African Multidisciplinary
Journal of Sciences and Artificial Intelligence

ISSN : 1595-7969

Index: Harvard, Boston, Sydney University, Dimensions, Lens, ResearchGet Scilit, Semantic, Google Scholar, Base etc

https://doi.org/10.58578/AMJSAI.v2i3.7231

Detection of Malware Attacks in Medical Mechatronics Distribution System Using Support Vector Machine

Bartholomew Idoko, Okoro Denis Isah, Sampson Agada, Samuel Owoicho Olofu
Federal Polytechnic, Ohodo, Enugu State, Nigeria
bartholomew.idoko@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Jun 15, 2025	Aug 3, 2025	Aug 15, 2025	Aug 20, 2025

Abstract

This study examines the cybersecurity challenges and solutions associated with medical mechatronics devices, which increasingly operate autonomously through advances in robotics, artificial intelligence (AI), and machine-to-machine communication. As the number of interconnected devices grows—from smart grids and home appliances to medical equipment and sensor–actuator testers—ensuring secure and trustworthy communication becomes critical. A sustainable defensive strategy for medical mechatronics requires robust systems capable of malware analysis and detection, informed by an understanding of cyber-attack stages such as reconnaissance, weaponization, delivery, exploitation, installation, and command and control. Traditional malware detection systems struggle with obfuscated malware, making AI and machine learning (ML) more effective tools for accurate detection and classification. This research proposes the use of a Support Vector Machine (SVM) model with a novel metric to enhance malware detection in medical mechatronics devices, thereby strengthening confidentiality, integrity, availability, and digital trust. The proposed SVM-based approach was compared with established SVM algorithms using a real dataset from medical mechatronics distribution systems across federal medical centers in Nigeria. Findings demonstrate the potential of the model to improve malware detection

AMJSAI Journal is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

accuracy and compliance with digital sovereignty standards, offering practical insights for enhancing cybersecurity in critical healthcare technologies.

Keywords: Security; Digital Trust; Privacy; Integrity; Dataset; Algorithm; Support Vector Machine; Malware Detection

Introduction

The advancement in technology has given birth to mechatronics devices being used in hospitals. These devices are powered by software which drives the hardware components and the wireless connection to link the system to the cyberspace which automatically expands its use and access [1]. Medical Mechatronics such as robotic surgical devices (defibrillator, active ankle-foot orthosis), advanced active prosthetic limbs, sophisticated da Vinci system, in-vitro diagnostic systems, etc. are machines used in hospitals for surgical operations, diagnosis and treatment of patients [2].

However, the major concern about medical mechatronics is the safety of the devices and confidentiality of patients' data being attacked by malware (Trojan Horse, keylogger, ransomeware, etc.) [3]. One of the main concerns for mechatronics devices connected in smart environments, such as digital hospitals, is the data, device, and communication medium security [4]. Machines, gadgets, data reservoirs, and communication mediums (private networks and VPN tunnels) all need to be secured from thieves, unnecessary rights, and damage in order to build digital trust. Data can be private, organisational, or business data. Similarly, [5] pointed out that the primary de facto barrier to the widespread deployment of digital clinics has been the security of mechatronics equipment and patient privacy.

Researchers have outlined the main issues with security, confidentiality, and privacy when deploying mechatronics in the healthcare industry [6]. These issues included:

a. Security: Protecting physical machines and devices in a health system's mechatronics environment from being compromised (like Distributed Denial of Service, or DDoS) and malware-infected object protection [7].

b. Confidentiality: A more straightforward, but save and sure way to share private and sensitive information.

c. User Privacy: Rights and Control over personal information, privacy technology, and methods (models, algorithms, and frameworks) for protecting privacy.

As hackers continue to refine their methods, malware attacks will become more frequent., Since AI and ML applications and research are being carried out in malware analysis and detection simultaneously, the significance of AI in research and applications in malware detection will continue to grow [8, 9]. The Mechatronics paradigm's sensing frameworks must deal with uncertainty issues that impact the availability of Quality of Service (QoS) and node performance in Wireless Sensor Networks (WSNs) [10]. The components of a service architecture framework, such as Mobile Ad hoc Networks (MANET), are wireless nodes with random mobility patterns assembled together. One of the main design challenges for the battery-operated MANET nodes is energy efficiency [11,12]. A lot of vulnerabilities existed in the mechatronics health instrument that if exploited by adversaries will lead to casualties.

Artificial Intelligence is a vast and developing field with several subfields, including Robotics, Machine Learning (ML) and Deep Learning (DL), and other simplified versions or subsets. [13]. ML, to put it brief, is the theory that computers may learn from data to become more creative and predictive, mimicking human brain processes to be precise [14]. Support Vector Machine (SVM) is a type of supervised machine learning model that can be applied in the field of malware detection. The main objective of SVM algorithm is to formulate the best line or the best decision boundary called the hyperplane that divides the n-dimensional spaces into classes so we can put the new data point in the right category. SVM is the most powerful classification techniques in ML. Our choice of SVM model was due to its ability to handle complex, high-dimensional data.

Medical professionals that handle mechatronics equipment and apps unethically handle and transmit data, which presents a number of difficulties to data security and privacy preservation and compromise [15]. Figure 1, shows the security challenges associated with medical mechatronics deployment and the need to protect the system against malware. An eHealth system powered by robots and other mechatronics devices [15] that provides key exchange and personal data transmission by a secured trusted authority is one example of an approach that has been proposed in response to security and privacy challenges in the deployment of mechatronics devices in a digitalized hospital. These approaches claim to ensure the preservation of privacy, data integrity, confidentiality, and availability of both data and resources in the medical mechatronics paradigm. Malware authors are aware of the

vulnerabilities associated with mechatronics devices and hence the need to automate the security of the critical infrastructure in the sector using machine learning algorithms.

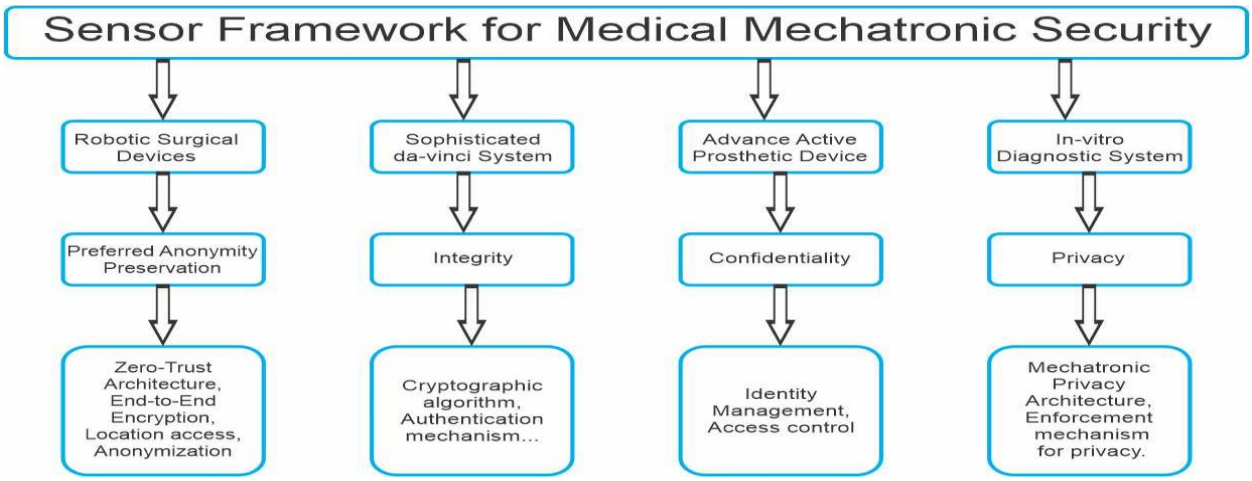


Fig. 1: Security issues associated with medical mechatronics deployment.

Design and Implementation of the Proposed Model

In this paper, we proposed an automated malware detection system for medical mechatronics using dataset from federal medical centers in Nigeria. This automated process of malware detection is more effective as compared to the conventional Intrusion Detective System (IDS). The system is designed to automate malware in medical mechatronics. Machine learning or SVM in particular was used to study the behaviour and properties of the medical devices/equipment. The dataset was analyzed, trained and embedded in the machine learning module for the design and implementation of the detection system.

2.1 System Requirement and Specification for the Model

We set up Cuckoo Sandbox as illustrated in figure 2 to obtain the malware behavioral reports and to guarantee that malware operates as intended, including all of its features. In the real world, several malware samples take use of various flaws that some software products may have. As a result, we packed a lot of functionality into the virtual computers the sandbox generated.

We suggest using a virtual box, or hypervisor, to house the Cuckoo virtual machines. VMcloak, an automated virtual machine production and cloaking tool for Cuckoo Sandbox,

was used to build the virtual computers [16]. The specs of our suggested virtual machine are as follows:

- 1 CPU core 3.2 Ghz
- 8 GB RAM
- Internet connection

The system specification for the virtual machine are:

- Windows 7 Professional 64bit without any updates, including Service Pack 1
- Adobe PDF reader 9.0
- Adobe Flashplayer 11.7.700.169
- Visual Studio redistributable packages 2005 - 2013.
- Java JRE 7
- .NET framework 4.0

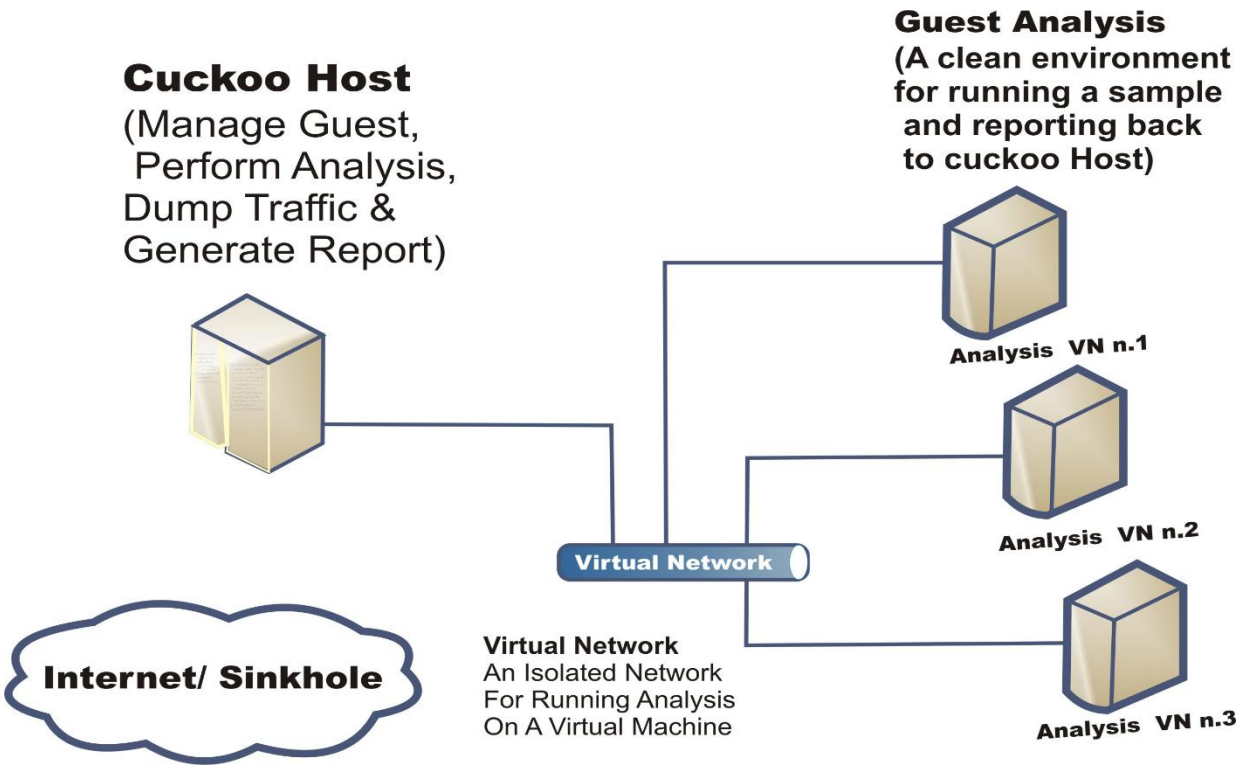


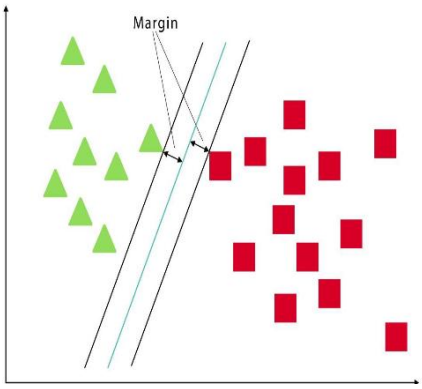
Fig. 2: Cuckoo Sandbox Architecture [17].

2.2 Model Configuration

The model was configured with specified kernel functions and hyper-parameters tailored to malware detection. These configurations are motivated by existing literature and preliminary experiments, aiming to capture the intricacies of malware attack instances on mechatronics devices. The research succeeded in putting the data through a unique learning process using SVM algorithm.

2.3 SVM Algorithm and Classification Scheme

The classification scheme of the proposed model is shown in figure 3. It explains malware data representation and classification of SVM model in critical environments (medical mechatronics). The model is provided with a set of input features derived from the malware sample in the data-set and each data points is represented by a point in a 3D space. However, the main objective of the SVM model is to find a hyperplane that separates the data into normal activities & malicious activities as shown in figure 4. Support vectors are the nearest vectors to the hyperplane and plays the role of defining the decision boundaries. The SVM utilizes the kernel tricks for the transformation of the input space to a higher dimensional space. The SVM algorithm is then trained to change the position of the hyperplane to increase the margin between the classes. Once the program is trained, the SVM will classify new unseen data points by examining the side of the hyperplane it falls whether it is malicious side or not. Our malware detection system uses a trained Support Vector Machine (SVM) model throughout the evaluation phase. We employ the scikit-learn library and the predict_ proba method to get probability estimates for each class. This produced an array of dimensions that show the likelihood that the samples will belong to the different classes. We also applied the predict method, which will directly provide the predicted class labels for the samples in our testing set. The dimensions of both outputs was communicated through print statements for a clearer understanding of the results.



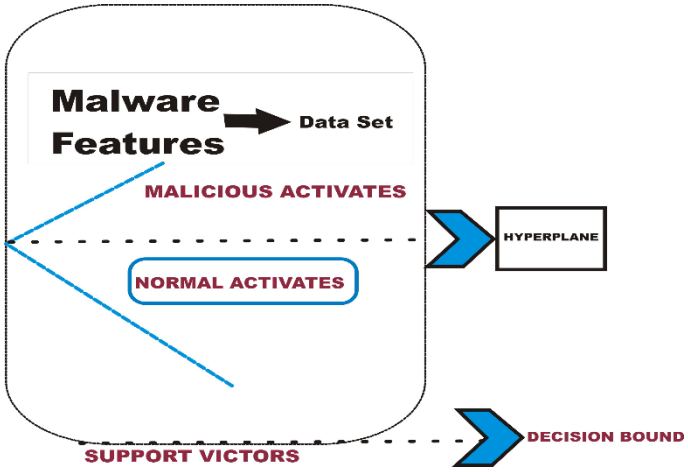


Fig. 3: SVM Classification Scheme. **Fig. 4:** SVM Algorithm

Two classes' of datasets employed are shown in Figure 4. As a result, the issue is in two dimensions, and a line is used to symbolize a hyperplane. Hyperplanes can generally have as many dimensions as we desire. We define our algorithm using the following mathematical equations:

$$R_{emp}(a) = \frac{1}{m} \sum_{i=1}^{m} i(f(x_i, a), yi) = \text{Training Error} \quad (1)$$

$$\underline{R}(a) = (L(f(x, a), y)\, dp\,(x,y) = \text{Test Error} \quad (2)$$

Where x and y = input & output sets respectively

(x_i, y_i) ……. (x_m, y_m) = Training Set

To predict y_i $y = f(x, a)$, where a, is the parameter of the classification function.

To minimize the training error, the model learn from f(x, a).

R_{emp} is the empirical risk, L is the loss function.

P(x, y) is the joint distribution function of x & y.

To minimize the training error and complexity term, we select the set of hyperplanes such that f(x) = (wx) + b:

$$\frac{1}{m} \sum_{i=1}^{m} l(w \cdot x_i + b, y_i) + ||w||^2 \text{ subject to } \min_i |w, x_i| = 1 \quad (3)$$

1.4 Dataset Selection and Processing

The Virus Share Repository which is accessible to the public at [18], provided the dataset used in this investigation. It provides the fundamental information that forms the basis of our research. One set of multivariate attributes is used to characterize each of the 15,000 instances or data points that make up the dataset. These characteristics are essential to the classification process since the Support Vector Machine (SVM) model uses them as input features. For a comprehensive knowledge of the dataset and the issue at hand, a thorough examination of these attributes is necessary.

Achieving a realistic evaluation is largely dependent on the dataset selected for this investigation. Real-world network traffic data with attributes like Source Port, Destination Port, Action, Bytes, and Elapsed Time forms the important features [19]. This dataset was chosen because it is appropriate for assessing the effectiveness of SVM malware detection and because it is relevant to mechatronics systems. The dataset is put through the routine preparation procedures of normalization, cleaning, and feature extraction [20]. To verify that each attribute is compatible with the SVM model, it is thoroughly analyzed. In order to enable efficient model training, features will be scaled and categorical variables will be suitably encoded.

1.5 Performance Evaluation

The algorithm's predictive performance analysis for malware detection in mechatronics system was carefully examined, paying close attention to important indicators that provide deep insights into the algorithm's effectiveness. Our thorough evaluation included the measurement of recall, accuracy, precision, and the F1-Score, all of which are essential measures of performance evaluation. Further optimization work was focused on improving the model responsiveness to guarantee quick detection in real-time situations.

1.6 Confusion Matrix

The confusion matrix provides a detailed analysis of the classification results of the algorithm, indicating the instances of true negatives (TN), true positives (TP), false positives (FP), and false negatives (FN). This analytical tool is essential for identifying

the advantages and disadvantages of the algorithm. The matrix, in particular, shows a low rate of false positives and false negatives, demonstrating the algorithm's resilience in accurately classifying malware and benign cases in mechatronics. Together, these many performance indicators confirm the algorithm's excellent detection power. The outcomes not only confirm its possible use in mechatronics settings but also provide a significant contribution to the development of malware detection systems in critical environment.

Table 1: Confusion Matrix Table

		Predicted Class	
		Positive	Negative
Actual Class	True	(TP)	(FN)
	False	(FP)	(TN)

i. **TN:** Correctly classifying as a negative result.
ii. **FN:** Falsely states that an observation is negative when in fact it is positive.
iii. **TP:** Correctly determine which category to target.
iv. **FP:** Calling a negative discovery falsely.

The next step was to use the formulas in (2) and (3) to determine the model's recall, precision, and accuracy, respectively.

i. **Precision:** Equation (4) represents the capacity of the classifier to correctly identify the non-negative class in equation 4.

$$\frac{TP}{TP+FP}\frac{TP}{TP+FP} \quad (4)$$

ii. **Recall:** The classifier's recall, which is determined by equation (5), is the fraction of positive predictions for a negative class that the classifier actually identified in equation 5.

$$\frac{TP}{TP+FN}\frac{TP}{TP+FN} \quad (5)$$

iii. **Accuracy:** According to equation (6), the accuracy is determined through division of the number of correctly labelled patterns by the total number of patterns in equation 6.

$$\frac{TP+TN}{TP+FP+FN+TN} \quad (6)$$

iv. **F-Score:** The last performance metric is F-Score which combines the precision and recall metrics to give a holistic view of the overall performance of the model. That is Precision + Recall.

Experimental Results

In this section, we tested our SVM algorithm and the results of the predictions is outlined in table 2. We compare the results of the proposed SVM model with three other models; SVDD, SSVM and RSVM. The fraction of the support vectors in these models was pegged at 10 percent which is close to our proposed model. Our SVM algorithms were tested on nearly 10,000 samples related to the classes of attacks and to the benign state of the medical mechatronics distribution systems. This shows that even with good detection rates of the other models, the proposed model achieved the best results that surpass the other models in terms of performance for all the types of attacks.

Table 2: Detection Accuracy Rate on the Medical Mechatronics Distribution System

Attack Class	SVDD	RSVM	SSVM	Our proposed Model
Class 1	88.8	81.5	92.6	100
Class 2	84.6	80.7	73.1	93.9
Class 3	86.9	82.6	91.3	92.1
Class 4	76.4	58.8	70.5	80.1

Table 3: Estimated Training Time (Seconds) of each Model

SVDD	RSVM	SSVM	Our proposed model
22.40	20.60	119.60	1.11

Table 4: Estimated Testing Time (Seconds) of each Model

SVDD	RSVM	SSVM	Our proposed model
0.023	0.008	0.031	0.003

Table 3 and 4 clearly shows that the estimated training and testing time for the proposed model is by far less than the other models w makes it more effective and efficient.

Conclusion

We successfully developed a security model of industrial processes and for mechatronic equipment used in hospitals. We have shown that the rise in the use of mechatronics devices connected to the internet has created a modern method of lunching attacks on mechatronics devices, however, the complex nature of these attacks does not corresponds to the low defensive mechanism provided by the IDS, hence the need for machine learning method to ensuring data confidentiality and digital sovereignty. We studied machine learning methods, and to be precise, SVM, so as to perfectly mitigate against malware attacks in medical mechatronics distribution system. We proposed a fast SVM model in which the hyperplane enclosing the training samples in the feature space defines the classifier. The sparse center of this hyperplane was estimated using only 10 percent of the training sample. We used an actual dataset to evaluate our approach, and we compared the outcomes with those of other common SVM models. In terms of estimated training and testing time, the suggested method was the fastest and produced the best detection accuracy rates. We recommend that this trusted model be implemented in health centers to help mitigate medical mechatronics distribution systems from being attacked.

References

[1].Kaissis, G., Makwowski, D., Ruckert, D. and Braren, F. (2020). "Secure, privacy-preserving and federated machine learning in medical imaging" Nature Machine Intelligent, 2020.

[2].Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W. & Gao, Y. (2021). A survey in federated learning Knowledged based systems.

[3]. Yanfang, Y., Li T., Adjeroh, D. & Sitharama S. (2017). A Survey on Malware Detection Using Data Mining Techniques. ACM Computing Surveys, 50(3):1.

[4]. Hoang, T., Ozmen, O., Jang, Y. ana Yavuz, A. (2019). Hardware Supported Oram in effect: Practical oblivious search and update on very large dataset. Proceedings on privacy enhancing technologies, 2019.

[5]. Sharmeta, A. F., Hernández-Ramos, J. L. & Moreno, V. M., 2014. A decentralized approach for security and Privacy challenges in the Internet of Things. *IEEE World Forum on Internet of Things (WF-IoT),* pp. 67-72.

[6]. Weber, M. & Boban, M., 2022. Security challenges of Mechatronics and the Internet of Things. *International Conference on Information and Communication Technology, Electronics and Mechatronics (MIPRO) IEEE,* pp. 638-643.

[7]. Chandy J (2022): International Journal for Research in Applied Science & Engineering Technology (IJRASET)ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538Volume-Available at www.ijraset.com.

[8] Johnson, A. & Grumbling, E. (2019): National Academies of Sciences, Engineering, and Medicine. Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. Washington, DC: The National Academies Press. https://doi.org/10.17226/25488.

[9] Zheng, M., Robbins, H., Chai, Z., Thapa, P. & Moore, T. (2022). "Cybersecurity Research Datasets: Taxonomy and Empirical Analysis,"presented at 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET '22).

[10] Wan, J. et al., 2018. Machine sensing framework with inter-cloud computing capability in vehicular networking. *Mechatronics Research,* 18(3), pp. 390-420.

[11] Yaacoub, E., Abdullah , K. & Adnan , A.-D., 2022. Cooperative wireless sensor and actuators for green mechanical devices. p*roceedings of the 8h ACM symposium on QoS and security for medical mechatronics,* pp. 89-101.

[12] Yao, X., Chen, Z. & Tian, Y., 2015. A lightwirght attribute-based encryption scheme for the Internt of Things. *Future Generation Computer Systems,* Volume 49, pp. 104-112.

[13] Bush, I. & Abiyev, R. (2023). 'Introduction to Machine Learning and IoT' Machine Learning and the Internet of Things in Education, Studies in Computational Intelligence 1115, Pp. 1-7. https://doi.org/10.1007/978-3-031-42924-8_1

[14] Helwan, A., Bush, I. & Abiyev, R. (2017). Machine learning techniques for classification of breast tissue. Procedia Computer Science, 120, 402–410.

[15] Francis, T., Madiajagan, . M. & Kumar, V., 2015. Privacy Issues and Techniques in E Health Systems. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research ACM,* pp. 113-115.

[16] Bremer, J. (2015). Welcome to VMCloak's documentation! WWW Document. Available at: http://vmcloak.readthedocs.io/en/latest/. [Accessed 29 May, 2024].

[17] Cuckoo Foundation (2015). Cuckoo Sandbox Book. WWW document. Available at: http://docs.cuckoosandbox.org/en/latest/introduction/what/. [Accessed 27 June, 2024]

[18] https://www.google.com/search?client=firefox-b-e&q=VIRUS+SHARE

[19] Tariq, H. (2024). "Behavioral Anomaly Detection in Mechatronic Systems Using Advanced Machine Learning Techniques." IEEE Transactions on Industrial Electronics, 67(10), 8452-8462.

[20] Amer, M. Goldstein, M. and Abdennadher, S. "Enhancing one-class support vector machines for unsupervised anomaly detection," in *Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description (ODD), August* 11-14,. New York, USA, 2013, pp. 8-15.