International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.39, June 2022 – www.ijais.org

Feature Selection based on Bat Algorithm and Residue Number System for Intrusion Detection System

Bukola Fatimah Balogun
Department of Computer Science
Kwara State University Malete,
Nigeria

Kazeem Alagbe Gbolagade
Department of Computer Science
Kwara State University Malete,
Nigeria

Ayisat Wuraola Asaju-Gbolagade
Department of Computer Science
University of Ilorin,
Nigeria

ABSTRACT

The Internet has grown rapidly in the last ten years. Consequently, the interconnection of computers and network devices has become so complex for monitoring that even the security experts do not fully understand its deepest inner workings. Personal computers have become very fast every year. It is not rare for a very ordinary person to connect to the Internet through 20 Mbs lines or faster. With this huge network data, the network security has become very important for monitoring the data. Machine Learning (ML) is a variant of Artificial Intelligence (AI) which uses algorithms to train and make accurate predictions on data. Dimensionality reduction in ML is used to remove redundant or irrelevant features, thereby improving the performance of classification. Chinese Remainder Theorem (CRT) is a modular arithmetic often used as a backward conversion algorithm in Residue Number System (RNS) to solve simultaneous linear congruence using a set of pair-wise relatively prime integers known as moduli set. In this paper, the Intrusion Detection System model was presented. The hybridized Bat algorithm and Chinese Remainder Theorem was used for feature selection and subsequently feature extraction was performed with Principal Component Analysis (PCA). The classification was done utilizing Naïve Bayes (NB). The dataset used for the experimental analysis was the Network Security Laboratory Knowledge Discovery Dataset (NSLKDD). In the experimental phase, 75% of the dataset was used for training and 25% for testing. The results obtained were measured in terms of accuracy, recall, sensitivity, specificity and precision.

General Terms

Network Security, Intrusion Detection, Feature Selection

Keywords

Intrusion Detection System, Bat algorithm, Residue Number System, Principal Component Analysis, Naïve Bayes

1. INTRODUCTION

An intrusion detection system is composed of various hardware and software components that work together to find traces of an attack or event that suggests an attack [1]. It is usually used to prevent unauthorized access to a computer system or network. Intrusion Detection System (IDS) has become an essential component of security infrastructure to identify and monitor suspicious activities. Since systems play an important role in society, they have to be built with the best possible rules to prevent intruders from breaching them. Securing these systems is a must to prevent unauthorized access to them.

Today, most people use the Internet to connect and communicate. Seamless data transfer is also expected of a secure network or communication channel. There has been a lot of research conducted to ensure that the data stored on the network are secure and reliable.

Traditional intrusion prevention solutions, including as firewalls, access control, and encryption, have proven ineffective in protecting networks and systems against more sophisticated attacks and malware [4]. The identification of threats or attacks is an important topic to tackle in the field of computer network security [2]. More companies are becoming susceptible to a wide range of attacks and dangers as the use of computer networks and internet connectivity grows exponentially [3]. As a result, Intrusion Detection System (IDS) proposed by Denning has become a critical component of security infrastructure, allowing users to detect, identify, and track intruders [5]. Since then, a lot of effort has gone into figuring out how to build IDS detection models that are both effective and accurate.

An intrusion detection system is usually deployed to prevent unauthorized access to a computer system. Some intrusion prevention techniques can be used as a first line of defense to protect computer systems. One of them is a firewall. However, just preventing intrusions isn't enough. As systems become more complex, exploitable weaknesses emerge owing to design and programming errors, as well as numerous penetration approaches. Therefore, Intrusion detection is required as another measure to protect our computer systems from such type of vulnerabilities [9]. This paper is organized as follows. Section 2 presents the related works. We describe the methodology in section 3. Section 4 proposed the results and discussion and section 5 concludes the paper.

2. RELATED WORK

Various Machine Learning techniques have been used to improve the accuracy of the Intrusion Detection System (IDS). In this section, we'll look at some of the most recent contributions in this field:

The authors [10] proposed a real-time intrusion detection system based on the Self Organizing Map (SOM); an unsupervised learning technique that is appropriate for anomaly detection in wireless sensor networks. The proposed system was tested using KDD’99 Intrusion Detection Evaluation dataset. The system groups similar connections together based on correlations between features. A connection may be classified as normal or attack. Attacks are classified again based on the type of attack. It took the system 0.5 seconds to decide whether a given input represents a normal behavior or an attack.

The authors [11] proposed an SVM-based intrusion detection system, which used a hierarchical clustering algorithm, leave one out, and the SVM technique. The hierarchical clustering algorithm provided the SVM with fewer, abstracted, and higher-qualified training instances that are derived from the KDD Cup 1999 training set. It was able to greatly minimize the training timeand improve the performance of SVM. The simple feature selection procedure (leave one out) was applied to eliminate unimportant features from the training set so the obtained SVM model could classify the network traffic data more accurately.

The study [12] presented a contribution to the network intrusion detection process using Adaptive Resonance Theory (ART1), a type of Artificial Neural Networks (ANN) with binary input unsupervised training. They presented the feature selection using data mining techniques, towards two-dimensional dataset reduction that is efficient for the initial and on-going training, and reduce the dataset both vertically and horizontally, numbers of vectors and number of features.

In the paper [13] proposed a genetic algorithm to search the genetic principal components that offers a subset of features with optimal sensitivity and the highest discriminatory power. The support vector machine (SVM) is used for classification. The results show that proposed method enhances SVM performance in intrusion detection.

The work [14] proposed hybrid technique combines data mining approaches like K Means clustering algorithm and RBF kernel function of Support Vector Machine as a classification module. The main purpose of proposed technique is to decrease the number of attributes associated with each data point. So, the proposed technique can perform better in terms of Detection Rate and Accuracy when applied to KDDCUP’99 Data Set.

The references[15]propose Principal Component Analysis technique for feature reduction and effective selection. The authors adopt a different approach to network analysis in order to reduce data features. Header fields of incoming packets are analyzed in vectors, these serve as import for the PCA algorithm. The System is designed in two phases. The training and testing phase are conducted over the full NSL-KDD dataset. PCA produces features which aredeemed weak. The test records are compared with the base profile during training phase and then the confusion matrix is used over the classification algorithms to determine performance. Results in the accuracy of detection time of each algorithm are measured. The following classifiers are tested upon within the investigation SVM, KNN, J48 tree, random Forest tree, classification, Adaboost, Nearest Neighbor, Naive Bayesclassifier and voting features classification.

The work [16] introduces the examination of KDD informational index regarding four classes which are Basic, Content, Traffic and Host in which all information properties can be arranged. The investigation is finished as for two noticeable assessment measurements, Detection Rate (DR) and False Alarm Rate (FAR) for an Intrusion Detection System (IDS). Because of this exact examination on the informational index, the commitment of each of four classes of properties on DR and FAR is indicated which can help improve the appropriateness of informational index to accomplish greatest DR with least FAR.

The authors [32] proposed Intrusion Detection using combination of various kernels based Support Vector Machine. In their proposed method, they employed the Grid-search technique to identify the optimal model for SVM with different kernel. Optimal model was selected by examining variety of different value combinations based on majority voting (MV) fusion. The entire KDD99 dataset was used to train and test the classifiers. The results obtained shows 91.27% accuracy for kernel Polynomial (KSVM+P+MV), 92.99% accuracy for kernel Radial Basis(KSVM+RB+MV), 93.19% accuracy for kernel Laplace (KSVM+L+MV) respectively. Combining the three approaches, an accuracy of 93.22% was recorded.

The authors [33] proposed a novel hybrid anomaly intrusion detection scheme based on combined feature selection known as GRRF-FWSVM method. The system was trained using CatBoost algorithm. The experimental analysis was carried out using KDD Cup 99. Result shows an improved detection accuracy of 98.55%.

The authors [34] presented an ensemble classifier approach for IDS using logistic regression, decision trees, and gradient boosting. Experimental evaluation was conducted using CSE-CIC-IDS2018 dataset. Chi-square and Spearman's rank correlation were used for optimal feature selection, and 23 out of 80 features were selected. Ensemble classifier was used based on logistic regression and a decision tree. The proposed model gave 98.8% accuracy, 97.1% recall and 97.9% F-score respectively.

In this paper, a novel feature selection algorithm based on Bat algorithm and Chinese Remainder Theorem (Bat-CRT) is proposed to achieve high detection accuracy for IDS(s).

3. INTRUSION DETECTION APPROACHES

The signatures of some attacks are known, whereas other attacks only reflect some deviation from normal patterns. Consequently, two main approaches have been devised to detect intruders[17].

3.1 Anomaly Detection

Anomaly detection assumes that intrusions will always reflect some deviations from normal patterns. Anomaly detection may be divided into static and dynamic anomaly detection[18]. A static anomaly detector based on the assumption that there is a portion of the system being monitored that does not change [18].

3.2 Misuse Detection

It is based on the knowledge of system vulnerabilities and known attack patterns. Misuse detection is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerability [19]. Ideally, a system security administrator should be aware of all the known vulnerabilities and eliminate them. The term intrusion scenario is used as a description of a known kind of intrusion; it is a sequence of events that would result in an intrusion without some outside preventive intervention [20].

3.3 Advantages and Disadvantages of Anomaly Detection and Misuse Detection

The main disadvantage of misuse detection approaches is that they will detect only the attacks for which they are trained to detect [21]. Novel attacks or unknown attacks or even variants of common attacks often go undetected. The main advantage of anomaly detection approaches is the ability to detect novel attacks or unknown attacks against software systems, variants of known attacks, and deviations of normal usage of programs regardless of whether the source is a privileged internal user or an unauthorized external user. The disadvantage of the anomaly detection approach is that well-known attacks may not be detected, particularly if they match the established profile of the user.

4. MATERIALS AND METHODS

This section discusses about the propose hybrid feature selection based on Bat algorithm and Residue Number System for IDS. The first phase of the model started with data preprocessing which is done using standardization method.

Subsequently, the feature selection is performed with Bat Algorithm and CRT is used to obtain the residues of the features gotten from Bat Algorithm. In the next phase, PCA was used to extract the features obtained in residues from CRT. Finally, we used Naïve Bayes as the classification algorithm. The proposed architecture is shown in figure 1.

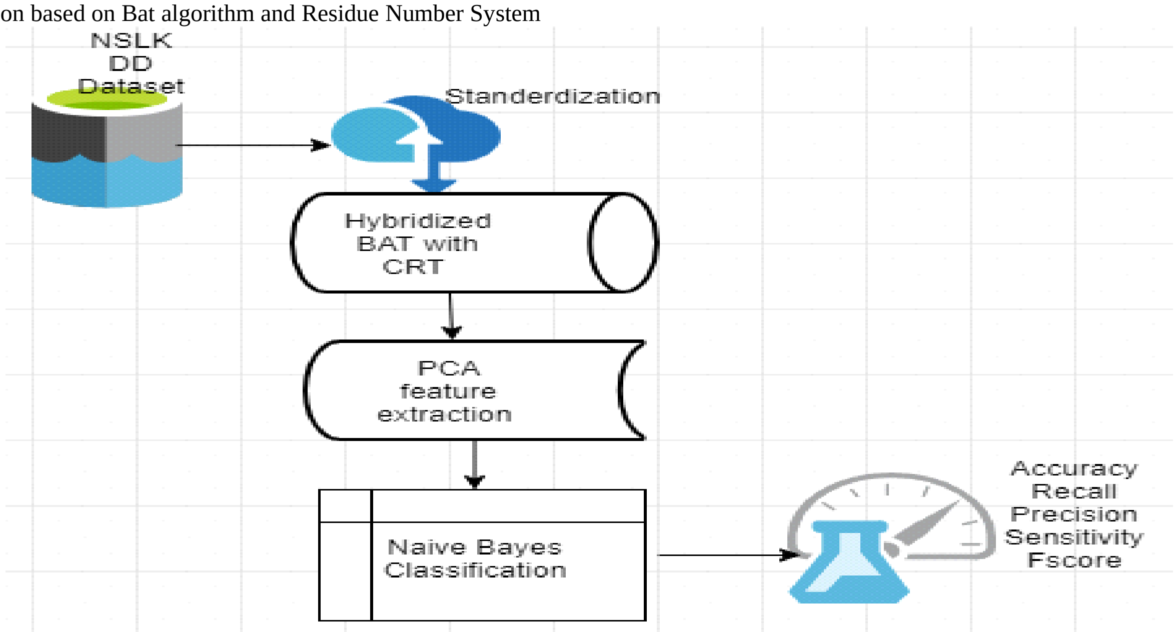

Figure 1: Architecture of the proposed system

4.1 Bat Algorithm

The BA is a new heuristic algorithm proposed by Yang [22] in 2012. It can solve continuous optimization problems and achieve good results. The algorithm simulates the action of bats, which use ultrasound to detect and locate prey [23].

4.2 Residue Number System

In RNS, a set of moduli which are all relatively prime and independent of one another are given. In this approach, integer numbers are represented by the remainders also known as residues of each modulus and operations of the arithmetic are individually based on those residues [24]. The foundation for an RNS representation is a set of relatively prime integers {m1,m2,m3, :::;mk} such that gcd (mi, mj) = 1 for i ≠ j, where the greatest common divisor gcd is of mi and mj . For such a system, M = †i=1 kmi is the dynamic range and any integer X C[0; M-1] and can be represented uniquely as X= (x1, x2, x3….; xk), where xi = |x|mi,0≤ xi < mi. The quest for RNS is the capability to afford carry-free addition as this results in high-speed arithmetic units.

The carry-propagation problem of conventional binary number system representation was then the main bottleneck and challenge of fast arithmetic operation and became the key justification and motivation driving and making researchers to venture into this alternative number system known as RNS for which the residue arithmetic operation in each of the modulus channels is carry free and independent [25].The significant property of RSD number representation systems is the ability to perform borrow-free subtraction and carry-free addition. Chinese Remainder Theorem, Mixed Radix Conversion and New Chinese Remainder Theorem are part of the popular algorithms used in Residue Number System. We used Chinese Remainder Theorem in this paper.

4.3 Principal Component Analysis

PCA is a popularly used dimensionality reduction approach [26] as a result of its flexibility in calculation. It is achieved with eliminating of the less important features in the high dimensional space which constitutes the main computational cost. PCA [27] applies to data sets with K features corresponding to L observations, which can be arranged in a matrix X of K columns and L rows. For intrusion detection, the attribute corresponds to quantitative values obtained from any security-related source of data, including DoS, Probe, User 2 Route, traffic and logs of applications and systems.

4.4 Naïve Bayes

The Naïve Bayes (NB) is a well-known classifier as a result of it computation and simplicity, both of which are gotten from its conditional independence property [28]. The naïve Bayes classifier operates on a strong independence assumption [29]. This means that the probability of one attribute does not affect the probability of the other.

4.5 Dataset Description

A total instance of 25192 will be filtered and extracted from the NSL KDD Cup Dataset with four major classes of attacks and the non-attack class which is normal was taken into consideration for the system experimental set up of this project as well as a total of 41 attributes.

4.6 Dataset Attacks

The dataset is grouped under the following sub-attacks:

Table 1. Attack labelling

ATTACKS	DATA LABELLING
Normal	1
DOS (Denial of Service)	2
Probe	3
U2R (User to Route)	4
R2l (Remote to local)	5

5. RESULT AND DISCUSSIONS

This stage projected the data into training and testing set, the data was spitted into training set and testing set of data. The system used 75% of the data for training the NB classification algorithm. The response value loads the class label; the split rate was set at 0.25 which is an indication of 25% hold out form the data for testing the efficiency and performance state of the classification algorithm.

5.1 Experimental Results Evaluation

The evaluation parameter shows how the NB classifier performed. The testing (probing) evaluation was achieved using the accuracy, recall, precision, sensitivity, specificity and F-score. The performance metrics used to evaluate the model are classification accuracy, sensitivity, specificity, precision and F-score.

5.1.1 Evaluation Parameters for Classification Phase

The Table 2 shows the evaluation parameters of the proposed model in terms of the accuracy, recall, precision, F-score, sensitivity and specificity.

Table 2. Evaluation Parameters for Classification Phase

Algorithm/Metrics	Accuracy	Recall	Precision	F-sore	Sensitivity	Specificity
Proposed BAT + CRT+ PCA+ NB	99.19	97.95	92.50	95.77	99.19	90.90

As revealed in Table 2 and Figure 2, the proposed model gave an accuracy of 99.19, recall of 97.95, precision of 92.50, F-score of 95.77, sensitivity of 99.19 and specificity of 90.90.

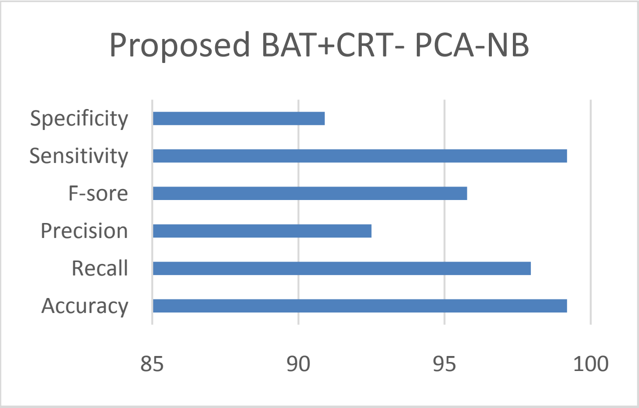

Figure 2. Performance of the proposed model

5.1.2 Comparison with existing works

We compared the proposed model BAT+CRT-PCA-NB in this section with other techniques as shown in Table 3, our proposal gave outstanding results when compared with the existing works. Many of the existing work emphasis on accuracy alone as the performance metrics. However, we used accuracy, recall and precision in this work as part of the performance metrics.

Table 3. Comparison with the existing works

Authors	Techniques	Accuracy	Recall	Precision
[33]	GRRF-FWSVM	98.55	X	X
[30]	PCA-F-NB	98.8	X	x
[31]	PCA-GA-MLP	99.0	X	x
[7]	SVM-RBF	84.1	X	x
[32]	KSVM-RB-MV	92.99	x	x
[32]	KSVM-P-MV	91.27	x	x
[34]	Chi-square + Spearman's rank + Emsemble Classifier	98.8	97.1	98.8
Our Proposal	**BAT+CRT-PCA-NB**	99.19	97.95	92.50

6. CONCLUSION

An intrusion detection system is a hardware or software tool that detects attacks by monitoring the flow of events. Detection of permission allows organizations to maintain their systems against the threats posed by the increasing interconnection between networks and enhance the reliability of their information systems. Intrusion detection systems are security monitoring systems that are used to identify abnormal behaviors and exploit abuse in computers or computer networks. In this paper, the system for detecting anomalies using hybridized Bat+CRT algorithms was investigated. The

NSLKDD data set was used to train and test the proposed model and the results showed that the proposed method has a better performance. The accuracy of the proposed method has improved by an average of 7% for all classes. In this research, CRT algorithm was used to improve the feature selection for intrusion detection system.

7. REFERENCES

[1] T. S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," *Comput. Stand. Interfaces*, vol. 28, no. 6, pp. 670–694, 2006, doi: 10.1016/j.csi.2005.07.002.

[2] P. Amudha, S. Karthik, and S. Sivakumari, "Classification Techniques for Intrusion Detection An Overview," *Int. J. Comput. Appl.*, vol. 76, no. 16, pp. 33–40, 2013, doi: 10.5120/13334-0928.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] E. Vasilomanolakis, S. Karuppayah, M. Muhlhauser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Comput. Surv.*, vol. 47, no. 4, pp. 1–33, 2015, doi: 10.1145/2716260.

[4] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Comput. Sci. Rev.*, vol. 32, pp. 1–23, 2019, doi: 10.1016/j.cosrev.2019.01.002.

[5] J. Mchugh, A. Christie, and J.H. Allen,"ROle of Intrusion Detection Systems," IEEE 17(5): 42 - 51, 2000, doi: 10.1109/52.877859.

[6] G. Hochman, A. Glöckner, and E. Yechiam, "Physiological measures in identifying decision strategies," *Found. Tracing Intuit. Challenges Methods*, vol. 3, no. 3, pp. 139–159, 2009, doi: 10.4324/9780203861936.

[7] V. Manekar and K. Waghmare, "Intrusion Detection System using Support Vector Machine (SVM) and Particle Swarm Optimization (PSO)," no. 3, pp. 2–6, 2014.

[8] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," *Doktors avhandlingar vid Chalmers Tek. Hogsk.*, no. 1530, pp. 83–99, 1999, doi: 10.1109/secpri.1997.601330.

[9] Wenke Lee, 1999 "A Data Mining Framework for Constructing Features and Models for Intrusion Detection Systems." Columbia University, UMI Number: 9949009.

[10] M. K. Siddiqui and S. Naahid, "Analysis of KDD CUP 99 Dataset using Clustering based Data Mining," *Int. J. Database Theory Appl.*, vol. 6, no. 5, pp. 23–34, 2013, doi: 10.14257/ijdta.2013.6.5.03.

[11] S. J. Horng *et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Syst. Appl.*, vol. 38, no. 1, pp. 306–313, 2011, doi: 10.1016/j.eswa.2010.06.066.

[12] T. Eldos, "on the Kdd ' 99 Dataset : Statistical Analysis for Feature Selection on the Kdd ' 99 Dataset : Statistical Analysis for Feature Selection Taisir Eldos *, Mohammad Khubeb Siddiqui and Aws Kanan," no. January 2012, 2014.

[13] I. Ahmad, M. Hussain, A. Alghamdi, and A. Alelaiwi, "Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components," *Neural Comput. Appl.*, vol. 24, no. 7–8, pp. 1671–1682, 2014, doi: 10.1007/s00521-013-1370-6.

[14] U. Ravale, N. Marathe, and P. Padiya, "Feature selection based hybrid anomaly intrusion detection system using K Means and RBF kernel function," *Procedia Comput. Sci.*, vol. 45, no. C, pp. 428–435, 2015, doi: 10.1016/j.procs.2015.03.174.

[15] Z. Dewa and L. A., "Data Mining and Intrusion Detection Systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, 2016, doi: 10.14569/ijacsa.2016.070109.

[16] A. Singh and A. Goyal, "Intrusion Detection System Based on Hybrid Optimization and using Neural Network: A Review," *Ijrece*, vol. 6, no. 3, pp. 1138–1143, 2018, doi: 10.13140/RG.2.2.23285.83681.

[17] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," *Comput. Secur.*, vol. 24, no. 4, pp. 295–307, 2005, doi: 10.1016/j.cose.2004.09.008.

[18] A. Jones and R. Sielken, "Computer system intrusion detection: A survey," *Comput. Sci. Tech. Rep.*, pp. 1–25, 2000.

[19] J. Raiyn, "A survey of cyber attack detection strategies," *Int. J. Secur. its Appl.*, vol. 8, no. 1, pp. 247–256, 2014, doi: 10.14257/ijsia.2014.8.1.23.

[20] M. Govindarajan and R. Chandrasekaran, "Intrusion detection using neural based hybrid classification methods," *Comput. Networks*, vol. 55, no. 8, pp. 1662–1671, 2011, doi: 10.1016/j.comnet.2010.12.008.

[21] A. K. Ghosh, J. Wanken, and F. Charron, "Detecting anomalous and unknown intrusions against programs," *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, pp. 259–267, 1998, doi: 10.1109/CSAC.1998.738646.

[22] X. S. Yang and A. H. Gandomi, "Bat algorithm: A novel approach for global engineering optimization," *Eng. Comput. (Swansea, Wales)*, vol. 29, no. 5, pp. 464–483, 2012, doi: 10.1108/02644401211235834.

[23] Y. Shen, K. Zheng, C. Wu, M. Zhang, X. Niu, and Y. Yang, "An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection," *Comput. J.*, vol. 61, no. 4, pp. 526–538, 2018, doi: 10.1093/comjnl/bxx101.

[24] I. S. Volume, "Computing and Information Systems," *Inf. Syst.*, vol. 9, no. 2, 2005.

[25] C. H. Chang, A. S. Molahosseini, A. A. E. Zarandi, and T. F. Tay, "Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications," *IEEE Circuits Syst. Mag.*, vol. 15, no. 4, pp. 26–44, 2015, doi: 10.1109/MCAS.2015.2484118.

[26] K. J. Chabathula, C. D. Jaidhar, and M. A. Ajay Kumara, "Comparative study of Principal Component Analysis based Intrusion Detection approach using machine learning algorithms," *2015 3rd Int. Conf. Signal Process. Commun. Networking, ICSCN 2015*, pp. 1–6, 2015, doi: 10.1109/ICSCN.2015.7219853.

[27] J. Camacho, R. Theron, J. M. Garcia-Gimenez, G. MacIa-Fernandez, and P. Garcia-Teodoro, "Group-Wise Principal Component Analysis for Exploratory Intrusion

Detection," *IEEE Access*, vol. 7, pp. 113081–113093, 2019, doi: 10.1109/ACCESS.2019.2935154.

[28] L. Koc, T. A. Mazzuchi, and S. Sarkani, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier," *Expert Syst. Appl.*, vol. 39, no. 18, pp. 13492–13500, 2012, doi: 10.1016/j.eswa.2012.07.009.

[29] R. Kanagalakshmi and V. N. Raj, "Network Intrusion Detection Using Hidden Naive Bayes Multiclass Classifier Model," no. 03, pp. 76–84, 2014.

[30] Soukaena Hassan Hashem, "Efficiency of SVM and PCA to Enhance Intrusion Detection System" vol. 3, no. 4, pp. 381–395, 2013.

[31] I. Ahmad, A. B. Abdullah, A. S. Alghamdi, M. Hussain, and K. Nafjan, "Features subset selection for network intrusion detection mechanism using genetic eigen vectors," *Proc. 2011 Int. Conf. Telecommun. Technol. Appl. (ICTTA 2011)*, vol. 5, no. November 2014, pp. 75–79, 2011.

[32] A. M. Hasan, M. Nasser, B. Pal, and S. Ahmad, "Intrusion Detection Using Combination of Various Kernels Based Support Vector Machine," *Int. J. Sci. Eng. Res.*, vol. 4, no. 9, pp. 1454–1463, 2013.

[33] Kavitha G., & Elango N.M (2020) "An Approach to Feature Selection in Intrusion Detection Systems Using Machine Learning Algorithms"*International Journal of e- Collaboration* 16(4) DOI: 10.4018/IJeC.2020100104.

[34] Q. R. S. Fitni and K. Ramli, "Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems," *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, 2020, pp. 118-124, doi: 10.1109/IAICT50021.2020.9172014.