SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I1P111

Volume 11 Issue 1, 143-149, January 2024
© 2024 Seventh Sense Research Group®

Original Article

A Hybrid Support Vector Machine and Artificial Neural Network Based Cyber Security Framework

Mohammed Ahmed[1], G. Rama Mohan Babu[2]

[1]Department of Computer Science Engineering, Dr. Y.S. Rajasekhar Reddy University College of Engineering and Technology, Acharya Nagarjuna University, Andhra Pradesh, India.
[2] Department of Computer Science Engineering (AI&ML), RVR & JC College of Engineering, Andhra Pradesh, India.

[1]Corresponding Author : ahmed.cse2016@gmail.com

Received: 19 October 2023 Revised: 29 November 2023 Accepted: 20 December 2023 Published: 13 January 2024

***Abstract** - Cyber security issues are frequently present in big organizations and government sectors. Cyber security threats would attempt to steal sensitive information from the organization. Thus, it is necessary to avoid the cyber security risks happening on the network to provide users with a secure environment. This was done in our previous research method by introducing the method, namely Big Data Cyber Security Framework (BDCSF). The classification technique used in this work tends to have more computational overhead and might reduce its accuracy with the presence of a large volume of data. These issues are focused on and avoided by proposing a Hybrid Support Vector Machine and Artificial Neural Network Threat Detection Method (HSVMANN-TDM). In this research work, feature selection is initially made at two levels. In the first level, clustering-based feature selection is made using the Improved K means algorithm. The second level cluster of features is given as input to the improved cat swarm algorithm to extract the final selected features. After feature selection, a hybrid SVM ANN algorithm is introduced for threat detection. Here, the output layer of the ANN algorithm will be given as input to the SVM algorithm. This research can predict the fraudulent transactions happening on the network more accurately. The numerical assessment of this research work proves that the proposed research method can perform better than previous works.*

***Keywords** - Cyber security framework, Optimal feature selection, Clustering-based feature selection, Classification framework, Credit card fraudulent detection.*

1. Introduction

The global proliferation of cyberthreats has an impact on all system clients. Diverse security monitoring frameworks safeguard PC systems and assets from cyberattacks. Security teams must concentrate on the most critical assets while leaving others unprotected due to the increasing number of tools, operating systems, platforms, and threats. This keeps the newest technologies up to date. A capable security-checking framework is desperately needed to filter the enormous system datasets produced by this technique [1].

This work used a sizable system dataset containing malware attacks to construct a specialized framework. One area that is just now starting to examine the application of significant information breakthroughs is digital security [2]. The feature determination model's task is to eliminate irrelevant features and make a set of features more and more useful [3].

It is possible to achieve improved accuracy rates and system performance by removing features from the dataset that are not relevant. Data mining techniques can be employed to accomplish this. To improve learning speed, the emphasis is placed on improvising feature reduction techniques [4]. One of the most exciting aspects of information mining is grouping. Group analysis's central concept is dividing massive informational articles into smaller subsets. Since each small subset is unique, the items are grouped based on reducing interclass distance and increasing intraclass closeness [5].

Extortion discovery includes recognizing rare misrepresentation exercises among various authentic exchanges as fast as conceivable [6]. Extortion detection solutions rapidly evolve to keep up with new approaching fraudulent systems worldwide. However, because of the extreme confinement of the ideas trade in the extortion site, the advancement of fresh misrepresentation recognition procedures is becoming increasingly difficult [7].

On the other hand, extortion identification is fundamentally a one-of-a-kind occasion issue, also known as exception research, oddity location, special case mining, uncommon classes, imbalanced data, and so on [8]. The quantity of fake exchanges is usually a shallow division of the complete exchanges. Identifying misleading trades precisely and effectively is now a demanding and challenging task. Thus, advancing proficient techniques that recognize uncommon extortion exercises from billions of accurate exchanges appears essential.

2. Related Works

Gunantara et al. [9] analyzed the different evolutionary algorithms for cyber security detection. The multi-criteria methods utilized in this work for the performance evaluation are Ant Colony Optimization, Particle Swarm Optimization, Genetic algorithm, and so on. This research aims to reduce cyber security crimes by accurately detecting them with a lessoned signal-to-noise ratio. And also, this research work focuses on balancing the load fluctuations, power consumption, and so on. The numerical evaluation of this work proved that the genetic algorithm attains better performance or equivalent performance. Lastly, the choice of the way combined by the GA strategy demonstrates the sets of ways consistently equal to the ACO and PSO techniques and show those that shift.

Hassani, and Jafarian [10] distinguished the beginning period of bosom malignant growth as essential to diminish the misfortunes of life utilizing half-and-half grouping procedures. This malignant growth has become the most unsafe sort of disease among ladies on the planet. Here, fuzzy ART algorithm attributes are estimated optimally using multi-criteria optimization algorithms. Thus, the performance of Fuzzy ART can be improvised efficiently. In any case, its exhibition is essentially improved by utilizing developmental streamlining techniques. These half-and-half arrangement procedures were tried on a preparation informational index given by the Wisconsin dataset for bosom disease [11, 12]. The best execution acquired from this calculation is 97.80% for precision and 98.92% for explicitness.

Zafar, and Soni [13] determined how meta-heuristic calculations can be delivered to stretch security and advancement in MANET. Heuristics gives customized solutions for specific problems, while the metaheuristic is designed to overcome difficulties and provide clear solutions for every search. Different security conventions utilized to verify versatile, specially appointed systems experience various disadvantages, prompting other security ruptures. Insightful enhancement methods outperform weaknesses of existing secure conventions by improving different execution parameters like start-to-finish delay, throughput, parcel conveyance division, and so forth, thus keeping Quality of Service (QOS) in specially appointed systems. These calculations bring about the briefest course for information transmission between different hubs and encroach protection and security confinements, bringing about upgraded cryptographic parameters and thus improving the security of MANET.

Khorram, and Baykan [14] analyzed evolutionary algorithms such as Particle Swarm Optimization, Ant Colony Optimization, k Nearest Neighbor, and Support Vector Machine over the cyber security implementation process. Authors utilized these algorithms to analyze cyber security threats to prevent and avoid them. This is done by using the NSL-KDD dataset, which can be utilized to perform training and testing. The analysis confirmed that the artificial bee colony algorithm leads to increased accuracy by selecting the most optimal features, and the KNN classifier is the more optimal classifier for resulting in the detection outcome [15, 16].

Saidala, and Devarakonda [17] attempted to detect cyber security threats by introducing a hybridized cuckoo search algorithm. The main advantage of this algorithm is that it works parallel to ensure increased accuracy in cyber threat detection. This research work is assessed in the heart disease dataset by using which assaults are detected based on dataset corruption. The numerical assessment of this research work tends to prove that the proposed work leads to increased accuracy, precision, recall, and f-measure rate. This method leads to accurate and better detection of heart issues happening. The exploratory outcomes show that the proposed strategy for foreseeing coronary illness is exceptionally aggressive.

Tsai et al. [18] gave a short study of metaheuristics for human services framework and a guide for analysts looking at metaheuristics and social insurance to build a progressively productive and successful medicinal services framework. This work starts with a talk of changes for medicinal services, trailed by a short audit of the highlights of "exceptional innovations for social insurance." Then, an enormous learnable information examination structure for the human services framework is introduced, giving an elite answer for the imminent difficulties of vast amounts of information.

Bajpai, and Dayanand [19] attempted to improve the security mechanisms to enhance the security level of big data. The main goal of this research work is to optimize the business processes by concentrating on knowledge and choices. To accomplish this, a large volume of information is processed to extract the knowledge related to the security threats on the network [20, 21]. By doing so, the security level of a business organization can be improved. They enable associations to perceive examples of movement that speak to organized dangers.

Sabar et al. [22] utilized the support vector machine for the classification process by using which security threats can be predicted accurately. This method is introduced to resolve the issues by adapting the hyper-heuristics structure. The main goal of this research work is to handle both the high-level and low-level features. This method uses threshold values to perform accurate classification; thus, the precise classification outcome can be ensured. The performance of the entire research work is enhanced by integrating the Pareto set with the SVM classifiers. The overall assessment of this research work tends to prove that the proposed SVM method can ensure an increased accuracy level in security threat detection.

3. Cyber Security Detection Framework

In this research work, feature selection is initially done at two levels. In the first level, clustering-based feature selection uses the Improved K means algorithm. The second level cluster of features is given as input to the improved cat swarm algorithm to extract the final selected features. After feature selection, a hybrid SVM ANN algorithm is introduced for threat detection. Here, the output layer of the ANN algorithm will be given as input to the SVM algorithm. This research can predict the fraudulent transactions happening on the network more accurately.

3.1. Two-Level Feature Selection Process

Feature selection is a fundamental strategy to diminish the dimensionality issue in information mining tasks. Improve the prescient exhibition of the characterization procedure by building different information grouping models dependent on the yield, including determination strategies. In this work, two-level feature selection is done to improve the presentation. In the principal level of feature selection, enhanced k implies calculation is utilized. The yield of this bunching calculation will be given as a contribution to the second degree of feature selection. In the subsequent level, improved cat swarm calculation is presented for the ideal feature selection result.

3.1.1. First-Level Feature Selection Using Improved K-Means Algorithm

Credit card transaction features would consist of many relevant and irrelevant features. In this section, feature selection is performed by introducing the two-level feature selection. In the first level, clustering-based feature selection is performed. This is done by using an improved k-means algorithm.

In contrast, the K-means algorithm is also a cluster analysis that undergoes processes like data preparation and similarity detection between different objects and finally groups them into different sets as output. This method chooses the initial k value for the increased accuracy level. In this method, the number of data points will be clustered based on initial k features chosen as cluster heads. The distance between multiple features will be calculated based on which most similar clusters will be chosen. Our dataset consists of two classes.

Thus, the clustering process would result in two clusters based on similarity. To make the data points in a group more similar to one another and distinct from the data points in other groups, a group or collection of data points can be clustered. It is essentially to find specific data from the collection of items based on similarities and differences. The features involved within these two clusters will be omitted as irrelevant features. The processing flow of the improved k-means algorithm is given below:

```
Input   : NF  → Number of features
          NC  → Number of clusters
          Fi  → $i_{th}$ feature

Output  : NCC→ Number of closest centroid
          Dist → Euclidean distance (Euclidean distance is
                 the line segment's length or distance
                 between two points) to the NCC
          Mj  → New centroids

Begin
Step 1: For i = 1 to n
Step 2: For j = 1 to k
          Measure the Euclidean distance between ith feature
          and new centroids
                  Dist (Fi, Mj)
Step 3: End for
        Predict the closest centroid mj to the ith feature Fi
                  Mj (new) = Mj (old) + Fi ;
                  NFj (new) = NFj (old) + 1
                  MSE = MSE + dist (Fi, Mj)
        Update the centroid and Euclidean distance
                  NCC = number of closest centroid
                  Dist  [i] = Euclidean distance to the NCC
Step 4: End for
Step 5: Update the centroids
        For j =1 to k
                  Mj (new)= Mj (new) / NFj (new)
```

3.1.2. Second-Level Feature Selection Using Improved Cat Swarm Algorithm

After feature clustering, the second-level optimal feature selection is performed using this work's Cat Swarm Optimization Algorithm. CSO is the evolutionary algorithm that works by adapting the food-foraging behaviour of cats. The foraging behavior in the CSO algorithm stores the grouped data once the feature selection process is completed.

Support Vector Machine is the Machine Learning algorithm that tends to classify the data based on hyperplanes. Typically, the CSO algorithm tends to have two modes: seeking and tracing. In the seeking mode of CSO, cats tend to search for their food location. In the tracing mode of CSO, cats tend to look for their prey in an idle state. Here, the mixing ratio defines the overall performance outcome of the CSO algorithm.

The CSO algorithm selects the most optimal solutions in the local set alone. However, the optimal decision can be made by interchanging the observed information with the cats in both seeking and tracing modes. This is not focused on the CSO algorithm, which tends to reduce performance. ICSO is a mighty swarm intelligence-based optimization that efficiently solves the problem. Moreover, the ICSO-based clustering algorithm gives better results than the existing clustering algorithms. Thus, an Improved Cat Swarm Optimization algorithm (ICSO) is introduced in this work.

In this work, the tracing mode of CSO is altered by allowing information exchanges between the different populations of cats. The cat swarm algorithm extracts the final selected features from the group of clusters. Thus, accurate decision-making can be made. The work procedure of ICSO is given below:

```
Input   : Number of features as cats
Output  : Selected features

Initialize the population of N cats (features)
Divide the features into G groups
While (termination condition is satisfied)
Initialize MR value
Separate the cats into seeking and tracing modes based on
MR value
While (number of iteration < max iteration)
    For i = 1 to k cats
            Find the fitness values
            Predict the best cat xbest
    End for
    Update the position of cats based on motion flags
    assigned by seeking mode and parallel tracing mode
    Update the motions flags of all cats
    Perform information exchanges between the cats
Repeat
Repeat
```

The above algorithm selects the most optimal features from the given input dataset. These selected features tend to provide better classification outcomes. The classification is processed in the following section.

3.2. Fraudulent Transaction Detection Using Hybrid SVM and ANN Method

The SVM-ANN half-breed classifier displayed in this paper forms the info that includes vectors in two phases, first by ANN and from that point by the SVM. The production of cross-breed ANN-SVM classifier consists of the accompanying:

a) Training a feed foreword ANN classifier in conventional route utilizing back proliferation (BP) calculation.
b) Replacement of yield layer of ANN by SVM.
c) Training of SVM by yield of the truncated ANN.

The essential point of supplanting the yield layer with SVM is to lessen the inclination of ANN to meet a nearby minimum coming about in under-fitting and simultaneously keep away from the propensity of SVM to over-fit.

A Modified Artificial Neural Network (M-ANN) is applied to predict refractivity, improving the dynamic performance of the two-dimensional sensors.

3.2.1. Artificial Neural Network

ANNs are portrayed as a significantly related display of fundamental processors called neurons. ANN takes inspiration from the natural learning system of human personality. ANNs have been commonly used starting late for convenient applications, for instance, structure affirmation, portrayal, work gauge, etc.

An ordinary ANN contains one input, yield, and covered layer. A couple of neurons are in each layer, and neurons in layers are related to neighboring layer neurons with different affiliation loads. The neurons of the information layer are supported with input-incorporated vectors. Each neuron of concealed and yield layers gets signals from the neurons of the past layer expanded by heaps of the interconnection between neurons.

The neuron starting there produces yield by passing the additional sign through a trade work. The regulated learning procedures commonly arrange multilayer neural frameworks. In the coordinated learning model, organize is given a game plan of information vector and the concentrated yield needed from the framework. Let, for example, the wellsprings of data and the required goal of a neural framework are:

$$\{p1, t1\}, \{p2, t2\},....,\{pQ, tQ\}$$

Where pQ is a commitment to the network, and tQ is its related objective.

The framework is arranged iteratively. Mean Square Error (MSE) among target and framework yield is resolved in each cycle. Mean square error is the fair value of errors and the average squared error values. The MSE at the kth cycle is given by:

$$F(x) = (tk - ak)2$$

Where F(x) is MSE work, tk and ak are the goals and yield vectors at the kth accentuation.

The framework arrangement is practiced by changing the heaps and tendencies with the objective that the MSE work F(x) is restricted. Back Propagation (BP) using the Levenberg-Marquardt count is often used to get ready ANN. BP is an incline plunge procedure that uses the decided MSE at each layer to adjust the estimation of the interconnecting burdens to the neuron to confine MSE.

This strategy of layer-wise weight change is reiterated until the base of the misstep work is cultivated or the MSE has come to such a low worth, which would have the alternative to gather the information vectors successfully. The Levenberg-Marquardt method is a possible option for algorithms rather than other methods, and this method is easy to handle a large set of parameters rapidly. The heaps at the mth layer in k + 1th accentuation are surveyed by:

$$w_{i,j}^{m} = w_{i,j}^{m}(k) - a\frac{\partial F(x)}{\partial w_{i,j}^{m}}$$

BP is a brisk and powerful figuring that achieves blend quickly. In any case, BP, like some other tendency hunt framework, gives clashing and flighty execution when applied to complex nonlinear streamlining issues, for instance, ANNs. Due to the stunning idea of getting ready ANNs, the screwup surfaces are amazingly bewildering.

Since BP can combine locally, the courses of action are astoundingly dependent upon the primary sporadic draw of burdens, in light of which BP count will most likely get trapped in a close-by plan that could be the overall game plan. This local association and frailty to live close by minima could show noteworthy issues while using ANNs for realistic applications.

3.2.2. Support Vector Machine

The Support Vector Machine is a Machine Learning algorithm that uses hyperplanes to classify data. The SVM algorithm tends to separate the data objects into two classes based on hyperplane value. Expect that in a given preparing test set, G= {xi, yi} where for each information vector xi has a place with Rd; there is an ideal worth having a place with class characterized by {+1, - 1}. Here, yi is either +1 or - 1, showing the class to which the point xi has a place. The xi is a d-dimensional genuine esteemed vector. SVM makes the arrangement capacity of the structure:

$$f(x) = (w, \Phi(x))+b$$

$$\Phi: R^{d} \rightarrow F, w \in F$$

Where, $\Phi(x)_{i=1}^{N}$ speaks to the information, including space, $\{w_i\}_{i=1}^{N}$ and b are the coefficients. These are assessed by limiting the accompanying danger work:

$$R(C) = C\frac{1}{I}\sum_{i=1}^{N} L_x\big(y_i, f(x)\big) + \frac{1}{2}||w||^2$$

Where, $L_X(y_i,f(x))$ The misfortune work estimates the surmised blunders between the expected yield yi and the determined yield f(xi), and C is a consistent regularization. $\frac{1}{2}||w||^2$ decides the exchange between the preparation blunder and the speculation execution.

4. Results and Discussion

The algorithms in this cyber security defense strategy are compared to benchmarked to guarantee accuracy and model complexity. The testing is carried out on the credit card transaction dataset from the UCI repository database. The UCI repository analyses the collected databases, data generators, and related domain theories. The confusion matrix is a metric for evaluating the performance of a classification system whose output can be divided into two or more classes. The metric utilized for the two-class classification job is determined by the confusion matrix shown in Table 1.

Table 1. Confusion matrix

Classes		**Anticipated**	
		Yes	**No**
Real	**Yes**	TP	FP
	No	FN	TN

The ratio of real positives to anticipated positives, as a function of correctly classified cases (TPs) and incorrectly classified cases (FNs), is known as recall.

$$\text{Recall} = \frac{\text{TruePositive}}{\text{TruePositive} + \text{FalseNegative}}$$

Precision is characterized as a proportion of the precision given that a specific class has been anticipated and indicates the extent of the positives identified, which are, in reality, right. Accuracy is the proportion of anticipated positives that are genuine positive.

$$\text{Precision} = \frac{\text{TruePositive}}{\text{TruePositive} + \text{False Positive}}$$

The F1-score measure is a consistently adjusted exactness and review. It takes the test's precision and survey into thought for preparing the score. It will generally be seen as a weighted typical of the precision and survey, where an F1-score significantly achieves its best motivating force under the least positive conditions score at 0.

$$\text{F1} - \text{Score} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

The higher the categorization accuracy, the better the system performance. This measure's strength lies in its simplicity, calculated using the expression.

Accuracy =TN+TP/ TN+FP +FN+TP

Figure 1 illustrates the precision comparison results of the newly introduced HSVMANN-TDM classifier and the available classifiers like BDCSF, SVM, and HH-SVM. Figure 1 demonstrates that the newly introduced HSVMANN-TDM yields a greater precision of 93.6, which is 5.10% better than BDCSF, 8.9% better than HH-SVM, and 14.07% better than SVM.

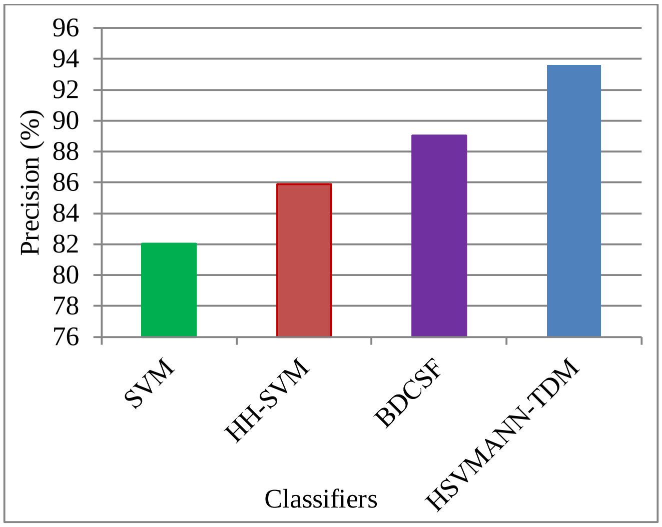

Fig. 1 Comparison of precision results vs. Classifiers

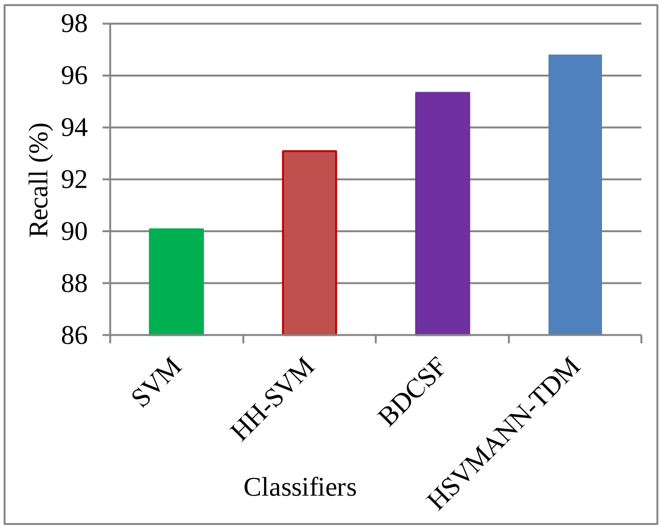

Fig. 2 Comparison of recall results vs. Classifiers

Figure 2 illustrates the results of the recall comparison of the HSVMANN-TDM and the available classifiers, such as BDCSF, SVM, and HH-SVM. Figure 2 demonstrates that the HSVMANN-TDM yields a more excellent recall of 96.8%, 1.53% better than BDCSF, 3.99% better than HH-SVM, and 7.46% better than SVM. Figure 3 illustrates the results of the f-measure comparison of the newly introduced HSVMANN-TDM and the available classifiers, such as BDCSF, SVM, and HH-SVM, correspondingly. Figure 3 reveals that the HSVMANN-TDM yields a higher f-measure of 94.6%, 2.72% better than BDCSF, 5.88% better than HH-SVM, and 10.15% better than the SVM algorithm. Figure 4 illustrates the results of the accuracy comparison of the newly introduced HSVMANN-TDM and the available classifiers like BDCSF, SVM, and HH-SVM correspondingly. Figure 4 reveals that the HSVMANN-TDM yields a higher accuracy of 92.7%, which is 3.91% better than BDCSF, 8.25% better than HH-SVM, and 14.33% better than SVM.

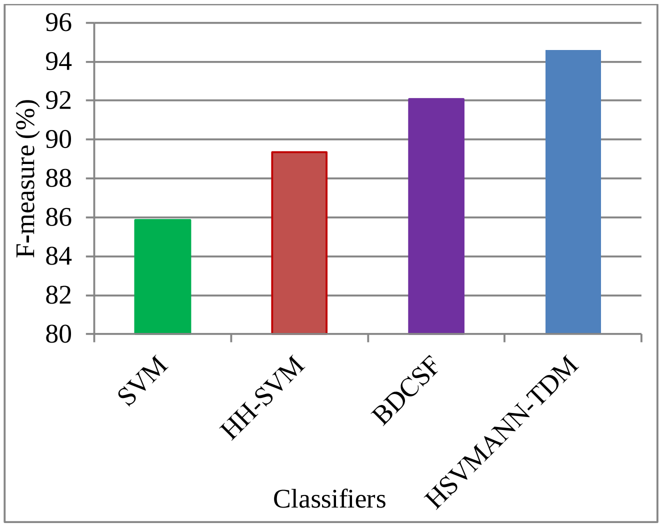

Fig. 3 Comparison of F-measure results vs. Classifiers

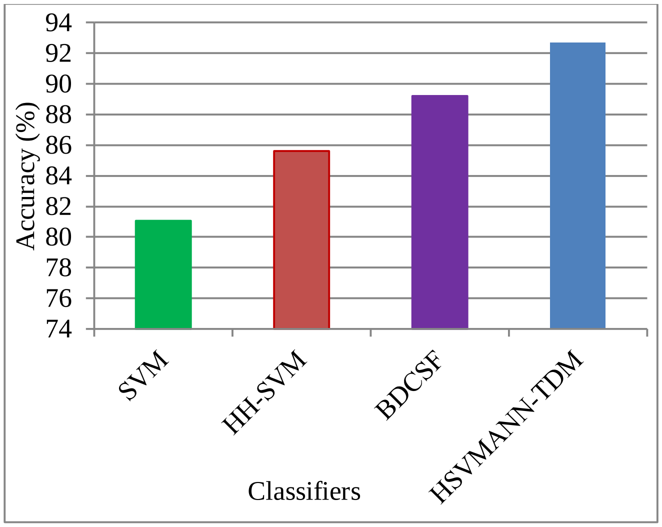

Fig. 4 Comparison of accuracy outcomes with classifiers

5. Conclusion

This research focused on implementing the cyber security framework to enhance security in various applications. This is done by introducing new techniques that lead to optimal and reliable detection of cyber security violations happening in the real world. To do so, here feature selection and classifier procedures are adapted. This research follows two steps of the feature selection process to improve the accuracy level of feature selection. In the first step, clustering and an optimization algorithm are implemented. This leads to increased performance of the classifier. These selected features will be learned using Hybrid SVM and ANN algorithms. The performance assessment uses the Matlab toolkit, considering the accuracy metric. This comparison proved that HSVMANN-TDM yields a higher accuracy of 92.7%, which is 3.91% better than BDCSF, 8.25% better than HH-SVM, and 14.33% better than SVM.

References

[1] T.T. Teoh et al., "Analyst Intuition Inspired High Velocity Big Data Analysis Using PCA Ranked Fuzzy k-Means Clustering with Multi-Layer Perceptron (MLP) to Obviate Cyber Security Risk," *2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, Guilin, China, pp. 1790-1793, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[2] R. Senthamil Selvi, and M.L. Valarmathi, "Enabling Data Security in Data Using Vertical Split with Parallel Feature Selection Using Meta Heuristic Algorithms," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 3, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] P. Venkata Krishna, K. Venkatesh Sharma, and A. MallaReddy, "A Machine Learning-Based Approach for Detecting Network Intrusions in Large-scale Networks," *International Journal of Computer Engineering in Research Trends*, vol. 10, no. 2, pp. 69-76, 2023. [CrossRef] [Publisher Link]

[4] Daniel Peralta et al., "Evolutionary Feature Selection for Big Data Classification: A MapReduce Approach," *Mathematical Problems in Engineering*, vol. 2015, pp. 1-12, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[5] T. Mohana Priya, and A. Saradha, "An Improved K-means Cluster Algorithm Using Map Reduce Techniques to Mining of Inter and Intra Cluster Data in Big Data Analytics," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 7, pp. 679-690, 2108. [Google Scholar] [Publisher Link]

[6] Mohiuddin Ahmed, Abdun Naser Mahmood, and Md. Rafiqul Islam, "A Survey of Anomaly Detection Techniques in Financial Domain," *Future Generation Computer Systems*, vol. 55, pp. 278-288, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] Samaneh Sorournejad et al., "A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective," *arXiv*, pp. 1-26, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Thejeswari, K. Sreenivasulu, and B. Sowjanya, "Cyber Threat Security System Using Artificial Intelligence for Android-Operated Mobile Devices," *International Journal of Computer Engineering in Research Trends*, vol. 9, no. 12, pp. 275-280, 2022. [CrossRef] [Publisher Link]

[9] Kamran Hassani, and Kamal Jafarian, "An Intelligent Method for Breast Cancer Diagnosis Based on Fuzzy ART and Metaheuristic Optimization," *XIV Mediterranean Conference on Medical and Biological Engineering and Computing*, pp. 200-204, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Tu N. Nguyen et al., "Cyber Security of Smart Grid: Attacks and Defenses," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Shanying Zhu, Vijayalakshmi Saravanan, and Bala Anand Muthu, "Achieving Data Security and Privacy Across Healthcare Applications Using Cyber Security Mechanisms," *The Electronic Library*, vol. 38, no. 5/6, pp. 979-995, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Sherin Zafar, and M.K. Soni, "A Novel Crypt-Biometric Perception Algorithm to Protract Security in MANET," *International Journal of Computer Network and Information Security*, vol. 6, no. 12, pp. 64-71, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[13] Tahira Khorram, and Nurdan Akhan Baykan, "Feature Selection in Network Intrusion Detection Using Metaheuristic Algorithms," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 4, no. 4, pp. 704-710, 2018. [Google Scholar] [Publisher Link]

[14] Priyan Malarvizhi Kumar et al., "Intelligent Face Recognition and Navigation System Using Neural Learning for Smart Security in Internet of Things," *Cluster Computing*, vol. 22, pp. 7733-7744, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. Shanthini et al., "Threshold Segmentation Based Multi-Layer Analysis for Detecting Diabetic Retinopathy Using Convolution Neural Network," *Journal of Ambient Intelligence and Humanized Computing*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ravi Kumar Saidala, and Naga Raju Devarakonda, "A New Parallel Metaheuristic Optimization Algorithm and Its Application in CDM," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, India, pp. 667-674, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[17] Chun Wei Tsai, "Metaheuristic Algorithms for Healthcare: Open Issues and Challenges," *Computers & Electrical Engineering*, vol. 53, pp. 421-434, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] Pelin Angin, Bharat Bhargava, and Rohit Ranchal, "Big Data Analytics for Cyber Security," *Security and Communication Networks*, vol. 2019, pp. 1-3, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Plabon Bhandari Abhi et al., "A Novel Lightweight Cryptographic Protocol for Securing IoT Devices," *International Journal of Computer Engineering in Research Trends*, vol. 10, no. 10, pp. 24-30, 2023. [CrossRef] [Publisher Link]

[20] Yassine Maleh et al., "Machine Intelligence and Big Data Analytics for Cybersecurity Applications," *Studies in Computational Intelligence*, vol. 919, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Nasser R. Sabar, Xun Yi, and Andy Song, "A Bi-Objective Hyper-Heuristic Support Vector Machines for Big Data Cyber-Security," *IEEE Access*, vol. 6, pp. 10421-10431, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Hung-Yi Lin, "Feature Selection Based on Cluster and Variability Analyses for Ordinal Multi-Class Classification Problems," *Knowledge-Based Systems*, vol. 37, pp. 94-104, 2013. [CrossRef] [Google Scholar] [Publisher Link]