Article

Effective One-Class Classifier Model for Memory Dump Malware Detection

Mahmoud Al-Qudah [1], Zein Ashi [2], Mohammad Alnabhan[3] and Qasem Abu Al-Haija [3],*

[1] Department of Cybersecurity, Princess Sumaya University for Technology, Jordan; mah2028173@std.psut.edu.jo
[2] Department of Cybersecurity, Princess Sumaya University for Technology, Jordan; zai20198121@std.psut.edu.jo
[3] Department of Computer Science, Princess Sumaya University for Technology, Jordan; m.alnabhan@psut.edu.jo
[4] Department of Cybersecurity, Princess Sumaya University for Technology, Jordan; q.abualhaija@psut.edu.jo
*Corresponding author: q.abualhaija@psut.edu.jo

Abstract: Malware complexity is rapidly increasing, causing catastrophic impacts on computer systems. Memory dump malware is gaining increased attention due to its ability to expose plaintext passwords or key encryption files. This paper presents an enhanced classification model based on One class SVM (OCSVM) classifier that can identify any deviation from the normal memory dump file patterns and detect it as malware. The proposed model integrates OCSVM and Principal Component Analysis (PCA) for increased model sensitivity and efficiency. An up-to-date dataset known as "MALMEMANALYSIS-2022" was utilized during the evaluation phase of this study. The accuracy achieved by the traditional one-class classification (TOCC) model was 55%, compared to 99.4% in the one-class classification with PCA (OCC-PCA) model. Such results have confirmed the increased performance achieved by the proposed model.

Keywords: novelty-class; one online-Class SVM (OCSVM); memory dump; malware; Principal Component Analysis (PCA); dimensionality reduction

1. Introduction

Computer systems have progressed and developed indivisibly to connect to our lives, drawing in the enchanted by attackers. As a result, computer systems are utilized frequently in business activities. Thus, many systems have been targeted unfriendly such as hacking information and botnet exploitation [1] [2]. Much malicious software affects computer systems as malware, making a system non-operational, harmful files or programs are added, a few crucial instruction sets are changed, or particular vital application files are removed. In particular, malware programs disrupt regular user activity in computer systems by conducting undesired or harmful actions [3]. Agreeing to the AV-Test Institute, the number of malware attacks on operating systems has increased by 722.505 million since 2022, compared to 13.365 million in 2008 [4].

Many malware, such as ransomware, spyware, rootkits, worm, viruses, bots, botnets, trojan horses, and other malware types, exist and target many parts of systems, especially memory dump files. Memory dump handles to discover a fault within the working applications or programs. Memory dumps files regularly contain information on the final state of programs and applications. Memory areas, program status, and other related points of interest make up this information and be tempting for attackers to steal passwords and encryption keys, causing a breach and threatening confidentiality, integrity, and authenticity [5].

Manual detection methods are implemented, causing a low-accuracy rate and time-consuming issues. Different learning systems, such as machine learning, derive appropriate training data to send into the system to generate the most rapid and accurate evaluation possible [6]. In contrast, a few machine learning techniques focus on speed, and others focus on precision and accuracy. Subsequently, selecting the measures that compare to the objective and input sort has a massive effect on model results [7] [8]

This paper aims to increase the model sensitivity, improve its ability to be generalizable, and improve its performance in detecting different types of memory dump malware, especially zero-day malware. Hence, the OCSVM classifier is utilized to identify any deviation from the normal memory dump file patterns as malware. Besides, a technique of dimensionality reduction, PCA, is combined with the OCSVM training phase in an attempt to achieve the desired goals.

The main objective of this research is to train the OCSVM classifier in the best manner to detect memory dump malware, especially zero-day malware. The "MalMemAnalysis2022" dataset[7] is utilized in two models. The first model TOCC is to train an OCSVM classifier and evaluate its performance. The second model OCC-PCA is to reduce the dataset dimensionality using the PCA technique before training the OCSVM classifier to improve its performance. Several accuracy matrices have been used to evaluate the performance of both models and determine whether the PCA has improved the model performance or not. The proposed model results from the results of related studies for benchmarking purposes.

The remaining part of this paper is structured as follows: section 2 provides a background of dump memory and its attacks, the concept of novelty detection, the OCSVM, and PCA classifiers. Section 3 demonstrates the literature reviews, whereas section 4 comprehensively describes the methodology. Section 5 analysis and evaluates the results. Section 6 is the conclusion.

2. Background

2.1. Memory dump and their attacks

A memory dump occurs when all of the information in RAM is written to a hard drive. Memory dumps are widely used to collect diagnostic information during a crash to aid in debugging and learning more about the event and help solve problems with operating systems and other programs. Many computer problems are unfixable because they need a reboot, yet the code that caused the problem is still stored in RAM at the time of failure. Due to the volatile nature of RAM, memory dumps save data that could otherwise be lost or overwritten. Some customers are concerned about privacy because these dumps might contain anything in the computer's dynamic RAM. These dumps may pose a security concern since they are saved on the hard drive. Hackers may be able to extract cleartext passwords or decryption keys from a memory dump that would be hard to obtain otherwise [1].

Some malware encrypts the user's data and demands payment to access the key needed to recover this information, knowns as ransomware. At the same time, Spyware was Developed in response to attempts to prevent keylogging and subvert the compromised machine to allow surveillance of a wide variety of system activity that could result in the user's personal information being compromised significantly. A Trojan horse is a program or application that is beneficial or appears to be helpful but contains secret code that, when run, performs an undesirable or dangerous function. Trojan horse programs act to do tasks that the attacker cannot work on directly. However, malware could be harmful and causes damage.

2.2. Novelty-detection

The detection of unique or uncommon data within a dataset is known as novelty detection. A machine learning system might be trained entirely on correct data to classify this data appropriately in novelty detection. However, one-class classification achieves novelty- detection, requiring distinguishing one class (the specified normal, positive class) from all other alternatives. The positive type is commonly considered well-sampled, whereas the opposite category is drastically under-sampled [9]. Outlier data and information are used in novelty identification and when looking for anomalies, outlier detection and novelty detection are both employed [10].

2.3. OCSVM and PCA classifier

OCSVM classifier uses techniques for outlying data identification to create a boundary separating the numeric values from the rest of the input space, and the domain of the minor class is measured. Data points outside preset parameters are known as outliers [11]. One of the methods in this family is OCSVM, which applies SVM concepts to one-class settings. Kernels that perform dots between points from the input data determine the distance in a high-dimensional space [12].

The PCA is a classifier that utilizes a statistical manner and reduces the dimensionality of the dataset by creating uncorrelated parameters and selecting from a linear collection of the input features from the original dataset that maximize variance and produce relevant features from the given entire dataset [13].

In this paper, the PCA classifier handles dataset features to minimize the feature number that can be enhanced OCSVM classifier in the training and testing phase. PCA relies on eliminating all features that are not necessary and concentrating effort on the crucial features that produce more robust results, which helped us achieve the best results.

3. Literature Review

Many researchers have been attracted to employing different one-class classification techniques due to their advantages. The main concern is detecting novel attacks efficiently as soon as they occur. Consequently, most experimental attempts are combined with various enhancement techniques to improve the one-class classifier performance. This section provides a comprehensive review of studies that adopted different class classification techniques. It focuses on how each study employed the classifier, what attempts were used to enhance the performance, the utilized datasets, and what results were achieved.

In [14], the authors presented lightweight NIDS using two simultaneous OCSVM-based subsystems. One of the systems has been taught to handle regular packets, and the other to handle attack packets. They employed the KDDCUP-99, NSL-KDD, and UNSW-NB15 datasets in their models. A dimensionality reduction technique used by a binary Pigeon Inspired Optimizer (Cosine PIO). Using a subset of features from each of the features in the three datasets, this technique is based. The accuracy rate of the OCSVM in their research was 97% for identifying benign records, which was regarded as less accurate than our suggested models, which used a PCA classifier to extract fresh features from every characteristic of the dataset and improved OCSVM to attain a 99.4% accuracy rate.

In [15], SIMCA and OCSVM models to identify impurities in cassava starch is proposed. Both models used a one-class technique. The SIMCA model used PCA instead of the OCSVM model, which used the OCSVM classifier. The data showed that the two models' accuracy rates, 78.8% and 86.9%, respectively, to forecast benign data better, our proposed model, which aims to increase the OCSVM generality, utilizes PCA in an OCC-PCA model presented.

According to [16], utilizing OC-SVM, WOC-SVM-DD, WOC-SVM(ND), and AWOC-SVM classifiers to implement on eight datasets. The result shows the viability and effectiveness of the WOC-SVM-DD classifier. The weight calculation procedure is improved with WOC-SVM-DD, which addresses limited sample and high-dimension classification. The experiment demonstrates the most outstanding performance of OCSVM, 99.3% AUC, when used in the banknote authentication dataset. This model did not apply dimensionality reduction automatically on their datasets.

In [17], an HIDS model that combines the C5 and OC-SVM classifiers is developed and evaluated The model is tested on the NSL-KDD and ADFA datasets. Three stages were conducted to reach high accuracy results; in stage 2, OCSVM with an RBF kernel was applied using LIBSVM to achieve a detection accuracy of 76.4% for the ADFA dataset and 72.17% for the NSL-KDD dataset. This model did not apply dimensionality reduction automatically on their datasets.

Authors in [18] presented a semi-supervised novelty identification technique based on OC-SVM for SMS spam detection. The researchers used a chi-squared feature selection algorithm, and only normal data was trained and had a 98% accuracy rate.

The contributors of [19] introduced an unsupervised deep learning strategy for IDS. NSL-KDD and UNSW-NB15 datasets were implemented, and the proposed CAE+OCSVM classifier was combined with a 1D CAE approach to a joint optimization framework. Convolutional autoencoder and CNN methods were implemented to accomplish significant feature illustrations on both datasets. This method boosts OCSVM's prediction accuracy to 91.58% with the NSL-KDD dataset and 94.28% with the UNSW-NB15 dataset, which is still under our suggested model's performance.

Besides, in [20] an anomaly-based NIDS that utilizes unsupervised methods to detect zero-day attacks was presented. Furthermore, unsupervised NIDS demonstrated their capacity to identify unidentified zero-day attacks provided that the malicious traffic diverges from legitimate traffic. The OCSVM produced the highest AUROC scores of 97% on the CIC-IDS-2017 dataset and 94% on the CSE-CIC-IDS-2018 dataset. At the same time, PCA achieved a good classification performance with the lowest recorded AUROC of 84% on the CSE-CIC-IDS-2018 dataset. This model did not apply dimensionality reduction automatically on their datasets.

Moreover, in [21], a cutting-edge NIDS model that used the OCSVM technique has been developed and tested. The suggested approach relies on identifying regular traffic. 97.61% accuracy rate was achieved in an experiment using a recent honey network. The pre-processing and testing phase was not described in depth. However, according to the experimental findings, OCSVM executes with 97.6% accuracy for predicted benign behavior.

In [22], the collaborators proposed an unsupervised learning models memory augmented autoencoder (MemAE), the results of the proposed model were compared with OCSVM and AE models. Three models were trained on benign records and implemented UNSW-NB15, NSL-KDD, and CICIDS 2017 datasets. The OCSVM model accuracy rate values were 94% on NSL-KDD, 81% on UNSW-NB15, and 76% on CICIDS 2017 datasets. MemAE was proposed as a solution to the over-generalization problem of autoencoders. This model did not apply dimensionality reduction automatically on their datasets.

Furthermore, in [23], a unique method for exploiting PMU data to detect cyberattacks on smart grids was suggested and built. It uses publicly accessible datasets on power system hacks and is based on semi-supervised anomaly identification. According to the results of eight algorithms, four semi-supervised algorithms are more efficient and accurate than the other four supervised algorithms. Deep autoencoder and PCA set as feature extraction techniques on four semi-supervised algorithms to train. Four semi-supervised techniques were set up with PCA and a deep autoencoder feature extraction approach. The OCSVM Classifier had 84%, 85%, and 86% accuracy rates for all features, PCA, and DAE, respectively. Table 1 shows a comparison of the proposed approach with other related works.

4. Methodology

This section describes the study's methodology and practice. Many phases were implemented to accomplish the desired goals and objectives. The pre-processing stage was applied to the dataset in five steps: partitioning the dataset, handling missing values, removing duplicate entries, and encoding. The OCC-PCA model utilized the PCA classifier on the dataset to minimize the number of features from 53 to 10 after the complete pre-processing phase. However, 53 features from a dataset were retained by the TOCC method. The OCSVM classifier was then implemented for two models using dataset training samples to train and learn. Two models will then be tested with the OCSVM classifier.

Table 1. A comparison of the proposed approach with other related works.

References	Dimensionality Techniques	Dataset	Classifier	Accuracy Rate
[14]	Cosine PIO	KDDCUP-99	OCSVM	97.00%
[15]	PCA	Cassava starch samples	OCSVM	86.90%
[16]	Manual	banknote authentication samples	OCSVM	99.30%
[17]	Manual	ADFA	OCSVM	76.40%
[18]	chi-squared	SMS Spam collection	OCSVM	98.00%
[19]	AE, CNN	UNSW-NB15	OCSVM	94.28%
[20]	Manual	CIC-IDS-2017	OCSVM	97.00%
[21]	manual	honey network	OCSVM	97.61%
[22]	Manual	NSL-KDD	OCSVM	94.00%
[23]	DAE, PCA	power system samples	OCSVM	86.00%
OCC-PCA	PCA	MalMemAnalysis-2022	OCSVM	99.40%

The MalMemAnalysis-2022 dataset was created in 2022 to imitate real-world settings similar to malware seen in the real. Collecting malicious and benign dumps, a MalMemAnalysis-2022 dataset consists of 58,596 records with 29,298 benign and 29,298 attack records, including 56 features and three main categories of memory dump malware (Ransomware, Spyware, and Trojan Horse)[7]. Many reasons for implementing this recent dataset are considered since it is a balanced binary classification dataset with a few missing values. Besides, we are among the earlier researchers to use this dataset. This methodology employs the Python programming language, and the OCSVM classifier is utilized in each approach to determine the experimental environment. After the testing step, the method offers information on the performance matrices used to assess the findings. Figure 1 depicts the methodology of the two proposed approaches.

4.1. Dataset pre-processing phase

The dataset goes through various processes in this phase to remove noise and then adapt it to the chosen machine learning methods, as mentioned in figure 1.

4.1.1. Dropping duplicate values

All duplicate rows with missing values were dropped. This stage eliminates duplicate features in the dataset for two approaches by removing the redundant feature column. The first column feature, knowns as "category" with the type "object," was dropped. Another two columns named "handles. nport" and "svcscan.interactive_process_services" were dropped since they have zeros numbers; the dataset, after removing three columns, has 53 features; the last column, formerly known as a "class" with the type "object" has been renamed to "label."

4.1.2. Handle missing values

The dataset's missing values and duplicated rows are dealt with in two approaches at this level. Although, depending on their implications, adjusting missing values by eliminating entire rows or replacing them with appropriate values as median [24].

4.1.3. Encoding dataset

To be acceptable for the two approaches, 0 and 1 numbers define all benign Attacks.

4.1.4. Values Normalization

The dataset's independent values are not fairly distributed; all values are set closely together to normalize with the classifier for the best accuracy and measurement performance.

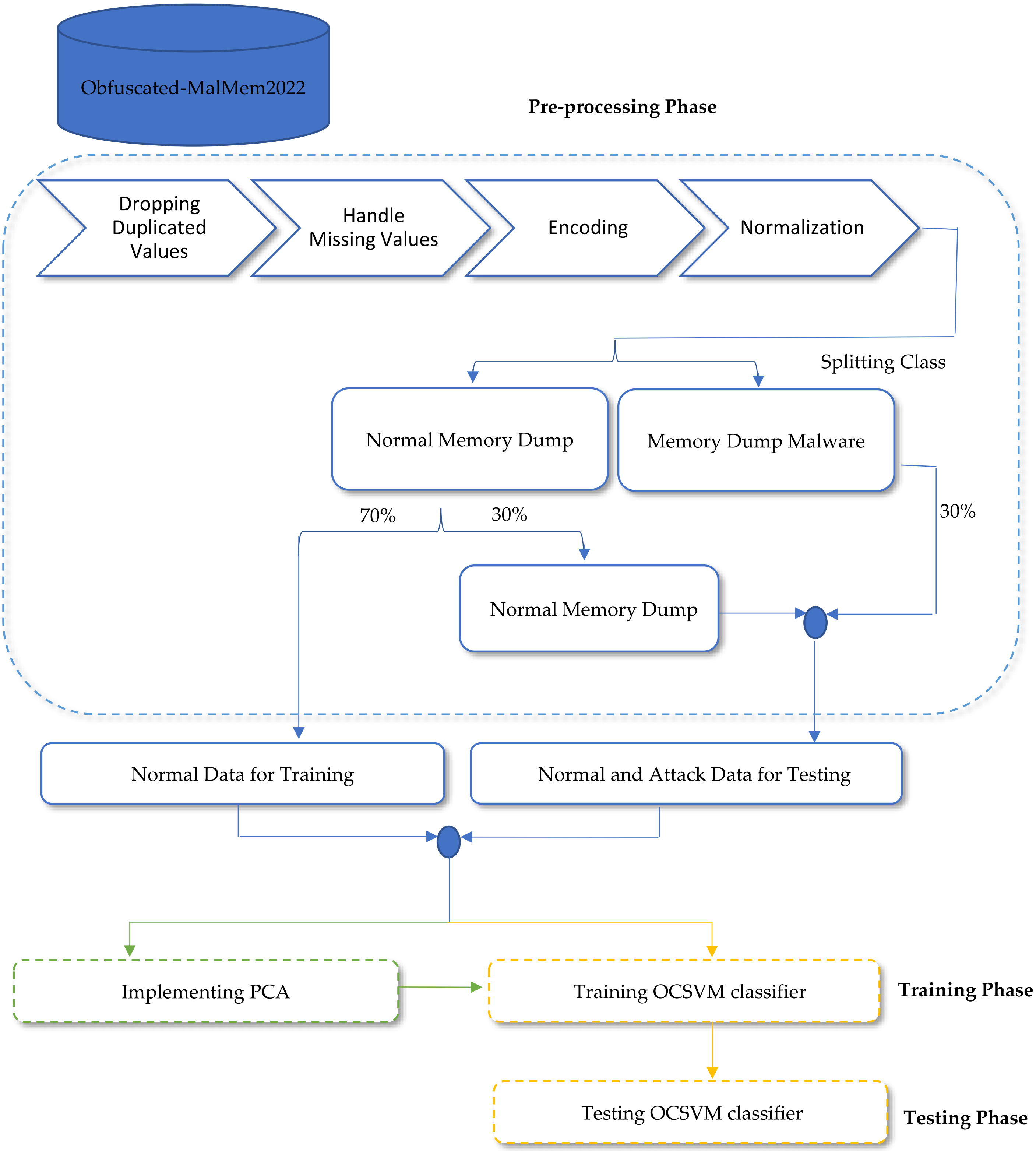

Figure 1. The methodology of the proposed approaches.

4.1.5. Dataset Partitioned

After completing all the previous steps in the pre-processing phase, all Duplicate rows, duplicate features, and missing values are dealt with by eliminating, dropping, or replacing. The dataset after that was divided into 28796 records for memory dump malware and 29231 for benign records. The comparison of the total number of dataset records before and after pre-processing phase for benign and malware depict in table 1. To prepare the OCSVM classifier to be trained and tested, malware records are divided into 30%, with 8770 records utilized for the testing phase, while the remaining 70%, with 20026 records, remain inactive. Benign records were split into 70%, with 20461 records for training the classifier, and 30%, with 8770 records, for the testing phase. Table 2 depicts the number of records in the training and testing phase.

Table 2. depicts the number of records in the training and testing phase.

Type of records	Training phase	Testing phase
benign	20461	8770
attack	NULL	8770

4.2. Training Phase

After completing dataset pre-processing, the OCSVM classifier was set to depend on benign records for each model to train the classifier. Twenty-nine thousand two hundred thirty-one benign records of the dataset were split into two halves; 70% of benign records will be utilized for the training classifier on both models, while 30% will be utilized for the testing phase, as mentioned in figure 1. On another side, in a 64-bit Windows 11 pro computer with 12 GB RAM and 1.80 GHz CPU, the ML models were implemented using Python 3.8, and SPYDER 4.2.5 provide libraries, Panda, Scikit-learn, and Numpy.

4.2.1. The OCC-PCA approach

Implementing automated dimensional reduction by utilizing a PCA classifier to select ten features (n=10) out of 53 feature selections from the dataset where "n" is the number of feature extractions; then, the OCSVM classifier trained on 20461 benign records.

4.2.2. The TOCC approach

This approach was trained using the identical 20461 benign records without utilizing any dimensional reduction techniques and dealt with 53 features from the dataset after pre-processing phase to train the OCSVM classifier.

4.3. Testing Phase

Testing the OCSVM classifier for both novelty-class techniques follows the completion of OCSVM classifier training for two approaches. The OCC-PCA and TOCC models use 8770 benign and 8770 malware records, totaling 30% Benign and 30% of malware records, respectively. A total of 17540 data were employed. The result demonstrates the prediction error for the final model and the suggested model's generalizability, as mentioned in figure 1.

5. Analysis and Evaluate the Results

In the evaluation phase, Confusion matrix variables consist of four variables, detecting benign records correctly as true negative (TN), correctly detecting attack records as true positive (TP), incorrectly recognizing benign records as false positive (FP), and incorrectly recognizing attack records as false negative (FN) [25]. It was developed by comparing actual label values to predicted label values in the testing phase and measuring performance for both models. Recall value is a way to measure how many predicted positives were true positives. The following equation (1) represents the recall value [26].

The precision value can measure the actual positive results among all projected positive results. The following equation (2) represents the precision value.

$$Precision = \frac{TP}{TP+FP} \tag{2}$$

Precision and recall can both be measured using the F1 measure. The following equation (3) represents the F1-measure.

$$F\,1 = 2\left(\frac{Precession\ X\ Recall}{Precession + Recall}\right) \tag{3}$$

The percentage of accurately predicted events from all predicted events, whether positive or negative, is measured by accuracy value. The following equation (4) represents the accuracy value.

$$Accuracy\ rate\ (AR) = \frac{TP+TN}{TP+FN+FP+TN} \quad (4)$$

The findings of the evaluation phase reveal that the TOCC approach achieved 880 true positive samples and 8963 true negative samples, while false positives had seven samples and false negatives had 7890 samples. Therefore, a high number of false positives in the TOCC approach demonstrates its low accuracy rate since this model considers a high number of features to train and test the OCSVM; it alludes to the sensitivity of OCSVM dealing with the number of features. At the same time, the OCC-PCA approach achieved 8725 true positive samples and 8715 true negative samples, while false positive 55 samples and false negative 45 samples. With this model, the OCSVM could accurately predict both normal and abnormal behavior, and tiny numbers suggest that this approach may reduce incorrect predictions made by the PCA algorithm. Depending on features used in the classifier during training and testing, these results are considered enhancing for the OCSVM classifier detection. Figure 2 depicts the confusion matrix of TOCC and the OCC-PCA models.

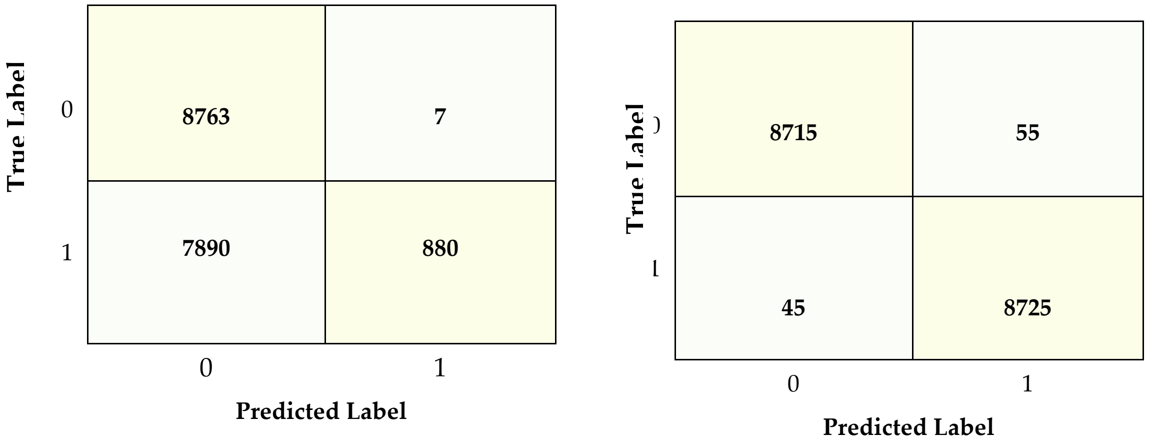

Figure 2. (a) Description TOCC confusion matrix; (b) Description OCC-PCA confusion matrix.

The performance matrices of the evaluation phase reveal that the OCC-PCA model achieved 99%, 99%, 99%, and 99.4% in precision, recall, F 1, and accuracy, respectively. In this model, the results illustrate that concentrating on significant recurrent features thus enhances the algorithm's performance and predictability to identify the proper behavior from the immoral behavior. Besides accurately, the algorithm's sensitivity in identifying and detecting normal behaviors can be enhanced and developed using the PCA algorithm. On another side, the TOCC model achieved 76%, 55%, 44%, and 55% precision, recall, F 1, and accuracy, respectively. It appears that these properties contain information that is not necessarily useful in the training and testing of the algorithm. As a result, the TOCC model demonstrates that the OCSVM algorithm interacts negatively when the number of properties is significant. In contrast to the OCC-PCA model, which uses the PCA algorithm to remove unnecessary properties, the OCSVM algorithm appears to affect the results in anticipating normal behaviors When making improving those predictions and concentrating on the necessary traits. Table 3 depicts the comparison between OCC-PCA and TOCC models.

Table 3. OCC-PCA and TOCC models result in comparison.\

Model	Precision	Recall	F1 Score	Accuracy
TOCC	76%	55%	44%	55%
OCC-PCA	99%	99%	99%	99.4%

Both [15] and [23]'s models employed the PCA classifier, although their findings were less conclusive than in this study. In [15], which provided the SIMCA and OCSVM models. Both models employed one-class approaches. The OCSVM model did this instead of the SIMCA model by employing PCA. The number of feature extractions or selections made available for PCA to be employed in the training phase is one component of the research cited that is not addressed. It is not mentioned if the PCA was carried out precisely either. The two models' accuracy rates were below average at 78.8% and 86.9%, respectively. Our suggested method, however, aims to expand OCSVM generality while simultaneously boosting performance using the OCSVM classifier. Whereas In [23]. Four semi-supervised techniques were illustrated using PCA and deep autoencoder feature extraction techniques. One flaw in this model is that PCA was set to extract 30 features, while DAE and PCA were reflected on the OCSVM Classifier, which had accuracy ratings of 84%, 85%, and 86% for each PCA, DAE, and all features separately. Respectively. Table 4 compares the OCC-PCA model and other models that utilize dimensionality reduction techniques and the PCA classifier.

Table 4. depicts the comparison between the OCC-PCA model and other models that utilize PCA.

References	Dimensionality Techniques	Dataset	Classifier	Accuracy Rate
[15]	PCA	Cassava starch samples	OCSVM	86.90%
[23]	DAE, PCA	power system samples	OCSVM	86.00%
OCC-PCA	PCA	MalMemAnalysis-2022	OCSVM	99.40%

Besides, by lowering the dimensionality of the data, the PCA classifier can be used to improve the OCSVM classifier and attain high accuracy rates. Additionally, the PCA can boost the precision of a classification model when the dimensions are large and the correlation between the variables is strong. As a result, the OCC-PCA approach and the nature of the OCSVM classifier in dealing with a low number of feature selections can be considered enhancements for detecting any attack. That can be seen as a mainly unknown attack or, in other names, a zero-day attack. The Accuracy rate of the OCC-PCA approach was achieved at 99.4%, and all performance matrices such as recall, precision, and F1 were achieved at 99%. Thus, PCA relies on eliminating all features that are not necessary and concentrating effort on the crucial features that produce more robust results, which helped us achieve the best results. At the same time, the TOCC approach performed poorly, with an accuracy rate of 55%, and caused exceedingly low sensitivity to recognize normal behavior during the test phase. In the future, after detecting normal flow, we suggest stepping over to the next layer by determining what kind of each attack is by utilizing multi-class classification. Figure 3 depicts performance evaluations of The OCSVM classifier results for both models.

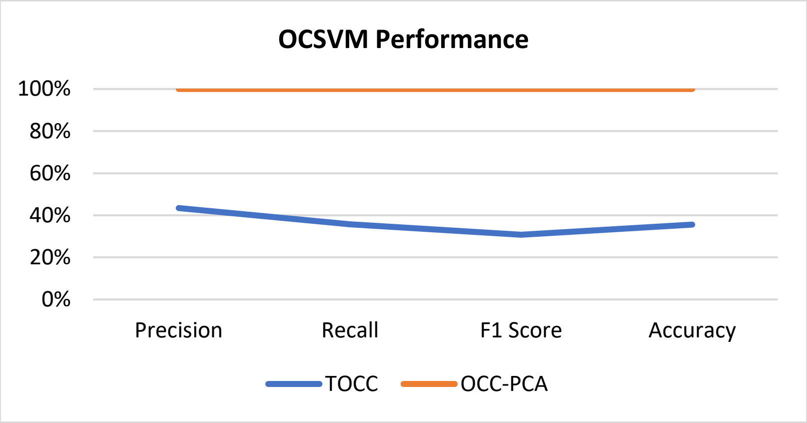

Figure 3. performance evaluations of The OCSVM classifier results for both models.

6. Conclusion

This paper presented an effective enhancement of one-class classification (OCSVM) by enforcing it with a dimensionality reduction technique known as Principal Component Analysis (PCA). This unified solution focuses on accurately detecting memory dump malware, even novel ones. The OCSVM classifier detects any deviation from the normal memory dump file patterns. Thus, it can detect any zero-day attack. The PCA is used to improve the performance of the OCSVM classifier in an attempt to achieve improved efficiency. An intensive evaluation methodology was implemented based on a recently published dataset known as “MalMemAnalysis2022” to compare the performance of the OCSVM classifier with and without the dimensionality reduction technique, PCA. The OCC-PCA model achieves a 99.4% accuracy rate and 99% for F1, recall, and precision scores, compared to the limited low performance of the TOCC model. Hence, an OCSVM classifier with dimensional reduction of the PCA classifier is recommended to identify benign behaviors.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gibert, D., Mateu, C., & Planes, J. . The rise of machine learning for detecting and classifying malware: Research payments, trends, and challenges. Journal of Network and Computer Applications 2020, 153, 102526. doi:10.1016/j.jnca.2019.102526.
2. Abu Al-Haija, Q.; Al-Dala’ien, M. ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. J. Sens. Actuator Netw. 2022, 11, 18. https://doi.org/10.3390/jsan11010018
3. McGraw, G., & Morrisett, G. Attacking malicious code: A report to the Infosec Research Council 2000. IEEE Software, 17(5), 33–41. doi:10.1109/52.877857.
4. Institute, A.-T. - T. I. I.-S. (n.d.). AV-ATLAS. AV-ATLAS. Available online: https://portal.av-atlas.org/.
5. What is a memory dump? - definition from Techopedia. Techopedia.com. Available online: https://www.techopedia.com/definition/20663/memory-dump#. (Accessed on 25 October 2022)
6. Qalaja, E. K., Al-Haija, Q. A., Tareef, A., & Al-Nabhan, M. M. Inclusive study of fake news detection for covid-19 with new dataset using supervised learning algorithms 2022. International Journal of Advanced Computer Science and Applications, 13(8). doi:10.14569/ijacsa.2022.0130867.
7. Carrier, T., Victor, P., Tekeoglu, A., & Lashkari, A.Detecting obfuscated malware using memory feature engineering 2022. Proceedings of the 8th International Conference on Information Systems Security and Privacy. doi:10.5220/0010908200003120.
8. Al-Haija, Q. A., Saleh, E., & Alnabhan, M.Detecting port scan attacks using logistic regression 2021. 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT). doi:10.1109/isaect53699.2021.9668562.
9. Novelty and outlier detection. scikit. Available online:https://scikit-learn.org/stable/modules/outlier_detection.html. (Accessed on 25 October 2022).
10. communicator, B. B. A. self-starter technical. An introduction to outlier detection techniques. Digital Vidya. Available online: https://www.digitalvidya.com/blog/outlier-detection/. (Accessed on 25 October 2022)
11. Noble, W. S. What is a support vector machine? 2006. Nature Biotechnology, 24(12), 1565–1567. doi:10.1038/nbt1206-1565.
12. Domingues, R., Filippone, M., Michiardi, P., & Zouaoui, J. A comparative evaluation of Outlier Detection Algorithms: Experiments and analyses 2018. Pattern Recognition, 74, 406–421. doi:10.1016/j.patcog.2017.09.037.

13. Carter, J., Mancoridis, S., & Galinkin, E.Fast, lightweight IOT anomaly detection using feature pruning and PCA 2022. Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing. doi:10.1145/3477314.3508377.
14. Alazzam, H., Sharieh, A., & Sabri, K. E. A lightweight intelligent network intrusion detection system using OCSVM and Pigeon Inspired Optimizer 2021. Applied Intelligence, 52(4), 3527–3544. doi:10.1007/s10489-021-02621-x .
15. Kelis Cardoso, V. G., & Poppi, R. J. Cleaner and faster method to detect adulteration in cassava starch using Raman spectroscopy and one-class support vector machine 2021. Food Control, 125, 107917. doi:10.1016/j.foodcont.2021.107917
16. Zhao, Y.-P., Huang, G., Hu, Q.-K., & Li, B. An improved weighted one-class support vector machine for Turboshaft Engine Fault Detection 2020. Engineering Applications of Artificial Intelligence, 94, 103796. doi:10.1016/j.engappai.2020.103796.
17. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., & Alazab, A.Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine 2020. Electronics, 9(1), 173. doi:10.3390/electronics9010173.
18. Yerima, S. Y., & Bashar, A. Semi-supervised novelty detection with one class SVM for SMS spam detection 2022. 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP). doi:10.1109/iwssip55020.2022.9854496.
19. Binbusayyis, A., & Vaiyapuri, T. Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM 2021. Applied Intelligence, 51(10), 7094–7108. doi:10.1007/s10489-021-02205-9.
20. Verkerken, M., D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. Towards model generalization for intrusion detection: Unsupervised Machine Learning Techniques 2021. Journal of Network and Systems Management, 30(1). doi:10.1007/s10922-021-09615-7.
21. Mahfouz, A., Abuhussein, A., Venugopal, D., & Shiva, S. Network intrusion detection model using one-class support vector machine 2020. Algorithms for Intelligent Systems, 79–86. doi:10.1007/978-981-15-5243-4_7.
22. Min, B., Yoo, J., Kim, S., Shin, D., & Shin, D. Network anomaly detection using memory-augmented deep autoencoder 2021. IEEE Access, 9, 104695–104706. doi:10.1109/access.2021.3100087.
23. Qi, R., Rasband, C., Zheng, J., & Longoria, R. Detecting cyber-attacks in smart grids using semi-supervised anomaly detection and Deep Representation Learning 2021. Information, 12(8), 328. doi:10.3390/info12080328.
24. Brink, H., Richards, J., Fetherolf, M., & Cronin, B. Real-World Machine Learning. Shelter Island: Manning. 2017.
25. Al-Haija, Q.A.; Alsulami, A.A. High Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. Electronics 2021, 10, 2113. https://doi.org/10.3390/electronics10172113
26. Ashi, Z., Aburashed, L., Qudah, M., & Qusef, A. Network intrusion detection systems using supervised machine learning classification and Dimensionality Reduction Techniques: A systematic review 2021. Jordanian Journal of Computers and Information Technology, 1. doi:10.5455/jjcit.71-1629527707.