Feature Selection Strategy for Network Intrusion Detection System (NIDS) Using Meerkat Clan Algorithm

https://doi.org/10.3991/ijim.v15i16.24173

Atheer R. Muhsen[1], Ghazwh G. Jumaa[1], Nadia F. AL Bakri[2(✉)], Ahmed T. Sadiq[1]
[1]University of Technology, Baghdad, Iraq
[2]AL Nahrain University, Baghdad, Iraq
Nadiaf_1966@yahoo.com

Abstract—The task of network security is to keep services available at all times by dealing with hacker attacks. One of the mechanisms obtainable is the Intrusion Detection System (IDS) which is used to sense and classify any abnormal actions. Therefore, the IDS system should always be up-to-date with the latest hacker attack signatures to keep services confidential, safe, and available. IDS speed is a very important issue in addition to learning new attacks. A modified selection strategy based on features was proposed in this paper one of the important swarm intelligent algorithms is the Meerkat Clan Algorithm (MCA). Meerkat Clan Algorithm has good diversity solutions through its neighboring generation conduct and it was used to solve several problems. The proposed strategy benefitted from mutual information to increase the performance and decrease the consumed time. Two datasets (NSL-KDD & UNSW-NB15) for Network Intrusion Detection Systems (NIDS) have been used to verify the performance of the proposed algorithm. The experimental findings indicate that, compared to other approaches, the proposed algorithm produces good results in a minimum of time.

Keywords—meerkat clan algorithm, selection of features, NIDS, NSL-KDD, UNSW-NB15

1 Introduction

Computer network attacks are several bad things so that information and services within computer networks are damaged, denied, and degenerated or destructed. In the field of computation, multiple attacks and security breaches now face the increasing risk of unintentional downtime. Intrusion Detection Network (NID) is an intrusion detection mechanism that attempts to detect unauthorized access to a computer network for signs of malicious activity through analysis of network traffic. In this huge area of Network Intrusion Detection (NID), several fields of study exist. An IDS (Intrusion Detection System) is a key element in the defense of the network these days, as it provides complete network support, IDS detects effective and failing intrusion efforts. The IDS aims at reporting all irregular device activity and identifying all non-antiques negatively. IDS will offer real-time reactions to any of these intrusion events by studying

activities closely and signing intrusion detection [1–3]. Because of the huge data with a large number of features, the demand for constructing a suitable machine learning model is demanded. Two approaches are used for dimensionality reduction, they are: feature extraction, which includes building a new feature space with low dimensionality, and the other approach is feature selection that emphasizes irrelevant and redundant features removal from the original feature set. The Extensive search to find the optimal feature subset is not possible in a rational time and might reduce the classifier's performance [2]. Thus many binary meta-heuristic algorithms are used to approximate the optimal solution by removing irrelevant features within a suitable computational time. Meta-heuristic algorithms are known as natural-based algorithms that are more appealing than conventional approaches for resolving optimization problems [4–6]. They function without derivatives and thus are suitable for high-dimensional space problems. The optimization process can go through two steps in any population-based meta-heuristic algorithm; they are exploration (diversification) where the algorithm explores the entire search space intending to find the likely states that may contain the global optima. In exploitation (intensification), the algorithm attempts to search the neighborhood of each solution state found in the exploration stage [7–11]. Feature selection methods choose attributes from original spaces set based on strategies like information gain, correlation, and decision table. Hall and Smith [3] proposed a subset of attributes to be related if these attributes are high connection with class and are not connected in terms of mutual information. Feature selection offers many advantages some of them are illustrated below: [12–13]

- It diminishes feature dimensionality also supports getting the better performance of the algorithm.
- It discards unnecessary, extraneous, or noisy data.
- It makes efficient data goodness which helps to get better the performance of learning technique.
- It enhances the precision of the output model.
- It assists in data grasp to acquire knowledge about the operation that created the data.

This paper presents a review of comparing between machine learning classification methods applied to analysis NSL-KDD dataset and UNSW-NB15 dataset then using some algorithms for feature selection to decrease the dimensionality of the datasets, then using the same classification methods and compare the results of different feature selection methods.

In this paper, have been introduced to identify network attacks with the aid of Random Forest and Modified Random Forest via Meerkat Clan Algorithm on NSL-KDD dataset and UNSW-NB15 dataset. So we sometimes need to increase searches in features to get the best of them.

2 Related work

In [14], It has been suggested to use a feature selection technique based on the Updated Artificial Immune System (MAIS). The proposed algorithm takes advantage of the benefits of the Artificial Immune System (AIS) to improve functional efficiency

and randomization. The experimental findings, which were based on the NSL-KDD dataset, revealed improved accuracy as compared to other feature selection algorithms (best first search, correlation, and information gain). In [15], The NSL-KDD dataset was used to characterize the network attack using five essential classification methods and three feature selection strategies. These techniques are (J48 decision tree, support vector machine, decision table, and Bayesian network). Several studies were carried out to achieve successful results by using NSL-KDD for preparation and checking in general attack (normal and anomaly) scenarios (within 4 attacks U2R, R2L, Probe, DO). In [16]. gives an insight into the existing Intrusion Detection Systems (IDS) along with their basic principles. Furthermore, it discusses how data mining with its core feature (knowledge discovery) can help to create a data mining based on IDS. The resulted data mining may demonstrate more solid behavior comparing with traditional IDS and accomplish a higher accuracy to instruction's unique types. In [17], Using the NSL-KDD dataset, various classification algorithms (J48, SVM, and Nave Bayes) were used and analyzed. These algorithms are used to find anomalies in the packets of a network. Furthermore, the NSL-KDD dataset is used to deduce the protocols' connections from the commonly used network protocol stack from an intruders' attack that results in irregular network traffic. In [18], Mostafa and Slay released the latest big UNSW-NB15 dataset, which contains features not included in the KDD'99 dataset. Only a few different features connect the UNSW-NB15 and KDD'99 datasets, making comparison difficult. This research examines the features used in the UNSW-NB15 dataset to minimize the number of features (the curse of dimensionality) and proposes a subset of features that are more relevant in detecting network traffic intrusions. In addition, the analyses can be compared to the KDD'99 dataset to see where the correlations and differences lie.

3 Feature selection methods via metaheuristics

The process that selects a subgroup of features based on certain criteria from all the available features is called feature selection. The criterion is utilized to increase classification performance. Feature selection approaches can be divided into two categories: The search space is decomposed into four classes; they are: "exhaustive", "random", "heuristic", "meta-heuristic". And the other is the strategy-based techniques which are decomposed into filter and wrapper feature selection approach [19–23].

In general, feature selection methods can be divided into three basic classes: wrapper, filter, and embedded methods. Wrapper methods utilize a learning algorithm iteratively to evaluate the truthfulness of selected feature subsets via classification accuracy. It is known to be more accurate, but it is computationally more expensive. Filter methods, however, are independent of any classification algorithms. The characteristics of the dataset are used to measure the relevance between a feature and the target label using measures such as distance and consistency. The feature selection using the filter approach is performed in one iteration, so they are easily scalable to high dimensions. In the embedded method; the learning algorithm is embedded with no iterative evaluations for the classification accuracy of the feature subset like in wrapper approaches.

During the training phase, the feature coefficients are set by minimizing the fitting miscalculations. Then, the selected features are resultant from the feature coefficients. Therefore, this method is suitable for high dimensional feature selection domains [5] [19] [20] [24–27].

4 Meerkat clan algorithm

The careful observation of the behavior of certain living things can illustrate how they plan their natural behavior into algorithms. This is why nature-stimulated algorithms are the new meta-heuristics discussed in this work. These new methods are meta-heuristics of global optimization, mainly gathered by selecting the best structure and by randomizing structures. The previous guiding principles, the algorithm combining to the optimal (use) and the far ahead prevents the lack of variety and the algorithm to limit local optima. Strong stability between use and research may lead to the achievement of global optimism. Meerkats are animals living socially in colonies of 5 to 30 people. They exchange both toilet and parenting duties, as sociable beings. Each mob has a male and a female alpha leader. Each mob has its ground where they sometimes move when no food is found or a tougher mob is forced to find. When the second occurs, the weaker mob tries to widen or stay until it gets tougher and retrieves the lost burrow. Every mob also has what is called a 'watchman,' that is to say, a person guarding the mob and when it can detect risks and tell the rest if there is a danger. The watcher watches either from the ground or from a tree or through the bushes. The watchman looks at both the burrow system and the other members of the mob feed for food. When a risk is observed, the watchman gives a loud bark sound, and the mob bolts quickly into its hiding holes [28].

The general steps below for MCA, which may be modified depending on the problems encrypted, are the prior explanation of Meerkat animal-inspired MCA [29–32].

a. Initialization: create a random clan of people and set the clan size, foraging size, care size, and the worst feed and caring rates of the other parameters.
b. Compute the fitness for the clan
c. Choose the best one as 'sentry'
d. Divide the clan into two groups (foraging & care)
e. Generate neighbors for foraging group
f. Select the worst people in the food and swap with the best people in the care group
g. Drop the worst in the care community and randomly construct another person
h. Substitute the best person for sentry, if best.

5 Proposal approach

There are several randomly feature selection methods, some of these depend on pure randomization, others depend on nature and swarm intelligence-inspired algorithms.

This paper presents an approach as a features selection algorithm based on MCA, the proposed algorithm is a wrapper feature selection type. In our approach, MCA has a good diversification and exploration, therefore, it produces a wide space from diversified solutions that goes back to its various stages and neighbors generation strategy. Initially, our proposed algorithm will drop the worst features depend on Mutual Information (MI), then generate random solutions (features), evaluate these solutions based on the classification method, select the best solution as the best features, divide the rest into 2 groups working and spare. Evaluate these features based on accuracy values of the classification method; select the best accuracy as best features. The main loop of MCA including the processing of the classical step of MCA on the working and spare groups. The neighbor's generation functions play a big role to diverse the solutions (features) then stay the betters in the working group, the worst (Fr) of the working group will immigrate to the spare group and replaced by the best ones from the spare group. The worst (Cr) of the spare group will be replaced by random ones. Through these steps, the population of features (solutions) has been getting better or improve. The steps of Mutual Information – Meerkat Clan Algorithm (MIMCA) for features selection are shown in the below algorithm.

```
Mutual Information – Meerkat Clan Algorithm (MIMCA)
Input: Parameters of MCA; X: Set of Features; Threshold;
Output: Best Subset Features;
Begin
    Find the Mutual Information (MI) value of X features;
    Drop the worst features (less than the Threshold value);
    A subset of Features F = The Remain Features;
    Initialize random solutions from a set of F;
    Evaluate these features using classification method;
    Best Features = best solution (features);
    Divide the solutions into two groups, working (m) &spare (c) (unless sentry);
    While terminated condition not met Do
            For i=1 to m
                Call neighbor_generat (NG, Best_Features, working(i),
            best_one);
                Working (i) = best_one from NG neighbors;
            end for
              Swap the worst Fr solutions in working group by best ones'
            solution in the spare group;
              Drop the worst Cr solutions from the spare group and generate
            ones' solution randomly;
              Evaluate the features in working and spare groups using clas-
            sification method;
            If there is a features best than Best_Features Then
              Best_Features=best features;
        end while
End
Output: best solutions.
```

The step of MI will decrease the consumed time of the MIMCA approach because the worst has been dropped, which to focus on the important real features.

6 Experimental results

6.1 Datasets and MIMCA parameters

Two standard NID datasets have been selected to verify the performance of the proposed two approaches, NSL-KDD and UNSW-NB15. Table (1) & (2) illustrate the features of NSL-KDD and description of NSL-KDD attacks respectively, Table (3) & (4) illustrate the features of UNSW-NB15 and description of UNSW-NB15 attacks respectively.

Table 1. The 41 features of the NSL-KDD dataset

#	Feature	#	Feature
1	duration	22	is_guest_login
2	protocol_type	23	Count
3	service	24	srv_count
4	flag	25	serror_rate
5	src_bytes	26	srv_serror_rate
6	dst_bytes	27	rerror_rate
7	Land	28	srv_rerror_rate
8	wrong_fragment	29	same_srv_rate
9	Urgent	30	diff_srv_rate
10	Hot	31	srv_diff_host_ra
11	num_failed_logins	32	dst_host_count
12	logged_in	33	dst_host_srv_count
13	num_compromised	34	dst_host_same_srv_rate
14	root_shell	35	dst_host_diff_srv_rate
15	su_attempted	36	dst_host_same_src_port_rate
16	num_root	37	dst_host_srv_diff_host_rate
17	num_file_creations	38	dst_host_serror_rate
18	num_shells	39	dst_host_srv_serror_rate
19	num_access_files	40	dst_host_rerror_rate
20	num_outbound_cmds	41	dst_host_srv_rerror_rate
21	is_host_login		

Table 2. Attacks types description of NSL-KDD dataset

Type	Description	Training No.	Testing No.
Normal	Normal transaction data.	67343	9711
DoS	Is an attack class that exhaustion the victim's resources as a result of that making the victim unable to process the request this would shut down the intended device or flood it in requests and therefore the authorized users cannot reach the device services, For example, ping to death and syn. flood.	45927	7458
Probe	Is trying to collect a datum on a Net and detect the system vulnerabilities. These vulnerabilities will take advantage to intrude the system. For example, Port scanning	11656	2421
U2R	Is it a type of attack that takes the advantage of authorized users and tries to reach the root of the system from some vulnerability? For example, buffer overflows attack."	52	200
R2L	Occurs when an attacker who can send a stream of bits to a device in a network but this attacker doesn't have an account on that device exploits some vulnerability to obtain local access to that device. For example password guessing."	995	2654

Table 3. The 42 features of the UNSW-NB15 dataset

#	Feature	#	Feature
1	dur	22	synack
2	spkts	23	ackdat
3	dpkts	24	smean
4	Sbytes	25	dmean
5	dbytes	26	trans_depth
6	rate	27	response_body_len
7	sttl	28	ct_srv_src
8	dttl	29	ct_state_ttl
9	sload	30	ct_dst_ltm
10	dload	31	ct_src_dport_ltm
11	slosis	32	ct_dst_sport_ltm
12	dloss	33	ct_dst_src_ltm
13	sinpkt	34	is_ftp_logn
14	dinpkt	35	ct_ftp_cmd
15	sjit	36	ct_flw_http_mthd
16	djit	37	ct_src_ltm
17	swin	38	ct_srv_dst
18	stcpb	39	is_sm_ips_ports
19	dtcpb	40	proto
20	dwin	41	service
21	tcprtt	42	State

Table 4. Attacks types description of UNSW-NB15 dataset

Type	No. Records	Description
Normal	2,218,761	Natural transaction data.
Fuzzers	24,246	Trying to bring a program or a network to a halt by feeding it randomly generated data.
Analysis	2,677	It includes a variety of port search, malware, and HTML file penetration attacks.
Backdoors	2,329	A method of gaining unauthorized access to a device or its data by circumventing a system authentication process invisibly.
DoS	16,353	A deliberate effort to prevent users from accessing a server or network resource, normally by momentarily interrupting or halting the services of a host connecting to the Internet.
Exploits	44,525	The attacker is aware of a security flaw in an operating system or piece of software and takes advantage of it by exploiting the flaw.
Generic	215,481	Without regard for the structure of the block cipher, a technique operates against all block ciphers (with a given block and key size).
Reconnaissance	13,987	This section contains all Strikes that can be used to mimic intelligence-gathering attacks.
Shellcode	1,511	A payload is a short piece of code that is used to hack a software flaw.
Worms	174	To propagate to other machines, the attacker replicates itself. It often spreads through a computer network, depending on security bugs on the target computer to obtain access.

Table 5. Shows the parameters of MIMCA which is choice to execute the experimental results

Parameter	Value
Meerkat Clan Size	80–100
Foraging group	50–60
Care group	29–39
Sentry	1
Threshold	0.15–0.2
NG : No. of Generated Neighbors	3–5
Max. Iteration	100–130
Fr : Worst Foraging Ratio	0.15
Cr : Worst Care Ratio	0.2

The experimental work is carried out using ORANGE [15] which is open-source data mining software and Python programming language.

6.2 Experiments based on the NSL-KDD dataset

NSL-KDD The data collection is split into two parts: preparation and research. Models based on MIMCA are trained first, then evaluated on different partitions of the data set. Table 6 shows the precision of the MIMCA model for various versions. In our experiments, 4 classification methods have been used DT: Decision Tree, BP-NN: Back-Propagation Neural Network, NB: Naïve Bayes, and Apriori algorithm. As a feature selection, we are used the proposed MIMCA and MI (Mutual Information),.

Table 6. Accuracy ratio for NSL-KDD dataset based on MIMCA and MI using 4 classification methods

Model	Feature Selection Method	No. of Features	Accuracy
Apriori	MIMCA	17	99.85%
Apriori	None	All	99.85%
DT	MIMCA	17	97.89%
DT	MI	17	97.89%
BP-NN	MIMCA	17	96.12%
BP-NN	MI	21	97.04%
NB	MIMCA	17	91.8%
NB	MI	21	95%

MIMCA obtained a result same as MI in DT and Apriority algorithm, but in less time, Table 7 illustrates the consumed time of experiments in Table 5.

Table 7. Average consumed time for NSL-KDD dataset based on MIMCA and MI using 4 classification

Model	Feature Selection Method	Consumed Time (Sec.)
Apriori	MIMCA	6.3
Apriori	None	175.4
DT	MIMCA	2.1
DT	MI	14.7
BP-NN	MIMCA	3.9
BP-NN	MI	66.1
NB	MIMCA	2.3
NB	MI	8.5

The final 17 selected features from NSL-KDD using MIMCA (with Apriority) are {5, 3, 6, 4, 30, 29, 33, 34, 35, 38, 12, 39, 25, 23, 26, 37, 32}. These features for all categories of the NSL-KDD dataset.

In addition to, using MIMCA to find the features selected for the category in NSL-KDD, Table 8 illustrates the best features for each category in the NSL-KDD dataset.

Table 8. Best features of each category in NSL-KDD dataset based on MIMCA

Category	Best Features Using MIMCA
Normal	3,37,36,30,38,12,22,39,16,20,15
DoS	30,4,39,25,26,38,5,32,2,3,37
Probes	36,23,24,12,6,39,8,10,16,7,11
R2L	1,10,7,6,21,38,9,8,3,27,31
U2R	13,17,14,10,15,14,30,33,31,36,3

6.3 Experiments based on the UNSW-NB15 dataset

In the UNSW-NB15 dataset, the experiments did not include the normal cases, they include only attacks. MIMCA based feature selection method has been found the best features for all categories of the UNSW-NB15 dataset. The accuracy of the MIMCA model with different models is shown in Table 9. In our experiments, 4 classification methods have been used DT: Decision Tree, BP-NN: Back-Propagation Neural Network, NB: Naïve Bayes, and Apriori algorithm. As a feature selection, we are used the proposed MIMCA and MI (Mutual Information).

Table 9. Accuracy ratio for UNSW-NB15 dataset based on MIMCA and MI using 4 classification methods

Model	Feature Selection Method	No. of Features	Accuracy
Apriori	MIMCA	13	87.74%
Apriori	None	All	87.74%
DT	MIMCA	13	85.56%
DT	MI	14	85.56%
BP-NN	MIMCA	16	80.16%
BP-NN	MI	16	81.34%
NB	MIMCA	14	80.21%
NB	MI	18	82.07%

Also, MIMCA obtained a result same as MI in DT and Apriori algorithm, but in less time, Table 10 illustrates the consumed time of experiments in Table 8.

Table 10. Average consumed time for UNSW-NB15 dataset based on MIMCA and MI using 4 classification methods

Model	Feature Selection Method	Consumed Time (Sec.)
Apriori	MIMCA	18.8
Apriori	None	175.4
DT	MIMCA	6.4
DT	MI	44.1
BP-NN	MIMCA	10.1
BP-NN	MI	178.5
NB	MIMCA	7.6
NB	MI	25.2

The final 17 selected features from UNSW-NB15 using MIMCA are {8, 9, 11, 12, 32, 10, 13, 28, 4, 42, 36, 7, 33, 29, 3, 41, 18}. These features for all categories of the UNSW-NB15 dataset.

In addition to, using MIMCA to find the features selected for the category in UNSW-NB15, Table 11 illustrates the best features for each category in the UNSW-NB15 dataset.

Table 11. Best features of each attack category in UNSW-NB15 dataset based on MIMCA

Category	Best Features Using MIMCA
DoS	6,11,15, 16,36,37,39,40,42,44,45
Fuzzers	6,11,14,15,16,36,37,39,40,41,42
Backdoors	6,10,11,14,15,16,37,41,42,44,45
Exploits	10,41,42,6,37,46,11,19,36,5,45
Analysis	6,10,11,12,13,14,15,16,34,35,37
Generic	6,9,10,11,12,13,15,16, 17,18,20
Reconnaissance	10,14,37,41,42,43,44,9,16,17,28
Shellcode	6,9,10,12,13,14,15,16,17,18,23
Worms	41,37,9,11,10,46,23,17,14,5,13

Essentially, the extracted features did not differ from several feature selection methods and classification techniques, but the consumed time is less than several methods, this is for both NSL-KDD and UNSW-NB15 datasets. This indicates that the MIMCA is an efficient feature selection technique within less time. Of course, some methods give results best than MIMCA, because it depends on the power of classification methods.

7 Conclusion

MIMCA is a feature selection technique that is proposed and evaluated in this paper. It is based on the diversification of candidate solutions in the MCA, which leads to improving these solutions during the MCA stages. The experiments on two important NID datasets (NSL-KDD & UNSW-NB15) verified that the MIMCA is a good technique for feature selection. The selected features are the same as most good standard methods but in the least consumed time. In the future, our objective aim to MCA for classified rules generation like association rules mining.

8 References

[1] N. Sultana, N. Chilamkurti, W. Peng, and R. J. N. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches", Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, 2019. https://doi.org/10.1007/s12083-017-0630-0

[2] D. Ibrahim, and N. M. Al-ruhaily, "Anomaly Detection in Wireless Sensor Networks: A Proposed Framework", International Journal of Interactive Mobile Technologies, vol. 14, no. 10, 2020. https://doi.org/10.3991/ijim.v14i10.14261

[3] M. Ibrahim, I. Obeidat, and N. Hamadneh, "Intensive Pre-Processing of KDD Cup 99 for Network Intrusion Classification Using Machine Learning Techniques", International Journal of Interactive Mobile Technologies, vol. 13, no. 1, 2019. https://doi.org/10.3991/ijim.v13i01.9679

[4] N. S. Alseelawi, E. K. Adnan, H. T. Hazim, H. T. S. Alrikabi, and K. W. Nasser, "Design and implementation of an e-learning platform using N-tier architecture", International Journal of Interactive Mobile Technologies, Article vol. 14, no. 6, pp. 171–184, 2020. https://doi.org/10.3991/ijim.v14i06.14005

[5] T. Shokooh, and M. H. Nadimi-Shahraki, "A binary metaheuristic algorithm for wrapper feature selection" International Journal of Computer Science Engineering (IJCSE) 8.5, pp. 168–172, 2019

[6] N. A. Hussien, H. A. Naman, M. Al-Dabag, Haider T. H. Salim, "Encryption System for Hiding Information Based on Internet of Things", International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[7] B. Lucija, and ViliPodgorelec, "Swarm intelligence algorithms for feature selection: a review." Applied Sciences 8.9, 1521, 2018. https://doi.org/10.3390/app8091521

[8] de Rosa, H. Gustavo, João P. Papa, and Xin-She Yang. "A Nature-Inspired Feature Selection Approach Based on Hypercomplex Information", Applied Soft Computing 2020: 106453. https://doi.org/10.1016/j.asoc.2020.106453

[9] B. Nupur, and S. Gupta, "Swarm Intelligence Based Nature Inspired Metaheuristics Used for Selecting Features in Opinion Mining", Available at SSRN 3566789, 2020.

[10] A. Almomani, O. hammed Alweshah, and Al. Saleh, "Metaheuristic Algorithms-Based Feature Selection Approach for Intrusion Detection", Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices 2019: 184. https://doi.org/10.1201/9780429504044-8

[11] M. Majdi, et al. "Feature Selection Using Binary Particle Swarm Optimization with Time Varying Inertia Weight Strategies", Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, 2018.

[12] D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection aMachine Learning Perspective", London. A Chapman and Hall Inc, 2014. https://doi.org/10.1201/b15088

[13] M. Almseidin, A. Abu Zuraiq, M. Al-kasassbeh, and N. Alnidami, "Phishing Detection Based on Machine Learning and Feature Selection Methods", International Journal of Interactive Mobile Technologies, vol. 13, no. 12, 2019. https://doi.org/10.3991/ijim.v13i12.11411

[14] A. Sadiq and J. H. Assi, "Modified Artificial Immune System as Feature Selection", Iraqi Journal of Science, vol. 59, no. 2A, pp. 733–738. 2018. https://doi.org/10.24996/ijs.2018.59.2A.11

[15] T. Sadiq, and J. H. Assi, "NSL-KDD Dataset Classification using Five Classification Methods and Three Feature Selection Strategies", Iraq, JACSTR, vol. 7, no. 1, 2017.

[16] M. Al-dabag, H. T. Salim, and R. Al-Nima, "Anticipating Atrial Fibrillation Signal Using Efficient Algorithm", International Journal of Online and Biomedical Engineering (iJOE), vol. 17, no. 2, pp. 106–120, 2021. https://doi.org/10.3991/ijoe.v17i02.19183

[17] H. Majeed, L. F. Jawad Haider Th. Salim, "Tactical Thinking and its Relationship with Solving Mathematical Problems Among Mathematics Department Students", International Journal of Emerging Technologies in Learning (iJET), vol. 16, no. 9, pp. 247–262, 2021. https://doi.org/10.3991/ijet.v16i09.22203

[18] N. Moustafa and J. Slay, "Unsw-nb15: A comprehensive data set for network intrusion detection", in MilCIS-IEEE Stream, Military Communications and Information Systems Conference. Canberra, Australia, IEEE publication, 2015. https://doi.org/10.1109/MilCIS.2015.7348942

[19] S. M. Najeeb, H. Al Rikabi, and S. M. Ali, "Finding the Discriminative Frequencies of Motor Electroencephalography Signal Using Genetic Algorithm", Telkomnika (Telecommunication Computing Electronics and Control), Article vol. 19, no. 1, pp. 285–292, 2021. https://doi.org/10.12928/telkomnika.v19i1.17884

[20] L. Wei, and J. Wang, "A brief survey on nature-inspired metaheuristics for feature selection in classification in this decade", IEEE 16th International Conference on Networking, Sensing and Control (ICNSC). IEEE, 2019.

[21] M. Rozlini, M. Yusof, and N. Wahidi, "A Comparative Study of Feature Selection Techniques for Bat Algorithm in Various Applications", MATEC Web of Conferences. vol. 150. EDP Sciences, 2018. https://doi.org/10.1051/matecconf/201815006006

[22] A. S. Hussein, R. S. Khairy, and H. Salim, "The Detection of Counterfeit Banknotes Using Ensemble Learning Techniques of AdaBoost and Voting", International Journal of Intelligent Engineering and Systems, vol. 14, no. 1, pp. 326–339, 2021. https://doi.org/10.22266/ijies2021.0228.31

[23] T. Ahmed Majid, A. Mustapha, and S. Der Chen, "Naive Bayes-guided bat algorithm for feature selection", The Scientific World Journal, 2013. https://doi.org/10.1155/2013/325973

[24] Yusta, Silvia Casado. "Different metaheuristic strategies to solve the feature selection problem", Pattern Recognition Letters 30.5, pp. 525–534, 2009. https://doi.org/10.1016/j.patrec.2008.11.012

[25] N. F. AL-Bakri, and S. H., Hashim, "A Modified Similarity Measure for Improving Accuracy of User-Based Collaborative Filtering", Iraqi Journal of Science, vol. 59, no. 2B, pp. 934–945, 2018. https://doi.org/10.24996/ijs.2018.59.2B.15

[26] N. F. AL-Bakri, and S. H., Hashim, "A Study on the Accuracy of Prediction in Recommendation System Based on Similarity Measures", Baghdad Science Journal, vol. 16, no. (1 Supplement), pp. 263–269, 2019. https://doi.org/10.21123/bsj.2019.16.1(Suppl.).0263

[27] N. F. AL-Bakri and S. Hassan, "A Proposed Model to Solve Cold Start Problem using Fuzzy User-Based Clustering", (SCCS) Mar 27, pp. 121–125, IEEE, 2019. https://doi.org/10.1109/SCCS.2019.8852624

[28] O. Zied , A. T. Sadiq Al Obaidiand, and H. S. Abdullah, "Meerkat Clan Algorithm: A New Swarm Intelligence Algorithm", Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 1, pp. 354–360, 2018. https://doi.org/10.11591/ijeecs.v10.i1

[29] N. F. AL-Bakri, and S. H., Hashim, "Collaborative Filtering Recommendation Model Based on k-means Clustering", Al-Nahrain Journal of Science, vol. 22, no. 1, pp. 74–79, 2019. https://doi.org/10.22401/ANJS.22.1.10

[30] N. F. AL-Bakri, A. F. Al-zubidi, A. B. Alnajjar, and E. Qahtan, Multi label restaurant classification using support vector machine. Periodicals of Engineering and Natural Sciences (PEN), 9(2), pp. 774–783, 2021.

[31] K. Mohammed, M. B. Mortatha, A. S. Abdalrada, H. ALRikabi, and N. Sciences, "A comprehensive system for detection of flammable and toxic gases using IoT", Periodicals of Engineering and Natural Sciences (PEN), vol. 9, no. 2, pp. 702–711, 2021.

[32] Zied O. Ahmed, Ahmed T. Sadiq Al Obaidi and Hasanen S. Abdullah, "Solving Flexible Job Shop Scheduling Problem Using Meerkat Clan Algorithm", Iraqi Journal of Science, vol. 59, no. 2A, pp. 754–761, 2018. https://doi.org/10.24996/ijs.2018.59.2A.13

9 Authors

Atheer R. Muhsen In 2001, he earned a B.Sc. in Computer Science from Baghdad University in Iraq. In 2017, he earned an M.Sc. in Computer Science from the University

of Technology in Baghdad, Iraq. Artificial intelligence methods and implementations, as well as the comuter network, are among his research interests.

Ghazwh G. Jumaa In 2006, she earned a B.Sc. in Computer Science from the University of Technology in Baghdad, Iraq. She earned an M.Sc. in Computer Science from the University of Technology in Baghdad, Iraq, in 2017. Artificial intelligence methods and technologies, as well as computer security, are among her research interests.

Nadia F.AL-Bakri received a B.Sc. degree in Computer Science from the University of Technology, Baghdad, Iraq, in 1988. In 2009 received M.Sc. degree in Computer Science from AL Nahrain University, Baghdad, Iraq & the Ph. D. degree in Computer Science from the University of Technology, Computer Science Department, Iraq in 2020. Her research interests in Artificial intelligence, Recommender System, Machine Learning & Web Security.

Ahmed T. Sadiq In 1993, 1996, and 2000, he earned a B.Sc., M.Sc., and Ph. D. in Computer Science from the University of Technology, Computer Science Department, Iraq. Since 2014, he has been a Professor of Artificial Intelligence. Artificial intelligence, computer security, pattern detection, and data mining are some of his research interests.

Article submitted 2021-05-20. Resubmitted 2021-06-26. Final acceptance 2021-06-27. Final version published as submitted by the authors.