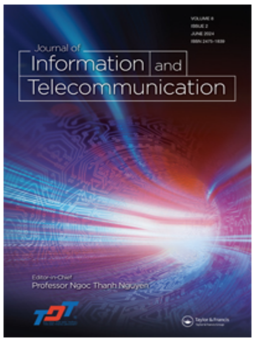

Feature selection in intrusion detection systems: a new hybrid fusion of Bat algorithm and Residue Number System

Yakub Kayode Saheed, Temitope Olubanjo Kehinde, Mustafa Ayobami Raji & Usman Ahmad Baba

To cite this article: Yakub Kayode Saheed, Temitope Olubanjo Kehinde, Mustafa Ayobami Raji & Usman Ahmad Baba (2024) Feature selection in intrusion detection systems: a new hybrid fusion of Bat algorithm and Residue Number System, Journal of Information and Telecommunication, 8:2, 189-207, DOI: 10.1080/24751839.2023.2272484

To link to this article: https://doi.org/10.1080/24751839.2023.2272484

JOURNAL OF INFORMATION AND TELECOMMUNICATION
2024, VOL. 8, NO. 2, 189–207
https://doi.org/10.1080/24751839.2023.2272484

OPEN ACCESS Check for updates

Feature selection in intrusion detection systems: a new hybrid fusion of Bat algorithm and Residue Number System

Yakub Kayode Saheed[a], Temitope Olubanjo Kehinde[b], Mustafa Ayobami Raji[c] and Usman Ahmad Baba[d]

[a]School of IT & Computing, American University of Nigeria, Adamawa, Nigeria; [b]Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University, Hong-Kong, Hong-Kong; [c]Department of Marketing, University of Texas Rio Grande Valley, Edinburg, USA; [d]Department of Computer Science, Pen Resource University, Gombe, Nigeria

ABSTRACT
This research introduces innovative approaches to enhance intrusion detection systems (IDSs) by addressing critical challenges in existing methods. Various machine-learning techniques, including nature-inspired metaheuristics, Bayesian algorithms, and swarm intelligence, have been proposed in the past for attribute selection and IDS performance improvement. However, these methods have often fallen short in terms of detection accuracy, detection rate, precision, and F-score. To tackle these issues, the paper presents a novel hybrid feature selection approach combining the Bat metaheuristic algorithm with the Residue Number System (RNS). Initially, the Bat algorithm is utilized to partition training data and eliminate irrelevant attributes. Recognizing the Bat algorithm's slower training and testing times, RNS is incorporated to enhance processing speed. Additionally, principal component analysis (PCA) is employed for feature extraction. In a second phase, RNS is excluded for feature selection, allowing the Bat algorithm to perform this task while PCA handles feature extraction. Subsequently, classification is conducted using naive bayes, and k-Nearest Neighbors. Experimental results demonstrate the remarkable effectiveness of combining RNS with the Bat algorithm, achieving outstanding detection rates, accuracy, and F-scores. Notably, the fusion approach doubles processing speed. The findings are further validated through benchmarking against existing intrusion detection methods, establishing their competitiveness.

ARTICLE HISTORY
Received 7 July 2023
Accepted 14 October 2023

KEYWORDS
Principal component analysis; intrusion detection system; Bat algorithm; Naïve Bayes; feature selection

1. Introduction

The internet has had a profound effect on every aspect of people's lives and businesses (Saheed et al., 2022b) over the past decade, thereby revolutionizing society. Until now, daily attacks on the internet have increased. Therefore, the Internet requires an

CONTACT Yakub Kayode Saheed yakubu.saheed@aun.edu.ng

efficient, sophisticated, trustworthy, and tangible security solution (Christiana et al., 2019). Important Internet computer security mechanisms include confidentiality, integrity, and authentication (CIA). Moreover, antiquated methods such as user authentication, firewalls, and encryption serve as the first line of defense against Internet computers. In addition, archaic techniques such as firewalls, encryption functions, and user authentication serve as the initial layer of protection against online computing systems (Yu et al., 2023).

Traditional intrusion detection systems (IDSs) use authentication, encryption, and decryption mechanisms. Installing an application on the host website enables a firewall, which is a type of traditional first-line defensive security system. As a result of the structure's lack of resiliency and adaptability, as well as its low detection rate, attackers can easily circumvent it. Anti-virus software, for instance, can be viewed as a second line of defense that addresses the shortcomings of the first (Hou et al., 2020). The application for virus prevention and detection is a signature-based solution that utilizes a database of individual signatures. The primary deficiency of second-tier defense mechanisms is their inability to detect unidentified attack signatures (Hou et al., 2020). Intrusion refers to any process that attempts to circumvent security components or compromise the CIA. IDSs are network security tools that can block and identify malicious or abnormal traffic if the firewall and data encryption are unable to provide effective and efficient protection (Christiana et al., 2019). IDS can be implemented as either a software product or a hardware application to analyze network packets automatically. IDSs are a type of security technology used to detect network intrusions, and they are widely employed in modern security applications (Li et al., 2009).

IDS are separated into two categories: IDS for anomalies and IDS for abuse. Anonymous IDSs are centred on normal network behaviour and are used to identify any act that meaningfully deviates from normal network behaviour (Aung & Min, 2018). First, it confirms whether the actual network performance has deviated from the typical network performance (Prasad et al., 2020). In contrast, misuse is a knowledge-based technology that aims to precisely describe the characteristics of an intrusion by identifying it through rule comparison (Moustafa et al., 2017). It can achieve a high level of accuracy with a low rate of false positives (Moustafa et al., 2017). Nonetheless, it builds a library of features and is incapable of detecting unknown attacks (Abdulhammed et al., 2019). Therefore, misuse detection focuses on the behaviour that corresponds to a known attack scenario (Ambusaidi et al., 2016; Wang et al., 2017).

Several ML studies have been proposed for IDSs to design systems with a low false alarm rate and high detection accuracy (Gu et al., 2019). The proposed approach by the authors (Yu et al., 2023) involves a hybrid network classifier that incorporates enhanced residual network blocks and bidirectional gated recurrent units. The present study justifies the research methodology by employing authorized experimental datasets within the domain of network detection, namely NSL-KDD, and UNSW-NB15. The findings of the experiment indicate that the method proposed in this scholarly article attains a greater level of precision, specifically 93.40% and 93.26%. The findings of the study indicate that there exists a gap in the accuracy of the models, which requires improvement. In their study, the authors presented several shallow learning algorithms, including Decision Tree, Random Forest, Naïve Bayes, K-Nearest Neighbor, Support Vector Machine, XGBoost, and Ensemble Technique. These algorithms were applied to both the NSL-KDD benchmark dataset and the more recent CICIDS-2017 IDS dataset. The researchers employed Recursive Feature Elimination and Feature Importance-based feature selection techniques on the NSL-KDD dataset, and Feature Importance-based feature selection on the CICIDS-2017 dataset. The identified deficiency in the research pertains to the challenge of interpreting the models. For classification, the authors (Sung & Mukkamala, 2003) introduced an anomaly-based detection system that abstracts both comprehensible fuzzy rules and precise network data traffic flow. The fuzzy method was based on the framework for agent evolution and the method used a genetic algorithm for feature reduction. Salo et al. (Gan et al., 2013) utilized PCA to reduce the number of features. The PCA identified the most significant characteristics by projecting the data set into a subspace with no overlap. In the study (Gu et al., 2019), a genetic algorithm (Hosseini Bamakan et al., 2016) was utilized as a method for selecting features. The study (Sung & Mukkamala, 2003) investigated the use of ACO as a strategy for feature selection. The authors demonstrated that by utilizing ant colony optimization, the optimal features are selected. A survey of the literature exposed that, the majority of researchers developed feature selection methods and built intrusion detection systems using completely random records (Dey et al., 2023) without considering the whole training and testing datasets. The researchers (Hou et al., 2020) have put up a technique called Fine-Grained Access Control (FGAC) that aims to increase data security in the context of mobile edge computing. Its purpose is to safeguard data during the process of accessing it. The initial design of FGAC introduced a dynamic fine-grained trusted user grouping strategy that is rooted in the principles of attributes and metagraphs theory. Furthermore, the integration of the scheme was executed in conjunction with the conventional role-based access control mechanism, which facilitated the allocation of roles to users in accordance with the credibility of their respective user groups. The researchers (Zhaofeng et al., 2020) have put forth a proposal for a decentralized trust management and secure usage control scheme for IoT big data, known as BlockBDM. Even in the case of a small network, traffic analysis is a difficult task due to the available computing power and the large volume of audited data with numerous attributes that IDS must analyze. The audit data documents various network link characteristics. Such as the audit data might include information about the network service available at the destination, the number of incorrect fragments, or the duration of the connection. Certain problem domain features can be associated in ways that are difficult for humans to discover. A real-time IDS requires less information to process. Several of these features are superfluous and redundant; consequently, they can be eliminated before processing (Smmarwar et al., 2022). The vast majority of these attribute characteristics are irrelevant for intrusion detection; certain disturbance data may even hurt the means of preventing intrusions. Additional and noisy attributes can increase computational time and diminish the IDS's precision (Çavuşoğlu, 2019). Consequently, we must select a subset of representative attributes from the feature vector of the dataset to reduce the dimension of the feature space and thereby enhance the performance and efficiency of the IDS.

Intrusion detection is a classification problem requiring the creation of a predictive model capable of identifying attack incidents. Mostly on one side, many attributes or features could contain defects liability; however, classifying anomalies intrusion detection is a complex task (Azizan et al., 2021; Gu & Lu, 2021; Saheed & Raji, 2022). On either hand, IDS typically operate daily in the real world. In addition, the instances in IDS databases are enormous, necessitating lengthy classification or clustering processes. Obtaining classification performance from a database of over 1 million instances will take many days. Moreover, if a dataset contains a large number of features and instances, its operation can consume a substantial amount of memory and computing resources (Yang, 2010). As a consequence, feature selection (FS) is crucial for IDSs datasets, which typically contain a large number of instances and features. This paper, therefore, proposes a hybrid feature-selection technique for intrusion detection. The following are the main contributions of this research;

- We develop a hybrid feature selection Bat algorithm and principal component analysis (Bat+PCA) for intrusion detection systems.
- We design and incorporate a novel RNS for increasing the speed of the Bat algorithm. The Bat+RNS technique represents integer values through their corresponding remainders, or residues, of each modulus. Subsequently, arithmetic operations are conducted on these residues in isolation.
- We create the wrapper method (Bat algorithm) for feature selection and the filter method for feature extraction (PCA). The wrapper method (bat algorithm) searches the space of all features for the optimal subset of features. Before the actual model learning algorithm is applied, the filter method (PCA) is used to select subsets of features from the wrapper (Bat algorithm). Therefore, our proposed model resulted in a hybrid feature selection and feature extraction model as against the traditional-baseline standalone model.
- We propose four different models for evaluating the performance of IDSs.
- We evaluate the performance of the proposed models in terms of DA, DR, precision, F-score, and training time.
- The present study showcases the assessment of the performance of a hybrid bat that incorporates RNS and PCA. The results are then compared with those of other related works that are considered state-of-the-art.

This paper is organized as follows. Section 2 of this paper reported the related work. The materials and methodology adopted were presented in section 3. We discussed and presented our experimental results in section 4. The conclusion and future work were summarized in section 5.

2. Related works

Mukkamala and Sung (2003) utilized FS for intrusion detection by ranking the input features according to each particular class mark using neural-based networks and SVM. The study (Li et al., 2009) introduced a wrapper-based approach for identifying the most relevant input features from training samples using the random-mutation hill climbing method and then utilized an L-SVM to aid in the output of a subset of selected input attributes. The authors, (Aung & Min, 2018) presented a hybrid intrusion detection system by implementing K-means for feature selection. The experimental analysis was conducted on the KDDCup'99 dataset. The discovered results significantly lower the system's computational time complexity. Prasad et al. (2020) presented a hybrid model for FS based on Bayes theorem (BT) and rough set theory (RST). The feature selection method calculated key features and prioritized them based on probability estimates. This method decreases false alarms, boosts the detection rate, and minimizes computational and training complexity. Comparisons with relevant classifications are also presented, demonstrating that the proposed technique outperforms existing classifications. The authors (Moustafa et al., 2017) presented a lightweight anomaly IDS based on the Dirichlet mixture model. The model performance was conducted on two popular datasets; the UNSW-NB15 and the NSLKDD dataset. Abdulhameed et al., (2019) presented two attribute dimensionality reduction techniques utilizing both Autoencoder and PCA for the feature dimensionality reduction. The experimental analysis was conducted on the CICIDS2017 dataset. After the feature selection stage, the authors classified the reduced features with Bayesian network, random forest, LDA, and QDA. The experimental results indicate that low-dimensional features improve performance in terms of false alarm rate, accuracy, detection rate, and the F-measure. The authors (Wang et al., 2017) present an effective intrusion detection method based on an augmented features SVM. They generate the original feature using the logarithm marginal density ratios based on the transformation concept. The empirical results indicate that it outshines existing methods in terms of false alarm, detection accuracy, detection rate, and training speed. In their work, the authors (Ambusaidi et al., 2016) proposed an analytical approach that utilizes mutual information to identify the most suitable classification feature. The proposed methodology for feature selection utilizing mutual information is capable of effectively handling data with both linear and non-linear dependencies. The performance of the model proposed known as LSSVM-IDS experimented on three IDS datasets known as Kyoto 2006, NSL-KDD, and KDD Cup '99dataset. The authors (Gan et al., 2013) suggested a combination approach that utilizes both PLS and CVM techniques. The PLS was utilized as the dimensionality reduction technique in the study. The researchers (Hosseini Bamakan et al., 2016) introduced parameter setting and feature selection at the same time, and the author devised a time-varying chaotic PSO (TVCPSO). A weighted optimal solution is presented in the proposed approaches, which considers the compromise between increasing the DR and decreasing the FAR, as well as the number of attributes. Experiments with the NSL-KDD data were utilized to assess the success of the new approaches. The author (Gu et al., 2019) proposes a framework for real intrusion detection that is built on SVM ensembles enhanced with features. On the original features, the logarithm marginal density ratios transform is performed to get fresh and higher-quality altered training data. An ensemble of SVM is applied to build the classification on the Kyoto2006+ dataset. Experiment findings reveal that the suggested technique can produce a robust performance, which holds enormous modest merits in comparison to other current approaches in respect of detection rate, accuracy, training speed, and false alarm rate. Sung and Mukkamala (2003) presented an SVM-RFE closed-loop feature selection method for IDS, their method recursively removed one attribute at one time and the performance was compared in the SVM testing data. The study categorizes the features rank into three and utilized three performance metrics which are training time, the accuracy of classification, and testing time. This study which is a heuristic method is very time-consuming and unknown attacks are not considered. In their study, the authors (Dey et al., 2023) presented a hybrid feature selection methodology that integrates filter techniques based on statistical tests, namely chi-square, Pearson's Correlation Coefficient (PCC), and Mutual Information (MI), with a metaheuristic approach using Non-Dominated Sorting Genetic Algorithm (NSGA-II) for feature optimization. The proposed methodology utilizes filter-based techniques to prioritize the characteristics for directed population initialization within NSGA-II, resulting in expedited convergence toward a resolution. The experimental results are juxtaposed with contemporary state-of-the-art methodologies. The analysis of results verifies the exceptional performance, exhibiting an accuracy rate of 99.48%. The proposed framework by the authors (Smmarwar et al., 2022) involves a hybrid feature selection approach that utilizes wrapping feature selection in combination with greedy stepwise and random forest framework to optimize the malware features. The framework under consideration exhibits the ability to effectively minimize a considerable number of attributes, resulting in an optimal feature that serves to augment the efficacy of the machine learning model. The framework employed three widely utilized machine learning classifiers, namely random forest (RF), decision tree (C5.0), and support vector machine radial basis function (SVM RBF). The models of RF, DT, SVM and RBF have demonstrated improved accuracy rates of 91.80%, 91.32%, and 82.33%, respectively, when applied to the static layer. The system developed in reference (Çavuşoğlu, 2019) involves an initial stage of data preprocessing on the NSL-KDD dataset, followed by the application of various feature selection algorithms to reduce the dataset size. Two novel methodologies have been suggested for the process of feature selection. The NSL-KDD dataset was utilized to conduct performance evaluations on the proposed system, which included tests for accuracy, detection rate, true positive rate, false positive rate, F-measure, Matthews correlation coefficient, and processing time. However, the feature selection phase was neglected in the work. In their study, the authors (Azizan et al., 2021) present a model for a network intrusion detection system (NIDS) that utilizes ML techniques. The proposed model evaluates the accuracy and precision of anomaly traffic detection using three different algorithms. The KDD methodology and CIC-IDS2017 dataset are utilized in the assessment process, as they are widely recognized as standard benchmarks for evaluating IDS. The SVM exhibits the highest accuracy among the three models, with an average accuracy result of 98.18%. In contrast, the RF and DJ models exhibit mean accuracy outcomes of 96.76% and 96.50%, correspondingly. The SVM algorithm achieved an average precision of 98.74, while the RF and DJ algorithms achieved 97.96 and 97.82, respectively. Notably, the SVM algorithm demonstrated a superior average precision compared to the other two algorithms. However, there is the curse of dimensionality issue in the work as a result of the feature selection phase that was neglected. Table 1 presents a comprehensive overview of the extant literature, including the employed methodology, obtained results, and identified research gaps. The literature showcases various approaches to feature selection in IDS. The large percentage of research in the literature, however, focused on prospective solutions from the perspectives of neural network technologies, filter-based approaches, which are prone to selecting redundant features, the K-means method, which can only handle numerical data, and the PLS technique, which is neither generalizable nor flexible.

In contrast to previous research, we suggested a cost-effective hybridized nature-inspired Bat method with the incorporation of residue number system feature selection and PCA feature extraction in IDS in this research. Because of its simplicity, generalization capability, ease of implementation, and flexibility, we chose the bat algorithm for feature selection. The residue number system, on the other hand, was chosen because of its

Table 1. A comprehensive review of the extant literature, including the employed methodologies, findings, and potential constraints.

Authors	Methodology	Results	Limitations
Authors (Gu & Lu, 2021)	NB-SVM	DA= 93.75; DR= 94.73	The feature selection stage was not considered
Authors (Moustafa et al., 2017)	GAA-ADS	DA= 92.80; DR= 91.30	The training time of the model was not considered.
Authors (Abdulhammed et al., 2019)	AE-QDA	DA =94.20; DR=96.40	The AE utilized has a slow running time and is prone to overfitting
Authors (Wang et al., 2017)	LMDRT-SVM	DA= 98.23; DR = 99.36	The model does not determine the local minima
Researchers (Ambusaidi et al., 2016)	CSV-ISVM	DR = 90.15	The model produced a large training time
Ref. (Gan et al., 2013)	PLS+CVM	DA= 99.87; DR = 99.74	Higher risk of overlooking real correlations of the features
Researchers (Hosseini Bamakan et al., 2016)	TVCPSO-SVM	DA= 98.30; DR = 97.05	The model has a large training time
Authors (Prasad et al., 2020)	BT-RST	DR = 97.96; DA = 96.38	The Bayes Theorem needs a prior probability distribution over the model parameters
Ref. (Gu et al., 2019)	DT-EnSVM	DA = 98.34; DR = 99.82; TT = 60.56	The DT is very unstable in the training phase
Ref. (Aung & Min, 2018)	K-means +KNN	DA = 97.89; TT = 0.20	The model requires high memory
Ref. (Dey et al., 2023)	Chi-square, Pearson correlation coefficient, mutual information	Accuracy = 99.48	The accuracy was used to evaluate the performance and accuracy alone cannot be used to justify the performance.
Ref. (Smmarwar et al., 2022)	RF, DT, SVM-RBF	DT Accuracy=91.80, RF= 91.32, and SVM=82.33	Accuracy alone was used to evaluate the model performance

inherent properties, which include the lack of carry-free addition, fault tolerance, parallelism, and modularity.

2.1. Motivation of the proposed system

The main motivation behind this research stemmed from six factors in the realm of intrusion detection systems (IDS) and optimization techniques:

a. **Enhanced Intrusion Detection Accuracy:** The primary goal of IDS is to accurately identify malicious activities in computer networks. By utilizing advanced bat optimization technique combined with the unique properties of the residue number system enhance the accuracy of feature selection, leading to more precise intrusion detection in this research work.
b. **Reduced Computational Complexity:** Intrusion detection often involves processing a large number of features, which can lead to high computational costs. The fusion of the bat algorithm and residue number system offer a way to effectively reduce the dimensionality of the feature space while maintaining or even improving detection accuracy. This reduction in computational complexity make real-time intrusion detection more feasible and efficient in our propose study.
c. **Handling High-Dimensional Data:** Modern networks generate vast amounts of data, resulting in high-dimensional feature spaces. Traditional feature selection methods might struggle to handle such complex data. Our proposed hybrid

approach could provide an effective means of tackling high-dimensional data by leveraging the optimization power of the bat algorithm and the unique number representation capabilities of the residue number system.

d. **Synergy of Optimization Techniques:** Combining different optimization algorithms can often yield superior results compared to using them individually. The bat algorithm is known for its ability to explore and exploit search spaces effectively, while the residue number system offers advantages in terms of parallelism and computation. The synergy of these two techniques lead to improved convergence speed and optimal feature subsets.
e. **Novelty and Innovation:** The combination of the bat algorithm and the residue number system for feature selection in intrusion detection is relatively unexplored. This novelty can attract attention from both the academia and industry. Researchers and practitioners are often interested in new approaches that can potentially outperform existing methods.
f. **Applicability to Real-World Scenarios:** Intrusion detection is a critical component of ensuring the security of computer networks and systems. Our propose hybrid approach proves to be successful, it could have direct practical implications for improving the robustness of real-world intrusion detection systems, making them more resilient to a wide range of cyber threats.

This research aims to address key challenges in IDS by leveraging the combined power of the bat algorithm and the residue number system for effective feature selection. This approach offers the potential to enhance accuracy, reduce computational complexity, handle high-dimensional data, and introduce a novel and innovative solution to the field of intrusion detection.

3. Proposed approach

This section discusses the proposed hybrid feature selection with bat algorithm and fusion of residue Number System for IDSs as shown in Figure 1. In the first line of this research, we adopt RNS and incorporated it with the Bat algorithm. Therefore, the first phase of the model started with data preprocessing which is done using the standardization method. Subsequently, the FS is performed with the bat algorithm to select eighteen (18) features and RNS is utilized to obtain the residues of the features gotten from the bat algorithm. In the subsequent phase, PCA was used to extract the features obtained from RNS in residues form. Then, we used NB and KNN for classifying NSLKDD network data. In the second line of this research, we performed feature selection without the fusion of RNS (that is by not adopting RNS). The PCA was used for extracting the components from the bat algorithm-selected features (Saheed & Raji, 2022). Subsequently, classification was performed with the NB and KNN algorithms.

3.1. Bat algorithm

In 2010, Xin-She Yang created a novel metaheuristic optimization algorithm (Yang, 2010). Microbats employ echolocation as a means of orienting themselves within their environment, detecting potential prey, and locating suitable roosting sites amidst low-light

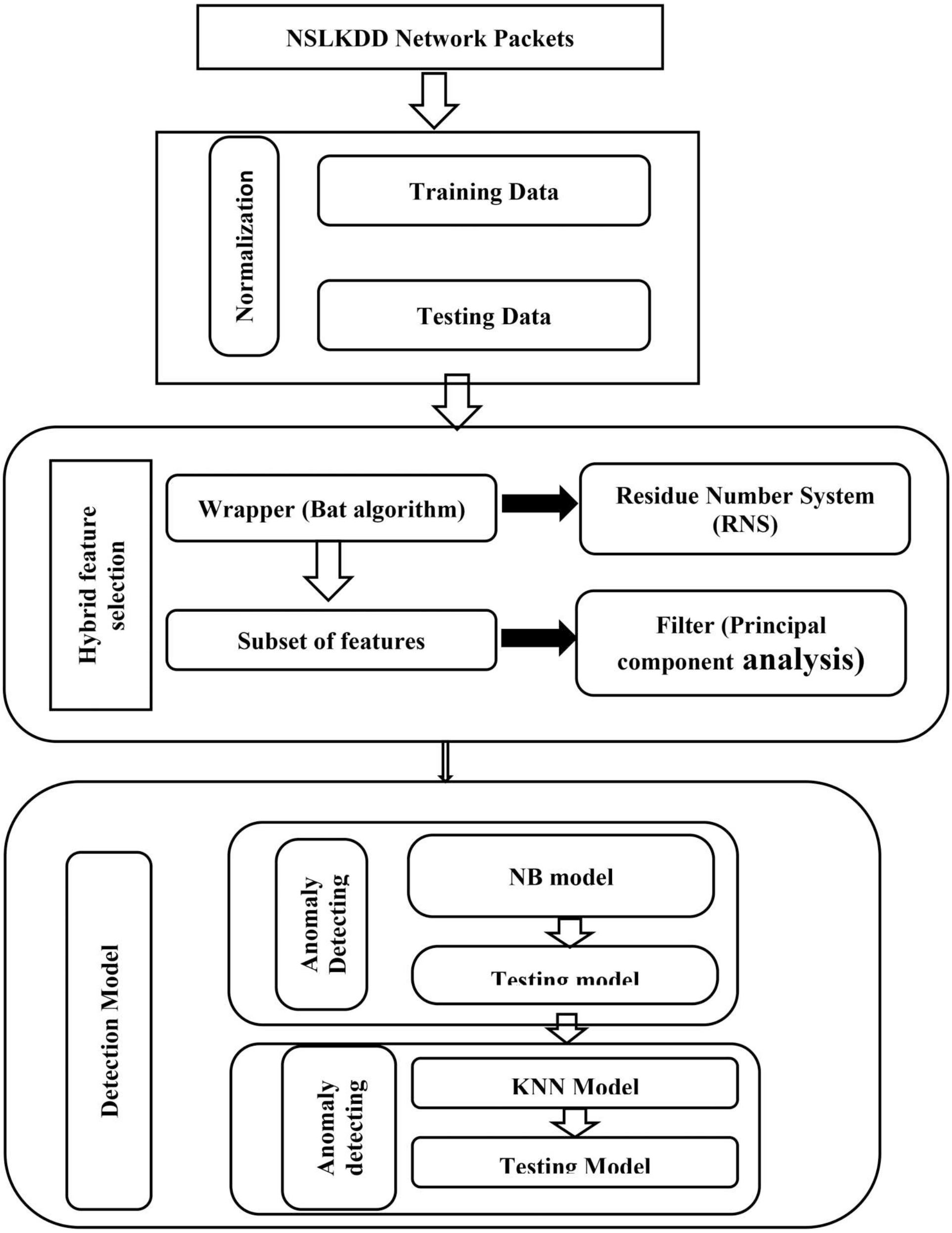

Figure 1. The proposed system architecture.

conditions (Reddy & Vijaya Kumar, 2012). The method of echolocation entails sending out a loud noise echo and then reacting to it bounce back via things. The Bat algorithm is a stochastic search algorithm that was developed by emulating the foraging behaviour of bats in their natural habitat, wherein they utilize echolocation to explore, detect, and capture prey (Yong et al., 2019). It mimics the use of bat ultrasound for basic detecting and links it to the optimized target feature. The bat algorithm was used to select the significant features in this study. The Bat algorithm selects sixteen features out of the forty features with one class label. The Bat algorithm can be represented in Equation (1).

$$F_i = F_{min} + rand(F_{max} - F_{min}) \tag{1}$$

Where fi denotes the bat's i pulse frequency. The frequency spectrum of the pulse is represented by the symbols F_{max} and F_{min}, while the variable rand follows a normal distribution within a specific range [0,1].

3.2. Residue Number System

RNS provides a set of moduli that are all substantially prime and unrelated to one another (Saheed & Gbolagade, 2017). RNS was used to increase the speed and reduction costs of Convolution Neural Networks (Valueva et al., 2020). We used RNS for increasing the speed of the Bat algorithm in this paper. The RNS is a novel number system described in terms of the set of reasonably prime moduli {P_1, P_2,..,P_n} that is gcd(Pi,Pj) = 1 for i ≠ j (Saheed & Gbolagade, 2016). K is a weighted binary number that can be written as = (k_1, k_2, … , k_n), where

$$ki = KmodPi = /K/pi, 0 \leq ki < P_i \tag{2}$$

For any integer K in the range, such a representation is unique. [0, M-1], where M = P_1, P_2, … ,P_n is the moduli set's dynamic range {P_1, P_2, … P_n}.

In RNS, each residue is represented by its modulus or base. The operations on the residues are performed modulo their respective moduli. This modulus independence allows operations to be carried out on each residue separately, without any carry-over effects or constraints between different digits or moduli. As a result, there is no need for carry propagation, and the complexity of arithmetic operations remains constant regardless of the size of the numbers.

3.3. Principal component analysis

PCA is a generally used feature extraction technique that utilizes linear transformation to map data after a high-dimensional feature vector to a reduce dimensional feature space (Harish & Kumar, 2017; Ibrahimi & Ouaddane, 2017). We utilized PCA to pick the greatest discriminative attributes (Peng et al., 2018). The principal components are the covariance matrix's symmetric eigenvectors (Saheed et al., 2022a). The PCA transformation can be expressed as Equation (3) (Taşpınar, 2015);

$$Y = Z^{i}_{uxv}.W_{uxj} \tag{3}$$

where Zu×v v is the projection matrix with v eigenvectors and Wu×j is the mean-centred data matrix. In this investigation, we extracted the components of the residues using PCA.

3.4. K-Nearest neighbour

KNN is a non-parametric pattern recognition technique that can be utilized for regression or classification (Saheed, 2022). KNN is a commonly used classifier in a variety of classification techniques. The rationale for using KNN is that it is straightforward and well-suited for multimodal groups. The classification performance is proportional to the number of picked nearest neighbours. The key factors in its categorization are the record set, the distance measures, which are typically Euclidean in nature, and the value of the K number of neighbours (Salih & Abdulrazaq, 2019). The KNN is used for the classification of the selected features in residue from the FS stage. The KNN can be described in the following manner;

$$D(x, y) = \sqrt{\Sigma_{(i=1)}^{k}(xi - yi)^2} \quad (4)$$

4. Results and discussion

4.1. Description of the dataset

The experimental research is carried out on the well-known NSLKDD dataset for intrusion detection. As discussed in (Moustafa & Slay, 2017), Tavallaee et al. created NSLKDD to overcome the obvious flaws with the KDDCupp '99 data collection. Though a number of the concerns raised by McHugh in (Godala & Vaddella, 2020) are present in the most recent version of the dataset, it may not be an exhaustive representation of real-world networks. Given that this dataset is still utilized in the majority of current NIDS research, we can assume it remains a useful benchmark for researchers comparing alternative methods.

4.2. Results

The experiment was conducted based on Bat with a fusion of RNS (Bat-RNS) in which sixteen (16) features were ranked (selected) out of the 2519240 records, and forty (40) features with one (1) class label as shown in Table 2. The features selected are then sent to PCA to extract features. Following the phase of feature extraction, the dataset was divided into training and testing phases. 25% of the data was used for testing the model via NB and KNN algorithms. Also, 75% was used for training the model with NB and KNN.

A hybrid feature selection based on the bat Algorithm with the fusion of RNS to split the training data and disregard the inappropriate features. In addition, the PCA was used as feature extraction in this paper which transforms the data into principal components. The NB and KNN were adopted for classification purposes in the first line of this research. In the second line of this research, the RNS was not incorporated for feature selection. Thus, the Bat algorithm was used for feature selection and PCA was used for feature extraction. Subsequently, the classification was carried out with NB and KNN. The

Table 2. Sixteen Selected Attributes by Bat-RNS.

Attributes number	Attributes name	Attributes number	Attributes name
ATT2	Type of protocol	ATT25	Server error rate
ATT3	Service	ATT26	Srverror rate
ATT9	Critical	ATT32	Dst host count
ATT12	Logged in	ATT33	Dst host server count
ATT14	Source shell	ATT34	Dst host the same server rate
ATT18	Number shells	ATT36	Dst host diff server rate
ATT22	Is guest Log in	ATT37	Dst host server diff host rate
ATT23	Count	ATT39	Dst host server error rate

confusion matrix of our propose model is given in Table 3. In the context of a confusion matrix table, the rows and columns represent different aspects of the classification outcomes. Here's how they are typically defined:

1. **Rows (Actual Classes):** The rows in the confusion matrix represent the actual or true classes of the instances being classified.
2. **Columns (Predicted Classes):** The columns in the confusion matrix represent the predicted classes assigned by the classification model. For each instance, the model makes a prediction about whether it belongs to the positive class or the negative class.

4.3. Time complexity of the proposed RNS+Bat algorithm

Here, we provide the time complexity for key operations in the RNS+Bat algorithm

1. Conversion to and from RNS:
   - The conversion of a number from the conventional number system to RNS involves calculating the residues for each modulus. The time complexity for this conversion process depends on the three moduli used and we have O(1) to O(3).
   - Conversely, converting a number from RNS back to the conventional number system requires combining the residues using the Chinese Remainder Theorem (CRT), with a time complexity of O(N^2) or O(N^3), where N is the number of moduli. N here is 3.
2. Arithmetic Operations:
   - Addition and subtraction operations in RNS are relatively straightforward and have a time complexity of O(N), as they involve performing the corresponding operations on each residue independently.
   - Multiplication and division operations in RNS are more complex. The time complexity of these operations depends on the specific algorithms used, which is the Carry Save Array (CSA) with a time complexity of O(N^2).
3. Modular Operations:
   - Modular operations in RNS, such as modular addition, subtraction, and comparison, have a time complexity of O(N).

For the Bat Algorithm operations;

1. Initialization:
   - The time complexity for initializing the population of bats is O(N), where N is the number of bats which is 4.

Table 3. Confusion matrix of Bat-RNS+PCA+NB.

	1	2	3	4	5
1	3331	10	22	0	0
2	121	2175	13	0	0
3	104	18	450	0	0
4	2	0	0	0	0
5	52	0	0	0	0

2. Echolocation:
   - The echolocation phase involves updating the bat positions based on their velocity and frequency. This operation is usually performed in each iteration of the algorithm.
   - The time complexity for updating the bat positions is O(N), as each bat's position needs to be updated.
3. Pulse Emission and Loudness Update:
   - The pulse emission phase involves generating a new solution based on the current bat's position and updating its loudness.
   - The time complexity for pulse emission is O(1) to O(N).
4. Local Search and Updating the Best Solution:
   - The local search phase involves refining the bat's solution in the search space using a local optimization method.
5. Convergence:
   - The time complexity for convergence evaluation is O(1).

4.4. Experimental results of Bat with the fusion of RNS for feature selection

We performed the proposed experimental analysis of feature selection with the fusion of RNS to select the 16 most significant attributes as depicted in Table 3. After which the PCA was used for extraction, thus, the performance of the Bat-RNS+PCA+NB and Bat-RNS+PCA +KNN concerning detection accuracy, detection rate, F-score, and precision was noted as shown in Table 4. In time-sensitive applications, the training time of classifiers was also accounted for (Saheed, 2022).

4.5. Experimental results of Bat feature selection and PCA feature extraction without fusion of RNS

Herein, we performed the proposed Bat+PCA+NB and Bat+PCA+KNN experimental analysis of Bat feature selection and PCA for feature extraction. After this, the PCA was used for extraction and classification performed with KNN and NB. The performance was noted concerning detection accuracy, detection rate, precision, and F-score. In time-critical applications, the classifier's training time was also considered in Table 5.

4.6. Comparison of the proposed Bat features selection methods with the fusion of RNS and without RNS

The approaches proposed in this paper were compared in this section to ascertain the influence of RNS on the Bat algorithm for feature selection. In the first performance results obtained as shown in Table 4, the Bat algorithm with a fusion of RNS gave an

Table 4. Performance of the Bat with a fusion of RNS.

Model/Metrics	Detection Accuracy	Detection rate	Precision	F-score	Training Time
Bat-RNS+PCA+NB	97.82	99.10	92.30	95.60	48.88
Bat-RNS+PCA+KNN	99.15	98.09	98.20	98.16	55.65

Table 5. Performance of the proposed Bat algorithm with PCA for feature extraction.

Model/Metrics	Detection Accuracy	Detection rate	Precision	F-score	Training Time
Bat+PCA+NB	97.81	99.04	92.27	95.50	55.99
Bat+PCA+KNN	99.12	98.03	98.13	98.11	56.43

Table 6. Performance evaluations of the proposed Bat-RNS+PCA+NB versus Bat+PCA+NB.

Model/Metrics	Detection Accuracy	Detection rate	Precision	F-score	Training Time
Bat-RNS+PCA+NB	97.82	99.10	92.30	95.60	48.88
Bat+PCA+NB	97.81	99.04	92.27	95.50	55.99

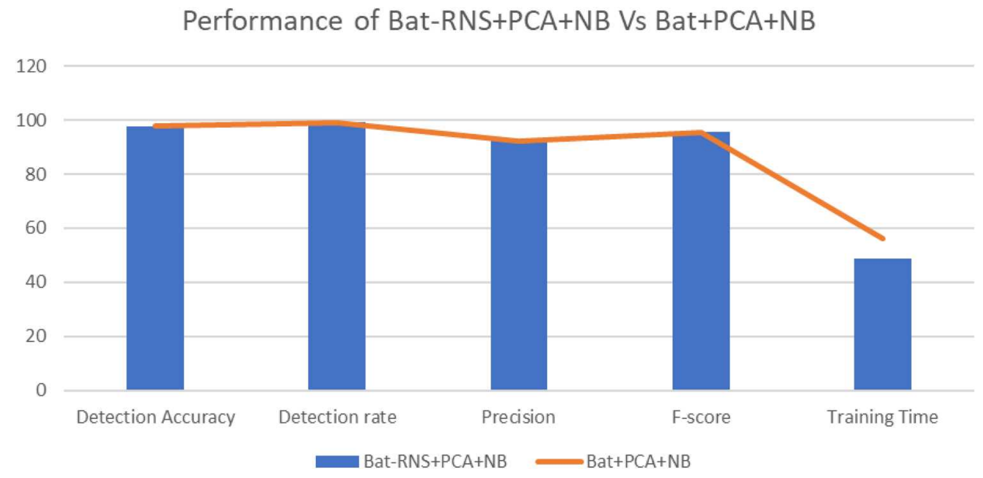

Figure 2. Performance of the Bat feature selection with a fusion of RNS and without RNS.

outstanding performance concerning all the performance measures as compared with the Bat algorithm feature selection with PCA feature extraction as shown in Table 5.

As observed in Table 6 and Figure 2, the Bat-RNS+PCA+NB gave a detection accuracy of 97.82%, a detection rate of 99.10%, a precision of 92.30%, an F-Score of 95.60 and a training time of 48.88 s. The method Bat+PCA+NB without fusion of RNS gave 97.81% accuracy, a detection rate of 99.04%, a precision of 92.27%, an F-score of 95.50%, and a training time of 55.99 s. This clearly showed that the RNS influences the performance of Bat-RNS+PCA+NB when compared with the Bat feature extraction Bat+PCA+NB without fusion of RNS. This is a result of the inherent speed, carry-free addition, and parallelism of RNS. The training time was also reduced with a fusion of RNS and high without the fusion of RNS.

On the other side, as can be seen in Table 7 and Figure 3, the Bat-RNS+PCA+KNN gave a detection accuracy of 99.15%, a detection rate of 98.09%, a precision of 98.20%, F-Score of

Table 7. Performance evaluations of the proposed Bat-RNS+PCA+KNN versus Bat+PCA+KNN.

Model/Metrics	Detection Accuracy	Detection rate	Precision	F-score	Training Time
Bat-RNS+PCA+KNN	99.15	98.09	98.20	98.16	55.65
Bat+PCA+KNN	99.12	98.03	98.13	98.11	56.43

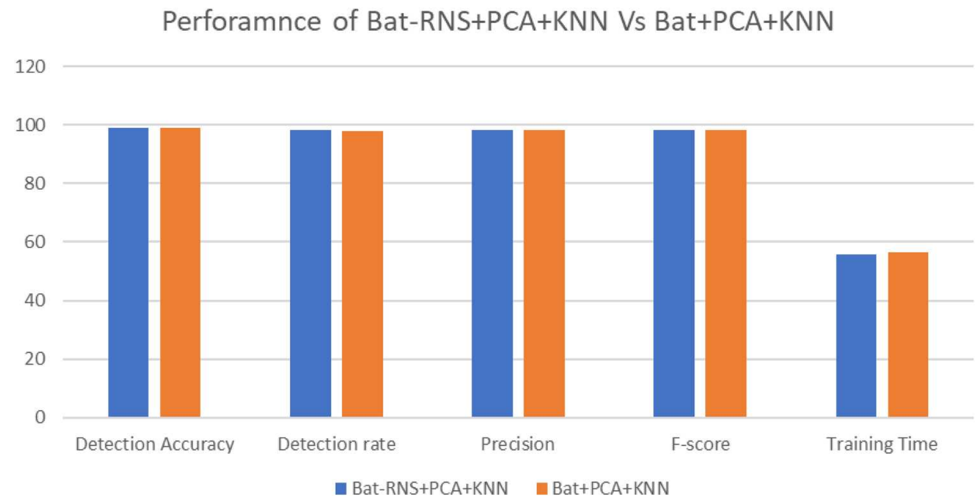

Figure 3. Performance of the Bat feature selection with a fusion of RNS using KNN for classification and without RNS using KNN for classification.

98.16% and training time of 55.65 s. The method Bat+PCA+KNN as shown in Table without fusion of RNS gave 99.12% accuracy, a detection rate of 98.03%, a precision of 98.13%, an F-score of 98.11%, and a training time of 56.43seconds. This clearly showed that the RNS influences the performance of Bat-RNS+PCA+KNN when compared with the Bat feature extraction Bat+PCA+KNN without fusion of RNS. This is a result of the inherent speed, carry-free addition, and parallelism of RNS. The training time was also reduced with the fusion of RNS as compared to without the fusion of RNS as seen in Table 7.

4.7. Comparison of the methods proposed with the state-of-the-art results

We compared the methods Bat-RNS+PCA+NB, Bat+PCA+NB, Bat-RNS+PCA+KNN, and Bat +PCA+KNN proposed in this paper with other reported studies. From Table 8 of comparison with previous studies, in terms of detection accuracy (DA), detection rate (DR), F-score, and validation dataset, our proposed methods outperform a vast majority of previous research. Though, our proposed methods showed better results in these categories in terms of F-score and training time. To further compare our results, about two of the previous work in Table 8 adopted the KDDCup 99 for the experimental analysis. This dataset has some issues as mentioned in (Tavallaee et al., 2009). We can, therefore, conclude that our proposed methods are competitive not only in terms of DA and DR but also in terms of training speed, F-score, and the validation dataset. The training speed was obtained as a result of the fusion of RNS which verify its effectiveness.

4.8. Threats to validity

The NSLKDD dataset is open source and was implemented in Python; hence, there is a risk of generalizing results to other computer languages, such as Java, R, etc. The volume of the dataset may also influence the likelihood of an attack on a class, and the dataset may

Table 8. Comparison of the Proposed models with existing methods reported in the literature.

Authors/methods	Detection Accuracy	Detection rate	F-score	Training Time (seconds)	Validation Datasets
Ref. (Gu & Lu, 2021) NB-SVM	93.75	94.73	x	x	UNSWNB15
Ref. (Moustafa et al., 2017) GAA-ADS	92.80	91.30	x	x	UNSWNB15
Ref. (Abdulhammed et al., 2019) AE-QDA	94.20	96.40	x	x	CICIDS2017
Ref. (Wang et al., 2017) LMDRT-SVM	98.23	99.36	x	x	NSLKDD
Ref. (Ambusaidi et al., 2016) CSV-ISVM	X	90.15	x	x	Kyoto2006
Ref. (Gan et al., 2013) PLS+CVM	99.87	99.74	x	x	KDDCup'99
Ref. (Hosseini Bamakan et al., 2016) TVCPSO-SVM	98.30	97.05	x	x	NSLKDD
Ref. (Prasad et al., 2020) BRS	97.96	96.38	x	x	CICIDS2017
Ref. (Gu et al., 2019) DT-EnSVM	98.34	99.82	x	60.56	Kyoto 2006
Ref. (Aung & Min, 2018) K-means+KNN	97.89	X	x	0.20	KDDCup'99
Bat-RNS+PCA+NB	97.82	99.10	95.60	48.88	NSLKDD
Bat+PCA+NB	97.81	99.04	95.50	55.99	NSLKDD
Bat-RNS+PCA+KNN	99.15	98.09	98.16	55.65	NSLKDD
Bat+PCA+KNN	99.12	98.03	98.11	56.43	NSLKDD

not be representative. In our investigation, this risk is addressed by validating the classifier output on a well-known dataset that has been extensively used in earlier research. Regarding external validity, empirical validation was conducted on the NSLKDD dataset in this study. Although this study's findings are generalizable to the domain of the IDSs, they may vary for other domains. Thus, there is a threat to external validity.

5. Conclusion and future work

This study employed the bat algorithm metaheuristic in conjunction with residue number system fusion for feature selection, while principal component analysis was utilized for feature extraction. We presented four hybrid models for NIDS in this paper. We adopted the combination of RNS and the bat algorithm for FS and extracted features using PCA. Subsequently, we classified using NB and KNN for two of the proposed methods. In the other two methods, we did not use RNS with the bat algorithm, but rather the bat algorithm with PCA, followed by NB and KNN classification. In terms of detection accuracy, detection rate, precision, and F-score, the two methods with RNS fusion performed better than the methods without it. The training time (speed) of the two methods with RNS fusion was significantly less expensive than that of the other two methods without RNS. Empirical evidence indicates that the integration of the residue number system enhances the performance of all classifiers. The Bat-RNS+PCA +NB algorithm achieved a high level of accuracy in detecting the target, with a detection accuracy of 97.82%, a detection rate of 99.10%, a precision of 92.30%, and an F-Score of 95.60. Additionally, the algorithm demonstrated efficient training, with a training time of 48.88 s. The results indicate that the incorporation of RNS has a significant impact on the efficacy of Bat-RNS+PCA+NB in contrast to Bat+PCA+NB, which solely employs bat feature extraction without RNS fusion. Additionally, our proposed method outperforms all existing models and is extremely competitive. This study only considers binary intrusion detection situations. Future research will focus on expanding the scope of our investigation to encompass a variety of attack types (multi-class classification). Also, the issue of data imbalance remains unresolved; however, the implementation of up-sampling and down-sampling methodologies in the field of machine learning may be deemed viable. Our future research endeavours will focus on investigating this particular area.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., & Abuzneid, A. (2019). Features dimensionality reduction approaches for machine learning based network intrusion detection. *Electronics*, *8*(3), https://doi.org/10.3390/electronics8030322

Ambusaidi, M. A., He, X., Member, S., Nanda, P., Member, S., & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE Transactions on Computers*, *9340*(NOVEMBER 2014), 1–13. https://doi.org/10.1109/TC.2016.2519914

Aung, Y. Y., & Min, M. M. (2018). Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms. *Proc - 17th IEEE/ACIS Int Conf Comput Inf Sci ICIS 2018*, pp. 34–38. https://doi.org/10.1109/ICIS.2018.8466537

Azizan, A. H., Mostafa, S. A., Mustapha, A., Foozy, C. F. M., Wahab, M. H. A., Mohammed, M. A., & Khalaf, B. A. (2021). A machine learning approach for improving the performance of network intrusion detection systems. *Annals of Emerging Technologies in Computing*, *5*(Special issue 5), 201–208. https://doi.org/10.33166/AETiC.2021.05.025

Çavuşoğlu, Ü. (2019). A new hybrid approach for intrusion detection using machine learning methods. *Applied Intelligence*, *49*(7), 2735–2761. https://doi.org/10.1007/s10489-018-01408-x

Christiana, A. O., Oluwatimilehin, F. R., & Yakub, S. (2019). Hybridized Huffman algorithm with block truncate coding For image compression. *Journal of Computer Science and Control Systems*, *12*(2), 5–8. [Online]. Available: http://electroinf.uoradea.ro/images/articles/CERCETARE/Reviste/JCSCS/JCSC_V12_N2_oct2019/JCSCS VOL 12 NO 2 OCTOBER 2019 Abikoye_Hybridized.pdf

Dey, A. K., Gupta, G. P., & Sahu, S. P. (2023). Hybrid Meta-Heuristic based feature selection mechanism for cyber-attack detection in IoT-enabled networks. *Procedia Computer Science*, *218*, 318–327. https://doi.org/10.1016/j.procs.2023.01.014

Gan, X. S., Duanmu, J. S., Wang, J. F., & Cong, W. (2013). Anomaly intrusion detection based on PLS feature extraction and core vector machine. *Knowledge-Based Systems*, *40*, 1–6. https://doi.org/10.1016/j.knosys.2012.09.004

Godala, S., & Vaddella, R. P. V. (2020). A study on intrusion detection system in wireless sensor networks. *International Journal of Communication Networks and Information Security*, *12*(1), 127–141.

Gu, J., & Lu, S. (2021). An effective intrusion detection approach using SVM with naïve Bayes feature embedding. *Computers & Security*, *103*, 102158. https://doi.org/10.1016/j.cose.2020.102158

Gu, J., Wang, L., Wang, H., & Wang, S. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Computers & Security*, *86*, 53–62. https://doi.org/10.1016/j.cose.2019.05.022

Harish, B. S., & Kumar, S. V. A. (2017). Anomaly based intrusion detection using modified fuzzy clustering. *International Journal of Interactive Multimedia and Artificial Intelligence*, *4*(6), 54. https://doi.org/10.9781/ijimai.2017.05.002

Hosseini Bamakan, S. M., Wang, H., Yingjie, T., & Shi, Y. (2016). An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization. *Neurocomputing*, *199*, 90–102. https://doi.org/10.1016/j.neucom.2016.03.031

Hou, Y., Garg, S., Hui, L., Jayakody, D. N. K., Jin, R., & Hossain, M. S. (2020). A data security enhanced access control mechanism in mobile edge computing. *IEEE Access*, *8*, 136119–136130. https://doi.org/10.1109/ACCESS.2020.3011477

Ibrahimi, K., & Ouaddane, M. (2017). Management of intrusion detection systems based-KDD99: Analysis with LDA and PCA. *Proc - 2017 Int Conf Wirel Networks Mob Commun WINCOM 2017*. https://doi.org/10.1109/WINCOM.2017.8238171

Li, Y., Wang, J. L., Tian, Z. H., Lu, T. B., & Young, C. (2009). Building lightweight intrusion detection system using wrapper-based feature selection mechanisms. *Computers & Security*, *28*(6), 466–475. https://doi.org/10.1016/j.cose.2009.01.001

Moustafa, N., Creech, G., & Slay, J. (2017). Big Data Analytics for Intrusion Detection System: Statistical Decision-Making Using Finite Dirichlet Mixture Models. pp. 127–156. https://doi.org/10.1007/978-3-319-59439-2_5.

Moustafa, N., & Slay, J. (2017). A hybrid feature selection for network intrusion detection systems: Central points. pp. 5–13. https://doi.org/10.4225/75/57a84d4fbefbb

Mukkamala, S., & Sung, A. H. (2003). Feature selection for intrusion detection with neural networks and support vector machines. *Transportation Research Record: Journal of the Transportation Research Board*, *1822*(1), 33–39. https://doi.org/10.3141/1822-05

Peng, K., Leung, V. C. M., & Huang, Q. (2018). Clustering approach based on mini batch Kmeans for intrusion detection system over Big data. *IEEE Access*, *6*(c), 11897–11906. https://doi.org/10.1109/ACCESS.2018.2810267

Prasad, M., Tripathi, S., & Dahal, K. (2020). An efficient feature selection based Bayesian and rough set approach for intrusion detection. *Applied Soft Computing*, *87*, 105980. https://doi.org/10.1016/j.asoc.2019.105980

Reddy, M. D., & Vijaya Kumar, N. V. (2012). Optimal capacitor placement for loss reduction in distribution systems using fuzzy and harmony search algorithm. *ARPN Journal of Engineering and Applied Sciences*, *7*(1), 15–19.

Saheed, Y. K. (2022). Machine learning-based blockchain technology for protection and privacy against intrusion attacks in intelligent transportation systems. In *Machine Learning, Blockchain Technologies and Big Data Analytics for IoTs: Methods, Technologies and Applications,* IET.

Saheed, Y. K. (2022). A binary firefly algorithm based feature selection method on high dimensional intrusion detection data. In S. Misra, & C. Arumugam (Eds.), *Illumination of artificial intelligence in cybersecurity and forensics. Lecture notes on data engineering and communications technologies* (Vol. 109, pp. 323–341). Springer Cham. https://doi.org/10.1007/978-3-030-93453-8_12

Saheed, Y. K., Ayobami, R. M., & Orje-Ishegh, T. (2022a). A comparative study of regression analysis for modelling and prediction of bitcoin price. In S. Misra, & A. Kumar Tyagi (Eds.), *Blockchain applications in the smart Era. EAI/springer innovations in communication and computing* (pp. 187–210). Springer Cham.

Saheed, Y. K., Baba, U. A., & Raji, M. A. (2022b). Big data analytics for credit card fraud detection using supervised machine learning models. In K. Sood, B. Balusamy, S. Grima, & P. Marano (Eds.), *Big data analytics in the insurance market (emerald studies in finance, insurance, and risk management)* (pp. 31–56). Emerald Publishing Limited.

Saheed, Y. K., & Gbolagade, K. A. (2016). Efficient image encryption scheme based on the moduli Set {2n - 1, 2n, 2n +1}. *Al-Hikmah Journal of Pure & Applied Sciences*, *3*, 15–21.

Saheed, Y. K., & Gbolagade, K. A. (2017). Efficient RSA cryptosystem decryption based on Chinese remainder theorem and strong prime. *Anale SeriaInformatică*, *XV*(2), 1–5.

Saheed, Y. K., & Raji, M. (2022). Effectiveness of deep learning long short-term memory network for stock price prediction on graphics processing unit. In *2022 International Conference on Decision Aid Sciences and Applications (DASA), Chiangrai, Thailand*, pp. 1665–1671. https://doi.org/10.1109/DASA54658.2022.9765181.

Salih, A. A., & Abdulrazaq, M. B. (2019). Combining best features selection using three classifiers in intrusion detection system. *2019 Int Conf Adv Sci Eng ICOASE 2019*, pp. 94–99. https://doi.org/10.1109/ICOASE.2019.8723671

Smmarwar, S. K., Gupta, G. P., & Kumar, S. (2022). A hybrid feature selection approach-based Android Malware Detection Framework Using Machine Learning Techniques. https://doi.org/10.1007/978-981-16-8664-1_30

Sung, A. H., & Mukkamala, S. (2003). Identifying important features for intrusion detection using support vector machines and neural networks department of computer science New Mexico institute of mining and technology. *Symp A Q J Mod Foreign Lit*, *1822*(1), 3–10.

Taşpınar, F. (2015). Improving artificial neural network model predictions of daily average PM10 concentrations by applying principle component analysis and implementing seasonal models.

Journal of the Air & Waste Management Association, *65*(7), 800–809. https://doi.org/10.1080/10962247.2015.1019652

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *IEEE Symp Comput Intell Secur Def Appl CISDA 2009*, no. June 2014. https://doi.org/10.1109/CISDA.2009.5356528

Valueva, M. V., Nagornov, N. N., Lyakhov, P. A., Valuev, G. V., & Chervyakov, N. I. (2020). Application of the residue number system to reduce hardware costs of the convolutional neural network implementation. *Mathematics and Computers in Simulation*, *177*, 232–243. https://doi.org/10.1016/j.matcom.2020.04.031

Wang, H., Gu, J., & Wang, S. (2017). An effective intrusion detection framework based on SVM with feature augmentation. *Knowledge-Based Systems*, *136*, 130–139. https://doi.org/10.1016/j.knosys.2017.09.014

Yang, X. S. (2010). A new metaheuristic Bat-inspired algorithm. *Studies in Computational Intelligence*, *284*, 65–74. https://doi.org/10.1007/978-3-642-12538-6_6

Yong, J. S., He, F. Z., Li, H. R., & Zhou, W. Q. (2019). A novel Bat algorithm based on cross boundary learning and uniform explosion strategy. *Applied Mathematics-A Journal of Chinese Universities*, *34*(4), 480–502. https://doi.org/10.1007/s11766-019-3714-1

Yu, H., Kang, C., Xiao, Y., & Ting, Y. (2023). Network intrusion detection method based on hybrid improved residual network blocks and bidirectional gated recurrent units. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2023.3271866

Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. (2020). Blockchain-Enabled decentralized trust management and secure usage control of IoT Big data. *IEEE Internet of Things Journal*, *7*(5), 4000–4015. https://doi.org/10.1109/JIOT.2019.2960526