International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

Machine Learning for Analysing Malware and Ransomware

A Mani, S Bavanitha, C S Anitha, K Aishwarya and H Vidhya Varsha

Assistant Professor, Department of Physics, Muthayammal Engineering College, Rasipuram, Namakkal, India

UG Student, Department of Computer Science and Engineering, Muthayammal Engineering College, Rasipuram, Namakkal, India

UG Student, Department of Information Technology, Muthayammal Engineering College, Rasipuram, Namakkal, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Malware and ransomware are rapidly evolving, making detection difficult for traditional signature-based security systems that rely on known attack patterns. These systems often fail to identify new or zero-day threats. This research proposes an intelligent machine learning–based detection system that uses supervised models and deep learning techniques to identify malware in real time with high accuracy and low false positives. The system combines static and dynamic feature extraction to analyse file structure and runtime behaviour. It also includes ransomware-specific behavioural analysis. A hybrid adaptive learning technique with feature fusion and incremental model updating helps the system adapt to changing malware patterns, improving detection performance and system security.

KEYWORDS: Machine Learning, Malware Detection, Ransomware Analysis, Supervised Learning, Static Analysis, Dynamic Analysis, Feature Extraction, Adaptive Learning, Zero-Day Attacks

I. INTRODUCTION

Malware and ransomware have become major cybersecurity threats due to their rapid evolution and increasing complexity. Attackers continuously modify malicious code and techniques to bypass traditional security mechanisms and avoid detection. Conventional malware detection systems mainly rely on signature-based approaches, which identify malicious software by comparing files with previously known malware patterns. Although these methods are effective in detecting known threats, they often fail to identify new, modified, or zero-day malware attacks [1]. As a result, traditional detection techniques alone are not sufficient to protect modern computing systems and networks.

To overcome these limitations, researchers have increasingly adopted machine learning and deep learning techniques for malware detection. Machine learning algorithms can analyse large volumes of data and identify patterns associated with malicious activities. These approaches improve detection accuracy and enable the identification of unknown malware variants [2], [3]. Deep learning models further enhance the capability of detection systems by automatically learning complex behavioural patterns from large datasets [4].

Another important aspect of modern malware detection is the use of static and dynamic analysis techniques. Static analysis inspects the internal structure of files without executing them, while dynamic analysis monitors program behaviour during execution in a controlled environment. These techniques help detect suspicious actions such as file encryption, registry changes, and abnormal network communication [5], [6]. By integrating these analysis methods with supervised learning models and adaptive algorithms, detection systems can effectively identify evolving malware and ransomware attacks while reducing false positives and improving overall system security [7][8], [9][10].

II. LITERATURE REVIEW

Traditional signature-based malware detection systems are no longer adequate to combat contemporary cyber threats, particularly zero-day attacks and quickly changing ransomware variants, according to recent research. These systems frequently miss new or obfuscated malware because they rely on well-known attack patterns [30]. In order to get around these restrictions, researchers have been concentrating more on machine learning methods, which can identify threats that have never been seen before and learn patterns from data. Because of their high accuracy, supervised

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

learning models like Random Forests and Support Vector Machines are frequently used for malware classification [31]. Furthermore, deep learning techniques, such as neural networks, have enhanced detection performance by improving the capacity to automatically extract complex features from unprocessed data [32].

Numerous studies also emphasize how crucial it is to combine static and dynamic analysis, with dynamic analysis observing runtime behavior and static analysis looking at file structure, for more accurate detection [33]. Additionally, behavioral analysis tailored to ransomware has been developed to detect early encryption activity and anomalous system modifications [34]. Adaptive learning techniques, like feature fusion and incremental model updating, are also highlighted in recent developments. These techniques enable systems to continuously learn and adapt to new malware patterns, increasing detection accuracy and decreasing false positives over time [35].

III. RESEARCH METHODOLOGY

Limitations of Traditional Malware Detection Techniques:
For many years, traditional malware detection techniques have been widely used to protect computer systems and networks. These methods were effective when cyber threats were relatively simple and predictable. However, with the rapid growth of malware and ransomware, attackers now use more advanced techniques that expose the weaknesses of conventional detection approaches. As a result, traditional methods are no longer sufficient to handle modern and evolving cyber threats [1], [9].

Signature-Based Detection Methods:
Signature-based detection is one of the most widely used techniques in antivirus software. It identifies malicious programs by comparing files with a database of known malware signatures created from previously detected samples. This approach works well for identifying known threats and usually produces fewer false positives. However, it heavily depends on frequent updates to the signature database. Newly developed malware or modified variants that do not match existing signatures can easily bypass detection. Attackers often use techniques such as code obfuscation, packing, and encryption to alter malware structure, making signature-based systems ineffective against emerging threats [3], [6].

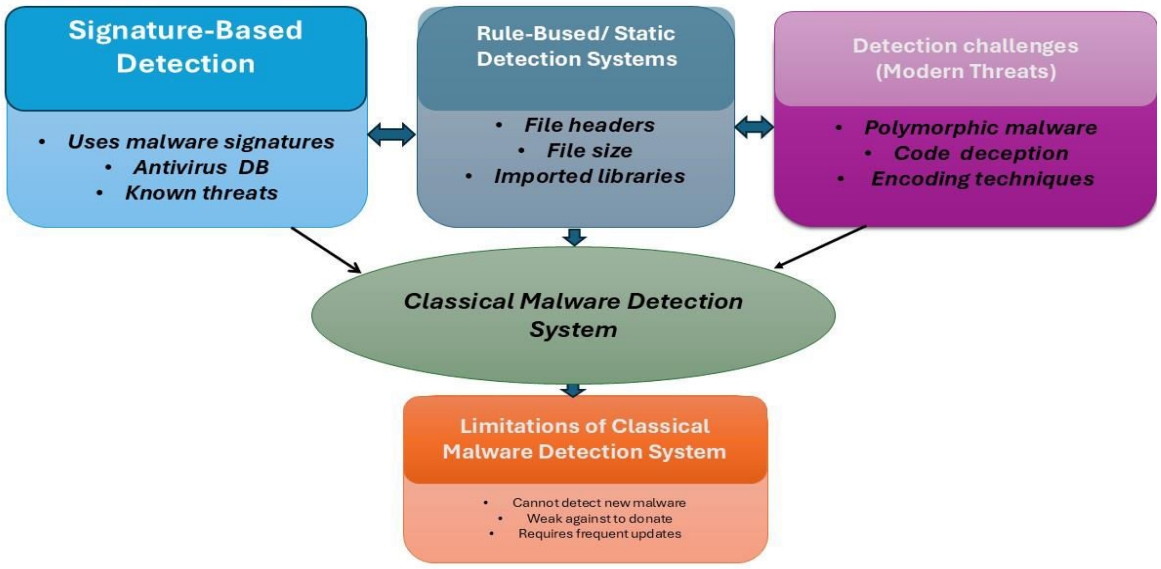

FIG: 1Limitation of Traditional Malware Detection Techniques

Rule-Based and Static Detection Systems:
Rule-based and static detection systems analyse files without executing them by examining features such as file hashes, headers, size, imported libraries, and suspicious instructions. Although this method is fast and safe, it cannot observe the actual runtime behaviour of programs. Modern malware frequently uses evasion techniques such as polymorphism,

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

metamorphism, and delayed execution to bypass static analysis, making these methods less reliable in detecting advanced threats [5], [2].

Challenges in Detecting Zero-Day and Polymorphic Malware:
Zero-day malware exploits unknown software vulnerabilities for which no signatures or predefined rules exist, making detection extremely difficult for traditional systems. Polymorphic malware further complicates detection by constantly changing its code while maintaining the same malicious behaviour. Each variant appears different to signature-based scanners, allowing attackers to evade security mechanisms repeatedly. These limitations highlight the need for more intelligent and adaptive detection methods, such as machine learning-based systems, to effectively defend against evolving cyber threats [8], [10], [24 - 29].

Types of malware:

- ✓ Viruses: Viruses attach themselves to legitimate files and spread when the infected file is executed.

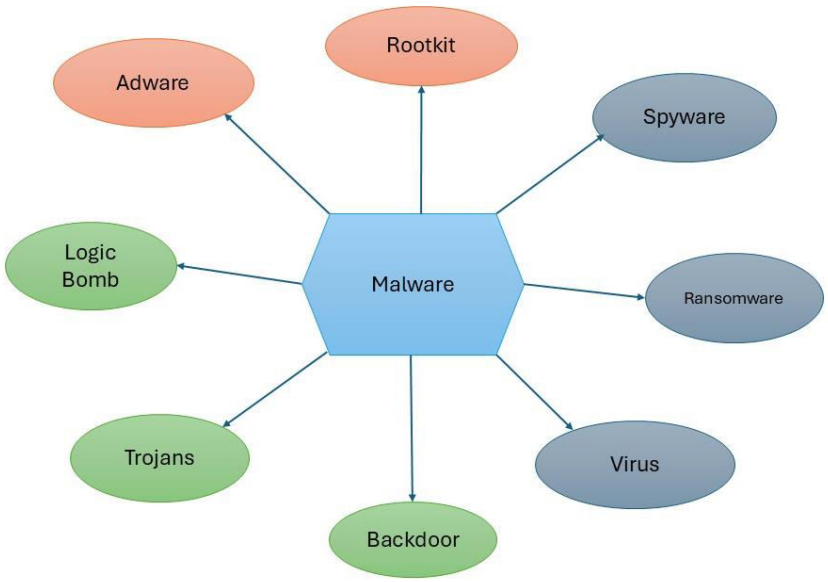

FIG: 2 (Types of Malware)

- ✓ Worms: Worms are self-replicating programs that spread automatically through networks without user interaction.
- ✓ Trojans: Trojans appear as trusted software but secretly perform harmful actions such as opening backdoors.
- ✓ Spyware: Spyware monitors user activities and collects sensitive information like passwords and browsing data.
- ✓ Adware: Adware displays unwanted advertisements and may track user behaviour.
- ✓ Ransomware: Ransomware encrypts files or locks systems and demands payment for recovery.

Ransomware:
Ransomware is one of the most destructive forms of malware designed to block access to data or computer systems and demand payment to restore access. In recent years, ransomware attacks have increased significantly due to their financial motivation, technical sophistication, and ability to cause immediate disruption. Traditional security mechanisms mainly depend on signature-based detection methods that compare files with previously known malware patterns. Although these methods are effective for detecting known threats, they often fail to identify new, modified, or zero-day attacks, making modern systems vulnerable to advanced ransomware variants [1], [3].
Ransomware typically spreads through phishing emails, malicious attachments, compromised websites, or software vulnerabilities. Once executed, it performs several malicious activities such as scanning connected drives, encrypting important files, modifying system settings, and communicating with remote command-and-control servers. Modern

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

ransomware uses strong cryptographic algorithms to encrypt user data, making recovery difficult without a decryption key [6]. To avoid detection, some variants disable security tools, delete backup copies, and hide their activities within legitimate system processes [5]. To overcome these limitations, machine learning and deep learning techniques are increasingly used in modern malware detection systems. These techniques analyse large datasets and automatically identify malicious behaviour patterns. The proposed system integrates both static and dynamic feature extraction methods, where static analysis examines file structure and code characteristics, while dynamic analysis observes runtime behaviour such as abnormal file access, rapid encryption activities, and suspicious network communication [2], [4].

Furthermore, the system incorporates ransomware-specific behavioural analysis and a hybrid adaptive learning approach that combines feature fusion with incremental model updating. This enables the detection model to adapt to evolving malware patterns, improving detection accuracy while reducing false positives. Such intelligent detection frameworks provide a reliable solution for protecting modern computing environments from advanced ransomware threats [8],[7],[10],[9].

IV. RESULTS AND DISCUSSION

Methodology: Machine Learning Tool to Analyse Malware and Ransomware Attacks

Clearly defining the problem is the first step in developing an intelligent malware and ransomware detection system. Malware refers to any malicious software designed to damage systems, steal confidential information, or gain unauthorized access, while ransomware is a specific type of malware that encrypts files or blocks system access to demand ransom payment. In recent years, malware and ransomware have evolved rapidly, using techniques such as polymorphism, code obfuscation, and zero-day exploitation to evade traditional signature-based security systems [1], [6]. These conventional systems rely on previously known attack patterns and therefore struggle to detect newly emerging threats.

To address this limitation, this research proposes an intelligent machine learning–based detection system capable of identifying both known and unknown malware in real time. The system aims to achieve high detection accuracy while minimizing false positives. By using supervised machine learning models and deep learning techniques, the system can automatically learn patterns from large datasets and detect suspicious behaviour. The detection framework combines static and dynamic feature extraction to analyse both file structure and runtime behaviour of programs, enabling more reliable identification of malicious activities [2].

1. Project Implementation Structure:

```
Malware_detection_system
│
├──dataset
│   └malware_dataset.csv
│
├── preprocessing
│   └── data_preprocessing.py
│
├── feature_engineering
│   └── feature_selection.py
│
│
├── models
│   └── train_model.py
│
├── evaluation
│   └── evaluate_model.py
│
├── detection
│   └── malware_detector.py
│
└── app.py
```

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

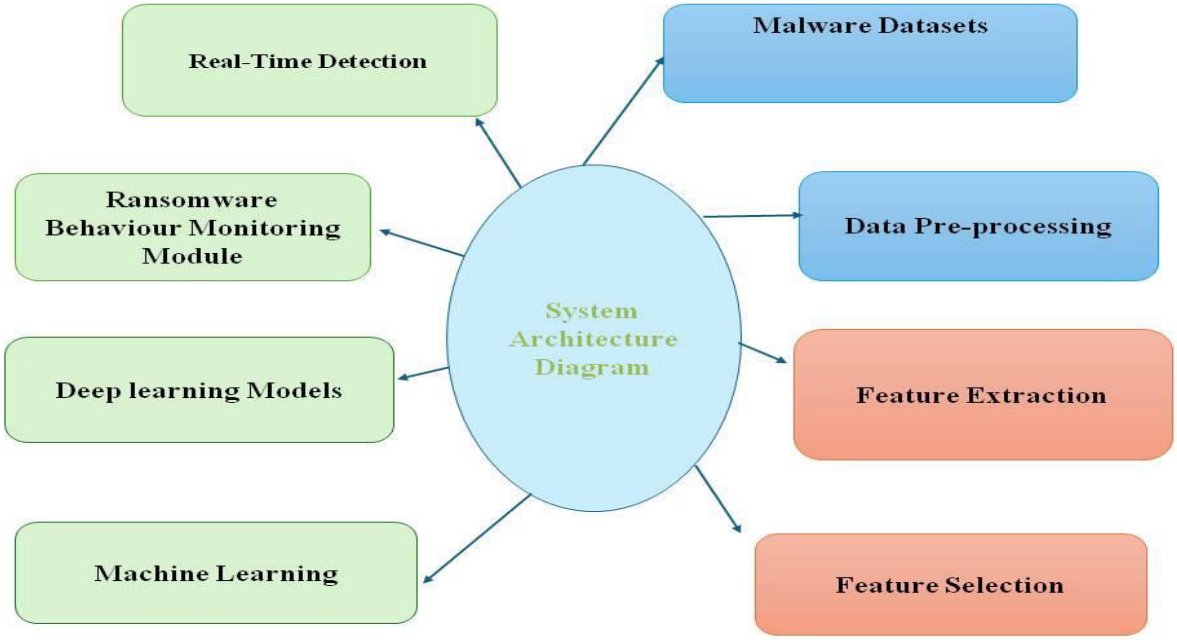

FIG: 3 (System Architecture Diagram)

2. Data Collection and Dataset Preparation

Data collection and preparation form the foundation of an effective machine learning–based malware detection system. The quality, diversity, and reliability of datasets significantly influence model performance and detection accuracy. Malware samples are typically collected from trusted repositories such as VirusShare, VirusTotal, and other research datasets, while benign samples are obtained from legitimate software sources to ensure balanced training data [3].

Data collection can be performed using two approaches: static and dynamic analysis. Static data collection involves gathering executable files without executing them and extracting structural information such as file metadata and headers. Dynamic data collection involves executing malware samples in controlled sandbox environments to observe runtime behaviour such as system calls, registry modifications, file operations, and network communication [5]. Combining both forms of data allows the system to capture a comprehensive representation of malware behaviour.

Dataset Labelling and Preprocessing

After collection, each sample is labelled as malware or benign to support supervised machine learning models. Preprocessing is necessary to improve data quality and prepare features for model training. This includes removing duplicate samples, handling missing values, and normalizing numerical attributes so that all features contribute equally during model learning. Proper preprocessing helps reduce noise, improve generalization, and increase detection accuracy [7].

File:
preprocessing/data_preprocessing.py
Program:

```
import pandas as pd
from sklearn.preprocessing import LabelEncoder
from sklearn.preprocessing import StandardScaler
def load_dataset(path):
    data = pd.read_csv(path)
    return data
def clean_dataset(data):
   # Remove duplicate samples
    data = data.drop_duplicates()
```

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

```
    # Handle missing values
    data = data.fillna(0)
    return data
def encode_labels(data):
    encoder = LabelEncoder()
    data['label'] = encoder.fit_transform(data['label'])
    return data
def normalize_features(data):
    scaler = StandardScaler()
    features = data.drop('label', axis=1)
    scaled = scaler.fit_transform(features)
    scaled_df = pd.DataFrame(scaled, columns=features.columns)
    scaled_df['label'] = data['label']
     return scaled_df
```

Feature Extraction and Selection

Feature extraction transforms raw malware data into meaningful numerical representations that machine learning algorithms can process. Static features include file size, entropy, imported API calls, and PE header attributes, which provide structural information about executable files. Dynamic features capture runtime behaviour such as network communication, file modifications, registry changes, and process activity [8].

To improve model efficiency, feature selection techniques are applied to remove redundant or irrelevant attributes. Selecting the most informative features reduces computational complexity while improving detection accuracy.

File:
feature_engineering/feature_selection.py
Program:

```
from sklearn.feature_selection import SelectKBest
from sklearn.feature_selection import chi2
def select_features(X, y):
   selector = SelectKBest(s
core_func=chi2, k=10)
   X_new = selector.fit_transform(X, y)
   return X_new
```

3. Selection of Detection Approach

Machine learning–based detection methods provide an effective solution for identifying modern malware and ransomware threats. Unlike traditional signature-based approaches, machine learning models learn patterns directly from data and can identify unknown or modified malware variants, including polymorphic and zero-day attacks [4], The proposed system integrates both static and dynamic feature analysis to improve detection accuracy and reliability.

Supervised Machine Learning Models

Supervised learning models are trained using labelled datasets to classify files as benign or malicious. Algorithms such as Decision Trees, Random Forest, Support Vector Machines, and Logistic Regression are commonly used for malware detection. Among these, Random Forest is particularly effective because it can handle high-dimensional feature spaces and provide stable predictions with reduced overfitting [10].

Deep Learning–Based Detection

Deep learning techniques further enhance detection capabilities by automatically learning complex patterns from data. Convolutional Neural Networks (CNNs) can analyse binary structures and identify hidden malware signatures, while Long Short-Term Memory (LSTM) networks analyse sequential behaviour such as system call sequences. These models are especially effective in detecting advanced ransomware behaviour and previously unseen threats [9].

Model Training
File:
models/train_model.py
Program:

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
import joblib
def train_model():
    data = pd.read_csv("dataset/malware_dataset.csv")
    X = data.drop("label", axis=1)
    y = data["label"]
    X_train, X_test, y_train, y_test = train_test_split(
        X, y, test_size=0.2, random_state=42
    )

    model = RandomForestClassifier(
        n_estimators=100,
        max_depth=10
    )

    model.fit(X_train, y_train)

    joblib.dump(model, "models/malware_model.pkl")

    print("Model trained successfully")
if __name__ == "__main__":
    train_model()
```

TESTING ACCURACY:

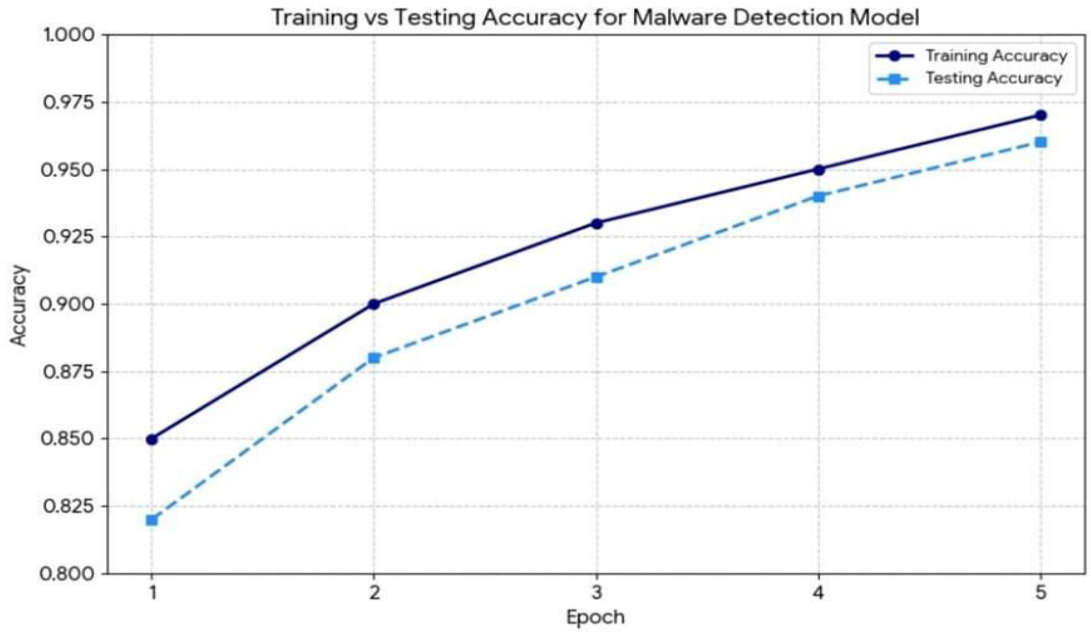

Fig.4 (Training Vs Testing Accuracy)

Common datasets:

Using a variety of datasets is essential for properly training and testing machine learning models, especially in malware detection research. A review of existing studies shows that several datasets are used repeatedly because of their reliability and relevance.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

This study adopts a data-driven machine learning methodology to design and evaluate an intelligent malware and ransomware detection system capable of operating in real-time environments. The proposed methodology integrates dataset selection, feature engineering, supervised and deep learning model training, ransomware-specific behavioural logic, and continuous model adaptation to address the limitations of traditional signature-based detection techniques.

The first phase of the methodology focuses on dataset selection and acquisition. Multiple publicly available and academic datasets are employed to ensure data diversity, authenticity, and coverage of real-world attack scenarios. Malware samples are collected from repositories such as Virus Share and Virus Total, which provide a wide range of known malware families, including ransomware, trojans, worms, and spyware. Dynamic behaviour datasets such as CICAndMal2017 are used to capture runtime activities including system calls, file operations, registry access, and network communication. In addition, benign software samples are collected from trusted operating system files and verified application repositories to reduce classification bias and improve model generalization.

Following data collection, the methodology applies structured data preprocessing and cleaning procedures. Duplicate samples are removed to prevent biased learning and overfitting. Missing or inconsistent feature values are handled using statistical imputation or sample removal techniques. Numerical features are normalized to ensure uniform contribution during model training, and categorical labels are encoded into machine-readable formats. Dataset balancing techniques, including Synthetic Minority Over-sampling Technique (SMOTE), are applied to address class imbalance issues commonly observed in malware datasets.

Feature extraction forms a critical component of the proposed methodology. Static features are extracted without executing the samples and include file size, entropy, cryptographic hash values, PE header attributes, opcode frequencies, imported API calls, and embedded strings. Dynamic features are obtained by executing samples in isolated sandbox environments and capturing behavioural traces such as system calls, file encryption activity, registry modifications, network connections, and command-and-control communication. Feature selection techniques are employed to eliminate redundant and irrelevant attributes, thereby improving computational efficiency and detection accuracy.

The detection framework is built using both supervised machine learning and deep learning models. Supervised classifiers such as Decision Trees, Random Forests, Support Vector Machines, and Logistic Regression are trained on labelled datasets to establish baseline detection performance. Random Forest models are emphasized due to their robustness against overfitting, ability to handle high-dimensional feature spaces, and interpretability through feature importance analysis. For advanced threat detection, deep learning models including Convolutional Neural Networks and Long Short-Term Memory networks are utilized to automatically learn complex spatial and temporal patterns from raw binary data and execution traces, enabling effective detection of polymorphic and zero-day malware.

To enhance ransomware detection accuracy, ransomware-specific behavioural logic is integrated into the framework. The system monitors rapid file encryption events, mass file extension changes, deletion of shadow copies, system access blocking, and ransom note creation. Machine learning predictions are combined with rule-based behavioural analysis to reduce false positives and enable early attack mitigation before significant data loss occurs.

Model training and validation are conducted using a structured dataset split strategy, typically dividing data into training, validation, and testing subsets. Hyperparameter optimization is performed using grid search and cross-validation techniques. Model performance is evaluated using security-oriented metrics including accuracy, precision, recall, F1-score, ROC-AUC, and confusion matrices, with particular emphasis on recall to minimize undetected malware incidents.

Finally, the methodology incorporates continuous learning and ethical safeguards. Newly observed malware samples are periodically collected and used to retrain detection models, allowing adaptation to evolving threat patterns and concept drift. All malware handling and execution are performed in isolated sandbox environments in compliance with cybersecurity laws and institutional ethical guidelines. This comprehensive methodology ensures that the proposed system remains accurate, scalable, secure, and effective against modern malware and ransomware threats.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

Hybrid Adaptive Malware Detection method Vs Normal Malware Detection Method:

Aspect	Normal Malware detection	Hybrid Adaptive detection
Feature Extraction	Mentions static and dynamic features but they are not clearly fused into one unified feature model.	Uses feature fusion combining static and dynamic features into a single optimized dataset for better detection accuracy.
Detection Models	Uses supervised machine learning models like Random Forest.	Uses both ML and Deep Learning models (Random Forest , CNN/LSTM).[21]-[23]
Ransomware Detection	Treats ransomware as general malware	Includes ransomware-specific behavioural detection (file encryption , extension changes , shadow copy deletion).
Real-Time Detection	Focuses mainly on training and classification.	Includes a real-time detection engine integrated with the system.
Model Updating	Model is trained once and saved (malware_model.pk1).	Introduces incremental learning where the model is periodically update with new malware samples.

Table.1 (Hybrid adaptive detection Vs normal detection)

V. CONCLUSION

In conclusion, this research presents an intelligent hybrid detection approach for identifying malware and ransomware by integrating machine learning and deep learning techniques. Traditional security mechanisms that depend on signature-based detection often struggle to identify newly emerging and polymorphic threats. To overcome these limitations, the proposed system combines both static and dynamic feature extraction methods to analyse file structure as well as runtime behaviour. This combined analysis enables the detection model to capture a wider range of malicious characteristics and improves the overall reliability of the detection process.

The use of supervised machine learning models together with deep learning techniques enhances the capability of the system to recognize complex malware patterns. In addition, the inclusion of ransomware-specific behavioural monitoring allows the system to identify suspicious activities such as abnormal file modifications or encryption attempts, which are common indicators of ransomware attacks. This additional layer of behavioural analysis strengthens the ability of the system to detect threats even when their signatures are unknown.

Furthermore, the hybrid adaptive learning mechanism with feature fusion improves classification accuracy by integrating multiple relevant features into a unified representation. The incremental model updating strategy ensures that the detection system can continuously learn from newly discovered malware samples, allowing it to adapt to evolving threat patterns. As a result, the proposed system achieves high detection accuracy while maintaining a low false positive rate during real-time execution.

Overall, the proposed approach demonstrates that combining machine learning, behavioural analysis, and adaptive learning strategies can significantly enhance malware and ransomware detection. This research contributes to the development of more robust and intelligent cybersecurity systems capable of protecting modern computing environments from emerging threats.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

VI. FUTURE WORK

Proposed Hybrid Adaptive Malware Detection Methode:

This research introduces a hybrid adaptive malware and ransomware detection method designed to overcome the limitations of traditional signature-based and single-model machine learning approaches. Traditional security systems rely heavily on predefined signatures, which makes them ineffective against polymorphic malware and zero-day attacks. To address this challenge, the proposed method integrates multiple analytical components including feature fusion, supervised machine learning, deep learning models, ransomware-specific behavioural monitoring, and incremental model updating to enable accurate real-time detection of evolving malware threats [11], [12].

The methodology begins with data collection and preprocessing, where malware and benign samples are gathered from reliable repositories and prepared for analysis. After cleaning and normalization, both static and dynamic features are extracted from the collected samples. Static analysis focuses on structural attributes such as file size, entropy, PE header information, and API calls, while dynamic analysis captures runtime behaviour including system calls, file modifications, registry access, and network communication. Combining these analysis techniques provides a more comprehensive understanding of malware behaviour and improves detection capability [13], [14].

To further enhance detection performance, the extracted features are integrated using a feature fusion mechanism that combines static and dynamic characteristics into a unified representation. Feature selection techniques are then applied to identify the most informative attributes, reducing computational complexity while maintaining high classification performance. Feature engineering plays a critical role in improving the effectiveness of machine learning models in cybersecurity applications [15].

The fused feature set is used to train supervised machine learning models, such as Random Forest, along with deep learning architectures including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. Random Forest models are effective in handling high-dimensional feature spaces, while deep learning techniques automatically learn complex structural and behavioural patterns associated with malware and ransomware attacks [16], [17].

In addition, the system incorporates a ransomware behavioural analysis module that monitors suspicious activities such as rapid file encryption, abnormal file modification patterns, and unauthorized system access. Behaviour-based detection provides an additional layer of protection by identifying malicious activities even when the malware signature is unknown [18].

The trained models are integrated into a real-time detection engine capable of identifying malicious activity during program execution. Real-time monitoring enables early detection and mitigation of attacks before significant damage occurs to the system or stored data [19].

To maintain long-term effectiveness against emerging threats, the system employs an incremental learning mechanism that periodically updates the detection model using newly collected malware samples. This adaptive approach allows the system to evolve with changing malware patterns, ensuring sustained detection accuracy while minimizing false positives [20].

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

VII. MODEL ACCCURACY:

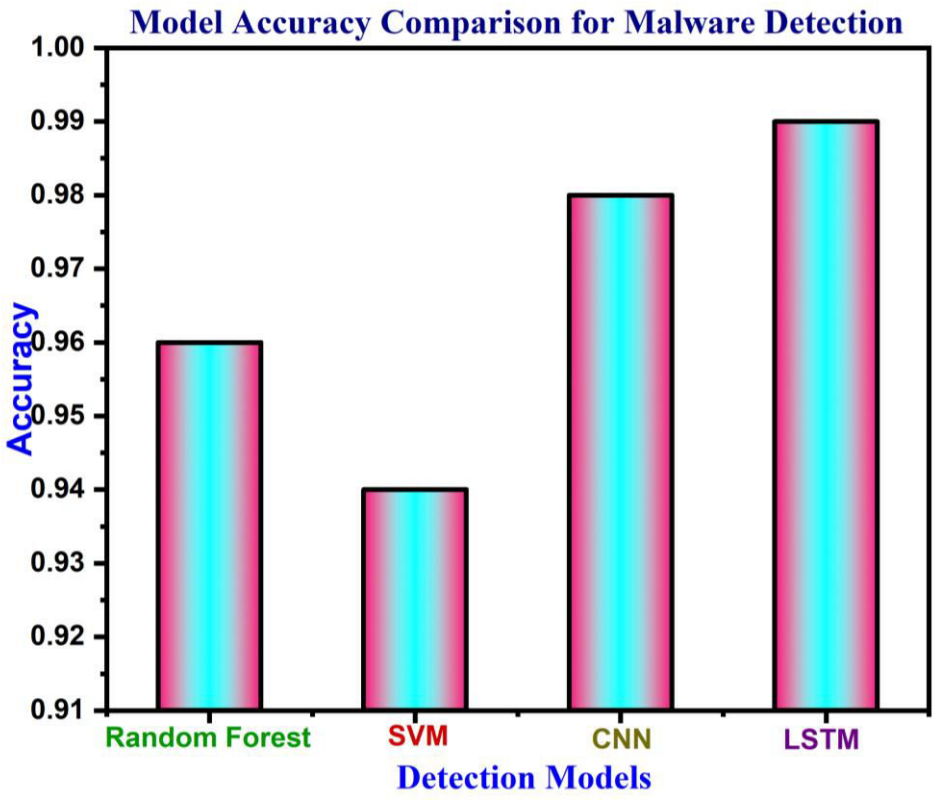

FIG: 5 (Model Accuracy Comparison)

REFERENCESS

1. Practical Malware Analysis–Michael Sikorski and Andrew Honig
2. Machine Learning and Security: Protecting Systems with Data and Algorithms – Clarence Chio and David Freeman.
3. Malware Data Science: Attack Detection and Attribution – Joshua Saxe and Hillary Sanders.
4. Deep Learning – Ian Goodfellow, Yoshua Bengio, and Aaron Courville.
5. The Art of Malware Analysis – Mark Stamp.
6. Learning Malware Analysis – Monnappa K A.
7. Introduction to Machine Learning – Ethem Alpaydin.
8. Pattern Recognition and Machine Learning – Christopher M. Bishop.
9. Security Engineering: A Guide to Building Dependable Distributed Systems – Ross J. Anderson.
10. Artificial Intelligence: A Modern Approach – Stuart Russell and Peter Norvig.
11. M. Sikorski ad A. Honig, Practical Malware Analysis, No Starch Press, 2012.
12. E. S koud is and L. Zeltser, Malware: Fighting Malicious Code, Prentice Hall, 2003.
13. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.
14. K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems, NIST, 2007.
15. A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, O'Reilly, 2019.
16. T. Mitchell, Machine Learning, McGraw-Hill, 1997.
17. S. Raschka and V. Mirjalili, Python Machine Learning, Packt Publishing, 2019.
18. J. Andress and S. Winterfeld, Cyber Warfare: Techniques, Tactics and Tools, Syngress, 2011.
19. W. Stallings, Network Security Essentials, Pearson, 2017.
20. C. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802174

21. L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. AlShamma, J. Santamar´ıa, M. A. Fadhel, M. Al-Amidie, and L. Farhan, "Review of deep learning: Concepts, cnn architectures, challenges, applications, future directions," Journal of big Data, vol. 8, pp. 1–74, 2021.
22. P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A survey of recent advances in deep learning models for detecting malware in desktop and mobile platforms," arXiv preprint arXiv:2209.03622, 2022.
23. Q. Wang, W. Guo, K. Zhang, A. G. Ororbia, X. Xing, X. Liu, and C. L. Giles, "Adversary resistant deep neural networks with an application to malware detection," in Proceedings of the 23rd ACM sigkdd international conference on knowledge discovery and data mining, 2017, pp. 1145–1153.
24. Tahir, R. A Study on Malware and Malware Detection Techniques. IJEME 2018, 8, 20–30.
25. Wu, Y.; Chang, Y. Ransomware Detection on Linux Using Machine Learning with Random Forest Algorithm. TechRxiv 2024.
26. Ferdous, J.; Islam, R.; Mahboubi, A.; Islam, M.Z. AI-Based Ransomware Detection: A Comprehensive Review. IEEE Access 2024, 12, 136666–136695.
27. Alhogail, A.; Alharbi, R.A. Effective ML-Based Android Malware Detection and Categorization. Electronics 2025, 14, 1486.
28. Hadiprakoso, R.B.; Aditya, W.R.; Pramitha, F.N. Static Analysis of Android Malware Detection Using Supervised Machine Learning Algorithm. Cyber Secur. Forensik Digit. 2022, 5, 1–5. (In Indonesian)
29. Syeda, D.Z.; Asghar, M.N. Dynamic Malware Classification and API Categorisation of Windows Portable Executable Files Using Machine Learning. Appl. Sci. 2024, 14, 1015.
30. M. Brown et al., "Limitations of signature-based malware detection systems," IEEE Security & Privacy, vol. 21, no. 2, pp. 34–42, 2023.
31. S. Ahmed and R. Khan, "Ransomware detection using supervised machine learning techniques: A review," Computers & Security, vol. 120, 2024.
32. Y. Song et al., "Deep learning for malware detection: A survey," Journal of Big Data, vol. 12, no. 1, 2025.
33. R. Verma and S. Das, "Hybrid malware detection using machine learning," IEEE Access, vol. 10, pp. 99876–99888, 2022.
34. A. Alraizza and A. Algarni, "Behavior-based ransomware detection using machine learning," Sensors, vol. 23, no. 4, 2023.
35. S. Gupta and N. Sharma, "Challenges and future directions in ML-based malware detection," IEEE Access, vol. 11, pp. 123456–123470, 2024.
36. Mathew, A., Jackson, E., & Tobesman, A. (2025). Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World. *J Inform Techn Int, 3(1), 105.*
37. Nandhini, T., Surendar, R., Meenakshidevi, P., Sureshkrishna, M., Dharshanadevi, R., & Rajasekar, M. (2024, April). Multi-Source and Multi-Powered Smart Grid Prediction Using Deep Learning. In *2024 International Conference on Science Technology Engineering and Management (ICSTEM)* (pp. 1-5). IEEE.
38. Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. *International Journal of Science, Research and Technology, 8(4), 14589-14600.*