JJEE
Volume 11 | Number 4 | Pages 692-704

Jordan Journal of Electrical Engineering

ISSN (print): 2409-9600, ISSN (online): 2409-9619

Homepage: jjee.ttu.edu.jo

Image-Based Hybrid Learning Framework for Ransomware Detection

Shorouq Al-Eidi[1*], Omar Khadrawi[2], Mohammed Jebreen[3], Sohaib Abusnineh[4]

[1, 2, 3, 4] Computer Science Department, Tafila Technical University, Tafila, Jordan

Email: saleidi@ttu.edu.jo

Received: Sep 06, 2025 *Revised: Nov 14, 2025* *Accepted: Nov 29, 2025* *Available online: Jan 20, 2026*

***Abstract*—** Ransomware is a significant cybersecurity threat that encrypts sensitive data or locks users out of systems, demanding payment for recovery. It mainly targets organizations dealing with personal, financial, or intellectual properties. Detecting ransomware is challenging due to its evolving techniques. This study proposes hybrid models that combine deep learning–based feature extraction architectures, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), with machine learning classifiers, including Random Forest (RF), K-Nearest Neighbors (KNN), and Support Vector Machine (SVM). Experiments conducted using a dataset of more than 26,548 gray-scale images show that the hybrid models outperform standalone machine learning and deep learning approaches. Notably, the CNN–RF hybrid model achieved the highest accuracy, with 97.39% for binary classification and 94.32% for multi-class classification. These results highlight the potential of hybrid models to strengthen ransomware detection and enhance overall cybersecurity.

***Keywords*—** Ransomware detection; Image processing; Machine learning; Deep learning; Hybrid models.

1. INTRODUCTION

The wide development in the digital technology known as the Internet has greatly influenced the dynamics in the education, business, and government sectors. On the other hand, this development has contributed to the rise in the number of cyber-attacks in the world. One major disruptive attack that has risen from the increase in the number of cyber-attacks is the attack by ransomware [14]. With time, ransomware is using evade techniques such as obfuscation, polymorphism, etc. Classic malware detection mechanisms of signature-based heuristic analysis are inefficient in overcoming these threats because of their dynamic nature. Therefore, new effective methods of detecting ransomware have become crucial.

These days, Machine Learning and Deep Learning methods are increasingly used in cybersecurity [11], serving as robust tools that provide sophisticated methods of analysis for ransomware attacks, thereby raising the performance level of detection. In machine learning, algorithms such as RF involve the classification of ransomware in analyzing static and behavioral characteristics; however, these methods are less adaptable owing to their reliance on human-engineered features. Deep Learning methods, on their part, automatically deduce complex characteristics in an attempt to identify patterns in the behavior of ransomware; however, these methods are often resource-intensive.

* Corresponding author
DOI: https://doi.org/10.5455/jjee.204-1757176378

This work proposes a hybrid framework that systematically benchmarks CNNs (extracting spatial features) and RNNs capturing sequential dependencies combined with classical machine learning classifiers-SVM, RF, and KNN. The framework allows for the comparison between spatial versus sequential feature representations. The results clearly show that the spatial features extracted from the image-based representations are generally better at masquerading ransomware behavior than the sequential features. Although RNN-based hybrids were included for completeness, the CNN-based hybrids fare better in performance. For a reliable evaluation, we make use of a dataset size of more than 26,548 images besides advanced preprocessing techniques. It shows that the framework makes a systematic evaluation of hybrid combination, hence confirming that integrating deep feature extraction together with robust ML classifiers enhances ransomware detection performance and resilience.

The remaining part of this article is outlined in the following order: Section 2 discusses the state of the art in the area of ransomware detection. Section 3 introduces the methodology of the new approach. Section 4 deals with the experimental results. Section 5 concludes the paper with findings and the direction of future research.

2. RELATED WORK

Ransomware detection has been widely studied using ML and DL and their combinations [2]. Recently, image-based analysis has emerged as a promising avenue, leveraging visual patterns in malicious operations [3, 4]. Earlier detection methods focused on using handcrafted features derived from static or behavioral ransomware characteristics. For example, Ahmed et al. [5] employed ML classifiers on Android network traffic traces, achieving 97.24% accuracy after feature reduction to 19 using correlation analysis.

Similarly, Anwar et al. [6] applied ML classifiers to 50,000 samples, achieving a 99.9% accuracy with RF, while SVM reached 74% and KNN 97%. Ciaramella et al. [7] transformed executable files into grayscale images and applied CNN (LeNet, AlexNet, and VGG16), with VGG16 model achieved 96.9% accuracy. Ganfure et al. [8] proposed DeepWare, training CNNs on hardware performance counter data represented as images, achieving 98.6% recall and robust zero-day detection capability for unseen ransomware families.

Dynamic analysis has also been leveraged for ransomware detection. Gulmac et al. [9] utilized sandbox execution extract API calls, DLLs, and registry operations, achieving 85% and 99% accuracy with DL models such as CNN, LSTM, and MLP. Gupta et al. [10] proposed a soft-voting ensemble of five ML classifiers (RF, AdaBoost, Extra Trees, XGBoost, and Decision Tree), achieving 98.42% accuracy. Masum et al. [12] combine feature selection with ensembles of various ML classifiers, such as RF, DT, and KNN. Herrera-Silva and Hernandez-Alvarez [11] used 50 behavioral features from ransomware samples in sandbox environments, obtaining over 99% accuracy with RF and neural networks. Rani et al. [13] compared different ML classifiers (Decision Tree, RF, SVM, KNN, XGBoost, and Logistic Regression), achieving 99% accuracy. Moreover, Rani et al. [14] and Smith et al. [16] reviewed ML-based detection models.

Shwetha et al. [15] addressed class imbalance using SMOTE and NearMiss coupled with CNN and CNN-LSTM models. Their SMOTE-CNN model achieved 98.9% accuracy, while CNN-LSTM with Near Miss worked better compared to others in handling imbalanced data conditions. Vehabovic et al. [17] used federated learning for imbalanced datasets, reaching 95%

binary classification and 84.15% accuracy in multiclass classification. Early detection methods using API sequences with VM and Gradient Boosted Trees also showed success rates [18].

Despite the progress in hybrid models, prior work often focused on using individual architectures leaving a gap in systemic comparative studies. This study addresses this gap by evaluating multiple hybrid combinations (CNN/RNN with RF/SVM/KNN) on common benchmark, providing empirical insights into the most effective architectural synergies for ransomware detections.

3. METHODOLOGY

This section outlines the proposed hybrid ransomware detection framework as depicted in Fig. 1, beginning with image processing, deep features extraction, ML-based classification and evaluation models. The goal is to build a comprehensive pipeline capable of effectively distinguishing benign samples from multiple ransomware families. Each phase is discussed in detail in the next subsections.

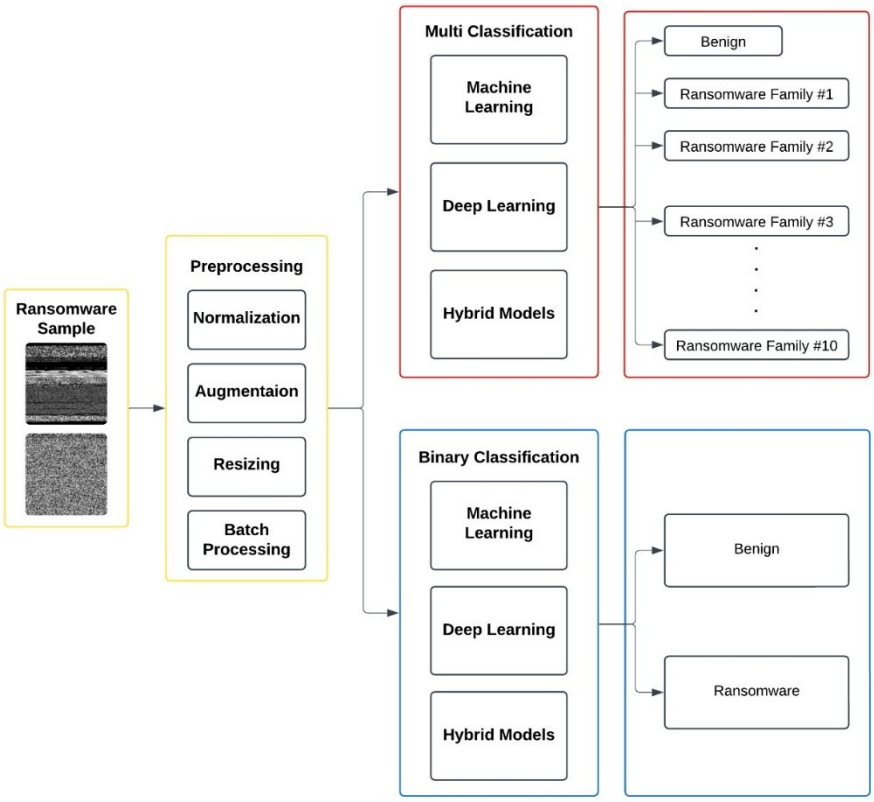

Fig. 1. Three-phase ransomware detection framework.

3.1. Dataset

This work utilized a dataset consisting of 26,548 grayscale images generated by converting executable files into 2D visual representation. More precisely, the dataset includes 14,012 benign samples and 12,536 ransomware samples divided into ten families: BetterSurf, Eksor.A, Obfuscator.AFQ, Occamy.C, OnLineGames.CTB, Reveton.A, Sfone, VB.IL, Zbot, and Zbot!CI. Each executable file was converted to a grayscale image by mapping its bytes into pixel intensities within the 0-255 range. This representation captures specific textural and structural features, allowing the models to learn meaningful spatial patterns and understand the diverse representation of benign and malicious files. Figure 2 shows some representative examples of

the analyzed dataset samples. Most are characterized by more heterogeneous and irregular textures, while benign files are much smoother and more homogeneous in structure. This composition ensures a diverse dataset for developing and evaluating both binary and multi-class ransomware detection models.

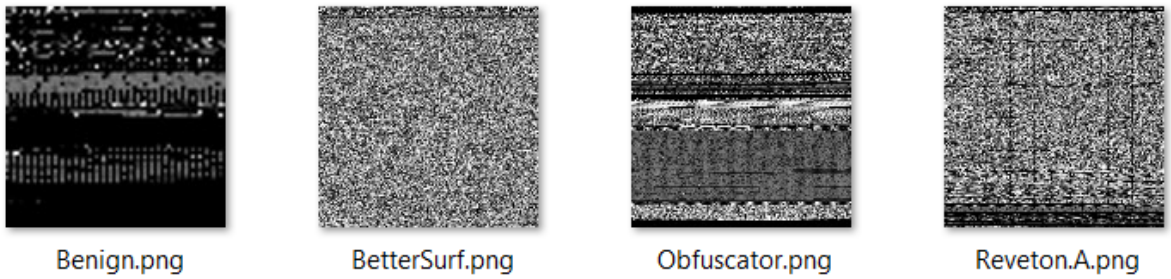

Fig .2. Sample grayscale executable image.

3.2. Preprocessing Dataset

Various preprocessing techniques have been adopted to accomplish consistency and universality throughout the dataset. Firstly, rescaling was adopted to make the values range between [0,1]. The images, which had an original size of 128x128 pixels, were resized to 64x64 pixels, with images processed in batches of 32 for optimal computational efficiency. Furthermore, one-hot encoding was adopted to transform the labels into categorical variables, which aided multi-class classification. Various techniques, which included rotation, were adopted to increase the diversity of the dataset, hence overcoming the issue of overfitting.

3.3. Feature Extraction

In this study, feature extraction was done by using CNN and RNN for the identification of both ransomware as well as the legitimate samples, based on spatial as well as sequential features. CNN extracts hierarchical spatial features like texture, structure, as well as patterns automatically from the corresponding gray-scale images, while the RNN makes use of the sequential dependencies for the analysis of the behavioral patterns in the ransomware samples. The extracted features from these deep learning algorithms can be fed to the machine learning algorithms RF, SVM, as well as KNN for enhanced accuracy of classification. The use of both deep learning as well as machine learning increases the potential.

3.4. Model Architectures

This paper discusses various models for ransomware detection, such as stand-alone machine learning, deep learning, and hybrid models, on binary and multi-class classification problems. For the extraction of features using deep learning, we implement two main architectures: a CNN (VGG16) and a standard RNN.

The CNN architecture consists of 16 learnable layers, customized for grayscale image inputs, starting with a 64×64×1 input layer. This contains five convolutional blocks totaling 13 convolutional layers: the first block contains 2 convolutional layers with 64 filters of size 3×3, the second block contains 2 convolutional layers with 128 filters, and the third, fourth, and fifth blocks each contain 3 convolutional layers with 256, 512, and 512 filters, respectively. The convolutional layers are all ReLU-activated and are succeeded by 2×2 max-pooling layers.

These are then followed by 3 fully connected layers: two comprising 4,096 units each with ReLU activation, and the final one is a softmax layer for classification. It was trained with the Adam optimizer, utilizing a learning rate of 0.001, a batch size of 32, over 50 epochs, and including dropout in the fully connected layers (rate=0.5) for regularization.

For the RNN model, we used conventional architecture with 4 neural layers: two recurrent and two dense. The network considers sequential patches, where every row of the 64×64 image is taken as one step with 64 features. This includes two RNN layers: the first one has 128 units, and the second layer with 64 units, using tanh activation. Further, these are followed by a dense layer of 64 units with ReLU activation before the final softmax output layer. This model was also trained with the Adam optimizer and a learning rate of 0.001, with a batch size of 32, for 50 epochs, and implemented dropout after every RNN layer to handle overfitting, using a rate of 0.3.

Besides the deep models, we also explored three classical machine learning classifiers: RF with 100 trees and the Gini impurity criterion; SVM with RBF kernel, C=1.0, γ='scale'; and K-Nearest Neighbors with k=5 and Euclidean distance. These were employed both as stand-alone models, as well as being used as classifiers in our hybrid framework. These hybrid models were developed by combining the deep feature extraction capability of CNN or RNN with the classification capability of ML models. In particular, features from the last pooling layer of CNN or the last RNN layer were extracted, flattened, and then used to train the RF, SVM, and KNN classifiers, leading to six hybrid combinations: CNN-RF, CNN-SVM, CNN-KNN, RNN-RF, RNN-SVM, and RNN-KNN. Hyperparameters for all models were carefully tuned based on a grid search approach with 5-fold cross-validation to explore optimal values related to learning rates, filter sizes, the number of units, the number of trees, and regularization parameters.

In this study, the dataset was split into 80% for training and 20% for testing in such a way that all classes were represented. To maintain a representative proportion of both benign and ransomware samples, stratified sampling was performed for both subsets. Randomization was controlled using a fixed random seed for reproducibility of experiments. Fine-tuning model hyperparameters was performed with the grid search optimization combined with 5-fold cross-validation on the training set. This approach ensured that the selected models were robust and resilient against overfitting, generalizing well to both binary and multi-class classification tasks.

3.5. Performance Evaluation

Quantitative assessment of anomaly detection quality relies on multi-dimensional measures that evaluate various attributes in relation to the complexity of the classification problem. Since ransomware detection involves both binary and multi-class scenarios, multiple accuracy and error metrics are used for evaluating the ensemble model prediction.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1 - score = \frac{2*(Precision+Recall)}{(Precision+Recall)} \quad (4)$$

4. RESULTS AND ANALYSIS

This section presents the experimental evaluation of the proposed ransomware detection model. The experiments address both binary and multi-class classification tasks to assess and compare baseline machine learning models, deep learning models, and their respective hybrid counterparts.

4.1. Binary Classification

The ransomware samples from different families were merged into one category labeled "ransomware" and differentiated from the "benign" class for the binary classification task. Overall, the performance of the tested models is summarized in Tables 1 and 2 and visualized in Figs. 3 to 6. Among the classic machine learning models, SVM showed the best F1-score and accuracy, reflecting its strong ability for modeling complex, nonlinear decision boundaries. RF and KNN also provided competitive results, showing stable precision and recall for both benign and ransomware classes. As for deep learning models, the CNN architecture inspired by VGG16 demonstrated the highest accuracy of 95.1%, outperforming RNN with an achieved accuracy of 91.02%. The CNN model also yielded a lower value of training loss equal to 0.1344, which indicated more stable convergence and an effective extraction of spatial features from image representations of executable files.

Table 1. Machine and deep learning results for binary classification.

Class	Metric	RF	KNN	SVM	CNN	RNN
Benign	Precision	97	98	98	98	87
	Recall	98	96	97	92	96
	F1-score	97	97	98	95	92
Ransomware	Precision	97	96	97	91	95
	Recall	97	97	98	98	84
	F1-score	97	97	98	94	89

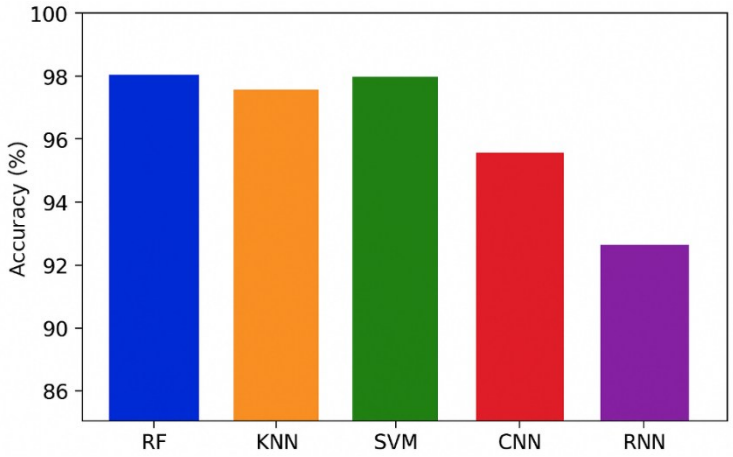

Fig. 3. Accuracies for binary classification.

Results indicated that the hybrid models, which combined deep feature extraction and machine learning classifiers, outperformed the standalone ML and DL models. According to Figs. 3 and 4, the CNN-RF hybrid model achieved the highest overall accuracy of 97.39%, with balanced precision, recall, and F1-scores for both classes. This demonstrates that the integration of powerful spatial representation from CNN with the robust classification of RF yield superior performance. Other hybrid models, such as CNN-SVM and RNN-RF, showed improved performance compared to their respective individual components but failed to perform better

than the CNN-RF model. Figure 5 demonstrates the superior learning stability and generalization of CNN by achieving faster and smoother convergence compared to RNN.

Table 2. Binary classification performance of hybrid models.

Class	Metric	CNN-RF	CNN-KNN	CNN-SVM	RNN-RF	RNN-KNN	RNN-SVM
Benign	Precision	97	98	98	92	90	86
	Recall	98	97	97	95	93	94
	F1-score	98	97	97	93	92	90
Ransomware	Precision	98	96	96	94	92	92
	Recall	96	97	98	90	89	82
	F1-score	97	97	97	92	90	87

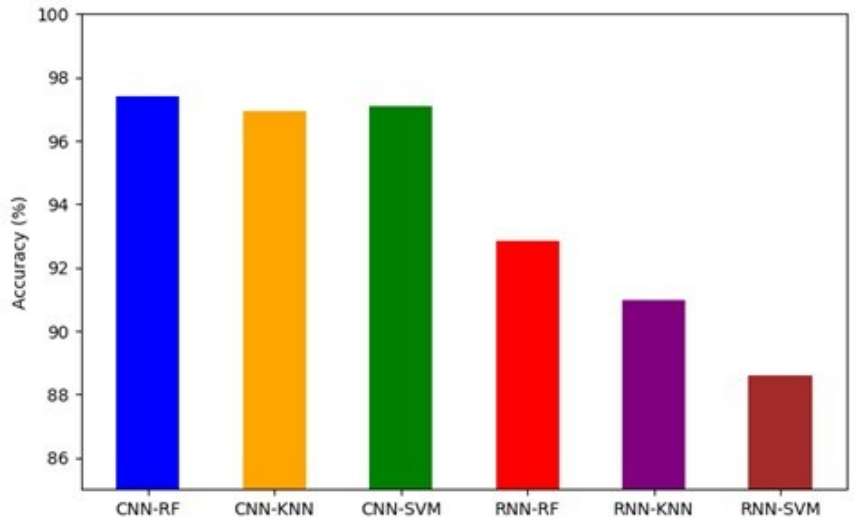

Fig. 4. Hybrid models accuracies for binary classification.

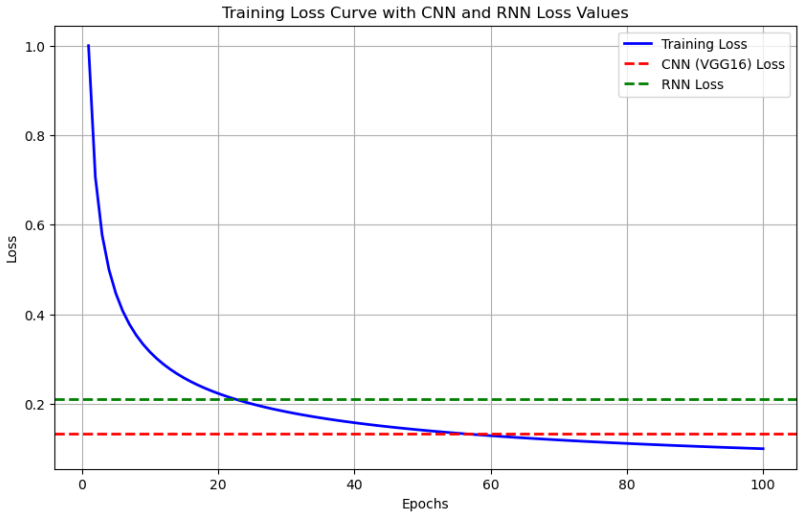

Fig. 5. Loss for deep learning in binary classification.

Further evidence for the effectiveness of the CNN-RF model is presented in Fig. 6, where a confusion matrix with high diagonal dominance and very few misclassified samples can be observed. From these results, one can draw conclusions on the high detection accuracy and reliability of the proposed hybrid approach in distinguishing ransomware from benign files for binary classification.

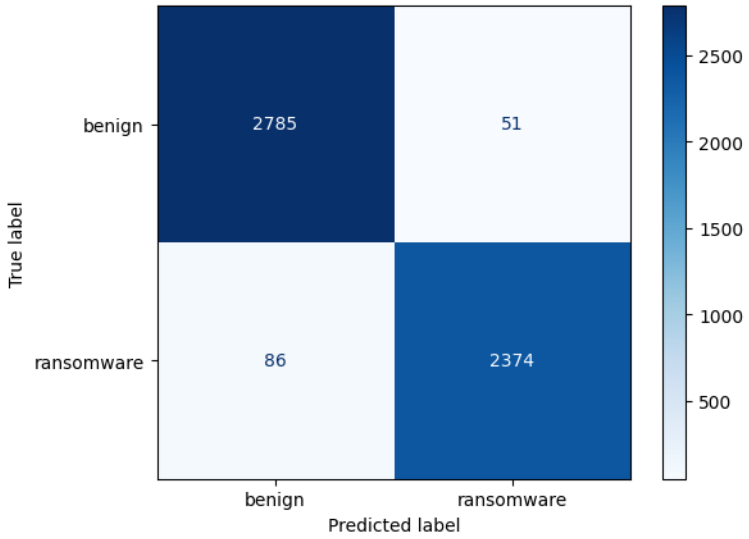

Fig. 6. Confusion matrix for binary classification using the CNN-RF model.

4.2. Multi-Class Classification

In the multi-class classification scenario, the task was extended to classify each ransomware sample by its respective family; therefore, there were eleven classes in total: ten were for ransomware families and one for the benign class. Performance metrics such as precision, recall, and F1-score are presented in Tables 3 and 4. Figures 7 to 10 present the comparative model accuracies. CNN led among individual models with an average F1-score of 95%, outperforming all traditional machine learning algorithms. RF did very well with particular families, like BetterSurf and Obfuscator.AFQ, with an F1 score greater than 90%, while the performance decreased whenever dealing with the more complex classes like Occamy, C, and Zbot. SVM also gave similar behavior, maintaining good performance for well-structured classes but facing difficulties with harder-to-classify ransomware variants. The RNN model exhibited inconsistent performance; it showed very good classification for Sfone and VB.IL and poorer accuracy in the case of Reveton.A and Zbot, making this classifier less reliable in general.

Hybrid models certainly improved with consistency for nearly all the families, validating their efficiency in generalization. In Figs. 7 and 8, the CNN-RF hybrid once again proved to have the best overall accuracy of 94.32%, which is stated by its strong F1-scores and balanced class-level performance.

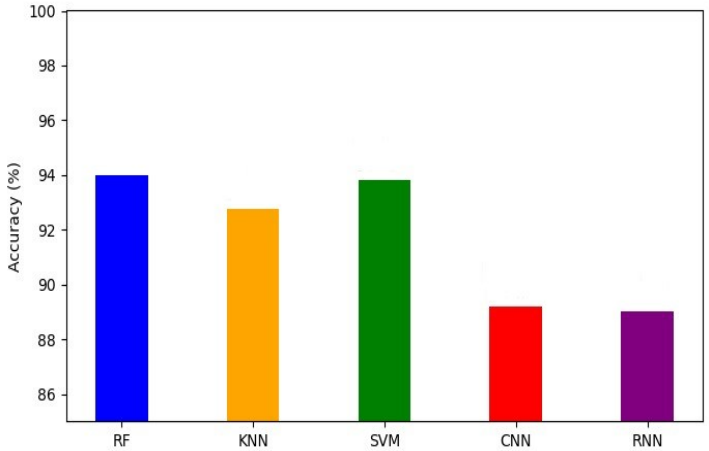

Fig. 7. Multi-class classification accuracy of models.

It effectively modeled variation in texture patterns and prevented inter-class confusion, as was also confirmed by the Confusion Matrix (Fig. 10) showing sharp separation between ransomware families. Other hybrids like CNN-KNN and RNN-RF also showed improvements over their base models, though performances varied on family complexity.

Table 3. Multi-classification performance of models.

Class	Metric	RF	KNN	SVM	CNN	RNN
BetterSurf	Precision	83	82	84	99	1.0
	Recall	99	98	1.0	1.0	1.0
	F1-score	90	89	91	99	1.0
Eksor.A	Precision	1.0	1.0	1.0	81	96
	Recall	1.0	1.0	1.0	84	90
	F1-score	1.0	1.0	1.0	83	93
Obfuscator.AFQ	Precision	1.0	97	94	98	1.0
	Recall	99	98	99	1.0	1.0
	F1-score	99	97	96	99	1.0
Occamy.C	Precision	79	41	49	58	52
	Recall	15	16	26	82	57
	F1-score	25	23	34	68	55
OnLineGames.CTB	Precision	97	94	93	74	72
	Recall	91	93	94	56	60
	F1-score	94	94	94	50	15
Reveton.A	Precision	83	75	84	50	1.0
	Recall	94	91	93	0	78
	F1-score	88	82	88	0.01	66
Sfone	Precision	1.0	1.0	1.0	1.0	1.0
	Recall	1.0	1.0	1.0	1.0	1.0
	F1-score	1.0	1.0	1.0	1.0	1.0
VB.IL	Precision	1.0	1.0	1.0	77	99
	Recall	1.0	1.0	1.0	96	87
	F1-score	1.0	1.0	1.0	85	92
Zbot	Precision	94	66	62	60	77
	Recall	61	51	56	66	66
	F1-score	74	57	59	30	40
ZbotICI	Precision	96	71	74	96	90
	Recall	55	58	67	94	96
	F1-score	70	64	70	95	93
benign	Precision	95	97	98	81	78
	Recall	99	97	97	98	97
	F1-score	97	97	98	89	86

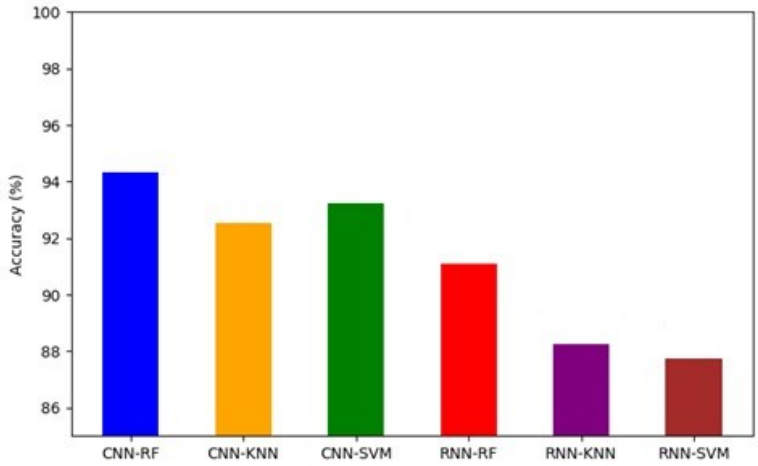

Fig 8: Multi-class classification accuracy of hybrid models.

Table 4. Multi classification performance of hybrid models.

Class	Metric	CNN-RF	CNN-KNN	CNN-SVM	RNN-RF	RNN-KNN	RNN-SVM
BetterSurf	Precision	84	83	83	83	80	79
	Recall	99	96	98	89	96	97
	F1-score	91	89	90	86	87	87
Eksor.A	Precision	1.0	1.0	1.0	1.0	1.0	1.0
	Recall	1.0	1.0	1.0	1.0	1.0	1.0
	F1-score	1.0	1.0	1.0	1.0	1.0	1.0
Obfuscator.AFQ	Precision	1.0	92	96	96	85	94
	Recall	98	99	99	96	94	87
	F1-score	99	95	98	96	89	90
Occamy.C	Precision	88	51	71	47	53	1.0
	Recall	19	19	66	55	60	45
	F1-score	31	28	33	32	53	60
OnLineGames.CTB	Precision	99	93	97	97	92	98
	Recall	94	96	97	90	90	88
	F1-score	96	95	97	93	91	93
Reveton.A	Precision	81	75	72	76	58	55
	Recall	92	86	89	64	61	41
	F1-score	86	80	79	70	59	47
Sfone	Precision	1.0	1.0	1.0	1.0	1.0	1.0
	Recall	1.0	1.0	1.0	1.0	1.0	1.0
	F1-score	1.0	1.0	1.0	1.0	1.0	1.0
VB.IL	Precision	1.0	99	1.0	1.0	1.0	1.0
	Recall	1.0	1.0	1.0	1.0	1.0	1.0
	F1-score	1.0	1.0	1.0	1.0	1.0	1.0
Zbot	Precision	98	58	69	91	60	85
	Recall	65	61	56	55	54	46
	F1-score	78	59	61	68	57	74
Zbot!CI	Precision	88	63	66	86	36	1.0
	Recall	56	56	46	61	34	55
	F1-score	68	60	54	56	35	66
Benign	Precision	95	97	97	92	93	87
	Recall	99	97	97	98	98	92
	F1-score	97	97	97	98	98	95

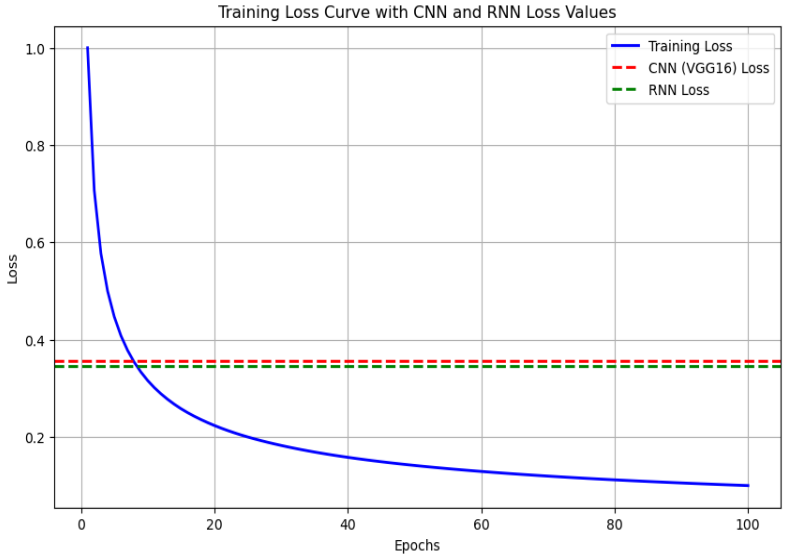

Fig. 9. Deep learning modes loss for multi classification.

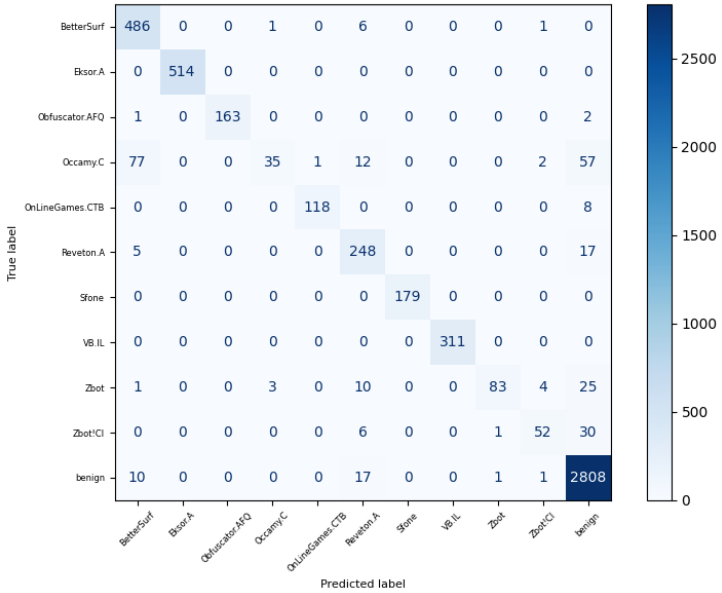

Fig. 10. Confusion matrix for multi-classification using the CNN-RF model.

The ROC curves of the hybrid models show in Fig. 11, for each of them, the balance between the TPR and FPR. A higher curve reflects greater discrimination capability. In the binary classification scenario, the CNN-RF model had the highest AUC value (AUC = 0.9739) among the models and hence was able to distinguish very well between ransomware and benign with very minimal false alarms. While the CNN-SVM and RNN-RF hybrids were competitive, they were slightly less sensitive for higher false positive regions. In a multi-class classification, as seen in the right plot, the CNN-RF model significantly outperformed other models again, reaching an AUC of 0.9432, confirming its robustness in differentiating between a multitude of ransomware families. The smooth curvature near the top-left corner of the graph reflects superior generalization and stable learning of diverse ransomware patterns. Overall, both binary and multi-class experiments showed that hybrid models show a significant boost to performance in ransomware detection, especially for CNN-RF. This synergy boosts generalization due to deep spatial feature extraction and robust ensemble classification, reducing false positives while reliably detecting diverse categories of ransomware.

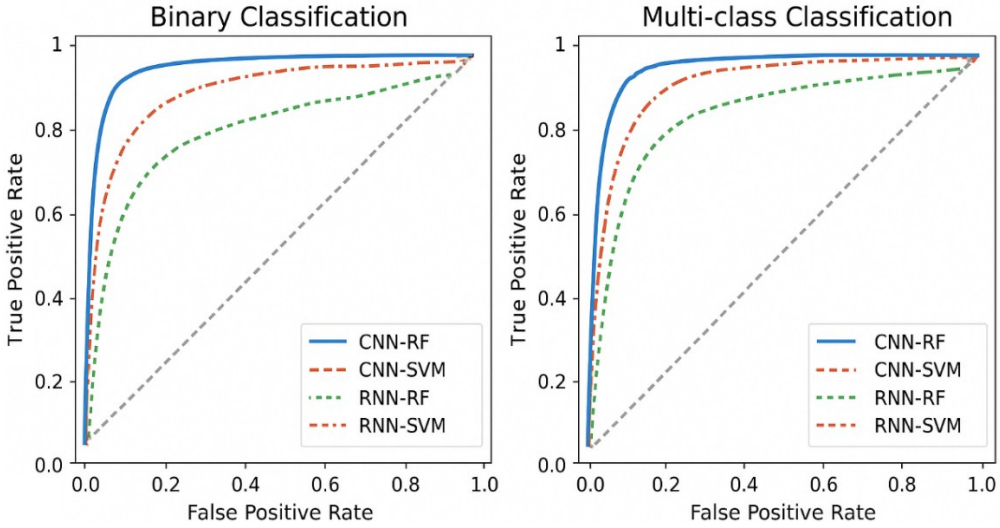

Fig. 11. ROC or hybrid models in binary and multi-class classification.

5. CONCLUSIONSS

The proposed study aimed at developing a comprehensive hybrid approach for the detection of ransomware by combining the extraction of deep features with the aid of CNN and RNN, and the usage of machine learning classifiers such as RF, SVM, and KNN. The study proved the efficiency of the proposed method as the obtained accuracy, precision, recall, and F1-score were high for the binary and multiple classes. The study has several limitations, which may be pointed out as: the first limitation is that all the models were tested for offline data, and hence, it is yet to be proved how accurate the models will be in real-time; the second limitation may be stated as the fact that the models were not tested for adversarial attacks or obfuscation, which may also play an important role.

The future scope of the present work involves real-time detection pipelines systems, increasing the increasing the efficiency of adversarial attacks or using an anomaly detection system, and the use of transfer learning for understanding the ability of the system to be applicable for different types of ransomwares. It not only provides practical applicability but also improves the robustness against the rising ransomware threats.

REFERENCES

[1] S. Al-Eidi, O. Darwish, Y. Chen, M. Elkhodr, ''Covert timing channels detection based on image processing using deep learning,'' International Conference on Advanced Information Networking and Applications, 2022, doi: 10.1007/978-3-030-99619-2_51.

[2] O. Darwish S. Al-Eidi, A. Al-Shorman, M. Maabreh, A. Alsobeh, P. Zahariev, ''LinguTimeX a framework for multilingual CTC detection using explainable AI and natural language processing,'' *Computers, Materials & Continua*, vol. 86, no. 1, pp. 1-21, 2026, doi: 10.32604/cmc.2025.068266.

[3] S. Al-Eidi, O. Darwish, Y. Chen, M. Maabreh, Y. Tashtoush, ''A deep learning approach for detecting covert timing channel attacks using sequential data,'' *Cluster Computing*, vol. 27, no. 2, pp. 1655-1665, 2024, doi: 10.1007/s10586-023-04035-5.

[4] S. Al-Eidi, O. Darwish, G. Husari, Y. Chen, M. Elkhodr, ''Convolutional neural network structure to detect and localize CTC using image processing,'' IEEE International IOT, Electronics and Mechatronics Conference, 2022, doi: 10.1109/IEMTRONICS55184.2022.9795734

[5] A. Ahmed, A. Shaahid, F. Alnasser, S. Alfaddagh, S. Binagag, D. Alqahtani, ''Android ransomware detection using supervised machine learning techniques based on traffic analysis,'' *Sensors*, vol. 24, no. 1, p. 189, 2023, doi: 10.3390/s24010189.

[6] S. Anwar, A. Ahad, M. Hussain, I. Shayea, I. Pires, ''Ransomware detection and classification using ensemble learning: a random forest tree approach,'' International Conference on Wireless Networks and Mobile Communications, 2023, doi: 10.1109/WINCOM59760.2023.10323025.

[7] G. Ciaramella, G. Iadarola, F. Martinelli, F. Mercaldo, A. Santone, ''Explainable ransomware detection with deep learning techniques,'' *Journal of Computer Virology and Hacking Techniques*, vol. 20, no. 2, pp. 317-330, 2023, doi: 10.1007/s11416-023-00501-1.

[8] G. Ganfure, C. Wu, Y. Chang, W. Shih, ''Deepware: imaging performance counters with deep learning to detect ransomware,'' *IEEE Transactions on Computers*, vol. 72, no. 3, pp. 600-613, 2022, doi: 10.1109/TC.2022.3173149.

[9] S. Gulmez, A. Kakisim, I. Sogukpinar, ''Analysis of the dynamic features on ransomware detection using deep learning-based methods,'' International Symposium on Digital Forensics and Security, 2023, doi: 10.1109/ISDFS58141.2023.10131862.

[10] G. Gupta, T. Thakur, A. Dey, ''Ransomware detection framework using soft voting-based ensemble learning,'' International Conference on Computational Modelling, Simulation and Optimization, 2023, doi: : 10.1109/ICCMSO59960.2023.00035.

[11] J. Herrera-Silva, M. Hernandez-Alvarez, ''Dynamic feature dataset for ransomware detection using machine learning algorithms,'' *Sensors*, vol. 23, no. 3, p. 1053, 2023, doi: 1424-8220/23/3/1053.

[12] M. Masum, M. Faruk, H. Shahriar, K. Qian, D. Lo, M. Adnan, ''Ransomware classification and detection with machine learning algorithms,'' Annual Computing and Communication Workshop and Conference, 2022, doi: 10.1109/CCWC54503.2022.9720869.

[13] N. Rani, S. Dhavale, ''Leveraging machine learning for ransomware detection,'' *arXiv preprint arXiv:2206.01919,* 2022, doi: 10.48550/arXiv.2206.01919.

[14] N. Rani, S. Dhavale, A. Singh, A., Mehra, ''Survey on machine learning-based ransomware detection,'' Proceedings of the Seventh International Conference on Mathematics and Computing, 2021, doi: 10.1007/978-981-16-6890-6_13.

[15] H. Shwetha, N. Vineeth, G. Asha, ''Deep learning approaches for ransomware detection: Assessing CNN and CNN-LSTM models using class imbalance methods,'' International Conference on Self Sustainable Artificial Intelligence Systems, 2024, doi: 10.1109/ICSSAS64001.2024.10760450.

[16] D. Smith, S. Khorsandroo, K. Roy, ''Machine learning algorithms and frameworks in ransomware detection,'' *IEEE Access*, vol. 10, pp. 117597-117610, 2022, doi: 10.1109/ACCESS.2022.3218779.

[17] A. Vehabovic, H. Zanddizari, N. Ghani, G. Javidi, S. Uluagac, M. Rahouti, E. Bou-Harb, M. Pour, ''Ransomware detection using federated learning with imbalanced datasets,'' IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT, 2023, doi: 10.48550/arXiv.2311.07760.

[18] W. Zanoramy, M. Abdollah, O. Abdollah, S. SMM, ''Ransomware early detection using machine learning approach and pre-encryption boundary identification,'' *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 47, no. 2, pp. 121-137, 2024, doi: 10.37934/araset.47.2.121137.