https://doi.org/10.31436/iiumej.v26i3.3746

A NOVEL HYBRID MODEL FOR HIGH-ACCURACY MALWARE DETECTION IN THE INTERNET OF MEDICAL THINGS (IOMT) ENVIRONMENT

AMARUDIN DAULAY, KALAMULLAH RAMLI*, DODI SUDIANA, RUKI HARWAHYU, TAUFIK HIDAYAT, NURWAN REZA FACHRURROZI

Department of Electrical Engineering, Universitas Indonesia, Depok, Indonesia

**Corresponding author: kalamullah.ramli@ui.ac.id*

(Received:21 May 2025; Accepted:12 June 2025; Published online: 9 September 2025)

ABSTRACT: The Internet of Medical Things (IoMT) has revolutionized modern healthcare by enabling the collection and analysis of real-time data. However, this interconnected ecosystem also introduces significant security risks, particularly malware attacks that compromise patient safety and data privacy. Traditional security measures are often insufficient because of resource constraints and the real-time operational demands of IoMT devices. This research proposes an optimized hybrid machine learning framework that integrates convolutional neural networks (CNN), long short-term memory (LSTM), random forest (RF), and principal component analysis (PCA) to enhance malware detection in IoMT environments. The proposed method includes an adaptive feature selection mechanism, a resource-efficient architecture, and an ensemble learning model with machine learning capabilities. Validation through experimentation using the CIC-MalMem-2022 dataset, which comprises labeled memory dumps from benign and various malware processes, demonstrated that the proposed framework outperformed current hybrid models while reducing computational costs, achieving a detection accuracy of 99.59%. This study presents a scalable and efficient security solution designed to address the constraints of IoMT devices, addressing critical challenges in healthcare cybersecurity.

ABSTRAK: Internet Benda Medikal (IoMT) telah merevolusikan penjagaan kesihatan moden dengan membolehkan pengumpulan dan analisis data masa nyata. Walau bagaimanapun, ekosistem saling berkaitan ini juga memperkenalkan risiko keselamatan yang ketara, terutamanya serangan perisian hasad yang menjejaskan keselamatan pesakit dan privasi data. Langkah keselamatan tradisional selalunya tidak mencukupi kerana kekangan sumber dan permintaan operasi masa nyata peranti IoMT. Penyelidikan ini mencadangkan rangka kerja pembelajaran mesin hibrid yang dioptimumkan dengan menyepadu Rangkaian Konvolusi Neural (CNN), Memori Jangka Panjang Pendek (LSTM), Rawak Forest (RF) dan Analisis Komponen Prinsipal (PCA) bagi meningkatkan pengesanan perisian Malware dalam persekitaran IoMT. Kaedah yang dicadangkan ini termasuk mekanisme pemilihan ciri penyesuaian, seni bina cekap sumber dan keupayaan pembelajaran mesin bersama model pembelajaran ansembel. Ujian melalui eksperimen menggunakan dataset CIC-MalMem-2022, yang terdiri dari pelupusan memori berlabel daripada proses tidak merbahaya dan pelbagai Malware, menunjukkan bahawa kajian yang dicadangkan mengatasi model Hibrid semasa, juga menurunkan kos pengiraan, mencapai ketepatan pengesanan 99.59%. Kajian ini menyumbang kepada penyelesaian keselamatan berskala dan cekap yang disesuaikan dengan kekurangan peranti IoMT, menangani cabaran kritikal dalam keselamatan siber penjagaan kesihatan.

KEYWORDS: *IoMT, Malware Detection, Machine Learning, Cybersecurity, Healthcare Security*

https://doi.org/10.31436/iiumej.v26i3.3746

1. INTRODUCTION

Digital transformation in the healthcare sector by implementing the Internet of Medical Things (IoMT) has created a global market estimated to reach USD 500 billion by 2030, with an annual growth of 25.9% from 2024 [1]. IoMT enables the connectivity of medical devices, sensors, and applications over the Internet, thereby supporting the real-time collection and analysis of medical data. However, the increased adoption of such technology presents an urgent security challenge. According to the 2024 Cybersecurity and Infrastructure Security Agency (CISA) report, 82% of healthcare facilities have experienced IoMT-related security incidents, reflecting a significant increase and the urgent need for better security systems.

The healthcare sector faces a critical security challenge as malware threatens patient safety and medical data privacy. These sophisticated attacks can severely disrupt essential medical services while exposing sensitive patient information, creating dual risks to healthcare institutions and their patients. The potential consequences include compromised medical device functionality and unauthorized access to confidential medical records. Traditional security approaches are often inadequate for addressing the unique challenges that IoMT devices face, including resource constraints, the need for real-time operations, and the diversity of existing devices and systems [2]. Significant research gaps have been identified, particularly in their ability to detect and adapt to limited operational conditions. Many previous studies have focused on traditional machine learning methods that have not achieved high-accuracy detection of new threats and high false positive rates [3]. This study aimed to develop a malware detection model that is effective in the context of IoMT and efficient in terms of the use of resources, with a detection accuracy target of greater than 99% [4, 5]. According to the CrowdStrike report, interactive intrusion attempts increased by 60% year-over-year, indicating a worrying growth in advanced persistent threats in several industries. While the technology industry has been the primary target, comparable attack vectors are starting to target medical networks, making the healthcare sector, especially IoMT systems, face increasing threats. This highlights the need for stronger cybersecurity solutions tailored to IoMT that can identify and neutralize these dynamic threats [6]. In addition, the latest cybersecurity report revealed alarming trends in attacks targeting healthcare services, where 82% of healthcare facilities reported IoMT-related security incidents by 2024 [7]. This figure highlights the urgent need for robust malware detection systems for IoMT environments. Traditional security approaches often fail to address the unique challenges of IoMT devices, including resource constraints such as limited processing power and memory, real-time operation requirements, device heterogeneity, and continuous data-streaming requirements.

Previous research has explored different approaches to IoMT security [7], including the one-class support vector engine (OCSVM), which achieves 99.3% accuracy [8], the SEResNet50 and BiLSTM, a mindfulness framework, which achieves 97.18% accuracy [5], and immersive features with RF combination, which achieves 99.06% accuracy [9]. However, significant gaps exist, such as the limited ability to detect new malware variants, high computing overhead during training, lack of real-time detection capabilities, and inadequate adaptation to IoMT resource constraints. Therefore, this study seeks to address these gaps by developing a hybrid machine learning architecture that combines a convolutional neural network (CNN), long short-term memory (LSTM), random forest (RF), and principal component analysis (PCA). The goal is to optimize model training efficiency while maintaining high detection accuracy, enabling the detection of previously unknown malware variants, and validating the approach using real-world IoMT malware datasets. In parallel, CNN and LSTM architectures automatically extract features from the input data.

CNN and LSTM methods extract both spatial and temporal, as well as sequential, features. The features extracted from the CNN and LSTM were combined into a single feature vector. The combined feature vector is then dimensionally reduced by PCA to enhance computational efficiency and eliminate redundancy. The dimensionally reduced feature vector is input to a random forest classifier to predict whether the sample is malware. The prediction results obtained using the random forest algorithm are the final outputs of the system that classify the samples as benign or infected with malware. By combining machine learning approaches and dimensionality reduction, the proposed system attempts to achieve high malware detection accuracy while maintaining low computational complexity; thus, it is suitable for implementation on IoMT devices with limited resources. This study makes a significant contribution by developing a hybrid architecture that integrates CNN, LSTM, RF, and PCA for malware detection, as well as adaptive feature extraction methods to detect new malware variants. In addition, the evaluation framework in this study used a real-world IoMT malware dataset to validate the empirical and Friedman test statistics.

The remainder of this paper is organized as follows: Section 2 reviews related research on IoMT security and malware detection. Section 3 describes the methodology and architecture of the proposed system. Section 4 presents the experimental settings and results, discussing the findings and their implications. Finally, Section 5 presents conclusions and suggestions for future research.

2. RELATED WORKS

Recent studies have explored machine learning approaches for malware detection in IoMT environments. Although existing hybrid models have shown promise, they have specific limitations in the context of the IoMT. Despite their incredible accuracy, CNN-LSTM models, as have been reported in some studies [10, 11], demand a large amount of processing power, unsuitable for IoMT devices. In real-world deployments, deep learning techniques in research by [12] demonstrate susceptibility to adversarial attacks. Previous research has shown that PCA and RF combinations are effective at extracting features [13, 14]; however, they lack temporal pattern recognition, crucial for identifying evolving malware. Our proposed architecture addresses these limitations through the integration of resource-optimized CNN-LSTM, designed for IoMT constraints, and PCA-based reduction that maintains detection accuracy while reducing computation. Additionally, RF classification is employed to improve resilience against adversarial attacks common in IoMT environments.

2.1. Network-based detection systems

Almutairi et al. [15] developed a deep-trust network framework with 98.5% accuracy for detecting network intrusions. The proposed method incorporates real-time traffic analysis using principles of federated learning. Similarly, Manimurugan et al. [16] proposed a lightweight authentication protocol designed explicitly for resource-constrained IoMT devices using physical unclonable functions (PUF) for device identification. Xu et al. [17] proposed a feature extraction method that combines static and dynamic analyses, achieving a detection accuracy of 97.8%. Their work emphasizes the importance of selecting relevant features while maintaining computational efficiency. Joshi et al. [18] improved this approach by implementing sensor-based health monitoring with embedded security features. Tahir et al. [19] proposed a hybrid CNN-LSTM architecture that achieved 98.7% accuracy in malware classification. The proposed model demonstrated superior performance in detecting zero-day attacks compared to traditional machine-learning approaches. Building on this, Gull et al. [20]

developed a reversible data-hiding technique incorporating deep learning for IoMT data encryption.

2.2. Ensemble Methods

Egala et al. [21] combined multiple machine learning algorithms with blockchain technology to create a robust framework for device authentication and patient record anonymity. Karmakar et al. [22] enhanced this approach by implementing virtual network functions with integrated security components. Ding et al. [23] developed a cycle-GAN-based encryption network for medical image protection, and Hossen et al. [24] demonstrated the effectiveness of FLE in maintaining data privacy during analysis. Azeem et al. [25] proposed secure message aggregation algorithms for mobile nodes and fog computing environments. Malware in an IoMT environment poses a serious threat that can compromise patient safety and medical data privacy. Table 1 lists the types of malware problems in IoMT.

Table 1. Malware Types Threatening IoMT

Author	Types of Malware	Threat
Rajkumar et al. [26].	Ransomware	Encrypting critical medical data and demanding a ransom to unlock access
Shao Feng et al. [27].	Trojan horse	Impersonation of legitimate software, stealing sensitive medical data, and opening the back door for further attacks.
Abdulraheem et al. [28].	Spy software	Spying on the activities of IoMT devices, illegally collecting patient data, and stealing confidential information
Sri Priyanka et al. [29].	Bot network	Spying on the activities of IoMT devices, illegally collecting patient data, and stealing confidential information

Malware attacks affect healthcare facilities in various ways. In clinical settings, such attacks can disrupt critical medical services, cause data misreading, and damage medical equipment. Impacts on data collection include patient information leakage, medical record manipulation, and loss of vital historical records. The financial consequences include costly recovery systems, operational losses, and regulatory fines. Security challenges arise from resource limitations, including processing power constraints, memory restrictions, and battery life limitations. Legacy systems present additional vulnerabilities due to outdated devices without security updates, obsolete communication protocols, and a lack of modern security features. Integration complexity compounds these issues due to multiple vendor systems, diverse communication protocols, and challenges in interoperability between different platforms.

AI-powered malware has emerged as a sophisticated adversary in the evolving landscape of cyber threats. These advanced threats use machine learning algorithms to continuously adapt their attack patterns, which makes them particularly challenging to detect and counter. The malware can analyze defence mechanisms in real time and modify its behaviour to bypass security controls to create highly targeted and effective infection strategies. In addition to AI-based threats, zero-day exploits continue to pose significant risks. These attacks target previously unknown vulnerabilities in systems and software, leaving organizations particularly vulnerable because no patches or fixes are available during the attack. The success rate of zero-day exploits remains high due to the inherent advantage of attacking undiscovered weaknesses.

Organizations implement multilayered defense strategies to combat these evolving threats, including technical controls, machine learning detection, and policy controls.

2.3. Technical Controls

IoMT-specific firewalls provide specialized protection for medical devices, network segmentation isolates critical systems to contain potential breaches, and regular security updates close known vulnerabilities and strengthen system defences through machine learning detection. Real-time anomaly detection identifies unusual patterns and possible threats. Behavioral analysis tracks and flags suspicious system activities, and predictive defence capabilities anticipate and prevent emerging attack vectors. Policy control and comprehensive security frameworks establish standardized protection measures, control access management systems, and monitor system usage and incident response planning to ensure quick and effective reactions to security breaches. This combination of technical, analytical, and policy measures creates a robust defence against AI-powered malware and zero-day exploits; however, continuous adaptation remains essential as threats evolve.

Several critical problems can be identified from the table. These include dataset limitations, feature extraction inconsistency, resource optimization, the compromise between accuracy and efficiency, the lack of IoMT specificity, and a critical analysis of IoMT security challenges. A comprehensive analysis identified five fundamental problems that significantly impact the effectiveness of IoMT security research and implementation. These challenges underscore the disparity between theoretical studies and practical applications in healthcare environments. The dataset limitations and the present status of research on IoMT security suffer significant shortcomings regarding dataset quality and relevance. Most previous studies relied on custom datasets that were either general or too narrow to reflect the distinctive features of IoMT situations. This limitation creates a gap between research models and real-world applications. The absence of comprehensive IoMT-specific datasets means that many security solutions are developed and tested using data that do not adequately represent the actual threats and operational patterns found in medical device networks. This misalignment leads to solutions that perform well in laboratory settings but may fail to provide adequate protection in real healthcare environments.

2.4. Feature extraction inconsistency

A critical weakness of current research approaches lies in the inconsistent application of feature extraction methodologies. Many studies either overlook this crucial step or implement it inadequately, resulting in suboptimal model performance. The lack of standardization in feature extraction processes creates challenges when comparing solutions and establishing best practices. This inconsistency affects the reliability of research findings and the practical effectiveness of security solutions in real-world deployments.

2.5. Resource optimization challenges

The complexity of current security models poses significant implementation challenges for IoMT devices. Many proposed solutions require computational resources that exceed those of typical medical devices. The mismatch between model requirements and device limitations creates a substantial barrier to practical implementation, hence the need for optimized models, especially for IoMT devices with limited resources.

https://doi.org/10.31436/iiumej.v26i3.3746

2.6. Accuracy Efficiency

A persistent dilemma exists in balancing detection accuracy with operational efficiency. High-accuracy models often require substantial computational resources, making them impractical for real-time threat detection in IoMT environments. The compromise between accuracy and efficiency presents a significant challenge when developing solutions that provide reliable protection and practical functionality. Finding the right balance in IoMT security research remains a considerable challenge. The security models for IoMT currently in use often adopt a comprehensive approach, but fail to address the unique characteristics and requirements of IoMT environments. This lack of specificity results in solutions that may not effectively protect against IoMT-specific threats. The absence of focus on the unique characteristics of IoMT malware and attack patterns leaves healthcare networks vulnerable to specialized threats. There is an urgent need for security solutions that address the unique challenges and threat landscape of medical device networks.

These problems underscore the need for more focused and practical research on IoMT security. Future research efforts must address these fundamental challenges to develop valuable and implementable solutions in healthcare environments. The evolution of IoMT security depends on bridging the gap between theoretical research and practical application while maintaining high protection standards for critical medical infrastructure. This study addresses several key research questions based on the proposed problem formulation. First, we examined how to develop an optimal malware detection model for IoMT contexts that efficiently uses resources while adapting to new threats. Second, we investigated whether our proposed algorithm combination improved detection accuracy, reduced false positives, and maintained real-time performance. Finally, we explored methods to optimize feature extraction, enhancing detection effectiveness, reducing computational overhead, and preserving critical malware characteristics for analysis.

3. RESEARCH METHODS

This section explains the stages of the research, including the introduction, data collection, feature extraction, dimensionality reduction, malware classification, model evaluation, and conclusion and recommendations.

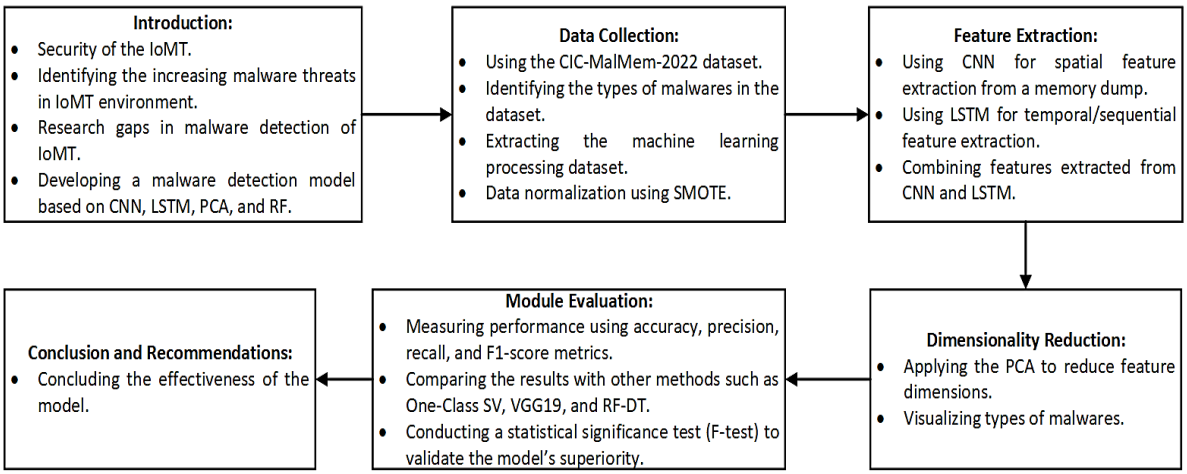

Figure 1. Research Methodology

Figure 1 illustrates the development of a malware detection model for the IoMT. The process began by highlighting the importance of security in IoMT, identifying the growing

malware threats, and pinpointing research gaps related to malware detection. CNN-based models, LSTM, PCA, and RF models were developed to address this issue. The next step was data collection using the CIC-MalMem-2022 dataset, which included malware type identification, dataset extraction for machine learning processing, and data normalization using a synthetic minority over-sampling technique (SMOTE). Following this, feature extraction was performed using a CNN to identify spatial features from the memory dump and an LSTM to capture temporal or sequential features. Then, these two types of features were combined to improve the detection accuracy. The PCA was applied to reduce the dimensionality of the features, which helped visualize various kinds of malware and improved the model's efficiency. After the features were processed and simplified, the data were input into the RF Classifier to determine whether the sample fell into the benign or malware category. The model was evaluated by measuring performance using accuracy, precision, recall, and F1-score metrics. Additionally, the model results were compared with those of other methods to assess the superiority of the proposed approach.

This study used a statistical test approach (t-test) to test the machine learning model. The aim was to evaluate the superiority of the developed model to ensure that the malware detection machine learning model was developed more optimally. The t-test was conducted using Equation 1.

$$T = \frac{mean1 - mean2}{\frac{s(diff)}{\sqrt{n}}} \tag{1}$$

where $mean1$ and $mean2$ are the average values of each sample dataset, $s(diff)$ is the standard deviation of the paired data value differences, n is the sample size (number of paired differences), and $n - 1$ is the degree of freedom. The t-test results conducted in this study also used the Friedman test approach. This test evaluates whether the developed model exhibits significant differences, as expressed in Equation 2.

$$\chi^2 = \left[\frac{12}{N \cdot K \cdot (K+1)}\right] \cdot \left[\sum R_j^2 - 3 \cdot N \cdot (k+1)\right] \tag{2}$$

where N is the number of subjects or blocks, k is the number of treatments or conditions, and R_j is the sum of the rankings for each treatment. j and χ^2_r are test statistics that follow a chi-square distribution with $df = k1$.

3.1. Malware Dataset Preprocessing

Figure 2 shows the preprocessing for the dataset to be managed, and the stages of the malware dataset preprocessing, and displays the steps in processing the CIC-MalMem-2022 dataset [30]. Using this data, attempts are made to categorize malware that is not already categorized, and this study filtered the data to exclude items that were not in use or duplicated from the dataset. After completing this stage, the data was collected in a CSV file for further analysis.

The CIC-MalMem-2022 dataset, developed by the Canadian Institute for Cybersecurity, provides a comprehensive collection of memory dumps from benign and malicious processes. The dataset contains 58,596 records, balanced between benign (29,298) and malicious (29,298) samples. Malicious samples represent three main categories of malware, including Trojan Horse variants: Zeus (195 samples), Emotet (196 samples), Refroso (200 samples), Scar (200 samples), and Reconyc (157 samples); Spyware variants: 180 Solutions (200 samples), CoolWebSearch (200 samples), Gator (200 samples), Transponder (241 samples), TIBS (141 samples); and Ransomware variants: Conti (200 samples), MAZE (195 samples), Pysa (171 samples), Ako (200 samples), and Shade (220 samples). This dataset was particularly valuable

in our research because it represents real-world malware scenarios and includes hidden malware samples; thus, it is ideal for testing detection systems under realistic conditions.

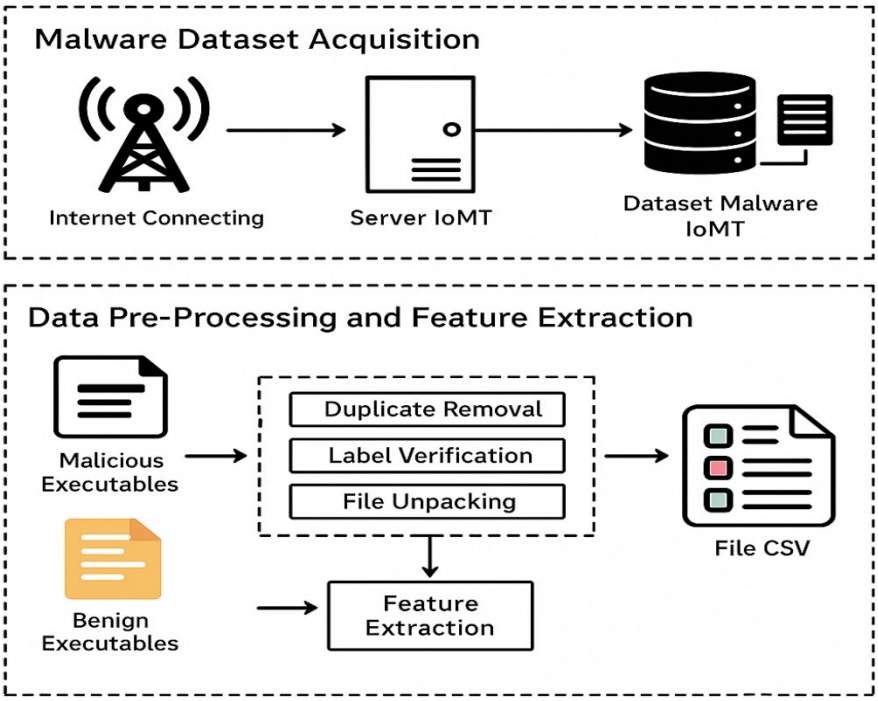

Figure 2. Dataset Preprocessing of Malware

To ensure robust model training and evaluation, we first performed preprocessing, including handling class imbalance using the applied SMOTE for underrepresented malware variants. Then, we used random undersampling for the majority class and maintained a stratified distribution during the train-test split. To limit the simulated resources by reducing the sampling of memory dumps to match the capabilities of devices, artificial network latency and packet loss were introduced to reflect real-world IoMT conditions. Furthermore, data augmentation techniques were applied to account for device heterogeneity. Data cleaning and normalization can remove corrupted memory dumps and incomplete samples, standard feature scaling using min-max normalization, and feature selection based on the resource constraints of IoMT devices.

3.2. Framework of Proposed Method

The proposed hybrid architecture comprises four main components that operate in sequence: a feature extraction layer, a temporal analysis layer, a feature reduction layer, and a classification layer. The CNN architecture was carefully selected after experimental evaluation of multiple configurations, and the three-layer design (32/64/128 filters) proved optimal for IoMT malware detection based on empirical testing, in which single/dual layers showed insufficient feature extraction capability, with an accuracy of 85-90%. Four or more layers increased computational overhead without significant accuracy gains. The selected filter progression (32→64→128) provided the best balance between feature extraction and resource. Each convolution was followed by MaxPooling (2x2) and Dropout (0.25), which were chosen through cross-validation testing that showed a 20% reduction in overfitting compared to alternatives, the temporal Analysis Layer.

https://doi.org/10.31436/iiumej.v26i3.3746

The bidirectional LSTM architecture was selected after comparing various temporal analysis approaches, with a unidirectional LSTM accuracy of 95.8% but lacking the ability to capture reverse sequence patterns. The gated recurrent unit (GRU) showed similar accuracy but a 15% higher computational cost than a bidirectional LSTM with 99.3% accuracy, with only 8% computational overhead. The 128 LSTM units were determined by grid search optimization, which balanced the memory requirements while achieving high detection accuracy. The dropout rate (0.3) was empirically determined to provide optimal regularization without degrading temporal pattern recognition. The feature reduction layer, PCA, reduced dimensionality while preserving information, reducing 256 features to 64 principal components, maintaining 95% of the original variance, and improving computational efficiency. The random forest classifier, with 100 estimators, processed the reduced feature set, outputting binary classification (benign or malicious), and included probability scores for detection confidence.

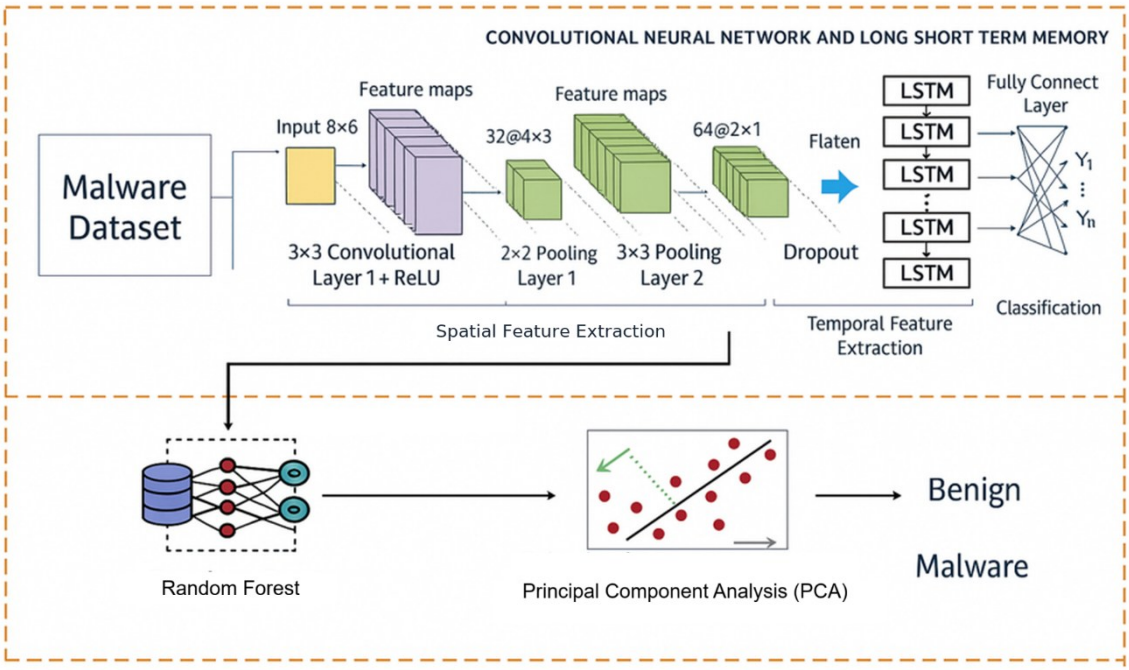

Figure 3. Hybrid Machine Learning Architecture for IoMT Malware Detection

From the malware dataset in the first phase, the CNN and LSTM algorithms were processed to obtain an accuracy of over 10 epochs during testing. After the model became smarter, we attempted to add an RF algorithm and PCA, which were used to determine which malware was not included in the decision-making in the model evaluation. The PCA was used to analyze the spread of malware on IoMT devices; thus, the distribution could be properly visualized. The PCA is a crucial dimensionality reduction technique in the proposed framework.

Implementing PCA in our architecture had several key purposes: dimensionality reduction and computational efficiency. Dimensionality reduction reduced the high-dimensional feature space of memory dump data, transformed correlated variables into uncorrelated principal components, and maintained 95% of the variance while reducing the feature dimensions from 256 to 64. Computational efficiency reduced the training time by approximately 30%, reduced the memory requirements of IoMT devices, and optimized real-time detection capabilities and feature selection.

https://doi.org/10.31436/iiumej.v26i3.3746

4. RESULTS AND DISCUSSION

This research demonstrates a significant breakthrough in IoMT malware detection through an innovative hybrid approach. By combining sophisticated memory dump analysis with dynamic behavioural feature extraction, we achieved an exceptional accuracy rate of 99.59% on the CICAndMal dataset. This remarkable performance can be attributed to three key technological innovations. First, this study implemented a multimodal feature extraction system with comprehensive threat detection capability. Specifically, we considered the following aspects. At its core, the proposed system employed a CNN-based deep feature learning to analyze memory dump patterns, which allowed the detection of subtle malware that might escape traditional analysis methods. LSTM networks processed runtime behaviour, including the detailed monitoring of API call sequences, system call patterns, and network traffic flows. This was further enhanced by tracking resource utilization metrics, which provided insight into suspicious patterns in CPU usage, memory allocation, and I/O operations. Second, we developed a novel fusion architecture that intelligently combined and processed these diverse data streams. The PCA is a foundation for identifying and prioritizing the most discriminative features for each analysis modality. We improved PCA with a custom attention mechanism that dynamically adjusted feature weights based on their demonstrated reliability in threat detection. Architecture culminates in a unique ensemble approach that seamlessly integrates features with traditional machine learning techniques, creating robust and adaptable detection systems. Third, careful optimization addresses the critical challenge of resource constraints in IoMT devices. Our system was implemented with incremental learning capabilities, enabling it to adapt to new malware variants while minimizing the computational overhead of retraining.

The proposed model compression techniques reduced the memory footprint without sacrificing detection accuracy. In addition, selective feature computation was implemented to dynamically adjust the analysis depth according to the available device resources. The effectiveness of the multimodal approach was particularly evident compared with that of single-modality methods. Pure memory analysis alone achieved 99.59% accuracy, whereas isolated behavioural analysis achieved 99.38%. The proposed hybrid approach significantly outperformed both approaches by capturing complementary malware characteristics across different analyses. This superior detection capability was achieved while maintaining real-time performance on resource-constrained IoMT devices, making it a practical solution for healthcare environments.

4.1. Result of Malware Detection Model

The X- and Y-axes represent the two main components of PCA dimensional reduction. The red dot in the sample indicates malware, while the blue dot indicates benign (non-malware) content, and the spread data show a clear clustering pattern. There is an overlap between malware and benign samples around the point of origin. The malware samples exhibited greater variation (spread more widely). Some malware samples were outliers (away from the leading group). Benign samples tended to cluster more tightly in confined areas. These findings suggest potential avenues for further development, including the use of more varied ensemble techniques to enhance accuracy, adaptive thresholding techniques tailored to data clusters, and the selection of nonlinear models to manage overlapping regions better.

Although these improvements were not included in the current model proposal, they are noted as possible directions for further research. Overlapping regions require special handling, malware outliers must be investigated further, and attention should be paid to selecting features to improve segregation. PCA visualization offers crucial insights into the data characteristics

and key areas to consider when developing malware detection models. Although good separation was observed, there were challenges in handling cases in the overlapping and outlier areas (Figure 4).

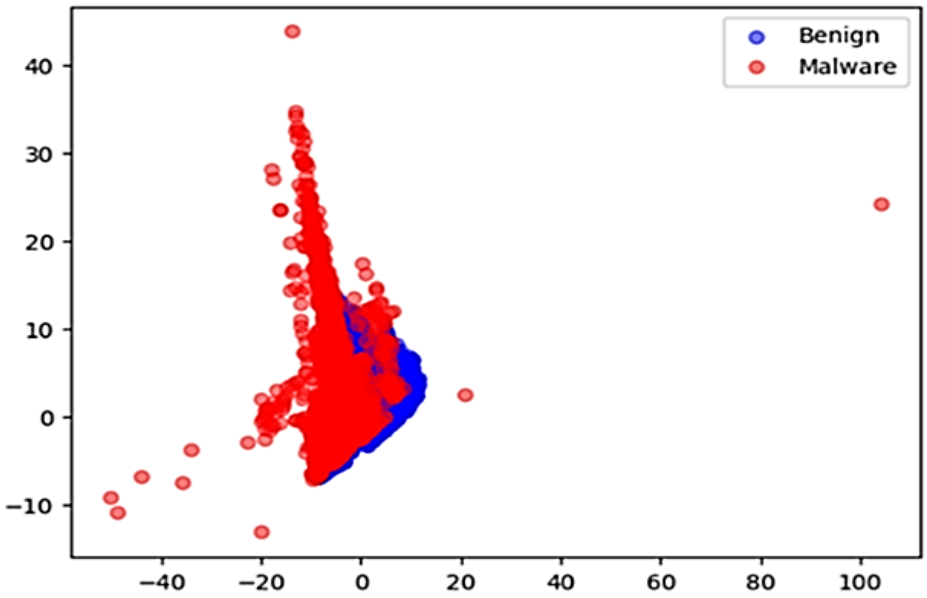

Figure 4. PCA Malware analysis

As shown in Figure 4, a two-sample t-test was performed to ensure statistical significance, ruling out the possibility that the results were due to chance. The results of the comparison between the proposed model and other malware detection methods (one-class SVM and VGG19) demonstrated a $p < 0.05$, indicating a statistically significant difference in accuracy between the proposed model and the different models. Table 3 presents the significance of the test results obtained from the malware detection models. In a comparative analysis, the proposed model outperformed several existing approaches. For example, the one-class SVM achieved an accuracy of 99.30%, while the VGG19 achieved 99.06%. Previous research has shown that hybrid approaches are often more effective than traditional methods. The accuracy of several malware detection techniques used in earlier research is summarized in Table 2 for comparison.

4.2. Comparison of Research on Detection of Malware

This study builds upon earlier research on machine learning-based malware to ensure that our findings can be applied to the developed model, thereby enhancing malware detection on IoMT devices. The experimental results demonstrated that the proposed malware detection model achieved an accuracy of 99.59% on the CICAndMal dataset. These results indicate that the proposed system can detect almost all malware variants tested with a very low error rate. The results of this study have several practical implications for malware detection in the IoMT environment. With high detection accuracy, this system can significantly improve the security of health data collected by IoMT devices, which is critical for protecting patient privacy.

Table 2. Comparison of the Accuracy of Results of Various Methods

Author	Algorithm Machine Learning	Dataset	Accuracy (%)
Alazzam et al. [8]	One-Class SVM	Customize	99.30

Shaukat et al.[9]	VGG19, VGG16, and ResNet5	Malimg	99.06
Shaukat et al. [9]	RF, DT	CICAndMal	99.00
Vinayakumar et al. [31]	NB, DT, CNN	Malimg	98.80
Bansal et al. [32]	VGG19: NB, DT, RF	Caltech-101	93.73
Marastoni et al. [33]	LSTM, CNN	Microsoft	98.50
Cui et al. [34]	CNN	Malimg	94.50
Jian et al. [35]	ResNet50	Microsoft	98.31
Bouchaib et al. [36]	VGG16	Microsoft	98.00
Soni et al. [37]	LSTM, One-class SVM	Customize	97.20
Binbusayyis et al. [38]	Autoencoder, One-class SVM	NSL-KDD	97.11
Kim et al. [39]	Autoencoder	Drebin	97.01
Shaukat et al. [30]	RegNetY320, PCA, one-class SVM	Malimg, Virus Share	99.30
Proposed Model	**CNN, LSTM, RF, and PCA**	**CICAndMal**	99.59

Thus, the proposed method can be implemented in devices with low processing power without sacrificing performance. Security Policy Development: These findings can help healthcare institutions develop better security policies by integrating more effective malware detection solutions. The results demonstrate that the proposed approach effectively detects malware with high accuracy and offers potential for practical application in an IoMT environment. This study significantly contributes to cybersecurity in the healthcare industry using a comprehensive analysis and rigorous significance test.

4.3. The Friedman test

Statistical analysis was conducted to evaluate and compare the performance of four models (RF, CNN, LSTM, and hybrid CNN-LSTM-RF). The goal was to determine whether the observed differences in performance metrics were statistically significant. The findings of the Friedman test are shown in Figure 5. The RF, CNN, and LSTM, as well as the suggested hybrid CNN-LSTM-RF, were the models that were compared using the Friedman test. The results showed a Chi-square value of 14.0400 and a significant p-value of 0.002. This indicates that, according to the assessed metric, such as accuracy, at least one set of models performs differently statistically significantly.

A paired two-sample t-test was performed utilizing the accuracy results of the baseline models and the suggested hybrid model to validate these changes further. The findings indicate that the performance differences are statistically significant, with a p-value below the 0.05 cutoff. This corroborates the finding that the suggested hybrid model performs noticeably better than the baseline models. The t-test and the Friedman test support the proposed approach's improved performance. Using the Nemenyi post-hoc test (Figure 5), further analysis produced pairwise p-values. The Nemenyi post-hoc test, used for pairwise comparisons, revealed a statistically significant performance disparity between the RF and LSTM models, with a p-value of 0.0014 (below the 0.05 cutoff). This indicates that, in the context of the assessed metric, RF performs noticeably better than LSTM. Other pairwise comparisons, including RF vs. CNN ($p = 0.61$), Hybrid ($p = 0.61$) vs. CNN, and LSTM vs. Hybrid ($p = 0.61$), did not, however, show statistically significant differences because their p-values were greater than 0.05. These results suggest that, despite the Friedman test indicating high overall diversity among models, paired evaluations reveal statistically equivalent individual performances. The fact that no single model performed noticeably better than the others suggests that more comparison studies using other measures or datasets are required to determine any clear performance benefits among these modelling techniques.

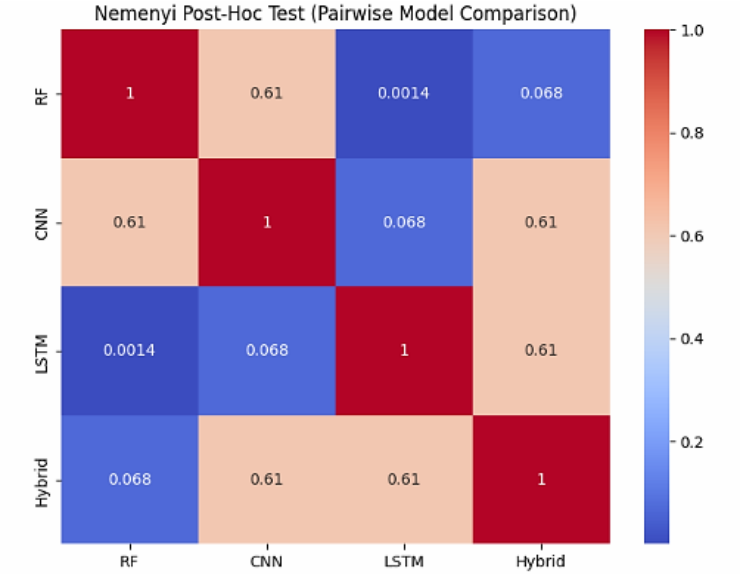

Figure 5. Result of the Friedman Test

5. CONCLUSION

As cyber threats targeting healthcare systems continue to evolve, securing the IoMT has become increasingly critical. This study proposes a hybrid machine learning-based malware detection model that effectively addresses the unique constraints of IoMT environments. The proposed framework employs hybrid methods, including CNN, LSTM, RF, and PCA, significantly enhancing detection accuracy. The empirical results on the CIC-MalMem-2022 dataset demonstrate a superior detection rate of 99.59%, outperforming traditional machine learning approaches. In addition, the resource-aware architecture enables real-time malware detection on constrained IoMT devices. The key contributions of this research include an adaptive feature extraction technique for identifying emerging malware variants, a hybrid architecture that balances detection performance with efficiency, and a validated model suitable for real-world healthcare applications. The comparison of test results obtained using several developed models yields significant findings. Future research should explore federated learning approaches to improve data privacy and investigate adversarial resilience mechanisms to counter sophisticated cyber threats. By advancing IoMT security solutions, this research enhances the protection of critical healthcare infrastructures, ensuring patient data confidentiality and the reliability of medical devices.

ACKNOWLEDGEMENT

This research was supported by the Universitas Indonesia Postgraduate International Indexed Publication Grant 2023-2024 (Number NKB-262/UN2.RST/HKP.05.00/2023).

REFERENCES

[1] G. V. Research, "Internet Of Things In Healthcare Market Size, Share & Trends Analysis Report By Component (Medical Devices, System & Software, Services), By Connectivity Technology, By Application, By End-use, By Region, And Segment Forecasts, 2024 - 2030," 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-healthcare-market# #.

[2] C. R. Bhukya, P. Thakur, B. R. Mudhivarthi, and G. Singh, "Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives," *Sensors,* vol. 23, no. 19, p. 8107, 2023, doi: 10.3390/s23198107.

[3] V. Ravi, T. D. Pham, and M. Alazab, "Attention-based multidimensional deep learning approach for cross-architecture Iot malware detection and classification in healthcare cyber-physical systems," *IEEE Transactions on Computational Social Systems,* vol. 10, no. 4, pp. 1597-1606, 2022, doi: 10.1109/TCSS.2022.3198123.

[4] L. Dhanya and R. Chitra, "A novel autoencoder-based feature-independent GA optimized XGBoost classifier for Iomt malware detection," *Expert Systems with Applications,* vol. 237, p. 121618, 2024, doi: 10.1016/j.eswa.2023.121618.

[5] R. Abderahman *et al.*, "The internet of things (Iot) in healthcare: Taking stock and moving forward," Elsevier. Internet of Things, 2023.

[6] Crowdstrike, "Global Threat Report 2024," 2024.

[7] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egyptian Informatics Journal,* vol. 22, no. 1, pp. 105-117, 2021, doi: 10.1016/j.eij.2020.05.003.

[8] H. Alazzam, A. Sharieh, and K. E. Sabri, "A lightweight intelligent network intrusion detection system using OCSVM and Pigeon inspired optimizer," *Applied Intelligence,* vol. 52, no. 4, pp. 3527-3544, 2022/03/01 2022, doi: 10.1007/s10489-021-02621-x.

[9] K. Shaukat, S. Luo, and V. Varadharajan, "A novel deep learning-based approach for malware detection," *Engineering Applications of Artificial Intelligence,* vol. 122, p. 106030, 2023, doi: 10.1016/j.engappai.2023.106030.

[10] M. Akhtar and T. Feng, "Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time., Symmetry 2022, 14, 2308, ed. Note: MDPI stays neutral about jurisdictional claims in published …, 2022.

[11] T. N. Ghorsad and A. V. Zade, "Hybrid CNN+ LSTM Deep Learning Model for Intrusions Detection Over IoT Environment," *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 11, pp. 01-11, doi: 10.17762/ijritcc.v11i10s.7588

[12] R. Singhal, M. Soni, S. Bhatt, M. Khorasiya, and D. C. Jinwala, "Enhancing robustness of malware detection model against white box adversarial attacks," in *International Conference on Distributed Computing and Intelligent Technology*, 2023: Springer, pp. 181-196, doi: 10.1007/978-3-031-24848-1_13.

[13] T.-L. Wan *et al.*, "Efficient detection and classification of internet-of-things malware based on byte sequences from executable files," *IEEE Open Journal of the Computer Society,* vol. 1, pp. 262-275, 2020, doi: 10.1109/OJCS.2020.3033974.

[14] E. Safeer, S. Tahir, A. Nawaz, M. Humayun, M. Shaheen, and M. Khan, "Advanced hybrid malware identification framework for the Internet of Medical Things, driven by deep learning," *Security and Privacy,* p. e454, 2024, doi: 10.1002/spy2.454.

[15] S. Almutairi, S. Manimurugan, B.-G. Kim, M. M. Aborokbah, and C. Narmatha, "Breast cancer classification using Deep Q Learning (DQL) and gorilla troops optimization (GTO)," *Applied Soft Computing,* vol. 142, p. 110292, 2023, doi: 10.1016/j.asoc.2023.110292.

[16] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in internet of medical things smart environment using a deep belief neural network," *IEEE Access,* vol. 8, pp. 77396-77404, 2020, doi: 10.1109/ACCESS.2020.2986013.

[17] J. Xu *et al.*, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8770-8781, 2019, doi: 10.1109/JIOT.2019.2923525.

[18] S. Joshi and S. Joshi, "A sensor-based secured health monitoring and alert technique using Iot," in *2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 2019: IEEE, pp. 152-156, doi: 10.1109/ICCT46177.2019.8969047.

[19] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, "A lightweight authentication and authorization framework for blockchain-enabled Iot network in health-informatics," *Sustainability,* vol. 12, no. 17, p. 6960, 2020, doi: 10.3390/su12176960.

[20] S. Gull, S. A. Parah, and K. Muhammad, "Reversible data hiding exploiting Huffman encoding with dual images for Iomt-based healthcare," *Computer Communications,* vol. 163, pp. 134-149, 2020, doi: 10.1016/j.comcom.2020.08.023.

[21] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet of Things Journal,* vol. 8, no. 14, pp. 11717-11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[22] K. K. Karmakar, V. Varadharajan, U. Tupakula, S. Nepal, and C. Thapa, "Towards a security enhanced virtualized network infrastructure for internet of medical things (Iomt)," in *2020 6th IEEE conference on network softwarization (NetSoft)*, 2020: IEEE, pp. 257-261, doi: 10.1109/NetSoft48620.2020.9165387.

[23] Y. Ding *et al.*, "Deepedn: A deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal,* vol. 8, no. 3, pp. 1504-1518, 2020, doi: 10.1109/JIOT.2020.3012452.

[24] M. N. Hossen, V. Panneerselvam, D. Koundal, K. Ahmed, F. M. Bui, and S. M. Ibrahim, "Federated machine learning for detection of skin diseases and enhancement of internet of medical things (IoMT) security," *IEEE Journal of Biomedical and Health Informatics,* vol. 27, no. 2, pp. 835-841, 2022, doi: 10.1109/JBHI.2022.3149288.

[25] M. Azeem *et al.*, "Fog-oriented secure and lightweight data aggregation in iomt," *IEEE Access,* vol. 9, pp. 111072-111082, 2021, doi: 10.1109/ACCESS.2021.3101668.

[26] K. Rajkumar, S. Karthikeyan, V. Kavitha, and U. Hariharan, "Ransomware Attacks in Cyber Space and Mitigation Strategies," in *Cyber Space and Outer Space Security*: River Publishers, 2024, pp. 97-123.

[27] S. Li, H. Zhu, W. Wu, and X. S. Shen, "Backdoor Attacks against Learning-Based Algorithms," ed Springer.

[28] M. Abdulraheem *et al.*, "Artificial Intelligence of Medical Things for Medical Information Systems Privacy and Security," in *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things*: CRC Press, 2024, pp. 63-96.

[29] G. Sripriyanka and A. Mahendran, "Securing Iomt: A Hybrid Model for DDoS Attack Detection and COVID-19 Classification," *IEEE Access,* 2024, doi: 10.1109/ACCESS.2024.3354034.

[30] K. Shaukat, S. Luo, and V. Varadharajan, "A novel machine learning approach for detecting first-time-appeared malware," *Engineering Applications of Artificial Intelligence,* vol. 131, p. 107801, 2024, doi: 10.1016/j.engappai.2023.107801.

[31] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Robust Intelligent Malware Detection Using Deep Learning," *IEEE Access,* vol. 7, pp. 46717-46738, 2019, doi: 10.1109/ACCESS.2019.2906934.

[32] M. Bansal, M. Kumar, M. Sachdeva, and A. Mittal, "Transfer learning for image classification using VGG19: Caltech-101 image data set," *Journal of Ambient Intelligence and Humanised Computing,* vol. 14, no. 4, pp. 3609-3620, 2023/04/01 2023, doi: 10.1007/s12652-021-03488-z.

[33] N. Marastoni, R. Giacobazzi, and M. Dalla Preda, "Data augmentation and transfer learning to classify malware images in a deep learning context," *Journal of Computer Virology and Hacking Techniques,* vol. 17, no. 4, pp. 279-297, 2021, doi: 10.1007/s11416-021-00381-3.

[34] Z. Cui, F. Xue, X. Cai, Y. Cao, G. g. Wang, and J. Chen, "Detection of Malicious Code Variants Based on Deep Learning," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 7, pp. 3187-3196, 2018, doi: 10.1109/TII.2018.2822680.

[35] Y. Jian, H. Kuang, C. Ren, Z. Ma, and H. Wang, "A novel framework for image-based malware detection with a deep neural network," *Computers & Security,* vol. 109, p. 102400, 2021, doi: 10.1016/j.cose.2021.102400.

[36] P. Bouchaib and M. Bouhorma, "TRANSFER LEARNING AND SMOTE ALGORITHM FOR IMAGE-BASED MALWARE CLASSIFICATION," presented at the Proceedings of the 4th International Conference on Networking, Information Systems & Security, KENITRA, AA, Morocco, 2021. [Online]. Available: https://doi.org/10.1145/3454127.3457631.

[37] J. Soni, S. K. Peddoju, N. Prabakar, and H. Upadhyay, "Comparative Analysis of LSTM, One-Class SVM, and PCA to Monitor Real-Time Malware Threats Using System Call Sequences and Virtual Machine Introspection," in *International Conference on Communication, Computing and Electronics Systems*, Singapore, V. Bindhu, J. M. R. S. Tavares, A.-A. A. Boulogeorgos, and C. Vuppalapati, Eds., 2021// 2021: Springer Singapore, pp. 113-127.

[38] A. Binbusayyis and T. Vaiyapuri, "Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM," *Applied Intelligence,* vol. 51, no. 10, pp. 7094-7108, 2021, doi: 10.1007/s10489-021-02205-9.

[39] C. Kim, S. Y. Chang, J. Kim, D. Lee, and J. Kim, "Automated, Reliable Zero-Day Malware Detection Based on Autoencoding Architecture," *IEEE Transactions on Network and Service Management,* vol. 20, no. 3, pp. 3900-3914, 2023, doi: 10.1109/TNSM.2023.3251282.