) which assists in reducing computational complexity during training cluster data. The machine learning model is trained using Decision Tree, Random Forest, and SVM algorithms which are controlled learning algorithms to detect botnet IoT attack. PCA method also used by Alshamkhany et al. [9] in reduction dimensional data. This method is able to ensure that only relevant features were selected and will contribute on computational efficiency and simplicity for the four learning models of machine learning, i.e.: k-Nearest Neighbor, Support Vector Machine, Naïve Bayes, and Decision Tree.

III. Research Methodology

A. Dataset

Experiments in this work use N-BaIoT dataset [16]. The N-BaIoT dataset is extracted using statistic method, which has 115 features of 89 files. Those file names are customized with traffic data which consist of Benign, Mirai (Ack, Scan, Syn, Udp, Udpplain), and Bashlite (Combo, Junk, Scan, TCP, UDP). Those data traffic captured from nine IoT devices, i.e.: one unit thermostats, two unit doorbells, one unit webcam, four security cameras, and one baby monitors. In this experiment, we only used less than 20% of data, taken from each file as shown in Table 1.

TABLE I. DISTRIBUTION OF 20% DATASET

Device	New Label Feature	Label File	Total data
Two doorbells, webcam, four security cameras, and baby monitors	Benign	Benign	111179
	Bashlite	Combo	103030
		Junk	52158
		Scan	51022
		Tcp	171969
		Udp	192873
	Mirai	Ack	128764
		Scan	107596
		Syn	146660
		Udp	246001
		Udpplain	104660
Total			1415912

B. Machine Learning Algorithms

We use five machine learning algorithms, i.e.: RF, DT, AD, k-NN and GB. In experimenting data classification, the dataset is divided into 70 % for training and 30% for testing.

1) Random forest

Random forest is set of decision tree which binded in a set of bootstrap sample resulted from original dataset. Nodes are divided based on entropy (or index Gini) from subset of chosen features. Subset created from original dataset, using bootstrap, has the same size with the original dataset [17].

2) Decision Tree

Decision tree is a technique with tree based where each track starts from root explained by data separation order until result on leaf knot is reached. When relations are used for classification, node represent goals [18].

3) Adaboost

AdaBoost (Adaptive Boosting) is machine learning algorithm which performs with weak classificatory combined into single strong classification. On each iteration, round-more weighting is given to the incorrectly learned examples during the previous iteration [19].

4) k-Nearest Neighbor

Machine learning algorithm of k-Nearest Neighbor is non-parametrics classification method. Classification is performed by determining new sample class based on closed neighbour class [20].

5) Gradient boosting

Gradient boosting creates new model from weak ensemble model with idea that each new model can minimize loss function orderly. This loss function is measured by gradient reduction method. With the used of loss function, each new model suit more accurate with observation, and thus whole accuracy improved [21].

C. Random Projection

Random projection can become a good alternative for optimal reduction dimensional method because random projection is not dimensional curse [22]. Random projection is cheaper in computation cost, most failed to catch information related to task because later space resulted without considering intrinsic structure from original data. In this case random projection has advantage on speed in improving linier separation [23]. In a matrix data $X \in \mathbb{R}^{N \times d}$, where N is total point and d is original dimension. In transforming X to lower dimension space, the random projection uses transformation in (1) [24,25].

$$X_{RP} = X.R \quad (1)$$

where $R \in \mathbb{R}^{d \times}$ is random matrix with Euclidean column and $X_{RP} \in \mathbb{R}^{N \times k}$ is low dimension subspace with lower dimension which expected by k.

In this work, we use feature number reduction 2, 3, 5, 10, and 15 which is randomly chosen. Those several features are used to know the impact caused by random projection method with low number of features, then it can generate reliable detection method with low number of features.

D. Performance Evaluation

Classification performance of botnet detection is evaluated by using confusion matrix [26]. Confusion matrix is a table which used to represent number of data for each class which are classified correctly and number of data which are not

classified correctly. The confussion matrix considers number of true positive (TP) instances, true negative (TN) instances, false positive (FP) instances, and false negative (FP) instances. Number of thresh performance in confusion matrix measures accuracy, precision, sensitivity, specificity, false positive rate, and false negative rate. Evaluation performance can be defined using (2)-(8).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

$$Precision = \frac{TP}{TP+FP} \quad (3)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (4)$$

$$Specificity = \frac{TN}{TN+FP} \quad (5)$$

$$False\ Possitive\ Rate = \frac{FP}{TN+FP} \quad (6)$$

$$False\ Negative\ Rate = \frac{FN}{FN+TP} \quad (7)$$

E. Analysis Tool

In the experiments we perform simulation using computer with the specification: Intel core i7 processor 9th gen, DDR4 RAM 16GB, SSD 512GB, and NVIDIA GTX1660 Ti, with operation system using windows 10 64-bit and using Python programming language for analysis.

IV. Result, Discussion, And Comparison

In this section, we present the experimental results and discussion on the measured performance, and also similar related previous research works.

A. Results and Discussion

1) Accuracy

Table 2 shows accuracy of each feature reduction used in each classification algorithm. In general the small number of features used will result in decrement on accuracy. Only DT which not impacted its accuracy and has the highest accuracy of 100%.

TABLE II. Comparison of Accuracy

Classifier Algorithm	Number of Features				
	2	*3*	*5*	*10*	*15*
k-NN	98.64	99.86	99.98	99.98	99.99
DT	**100**	**100**	**100**	**100**	**100**
RF	99.99	99.99	100	100	100
AD	93.9	95.19	96.21	97.52	97.37
GB	96.52	98.48	99.39	99.76	99.8

2) Precision

Table 3 shows precision of each feature reduction used in each classification algorithm. Same as accuracy performance, in general, less number of features used will result in decrement on precision. Again DT is not impacted on its precision and has the highest precision, i.e.: 1.

TABLE III. Comparison of Precision

Classifier Algorithm	Number of Feature				
	2	*3*	*5*	*10*	*15*
k-NN	0.9789	0.9983	0.9997	0.9998	0.9998
DT	1	1	1	1	1
RF	0.9999	0.9999	1	1	1
AD	0.9013	0.9166	0.938	0.9607	0.9702
GB	0.9488	0.9796	0.9907	0.9957	0.9963

3) Sensitivity

Table 4 shows sensitivity of each feature reduction used in each classification algorithm. Slightly different with accuracy and precision metrics, sensitivity values are not impacted by feature reduction process for DT and RF and achieve the best value of 1. In contrast, for k-NN and GB the feature reduction process impacts the sentivity value, where the less number of fetures used decreases the sensitivity value. While AD has fluctuative sensitivity values.

TABLE IV. Comparison of Sensitivity

Classifier Algorithm	Number of Features				
	2	*3*	*5*	*10*	*15*
k-NN	0.9724	0.997	0.9989	0.9992	0.9994
DT	1	1	1	1	1
RF	1	1	1	1	1
AD	0.9649	0.9571	0.9843	0.9596	0.9652
GB	0.9436	0.9881	0.9928	0.9955	0.9958

4) Specificity

Table 5 shows specificity of each feature reduction used in each classification algorithm. Same pattern as sensitivity value, in general, less feature used will reduce specificity value. Only DT and RF are not impacted and has the highest specificity value of 1.

TABLE V. Comparison of Specificity

Classifier Algorithm	Number of Features				
	2	*3*	*5*	*10*	*15*
k-NN	0.9992	0.9999	0.9999	0.9999	0.9999
DT	1	1	1	1	1
RF	1	1	1	1	1
AD	0.9672	0.9729	0.9888	0.9959	0.9971
GB	0.995	0.9985	0.9988	0.9992	0.9992

5) False positive rate

Table 6 shows FPR of each feature reduction used in each classification algorithm. DT and RF are not impacted by feature reduction and has lowest value of 0. Different with k-NN which has lowest value when using 2 features but has highest FPR when used 3 features. Even for AD and GB, there are slightly increment FPR values when used lower number of features.

TABLE VI. COMPARISON OF FPR

Classifier Algorithm	Number of Features				
	2	*3*	*5*	*10*	*15*
k-NN	0.0008	8.5022	4.2479	2.5011	2.0042
DT	0	0	0	0	0
RF	0	0	0	0	0
AD	0.0328	0.0271	0.0111	0.0041	0.0028
GB	0.005	0.0015	0.0011	0.0008	0.0007

6) False negative rate

Table 7 shows FNR of each feature reduction used oinn each classification algorithm. Same condition as sensitivity value, because FNR is reflection of sensitivity. DT and RF are not impacted by feature reduction with value of 0. This is in contrast with k-NN and GB where more features used then result in increment of FNR. While, AD has fluctuative FNR values.

TABLE VII. COMPARISON FNR CLASSIFICATION

Classifier Algorithm	Number of Features				
	2	*3*	*5*	*10*	*15*
k-NN	0.0275	0.003	0.0011	0.0007	0.0006
DT	0	0	0	0	0
RF	0	0	0	0	0
AD	0.0351	0.0429	0.0157	0.0405	0.0347
GB	0.0564	0.0119	0.0072	0.0044	0.0042

7) Time Execution

Table 8 shows time execution of each feature reduction used in each classification algorithm. The use of feature reduction is very impactful on the detection process in term of execution time. It can be seen from all classification algorithms that use less number of features have faster execution time. DT has the fastest execution time of each feature used in each classification algorithm.

TABLE VIII. COMPARISON OF EXECUTION TIME (IN SECONDS)

Classifier Algorithm	Number of Features				
	2	*3*	*5*	*10*	*15*
k-NN	28.16	29.16	33.06	38.72	52.61
DT	8.44	9.42	13.27	19.83	29.42
RF	163.74	164.74	265.4	332.37	405.46
AD	81.98	88.69	94.71	133.22	175.67
GB	286.71	400.18	510.16	1019.45	1484.93

B. Comparison With Existing Related Works

After obtaining experiment results, we compare them with previous existing related research works that use same dataset as tabulated in Table 9. Comparison result shows that most of accuracy level decrease when using lower number of features. Only research results by Bahsi et al. [11] which use Fisher score method and k-NN classification algorithm that able to improve accuracy when using lower number of features. Nevertheless, random projection approach combined with DT classification algorithm implemented in this work performs better.

TABLE IX. COMPARISON ACCURACY WITH RELATED WORK

Ref	Method	Feature				
		2	*3*	*5*	*10*	*15*
[11]	Fisher score + DT	98.43	98.51		98.97	
	Fisher score + k-NN	98.05	97.24		94.97	
[12]	Entropy-SVM		93.15	92.33	88.27	
	Entropy-Iso. For		83.85	95.61	65.27	
	Variance-SVM		64.03	69.04	91.32	
	Variance-Iso. For		41.91	39.57	88.62	
	Hopkins-SVM		79.01	85.65	88.26	
	Hopkins-Iso.For		57.43	57.23	57.68	
Proposed approach	Random Projection-k-NN	98.64	99.86	99.98	99.98	99.99
	Random Projection-DT	**100**	**100**	**100**	**100**	**100**
	Random Projection-RF	99.99	99.99	100	100	100
	Random Projection-AD	93.9	95.19	96.21	97.52	97.37
	Random Projection-GB	96.52	98.48	99.39	99.76	99.8

V. CONCLUSION AND FUTURE WORK

Result of our experiment prove the importance to have approach or model which able to detect botnet IoT attack with fast time and accurate result. Our work has shown that using dimensionality reduction method which combined with DT classification able to detect botnet in 8.44s with accuracy level 100%, only using 2 feature. Proposed approach has been compared with multi classifier and also compared with same work, then approach random projection with DT shows better performance with using less feature compare to others. On the next work researcher will try to explore the impact of using dimensionality reduction method from other energy resource, and computational complexity.

REFERENCES

[1] S. Pokhrel, R. Abbas, and B. Aryal, "IoT Security: Botnet detection in IoT using Machine learning," *arXiv*, pp. 1–11, 2021.

[2] B. C. Chifor, I. Bica, V. V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 740–749, 2018.

[3] W. Jung, H. Zhao, M. Sun, and G. Zhou, "IoT botnet detection via power consumption modeling," *Smart Heal.*, vol. 15, no. December 2019, p. 100103, 2020.

[4] J. Kim, M. Shim, S. Hong, Y. Shin, and E. Choi, "Intelligent detection of iot botnets using machine learning and deep learning," *Appl. Sci.*, vol. 10, no. 19, pp. 1–22, 2020.

[5] K. Alieyan, A. Almomani, R. Abdullah, B. Almutairi, and M. Alauthman, "Botnet and Internet of Things (IoTs)," in *Security, Privacy, and Forensics Issues in Big Data*, no. February, 2019, pp. 304–316.

[6] C. H. Lee, Y. Y. Su, Y. C. Lin, and S. J. Lee, "Machine learning based network intrusion detection," *2017 2nd IEEE Int. Conf. Comput. Intell. Appl. ICCIA 2017*, vol. 2017–Janua, pp. 79–83, 2017.

[7] S. Miller and C. Busby-Earle, "The role of machine learning in botnet detection," *2016 11th Int. Conf. Internet Technol. Secur. Trans. ICITST 2016*, no. December, pp. 359–364, 2017.

[8] R. Abdulhammed, H. Musafer, A. Alessa, M. Faezipour, and A. Abuzneid, "Features dimensionality reduction approaches for machine learning based network intrusion detection," *Electron.*, vol. 8, no. 3, pp. 1–27, Mar. 2019.

[9] Y. Kiarashinejad, S. Abdollahramezani, and A. Adibi, "Deep learning approach based on dimensionality reduction for designing electromagnetic nanostructures," *npj Comput. Mater.*, vol. 6, no. 1, pp. 1–12, 2020.

[10] M. A. Salam, A. T. Azar, M. S. Elgendy, and K. M. Fouad, "The Effect of Different Dimensionality Reduction Techniques on Machine Learning Overfitting Problem," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 4, pp. 641–655, 2021.

[11] H. Bahsi, S. Nomm, and F. B. La Torre, "Dimensionality Reduction for Machine Learning Based IoT Botnet Detection," in *2018 15th International Conference on Control, Automation, Robotics and Vision, ICARCV 2018*, 2018, pp. 1857–1862.

[12] S. Nomm and H. Bahsi, "Unsupervised Anomaly Based Botnet Detection in IoT Networks," in *Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018*, 2019, pp. 1048–1053.

[13] M. Alqahtani, H. Mathkour, and M. M. Ben Ismail, "IoT Botnet Attack Detection Based on Optimized Extreme Gradient Boosting and Feature Selection," *Sensors*, vol. 20, no. 21, pp. 1–21, 2020.

[14] M. G. Desai, Y. Shi, and K. Suo, "IoT Bonet and Network Intrusion Detection using Dimensionality Reduction and Supervised Machine Learning," *2020 11th IEEE Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2020*, pp. 0316–0322, 2020.

[15] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, "Botnet Attack Detection using Machine Learning," in *Proceedings of the 2020 14th International Conference on Innovations in Information Technology, IIT 2020*, 2020, no. November, pp. 203–208.

[16] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici., "N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Sep. 2018.

[17] S. Suthaharan, *A Cognitive Random Forest: An Intra- and Intercognitive Computing for Big Data Classification Under Cune Condition*, 1st ed., vol. 35. Elsevier B.V., 2016.

[18] B. Charbuty and A. Abdulazeez, "Classification Based on Decision Tree Algorithm for Machine Learning," *J. Appl. Sci. Technol. Trends*, vol. 2, no. 01, pp. 20–28, 2021.

[19] A. Rehman Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, and X. Liu, "Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Trans. Emerg. Telecommun. Technol.*, no. June, pp. 1–18, 2020.

[20] H. Saadatfar, S. Khosravi, J. H. Joloudari, A. Mosavi, and S. Shamshirband, "A new k-nearest neighbors classifier for big data based on efficient data pruning," *Mathematics*, vol. 8, no. 2, pp. 1–12, 2020.

[21] S. Rahman, M. Irfan, M. Raza, K. M. Ghori, S. Yaqoob, and M. Awais, "Performance analysis of boosting classifiers in recognizing activities of daily living," *Int. J. Environ. Res. Public Health*, vol. 17, no. 3, 2020.

[22] E. Bingham and H. Mannila, "Random projection in dimensionality reduction: Applications to image and text data," *Math. Educ.*, vol. 11, no. 6, pp. 1495–1503, 2016.

[23] H. Xie, J. Li, and H. Xue, "A survey of dimensionality reduction techniques based on random projection," *arXiv*, pp. 1–10, 2017.

[24] T. I. Cannings, "Random projections: Data perturbation for classification problems," *Wiley Interdiscip. Rev. Comput. Stat.*, vol. 13, no. 1, pp. 1–24, 2021, doi: 10.1002/wics.1499.

[25] C. Grellmann, J. Neumann, S. Bitzer, P. Kovacs, A. Tonjes, L. T. Westly, O. A. Andreassen, M. Stumvoll, A. Villringer, and A. Horstmann., "Random projection for fast and efficient multivariate correlation analysis of high-dimensional data: A new approach," *Front. Genet.*, vol. 7, no. JUN, pp. 1–19, 2016.

[26] A. Tharwat, "Classification assessment methods," *Appl. Comput. Informatics*, vol. 17, no. 1, pp. 168–192, 2018.

A Dimensionality Reduction Approach for Machine Learning Based IoT Botnet Detection

ORIGINALITY REPORT

14%
SIMILARITY INDEX

PRIMARY SOURCES

1	www.mdpi.com Internet	60 words — 2%
2	Susanto, Deris Stiawan, M. Agus Syamsul Arifin, Mohd. Yazid Idris, Rahmat Budiarto. "IoT Botnet Malware Classification Using Weka Tool and Scikit-learn Machine Learning", 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), 2020 Crossref	41 words — 1%
3	hull-repository.worktribe.com Internet	39 words — 1%
4	journal.frontiersin.org Internet	39 words — 1%
5	online-journals.org Internet	24 words — 1%
6	link.springer.com Internet	21 words — 1%
7	Deris Stiawan, Mohd. Yazid Idris, Reza Firsandaya Malik, Siti Nurmaini, Rahmat Budiarto. "Anomaly detection and monitoring in Internet of Things communication",	19 words — 1%

2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), 2016
Crossref

8 Kurniabudi, Abdul Harris, Albertus Edward Mintaria, Darmawijoyo, Deris Stiawan, Mohd Yazid bin Idris, Rahmat Budiarto. "Improving the Anomaly Detection by Combining PSO Search Methods and J48 Algorithm", 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), 2020
Crossref
16 words — 1%

9 Mustafa Alshamkhany, Wisam Alshamkhany, Mohamed Mansour, Mueez Khan, Salam Dhou, Fadi Aloul. "Botnet Attack Detection using Machine Learning", 2020 14th International Conference on Innovations in Information Technology (IIT), 2020
Crossref
15 words — 1%

10 www.oncotarget.com
Internet
13 words — < 1%

11 Madhuri Gurunathrao Desai, Yong Shi, Kun Suo. "IoT Bonet and Network Intrusion Detection using Dimensionality Reduction and Supervised Machine Learning", 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020
Crossref
12 words — < 1%

12 www.mysciencework.com
Internet
12 words — < 1%

13 repository.tudelft.nl
Internet
11 words — < 1%

14 arxiv.org
Internet
10 words — < 1%

15	ascelibrary.org Internet	10 words — < 1%
16	S. Suthaharan. "A Cognitive Random Forest", Elsevier BV, 2016 Crossref	9 words — < 1%
17	"Machine Learning and Data Mining for Emerging Trend in Cyber Dynamics", Springer Science and Business Media LLC, 2021 Crossref	8 words — < 1%
18	export.arxiv.org Internet	8 words — < 1%
19	section.iaesonline.com Internet	8 words — < 1%
20	www.arxiv-vanity.com Internet	8 words — < 1%
21	www.nature.com Internet	8 words — < 1%
22	"Soft Computing and Signal Processing", Springer Science and Business Media LLC, 2021 Crossref	7 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	ON	EXCLUDE MATCHES	OFF