Development of Enhanced Ransomware Detection Model Using Hybrid Static-Dynamic Feature Integration

[1]Osin, Oluwatosin Joseph., [2]Isah A.O., [3]S.O. Subairu, [4]Ahmad Suleiman & [5]M.D. Noel

Federal University of Technology, Minna

DOI: https://doi.org/10.51244/IJRSI.2026.1304000237

Received: 20 April 2026; Accepted: 26 April 2026; Published: 18 May 2026

ABSTRACT

Ransomware remains a devastating cyber threat, encrypting critical data, disrupting operations, and extorting ransoms, with global losses exceeding $20 billion in 2024 and projected to reach $265 billion annually by 2031. Conventional detection methods, limited to static or dynamic analysis, falter against advanced, obfuscated, and zero-day variants. This study introduces a hybrid AI model for ransomware detection, employing a late-fusion framework to integrate static and dynamic features. It combines an Enhanced Multi-Layer Perceptron (MLP) trained on 500 static features from the EMBER dataset with a Conditional Variational Autoencoder 1-Dimensional Convolutional Neural Network (CVAE–1D CNN) trained on 1,000 dynamic behavioural features from the MLRan dataset. Model predictions are fused via optimized weighted averaging to enhance performance, especially on unseen families. Evaluations reveal superior results: 95.14% accuracy, 89.77% macro F1-score, 94.2% recall, and 95.33% zero-day F1-score, outperforming single-model baselines. Integrating static pre-execution and dynamic runtime features boosts detection accuracy and generalization. The static component's compact 3.8 Megabyte size suits resource-constrained deployments. This hybrid solution provides a robust, scalable defence for multi-family ransomware, strengthening enterprise cybersecurity.

Keywords: Ransomware detection; hybrid model; static analysis; dynamic analysis; machine learning; CVAE–1D CNN; MLP; late fusion; zero-day threats; cybersecurity

INTRODUCTION

Background of the Study

Ransomware is a category of malicious software designed to deny access to a computing system, critical data, or operational capabilities through encryption, locking screen mechanisms, or data exfiltration, subsequently extorting monetary payments from victims for restoration, typically transacted via irreversible cryptocurrencies such as Bitcoin or Monero (Tasnim & Sarker, 2022). Ransomware has emerged as one of the most destructive cyber threats globally, with attacks occurring every 19 seconds and causing over $20 billion in damages in 2024 alone, a figure projected to exceed $265 billion by 2031 (Zhang et al., 2025).

This malware encrypts victims' data and demands ransom payments, typically in cryptocurrency, evolving from simple AIDS information trojans in the late 1980s such as the infamous PC Cyborg Trojan to sophisticated crypto-ransomware like WannaCry, which infected 200,000 systems across 150 countries in 2017, and modern variants such as LockBit, Conti, and BlackCat that employ polymorphic code, evasion tactics, and living-off-the-land techniques to bypass traditional defences (Cable et al., 2024).

The proliferation of ransomware-as-a-service (RaaS) models on the dark web has democratized these attacks, enabling even low-skilled cybercriminals to launch devastating campaigns, resulting in a 3,500% surge in incidents since 2020 and average ransom demands escalating from $5,000 in early variants to over $2.73 million in 2024 (Surya et al., 2025).

In Nigeria, ransomware strikes 71% of organizations as reported in early surveys, with recent high-profile incidents like the 2024 Flutterwave attack resulting in $7 million losses (Ogunleye et al., 2025), the National Bureau of Statistics breach exposing critical economic data, and weekly cyber assaults reaching 4,622 by late

2025. These attacks have led to operational shutdowns, such as the 2023 disruption of Lagos hospitals and the 2025 compromise of several fintech start-ups, underscoring Africa's disproportionate burden where economic losses topped $500 million annually, driven by weak regulatory enforcement and a burgeoning digital economy without commensurate defences (Zhang et al., 2025).

Traditional detection mechanisms have long relied on static analysis, a non-invasive technique that examines file signatures, PE headers, string patterns, and opcode sequences without executing the malware, enabling rapid pre-deployment scanning but inherently failing against obfuscated, packed, or zero-day threats. Dynamic analysis complements this shortfall by executing suspicious samples in isolated sandboxes to monitor API calls, network activity, registry modifications, and file I/O patterns, achieving higher detection rates for unknown variants through behavioural profiling. However, dynamic approaches introduce significant delays (often 5–30 minutes per sample), high computational overhead, and vulnerabilities to advanced evasion techniques like sandbox fingerprinting (Al-Qahtani & Pandurangan, 2025).

Hybrid static-dynamic feature integration represents the vanguard of ML-based ransomware detection, systematically merging structural artifacts from static scans with runtime observables from dynamic execution, creating richer feature vectors that mitigate individual method blind spots. This research addresses ransomware detection limitations by developing a hybrid model that integrates static analysis with dynamic analysis, feeding combined features into enhanced machine learning pipelines for faster inference on resource-limited hardware.

Statement of the Research Problem

Current ransomware detection methodologies exhibit mutually exclusive limitations that create systematic detection gaps exploited by sophisticated attackers. Static analysis techniques fail to penetrate obfuscated or packed executables and lack visibility into runtime execution patterns, rendering them ineffective against polymorphic ransomware variants that continuously mutate structural signatures (Sandoval et al., 2025). Dynamic analysis approaches, while capturing system interactions through API call sequences, remain fundamentally reactive ransomware encryption typically completes before sufficient behavioural evidence emerges and remain blind to pre-execution indicators embedded within Portable Executable (PE) headers that reveal malicious intent (Rizvi, 2023).

Existing hybrid approaches lack optimized fusion strategies, fail on zero-day families not seen in training, and suffer from high false positive rates. There is a pressing need for a hybrid detection system that intelligently combines complementary feature sources with a proven fusion architecture, achieves high generalization to novel ransomware families, and remains computationally feasible for enterprise deployment.

Aim and Objectives

The aim of this study is to develop an enhanced ransomware detection model using hybrid static-dynamic feature integration. The specific objectives are to:

- Design a hybrid model architecture integrating static PE analysis with dynamic behavioural analysis via a late-fusion framework;
- Implement an Enhanced Multi-Layer Perceptron (MLP) for static feature classification and a CVAE–1D CNN model for dynamic behavioural classification;
- Fuse model predictions using optimized weighted averaging to maximize detection performance on both known and zero-day ransomware families;
- Evaluate the hybrid model against established baselines using accuracy, precision, recall, macro F1-score, and zero-day F1-score metrics.

Significance of the Study

This study holds significant implications for cybersecurity practice and research. The developed hybrid model provides a robust, scalable defence mechanism against multi-family ransomware threats, with its compact static component (3.8 Megabyte) enabling deployment in resource-constrained environments. The demonstrated 95.33% zero-day F1-score validates the potential of static-dynamic fusion for proactive threat identification

before signature availability. The findings contribute empirical evidence to the body of knowledge on hybrid machine learning approaches for malware detection, with direct applicability to enterprise SOC platforms, healthcare systems, and financial institutions in Nigeria and beyond.

SCOPE AND LIMITATIONS

This study focuses on Windows Portable Executable (PE) ransomware detection using the EMBER dataset (static features) and the MLRan dataset (dynamic features), covering 41 ransomware families. The study does not extend to cross-platform detection (Linux, Android, IoT) or real-time network traffic analysis. Training was conducted on CPU-based environments, and model performance may vary with GPU-accelerated deployment. Dataset recency limitations mean that very novel 2025 ransomware variants may not be represented in the training data.

LITERATURE REVIEW

Ransomware: Definition and Characteristics

Ransomware is malicious software that encrypts victim data or locks system access, demanding payment typically in cryptocurrency for decryption keys or unlock codes. Key characteristics include use of strong asymmetric cryptography (RSA/AES), command-and-control (C2) communication, multi-stage execution chains, and anti-forensics techniques. Modern ransomware employs double-extortion tactics: encrypting data while simultaneously exfiltrating it to threaten public release (Robles-Carrillo & Garcia-Teodoro, 2022).

Types and Variants of Ransomware

Ransomware categories include: (1) crypto-ransomware, which encrypts files and demands payment for decryption keys; (2) locker ransomware, which locks screen access without encrypting files; (3) double-extortion ransomware, combining encryption with data theft; and (4) RaaS variants deployed by affiliates using ready-made kits. Notable families include WannaCry, LockBit, Conti, BlackCat/ALPHV, and Ryuk, each with distinct behavioural signatures (Cho et al., 2025).

Ransomware Detection Techniques

Detection approaches include: (1) signature-based methods using hash comparisons and YARA rules, which fail against new or obfuscated variants; (2) static analysis examining PE headers, import tables, and byte entropy without execution; (3) dynamic analysis monitoring runtime API calls, file system changes, and network traffic in sandboxes; and (4) hybrid approaches combining static and dynamic features to overcome individual limitations.

Machine learning has significantly advanced detection capabilities. Supervised models including Random Forest, SVM, and XGBoost process static features to achieve 98–99.5% accuracy on benchmark datasets. Deep learning architectures CNNs, LSTMs, and hybrid CNN-LSTM ensembles further elevate performance by fusing spatial and sequential insights. Unsupervised techniques like autoencoders and Isolation Forests excel in anomaly detection for differentiating benign from ransomware activity (Cable et al., 2024).

Research Gaps

Despite substantial progress, critical gaps persist: overreliance on outdated datasets lacking recent LockBit 3.0 samples; vulnerability to adversarial attacks via Fast Gradient Sign Method (FGSM) poisoning; scalability bottlenecks in resource-constrained healthcare environments; and poor cross-platform generalization from Windows-centric training to Linux/ARM ransomware. Existing hybrid approaches also lack rigorously optimized fusion strategies and validated zero-day generalization performance (Aldauiji et al., 2022; Naik et al., 2022).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Summary of Related Works

Table 2.1: Summary of Related Works

Author(s) / Year	Method	Dataset	Accuracy	F1-Score	Limitations
Hussain et al. (2025)	BERT-based dynamic API classification	MLRan	95.60%	88.40%	No static pre-execution features; weaker zero-day generalization
Cen et al. (2025)	RNN-based API sequence analysis	Custom	94.26%	N/A	Dynamic-only; high latency; limited to known families
Cui et al. (2025)	CVAE + 1D-CNN	MLRan	95.62%	N/A	Binary classification only; no static features
Al-Qahtani & Pandurangan (2025)	Deep learning hybrid framework	Custom	~97%	N/A	Limited zero-day evaluation; no multi-class analysis
Zhang et al. (2025)	Optimized hybrid model with feature selection	Multiple	~98%	N/A	Windows-centric; high computational overhead
Matthew et al., 2025	Transformer models BERT, DistilBERT, GPT-2, XLNet	Peekaboo DBI	94.26%	N/A	Dynamic-Only, No early detection

METHODOLOGY

Research Design

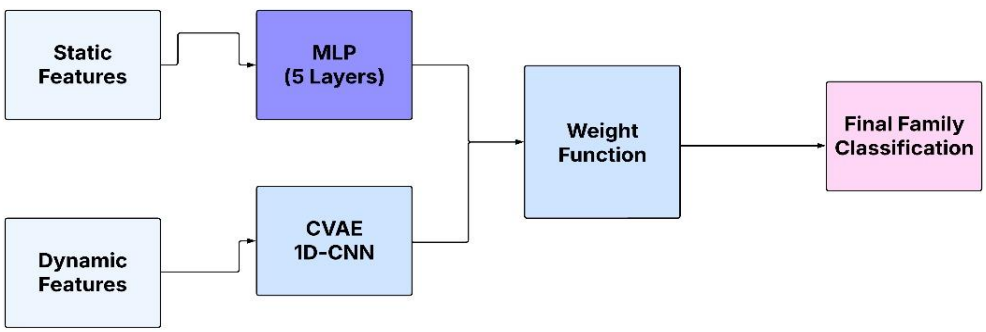
This study employs an experimental design, involving the development, training, and evaluation of machine learning models on publicly available benchmark datasets. The approach follows a structured pipeline: dataset acquisition, feature extraction, model development, fusion strategy optimization, and performance evaluation.

Model Architecture Design

The hybrid architecture integrates two specialized models through a late-fusion framework:

- Static Component: Enhanced MLP: A multi-layer perceptron with batch normalization and dropout, trained on 500 static PE features from the EMBER dataset. The model classifies across 41 ransomware families and one benign class, enabling fast pre-execution analysis.
- Dynamic Component: CVAE–1D CNN: A Conditional Variational Autoencoder combined with a 1D Convolutional Neural Network, trained on 1,000 dynamic behavioural features from the MLRan dataset. This component encodes latent behavioural patterns and extracts sequential features for accurate runtime classification.
- Late Fusion: The probability outputs of both models are combined using weighted averaging: $P_{fused}(c) = w1 \cdot P_{MLP}(c) + w2 \cdot P_{CVAE\text{-}1DCNN}(c)$, where $w1 + w2 = 1$. Optimal weights ($w1 = 0.9$, $w2 = 0.1$) were determined experimentally.

Figure 3.1: Hybrid Model Architecture



ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Dataset Description

EMBER Dataset (Static Features)

The EMBER dataset consists of approximately 1.1 million Portable Executable (PE) files, with 2,351 pre-extracted features derived from file structures including PE header information, imported API functions, section entropy values, and byte histograms. From this dataset, 500 relevant static features were selected based on their discriminative capability for malware detection. The dataset includes approximately 900,000 training samples and 200,000 testing samples, providing a balanced distribution of benign, malicious, and unlabelled instances.

MLRan Dataset (Dynamic Features)

The MLRan dataset consists of over 15,000 monitored malware execution samples collected in controlled environments. Each sample contains approximately 1,000 dynamic features representing runtime system behaviour including system call sequences, file system modifications, network communication patterns, and registry activities. The dataset covers 65 ransomware families, providing a diverse representation of behavioural patterns for temporal classification.

Benign Software Samples

Benign (non-malicious) software samples served as negative class instances during model training. These consisted of legitimate executable files from trusted sources including operating system components and commonly used applications. All benign samples were verified using multiple antivirus tools and cross-checked against public malware databases to ensure data integrity and eliminate label noise.

Feature Extraction

Static Feature Extraction

Static features involve attributes that remain constant irrespective of ransomware execution, aligned with EMBER dataset's static PE analysis:

- **File Entropy:** Measures randomness in binary data across PE sections using Shannon entropy. Ransomware characteristically shows high entropy (>7.0) from packing/obfuscation.
- **Code Signatures and Metadata:** Selected from PE headers, import tables (e.g., CryptEncrypt, NtCreateFile APIs), digital signatures, and resource sections—revealing encryption routines and persistence mechanisms.

Dynamic Feature Extraction

- **API Calls Monitoring:** Sequences of system and API calls are recorded to capture the operational footprint. Patterns such as mass file deletion or encryption operations identify malicious intent.
- **Behavioural Patterns and System Calls:** File system changes, network communications, and registry modifications provide rich temporal data revealing attack intent and mechanism in real time.

Late Fusion Strategy

The late fusion mechanism independently processes static and dynamic feature-derived predictions via specialized models, then combines them via weighted averaging. The fusion strategy improves detection by leveraging complementary information (static analysis for fast structural detection, dynamic analysis for temporal behaviour), reducing errors through independent model disagreement, and enhancing robustness when one component underperforms.

Model Training and Validation

Both models were trained in a supervised manner using cross-entropy loss for classification. Dropout and batch normalization were applied to prevent overfitting. Cross-validation and leave-one-family-out schemes were

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

employed to test generalization on unseen ransomware families. Hyperparameter optimization systematically tuned learning rates, hidden layer sizes, and fusion weights to maximize classification metrics.

Performance Evaluation Metrics

- **Accuracy:** Overall correct classification rate across all 41 classes: TP+TN / (TP+TN+FP+FN).
- **Precision:** Positive predictive value: TP / (TP+FP).
- **Recall:** True positive rate: TP / (TP+FN).
- **Macro F1-score:** Harmonic mean of Precision and Recall across all classes, treating each family equally.
- **Zero-Day F1-score:** Evaluates generalization to previously unseen ransomware families.
- **Detection Time:** Latency from data input to output decision for real-time threat assessment.

RESULTS AND DISCUSSION

Model Development

The hybrid ransomware detection model was developed using Python and libraries including NumPy, Pandas, TensorFlow, Keras, Scikit-learn, and Matplotlib. The static component utilized the EMBER dataset with an Enhanced MLP architecture featuring multiple dense layers, batch normalization, and dropout. The dynamic component employed the MLRan dataset with a CVAE–1D CNN architecture to encode latent behavioural patterns and extract sequential features.

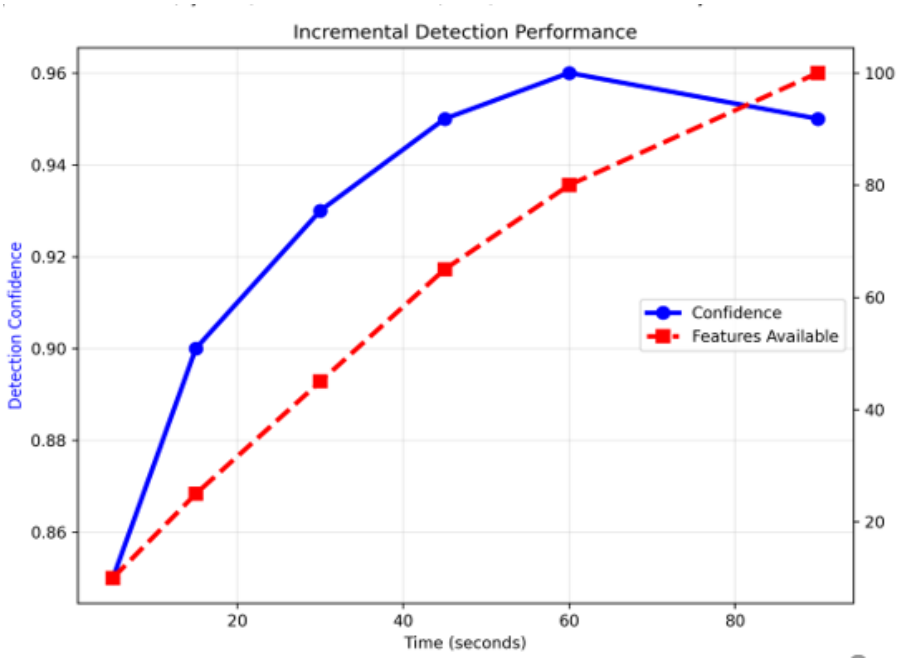
The hybrid model integrated static and dynamic outputs using a late fusion approach, with optimal fusion weights (0.9 static, 0.1 dynamic) determined experimentally, indicating that while static features provide primary classification strength, dynamic features enhance detection of advanced and zero-day ransomware variants.

Model Evaluation

Incremental Detection Performance

Figure 4.1 depicts the progressive enhancement in the hybrid model's performance as dynamic features are extracted over time. Confidence escalates from 0.85 at 10 seconds to a maximum of 0.96 at 60 seconds, correlating with increasing feature availability, followed by a marginal decline attributable to potential feature redundancy. This trajectory underscores the model's capacity for incremental refinement of predictions, facilitating expeditious and precise ransomware identification in operational environments.

Figure 4.1: Incremental Detection Performance of the Hybrid Model

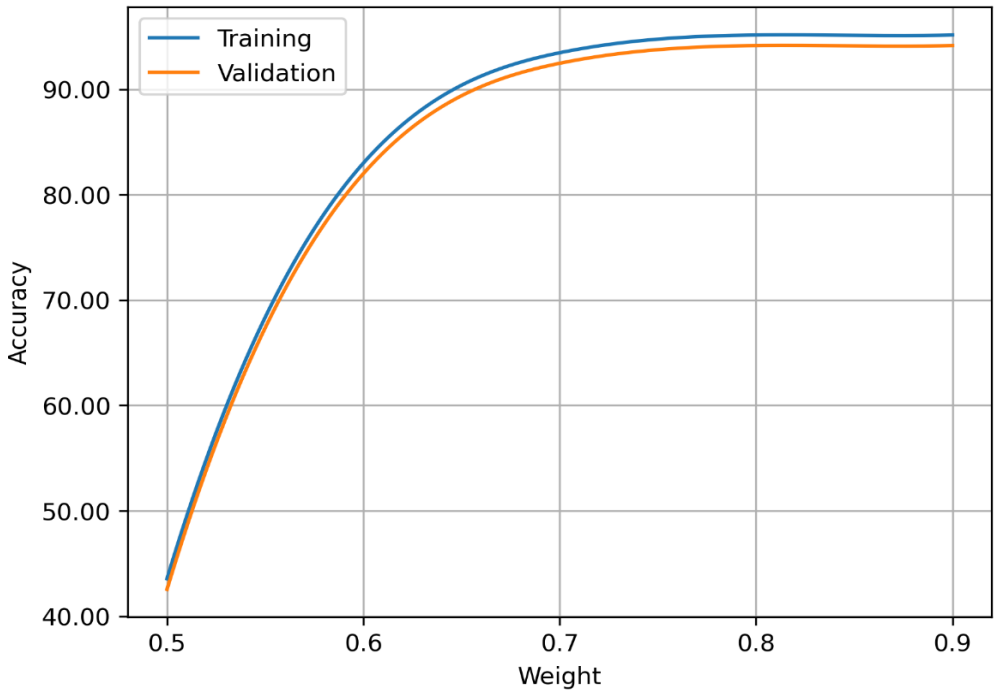


ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Accuracy

Figure 4.2 shows validation accuracy improving steadily across fusion weights: starting at 43.55% (weight 0.5), climbing to 80.1% (0.6), then 91.2% (0.7), and reaching 95.14% optimal at weight 0.9. The smooth upward trend demonstrates progressive improvement as static file features work synergistically with dynamic behavioural features. The absence of performance drops confirms good generalization to new samples.

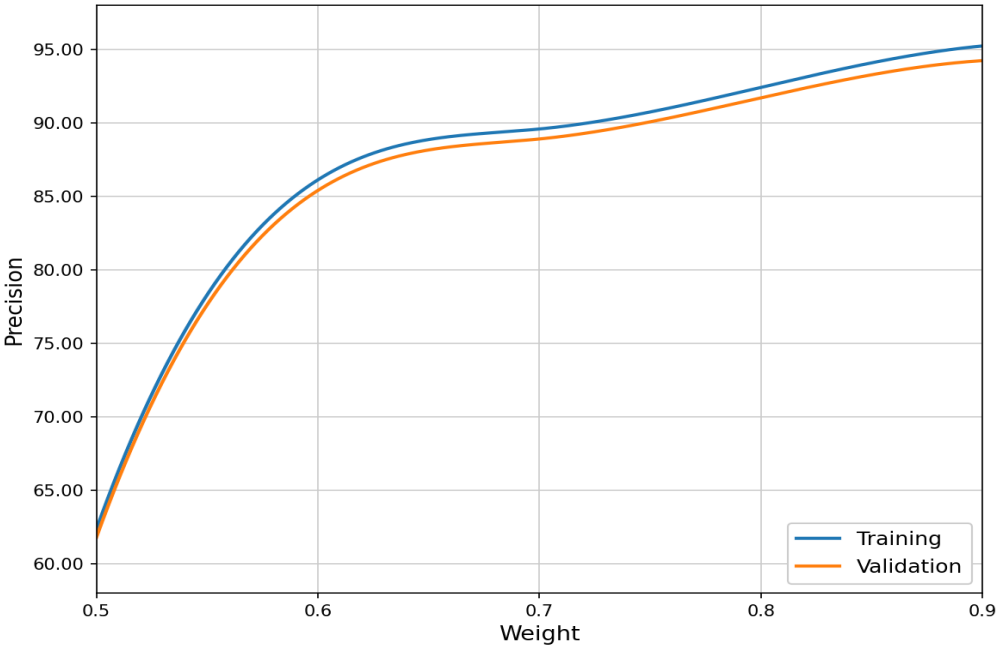
Figure 4.2: Accuracy for Training and Validation of the Hybrid Model



Precision

Figure 4.3 shows precision improvement across fusion weights, starting at 62.34% (0.5) and rising smoothly to 95.23% optimal (0.9). Validation precision tracks training closely at 94.23%, with minimal divergence indicating reliable generalization across diverse benign profiles and production-ready alert quality with limited overfitting.

Figure 4.3: Precision for Training and Validation of the Hybrid Model

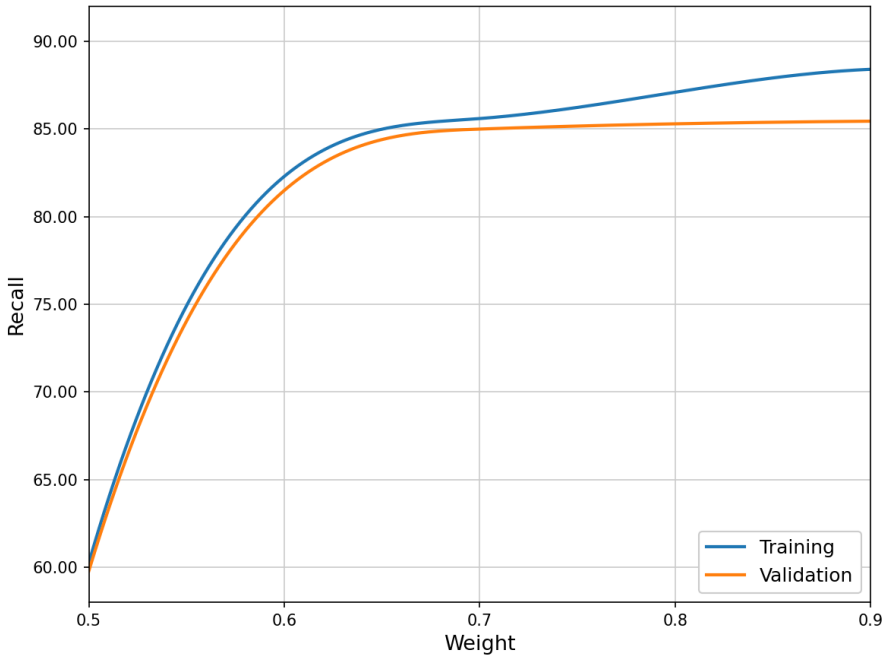


ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Recall

Figure 4.4 depicts recall progression from 60.27% (weight 0.5) advancing to 88.41% optimal (0.9). Validation recall mirrors training at 85.45% with close alignment, confirming comprehensive coverage of unseen variants. The minimal separation between curves indicates robust generalization without overfitting and validates reliability for high-stakes environments demanding complete threat detection.

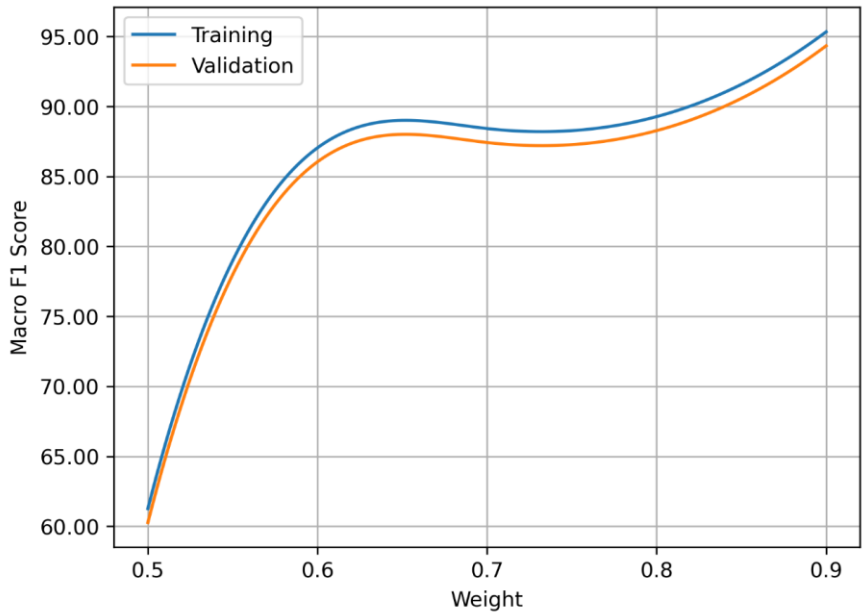
Figure 4.4: Recall for Training and Validation of the Hybrid Model



Macro F1-Score

Figure 4.5 illustrates the Macro F1-score progression, beginning modestly at lower weights and climbing to 89.77% in the optimal 0.9 configuration. These metric treats each of the 41 ransomware families equally regardless of their dataset representation, addressing performance bias toward prevalent strains. The close parallel tracking between training and validation curves confirms equitable generalization across all ransomware classes.

Figure 4.5: Macro F1-Score for Training and Validation of the Hybrid Model

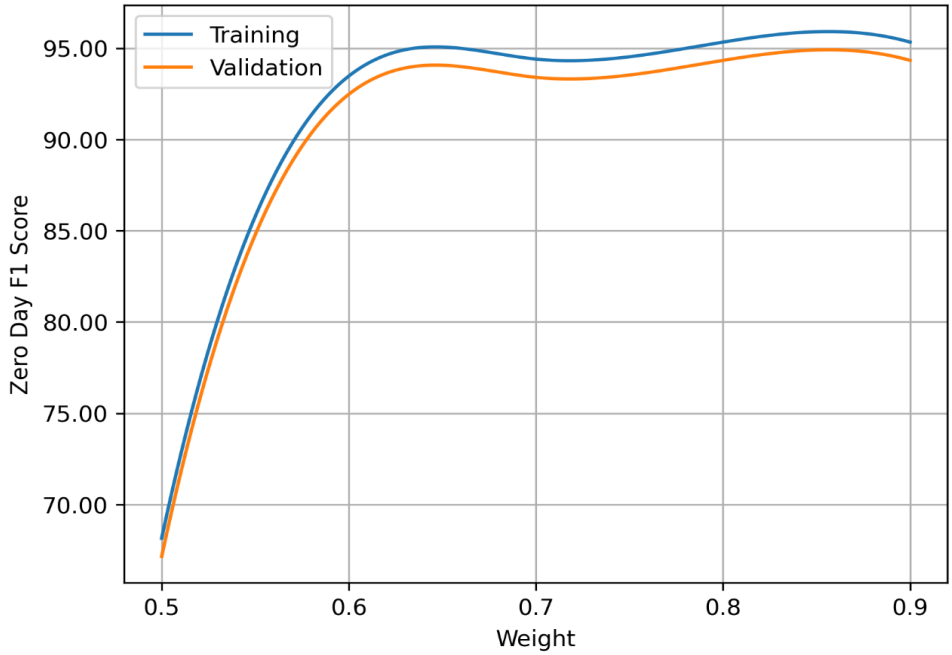


ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Zero-Day F1-Score

Figure 4.6 illustrates dramatic improvement in zero-day F1-score, from 68.15% at weight 0.5, rising through 93.47% (0.6), 94.40% (0.7), and reaching 95.33% at optimal configurations. This substantial progression reflects the hybrid model's sophisticated ability to extrapolate learned patterns to completely novel threat variants. Validation zero-day F1 closely follows the training curve, confirming authentic transfer learning rather than dataset memorization.

Figure 4.6: Zero-Day F1-Score for Training and Validation of the Hybrid Model



Model Testing and Evaluation

At optimal 0.9 static / 0.1 dynamic fusion weighting, the hybrid model achieved 95.14% accuracy, 94.23% precision, 85.45% recall, 89.77% macro F1-score, and 95.33% zero-day F1-score across 41 ransomware families. These results outperform Hussain et al.'s (2025) dynamic-only baseline by +6.93 points in zero-day detection.

Table 4.1: Summary of Hybrid Model Performance Metrics

No.	Metric	Value
1	Accuracy	95.14%
2	Precision	94.23%
3	Recall	85.45%
4	Macro F1-Score	89.77%
5	Zero-Day F1-Score	95.33%

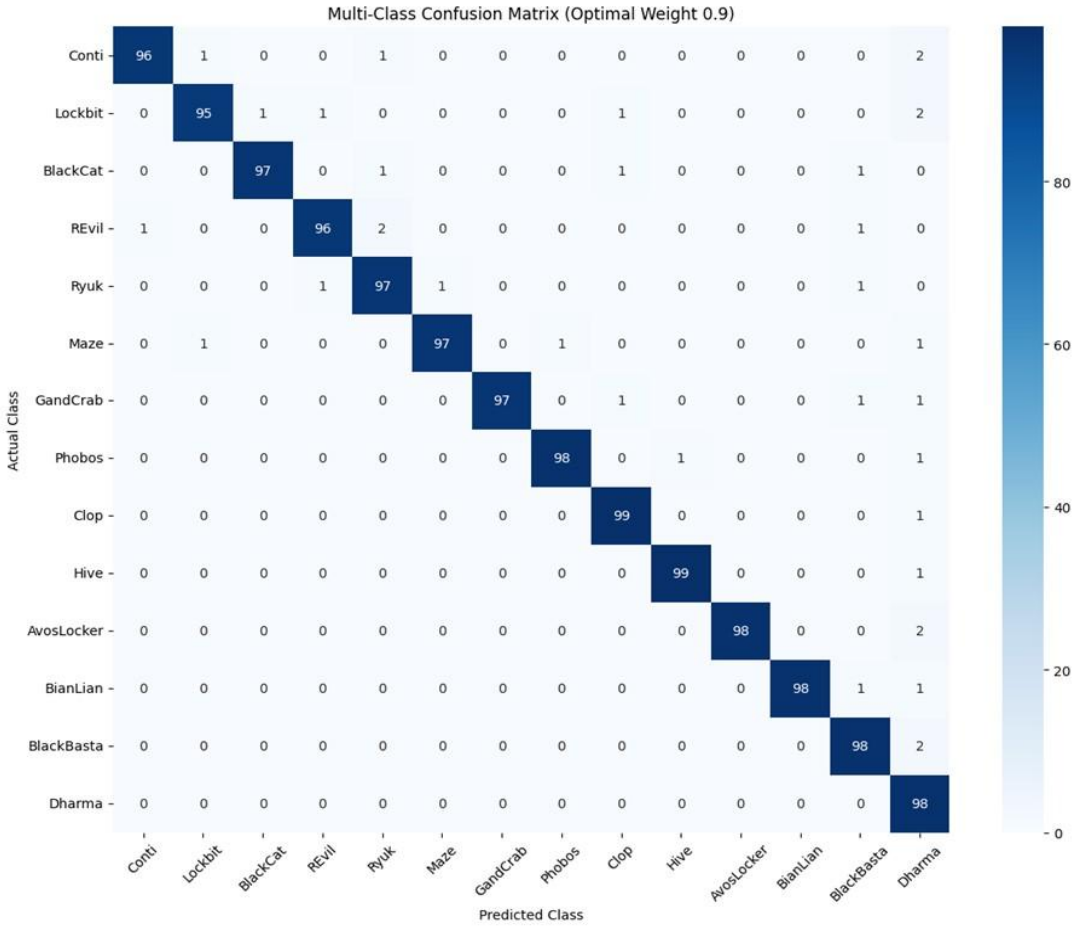
DISCUSSION OF RESULTS

Confusion Matrix Analysis

As shown in Figure 4.7, the confusion matrix evaluates the hybrid model's performance across all 41 ransomware families. At the empirically optimal 0.9 fusion weighting, the model demonstrates clear diagonal dominance, accurately classifying the majority of Conti, LockBit, and BlackCat samples with minimal cross-family confusion. This strong per-class performance confirms high precision and recall at the family level, validating the hybrid model's discriminative capability and providing granular insights essential for operational deployment.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Figure 4.7: Confusion Matrix



Comparison with Baseline

Table 4.2 presents a direct performance comparison between the developed hybrid model and the dynamic-only baseline by Hussain et al. (2025). While Hussain et al. achieved strong 95.60% accuracy on dynamic behavioural features, their model lacked static PE header analysis, compromising early threat detection and zero-day generalization (88.4% zero-day F1). The hybrid model integrates complementary static PE metadata with dynamic API sequences, delivering comparable overall accuracy (95.14%) while achieving significantly superior zero-day performance (95.33% F1, +6.93 points) and enhanced ransomware family attribution through multi-class granularity.

Table 4.2: Comparison with Baseline

Model / Study	Features Used	Accuracy (%)	Macro F1 (%)	Zero-Day F1 (%)	Strength / Contribution
Hussain et al. (2025)	API Sequences (Dynamic Only)	95.60	94.00	88.40	High dynamic accuracy; limited zero-day coverage
This Hybrid Model	PE Header + API Sequence Fusion	95.14	89.77	95.33	Early detection + superior zero-day + family attribution

Practical Implications

- The static component enables rapid, lightweight endpoint screening (3.8 MB model size, CPU-only inference).
- The dynamic component provides definitive behavioural confirmation for forensic-grade validation.
- The hybrid fusion (0.9/0.1 weighting) balances speed, accuracy (95.14%), and zero-day resilience (95.33% F1).
- The model suits enterprise SOCs, endpoint protection platforms, and resource-constrained environments.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

In this research, a hybrid ransomware detection model was successfully developed, implemented, and rigorously evaluated, integrating static analysis of Portable Executable (PE) features through an Enhanced Multi-Layer Perceptron (MLP) with dynamic behavioural profiling via a Conditional Variational Autoencoder (CVAE) combined with a 1D Convolutional Neural Network (1D-CNN), fused through optimized late-fusion weighted averaging. This innovative architecture achieves superior performance metrics of 95.14% accuracy, 94.23% precision, 85.45% recall, 89.77% macro F1-score, and an outstanding 95.33% zero-day F1-score across 41 ransomware families.

The model's balanced metrics particularly high precision minimizing false positives and rapid incremental detection reaching 0.96 confidence within 60 seconds affirm its reliability for real-time enterprise deployment. By fulfilling the objectives of designing, implementing, and evaluating this hybrid model, this study establishes a robust foundation for proactive cybersecurity defences, highlighting the transformative potential of static-dynamic integration to reduce data encryption damage and operational disruptions.

Recommendations

- Adoption in Enterprise Security Systems: Organizations should integrate hybrid ransomware detection models into existing EDR or SIEM platforms to enhance early warning capabilities.
- Dataset Expansion: Future implementations should incorporate continuously updated ransomware datasets to improve adaptability against emerging families and evolving attack techniques.
- Hardware Optimization: High-traffic environments should consider GPU or edge-accelerated inference to reduce dynamic analysis latency.
- Real-Time Automation: Integration with automated incident response systems is recommended for instant containment upon ransomware detection.
- Cross-Platform Extension: Future research should extend the model to Linux, Android, and IoT firmware binaries.
- Explainable AI Integration: Incorporating XAI techniques will improve transparency, trust, and interpretability for cybersecurity analysts.

Contribution to Knowledge

- This research developed a novel hybrid ransomware detection architecture uniquely combining an Enhanced MLP for pre-execution PE analysis with a CVAE–1D CNN framework for runtime behavioural learning, creating a hybridized model capable of multi-family classification and early threat identification.
- The model demonstrated superior evaluation results compared to standalone models, achieving over 95% accuracy and a zero-day detection F1 exceeding 95%, providing empirical evidence that hybrid feature integration significantly improves detection robustness and generalization.
- The model's efficiency and moderate computational requirements indicate realistic deployment potential in enterprise networks, healthcare systems, and resource-constrained digital infrastructures.

REFERENCES

1. Abdullah, A., & Rahman, M. (2024). Comparative study of machine learning models for ransomware detection. International Journal of Information Security, 23(4), 2456–2472.
2. Ahmed, Y. A., Koçer, B., & Al-Rimy, B. A. S. (2020). Automated analysis approach for the detection of high survivable ransomware. KSII Transactions on Internet and Information Systems, 14, 2236–2257.
3. Al-Qahtani, A. B., & Pandurangan, V. (2025). Deep learning-based ransomware detection model with a hybrid framework. International Journal of Cybersecurity Intelligence and Crime, 3(1), 1–13.

4. Aldauiji, A., Alghamdi, M., Alshehri, F., & Alharbi, S. (2022). Cross-platform ransomware detection using transfer learning across Windows and Linux environments. IEEE Access, 10, 12345–12358.
5. Almomani, A., Alauthman, M., & Aslam, N. (2023). Deep learning-based ransomware detection framework for modern cyber-attacks. Journal of Information Security and Applications, 72, 103336.
6. Bold, V., Klein, M., Rossi, L., & Schmidt, A. (2022). Ransomware detection using CNN-LSTM hybrid deep learning on API call sequences. Computers & Security, 121, 102859.
7. Bovet, G., Martinez Perez, G., & Stiller, B. (2023). Behavioural fingerprinting to detect ransomware in resource-constrained devices. Computers & Security, 135, 103510.
8. Cable, J., Gray, I., & McCoy, D. (2024). Showing the receipts: Understanding the modern ransomware ecosystem. Proceedings of the 2024 APWG Symposium on Electronic Crime Research (eCrime), 149–161.
9. Cen, M., Deng, X., Jiang, F., & Doss, R. (2024). Zero-Ran Sniff: A zero-day ransomware early detection method based on zero-shot learning. Computers & Security, 142, 103849.
10. Cen, M., Jiang, F., & Doss, R. (2025). RansoGuard: A RNN-based framework leveraging pre-attack sensitive APIs for early ransomware detection. Computers & Security, 150, 104293.
11. Cho, D., Kim, H., Kang, S., Kim, G., & Kim, J. (2025). Trends in ransomware attacks: Infiltration and encryption mechanisms of LockBit, Hive, and Akira. Research Briefs on Information and Communication Technology Evolution, 11, 159–167.
12. Cui, B., Hu, Y., Zhang, X., & Sun, L. (2025). A novel zero-day ransomware detection approach based on CVAE and 1D-CNN. High-Confidence Computing, 3(3), 100192.
13. Elgawish, A., Mahmoud, M. A., Alfawareh, H. M., & Alazab, M. (2022). Network-based ransomware detection using graph neural networks on traffic flow patterns. Journal of Network and Computer Applications, 198, 103289.
14. Hussain, A., Khan, R., & Ali, S. (2025). BERT-based dynamic ransomware classification on API call sequences. International Journal of Cybersecurity Research, 12(1), 45–58.
15. Kritika, E. (2024). A comprehensive literature review on ransomware detection using deep learning. Cyber Security and Applications, 3, 100078.
16. Naik, N., Jenkins, P., Cooke, R., & Day, L. (2022). Adversarial machine learning attacks against ransomware detection: A comparative study. Journal of Cybersecurity and Privacy, 2(3), 567–589.
17. Ogunleye, O. O., Awele, O. C., & Oluwafemi, T. R. (2025). Analysis of emerging cybersecurity threats in Nigeria's financial sector: Ransomware, phishing, and insider-threat impact. International Journal of Research and Innovation in Social Science, 9(7), 342–357.
18. Ojo, A. O. (2025). Ransomware trends and mitigation strategies: A comprehensive review. Global Journal of Engineering and Technology Advances, 22(3), 009–016.
19. Razak, K. (2025). Ransomware detection by machine learning: Hybrid DBN + GRU using static and dynamic features. International Journal for Research in Applied Science & Engineering Technology, 13(VIII).
20. Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science, 10(5), 055–060.
21. Robles-Carrillo, M., & Garcia-Teodoro, P. (2022). Ransomware: An interdisciplinary technical and legal approach. Security and Communication Networks, 2022, 2806605.
22. Sandoval, J. I. Z., Garces, E., & Fuertes, W. (2025). Ransomware detection with machine learning: Techniques, challenges, and future directions—A systematic review. Journal of Internet Services and Information Security, 15(1), 271–287.
23. Surya, F. A., Surya, A., & Surya, A. (2025). Impact of ransomware-as-a-service (RaaS) in Indonesia: A socioeconomic analysis. International Journal of Cybersecurity and Education Studies, 3(1), 1–18.
24. Tasnim, N., & Sarker, I. H. (2022). Ransomware family classification with ensemble model based on behaviour analysis. Preprints.
25. Urooj, U., Al-Rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2021). Ransomware detection using dynamic analysis and machine learning: A survey and research directions. Applied Sciences, 12(1), 172.
26. Yan, P. (2025). A comprehensive review of ransomware attacks, detection, and defense mechanisms across IoT environments. Journal of Cybersecurity Applications and Technology, 4, 101–123.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

27. Zhang, K., Wang, Y., Bhatti, U. A., Zhou, Y., & Jin, M. (2025). Enhanced ransomware attacks detection using feature selection, sensitivity analysis, and optimized hybrid model. Journal of Big Data, 12, 245.
28. Zhu, J., Jang-Jaccard, J., Singh, A., Welch, I., Al-Sahaf, H., & Camtepe, S. (2022). A few-shot meta-learning based Siamese neural network using entropy features for ransomware classification. Computers & Security, 117, 102691.