Advances in Artificial Intelligence and Machine Learning; Research 5 (2) 3866-3882 Received 22-03-2025; Accepted 14-06-2025; Published 21-06-2025

Malware Traffic and Ransomware Anomaly Detection Based on Wavelet Time-Frequency Analysis and Deep Learning

Wei-Yu Chen cwy4@ulive.pccu.edu.tw
Department of Education and Learning Technology
Chinese Culture University
Department of Computer and Engineering
Tatung University
Taipei, Taiwan

Tsang-Long Pao tlpao@gm.ttu.edu.tw
Department of Computer and Engineering
Tatung University
Taipei, Taiwan

Yucheng Kao ykao@gm.ttu.edu.tw
Department of Information Management
Tatung University
Taipei, Taiwan.

Corresponding Author: Wei-Yu Chen

Abstract

This study proposes a method for detecting malicious software traffic using wavelet time-frequency analysis combined with machine learning. The public CICIDS2017 intrusion detection dataset was utilized to extract network flow data, on which wavelet transforms were applied to obtain spectral features (such as multi-scale energy distributions and entropy). These features were used to train classification models including Support Vector Machine (SVM), Random Forest (RF), and a deep neural network. Experimental results show that wavelet-derived features significantly improve anomaly detection performance. In particular, the neural network model achieved over 97% detection accuracy, outperforming the traditional classifiers. The wavelet analysis enabled the models to accurately distinguish normal versus ransomware-like malicious traffic, even for attacks with subtle or evolving patterns. These findings demonstrate that wavelet time-frequency analysis can enhance the detection of malware traffic and provide robust recognition capability against unknown attacks.

Keywords: Wavelet transform, Time-frequency analysis, Network anomaly detection, Ransomware traffic, Deep learning, Intrusion detection system.

Citation: Wei-Yu Chen, et al. Malware Traffic and Ransomware Anomaly Detection Based on Wavelet Time-Frequency Analysis and Deep Learning. Advances in Artificial Intelligence and Machine Learning. 2025;5(2):219.

1. INTRODUCTION

In recent years, the widespread use of the Internet and the proliferation of IoT devices have led to a surge in malicious network traffic. Ransomware has become a major cybersecurity threat, encrypting victims' files and demanding ransom, which causes severe financial losses and operational disruptions. Traditional malware detection largely relies on known signatures or rules, matching packet content or connection patterns to identify attacks. However, signature-based intrusion detection systems (IDS) are often ineffective against unknown or morphing attacks, failing to detect brand-new ransomware variants or cleverly obfuscated traffic. For example, the 2017 WannaCry ransomware attack exploited a zero-day vulnerability to spread rapidly; its traffic characteristics initially had no known signature and thus evaded many traditional defenses [1]. This highlights the need for behavior-based anomaly detection that can identify malicious traffic without relying on prior signatures.

Anomaly detection analyzes the statistical and temporal behavior of traffic to recognize patterns deviating from normal baselines. In this context, signal processing techniques, especially the wavelet transform, offer significant advantages for network traffic analysis. Wavelet transforms decompose non-stationary signals into different frequency components while preserving time information, producing a time-frequency representation. In contrast to the classical Fourier transform which provides only a global frequency spectrum, the wavelet transform enables observation of how traffic features evolve over time at multiple scales. Using multi-resolution wavelet analysis, one can capture high-frequency bursts or spikes (e.g. short intense attack traffic) as well as low-frequency trends (e.g. long-duration stealthy connections). This capability makes wavelets particularly suitable for detecting network anomalies that have localized time-frequency patterns, such as the sudden surges or periodic beacons often seen in malware communications.

Recent research has increasingly applied wavelet-based techniques in intrusion detection. For example, Huang et al. [2], embedded a discrete wavelet transform into a real-time IDS and found that appropriate wavelet basis choices improved detection rates for DoS and port scan attacks. Zhan et al. [3], proposed a wavelet-kernel SVM for network intrusion detection, achieving 96.67% accuracy on a benchmark dataset by using wavelet functions in the classifier. Wu and Ding (2020) [4], built a wavelet-based anomaly detection system that leveraged time-frequency features to attain high detection accuracy. In the automotive domain, Bozdal et al. (2021) [5], applied wavelet analysis to CAN bus intrusion detection, demonstrating effective real-time anomaly detection on embedded systems. Moreover, a recent comprehensive review highlights the growing adoption of wavelet transforms in cybersecurity solutions for identifying complex attack patterns. Wavelet analysis has shown outstanding performance due to its ability to capture both short-time and long-time signal behaviors in network traffic.

At the same time, deep learning methods have achieved remarkable success in malware and ransomware detection in recent years. Many studies report that deep neural networks can learn complex patterns of malicious behavior with high accuracy [6–8]. For instance, Hussain et al. (2024) [9], developed a group-normalization BiLSTM model for ransomware classification that achieved 99.99% detection accuracy on recent malware datasets pmc.ncbi.nlm.nih.gov. Singh et al. (2023) [10], presented an ensemble deep learning approach (RANSOMNET+) that attained over 99% precision and 99% accuracy in detecting ransomware in cloud data mdpi.com. In another study, Gulmez et al. (2024) [11], introduced an explainable ransomware detection system "XRan," which

employs a convolutional neural network (CNN) to identify ransomware and uses model-agnostic explainers (LIME) for interpretability dl.acm.org. These works show the promise of modern machine learning in malware defense. However, purely deep learning approaches can act as "black boxes" and may require large training data, whereas signal processing features like wavelets can provide interpretable insights and robustness even with limited data.

In this paper, we integrate the strengths of wavelet time-frequency analysis with machine learning to detect malware and ransomware traffic anomalies. By extracting wavelet-based spectral features from network flows, and feeding them to both classic classifiers and a neural network, we aim to improve detection accuracy and understandability. We focus on a challenging scenario of detecting ransomware-like traffic in an enterprise network using the CICIDS2017 benchmark dataset [12]. The contributions of this work are summarized as follows: (1) We develop a feature extraction approach using wavelet transforms to capture multi-scale network traffic patterns associated with malicious behavior. (2) We design and implement an anomaly detection framework combining these wavelet features with both traditional machine learning (SVM, RF) and deep learning (neural network) models, and evaluate their performance on real traffic data. (3) We analyze the models' results and feature importance to highlight how specific time-frequency characteristics (e.g. burst frequencies, spectral entropy) indicate ransomware activity, providing an interpretable perspective. Experimental results demonstrate that our wavelet-based approach achieves high detection rates, outperforming models using only time-domain features. The proposed methodology can detect ransomware traffic anomalies with high accuracy and offers potential for early detection of new attacks that lack signatures.

2. LITERATURE REVIEW

2.1 Intelligent Intrusion Detection Systems (IDS)

Traditional intrusion detection techniques are broadly categorized into signature-based (misuse) and anomaly-based approaches. Signature-based IDS rely on known attack patterns or rules; they are effective for detecting previously observed threats but cannot identify novel or obfuscated attacks. In contrast, anomaly-based IDS establish a baseline of normal behavior and flag deviations as potential intrusions, which enables detection of new or evolving attacks. The drawback, however, is that anomaly detectors often suffer higher false alarm rates due to the difficulty of precisely modeling "normal" behavior. Because ransomware and other modern malware rapidly adapt their tactics, purely signature-driven systems struggle to keep pace [1]. For instance, many signature and rule-based defenses failed against new ransomware variants that employed encryption and obfuscation techniques [13]. These limitations highlight the need for more intelligent IDS that leverage machine learning to generalize beyond known signatures and detect malicious behavior based on statistical patterns. Over the past decade, researchers have increasingly integrated AI and machine learning into IDS to improve adaptability [8]. Early data mining and statistical learning methods were applied to model network traffic and identify outliers indicative of attacks. Modern anomaly-based IDS commonly use machine learning classifiers or clustering to automatically learn the characteristics of benign versus malicious traffic. The advantage of ML-driven solutions is their ability to abstract complex relationships in data, enabling the system to recognize subtle intrusions or zero-day exploits that do not match any predefined signature. At the same time, hybrid detection strategies have emerged, combining signature and anomaly techniques to capitalize on the strengths of each. Such

hybrid IDS can catch a wider range of threats, although designing an optimal balance to minimize false positives remains an active research problem. Overall, the evolution of IDS is trending toward intelligent, learning-based models [6, 7, 14], that continuously adapt to new attacks, addressing the inadequacy of manual signature updates in today's fast-changing threat landscape.

2.2 Wavelet Analysis Theory

Wavelet transform is a technique that projects a signal onto scaled and shifted versions of a base wavelet function. Mathematically, the continuous wavelet transform (CWT) of a signal *x(t)* is defined as:

$$W_x(a,b) = \int_{-\infty}^{+\infty} x(t) \frac{1}{\sqrt{a}} \emptyset \left(\frac{t-b}{a} \right) dt \tag{1}$$

where $x(t)$ is the scaled and translated **mother wavelet** $\emptyset$ (t), with scale $a > 0$ (inversely proportional to frequency) and translation b shifting in time). By varying a and b, the wavelet transform captures the signal's characteristics at different frequencies and times. In contrast, the Fourier transform projects onto fixed sinusoidal basis functions and cannot provide time localization information; and while the short-time Fourier transform (STFT) introduces a time window, it uses a fixed window length and thus cannot simultaneously achieve high resolution in both high and low frequency components. Wavelet transform offers adaptive resolution: it automatically uses fine time resolution (short window) at high frequencies and fine frequency resolution (long window) at low frequencies. This property makes wavelets especially suitable for analyzing traffic signals that have bursty or evolving behavior.

The Discrete Wavelet Transform (DWT) is implemented via filtering and down-sampling for digital signals. A common method is to use the Mallat algorithm for multi-scale decomposition: the signal is passed through a low-pass filter g[n] and a high-pass filter h[n], yielding a low-frequency approximation A1 and high-frequency detail $D1$ Then $A1$ is iteratively filtered and down-sampled to produce $A2$ and $D2$, and so on, up to the desired level. In this way, this study obtain detail coefficients Dj at various levels j and a final approximation AJ. Each decomposition level's coefficient count is halved due to down-sampling, while the time span covered doubles. *FIGURE 1* illustrates an example of a Morlet mother wavelet, whose oscillation is confined to a finite time window, reflecting the wavelet's good localization in time and frequency. (Morlet wavelets essentially resemble a sinusoid weighted by a Gaussian envelope, allowing analysis of local oscillatory components.)

2.3 Wavelet Transform in Network Traffic Analysis

Time–frequency analysis techniques have become invaluable for inspecting non-stationary network traffic signals (e.g. packet flows) to detect anomalies. In particular, the wavelet transform provides a multi-resolution view of network data, decomposing traffic time series into frequency components while preserving temporal locality. Unlike the classical Fourier transform which yields a single global spectrum, wavelet analysis produces a rich time–frequency representation that reveals how traffic patterns evolve over time. This is crucial for intrusion detection, as many cyber-attacks manifest as transient bursts or periodic behaviors that might be averaged out in a pure frequency-domain analysis. By using scalable window functions (mother wavelets) that stretch for low-

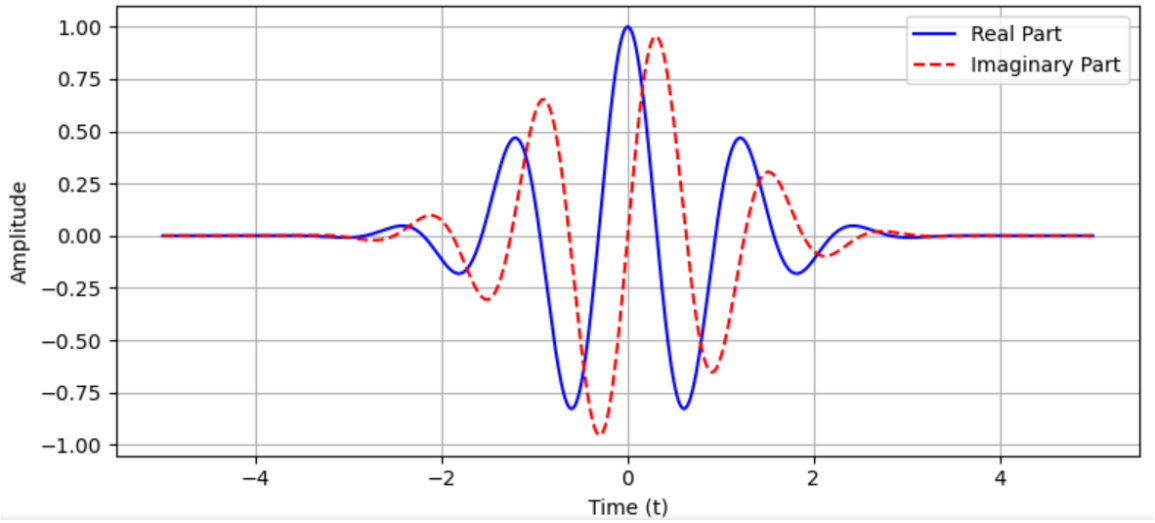

Figure 1: Morlet Mother Wavelet

frequency trends and compress for high-frequency events, the wavelet transform can simultaneously capture long-duration anomalies (e.g. slow stealthy scans) and short-lived spikes (e.g. bursty denial-of-service packets) in network traffic. These properties make wavelets well-suited for analyzing network signals that exhibit time-varying statistics, providing insights (such as sudden changes, trends, or repetitive patterns) not readily apparent with traditional Fourier or statistical methods [3, 5, 15]. Wavelet transforms have been successfully integrated into IDS frameworks as a feature extraction and signal pre-processing tool. Researchers as early as Zhan et al. (2014) [3], demonstrated that incorporating wavelet-based kernels in an SVM classifier improved detection accuracy for communication network intrusions. More recently, Bozdal et al. (2021) [5], developed WINDS, a wavelet-based IDS for in-vehicle CAN bus security, and showed that continuous wavelet transform (CWT) features outperformed simple frequency-count–based detectors across multiple attack types. The CWT's fine-grained time–frequency coefficients enabled the system to detect anomalies in CAN traffic that were missed by fixed-window frequency analysis. In general network environments, wavelet-derived metrics (e.g. multi-scale energy or entropy) can be computed from flow statistics to characterize normal vs. malicious behavior. For example, recent work [15], combined CWT with autoencoders to flag network anomalies via reconstruction error, achieving high accuracy in identifying traffic spikes and irregular oscillations associated with attacks. The advantage of wavelet-based analysis is evident in its ability to localize subtle changes in traffic patterns that may indicate malware communications or data exfiltration. By integrating wavelet transforms into IDS, one can enrich the feature set with time–frequency information, improving the detection of complex attacks (like multi-stage or low-and-slow intrusions) that evade detection in purely time-domain or frequency-domain analysis.

2.4 Machine Learning Models in IDS

A wide array of machine learning models has been applied to intrusion detection, ranging from traditional classifiers to state-of-the-art deep learning networks. Support Vector Machines (SVM)

and Random Forests (RF) are among the classic algorithms extensively used in IDS research and deployments [8]. These models can handle high-dimensional network data and have shown strong performance in distinguishing normal versus malicious traffic patterns. For instance, SVM-based detectors can learn decision boundaries for complex attack classes, while RF (an ensemble of decision trees) can effectively capture nonlinear relationships in features derived from packet headers, flows, or system logs. Several studies report that such traditional ML models achieve high accuracy on benchmark intrusion datasets and offer faster inference with lower resource usage compared to deep neural networks [8]. Notably, their results tend to be more interpretable – security analysts can extract meaningful rules or feature importances (e.g. which protocol fields contribute to a detection) from tree-based models and SVM decision functions. According to a recent experimental study, algorithms like SVM and RF remain promising for real-world IDS deployments due to their versatility and explainability, making them attractive for organizations that require reliable and transparent detection outcomes. However, one must also acknowledge that these models rely on manually engineered features and may struggle to automatically capture complex spatio-temporal patterns present in modern attack traffic. Deep learning approaches have therefore gained traction for building more powerful IDS that automatically learn feature representations from data [6, 7]. Convolutional Neural Networks (CNNs), in particular, have proven effective in recent studies for intrusion detection tasks [16, 17]. CNNs can be applied to network traffic by transforming flow statistics or payload data into a suitable numeric matrix (or even image) form, where the convolution layers can detect local patterns indicative of attacks. For example, researchers have converted raw network traffic into 2D grids (using techniques like a "zigzag" reshaping) and then used deep CNN models to classify traffic, significantly reducing false alarm rates compared to earlier methods [16]. In the IoT domain, Saba et al. (2022) [17], proposed a CNN-based anomaly detector that was trained on recent IoT intrusion datasets, achieving over 99% detection accuracy on the NID-2020 dataset and ~93% on the Bot-IoT dataset. Such results underscore CNNs' ability to automatically extract salient features (e.g. patterns in traffic bursts, protocol headers, or inter-arrival times) that distinguish benign from malicious behavior. Deeper architectures (e.g. ResNet or Inception-based CNNs) have also been explored to improve feature extraction, sometimes in combination with other models. For instance, hybrid frameworks have been built where CNN layers capture spatial characteristics of traffic data and feed into recurrent layers (like LSTM) to capture temporal dynamics [7, 10, 14]. These deep learning models consistently report high detection rates, often outperforming classical methods especially for sophisticated attacks or large-scale data. The trade-off is that neural networks generally require more computational resources and training data; combinations of CNN with RNN tend to boost accuracy at the cost of longer training and inference times. Nonetheless, the trend in the literature shows a clear shift toward deep learning-driven IDS, owing to their superior ability to model complex, high-dimensional intrusion patterns.

2.5 Deep Learning-Based IDS

The past few years have witnessed rapid advancements in applying sequence modeling and attention-based deep learning architectures to intrusion detection, with a focus on improving detection of novel attacks like ransomware. Recurrent neural networks such as LSTM (Long Short-Term Memory) and their bidirectional variants (BiLSTM) have been widely adopted to capture temporal dependencies in network traffic and system event sequences [18, 19]. An LSTM can learn the progression of an attack over time (for example, a slow port scan followed by exploitation), retaining long-term context that static classifiers might miss. Yin et al.'s seminal 2017 work [18], showed that

an LSTM-based IDS could reach high accuracy on benchmark data, and current research continues to build on that foundation. Hussain et al. (2024) [9], recently introduced a Group Normalization BiLSTM model for ransomware detection, which achieved 99.99% accuracy in distinguishing ransomware from normal activity on the CIC-MalMem-2022 dataset. This model processes malware behavior both forward and backward in time, enhancing the context for identifying obfuscated ransomware patterns. In general, BiLSTM networks have demonstrated excellent performance on malware traffic classification, outperforming unidirectional LSTMs in capturing the full sequence of attack events. The ability of LSTM-based models to learn complex temporal patterns has made them effective for detecting both fast-propagating attacks and "low-and-slow" incursions. However, deep recurrent models can be computationally intensive and often behave as black boxes, which motivates the exploration of more efficient or interpretable architectures in recent literature. Transformer-based architectures have emerged as a promising direction for IDS owing to their strength in modeling long-range dependencies with attention mechanisms [20, 21]. Transformers, originally popularized in NLP, allow the model to attend to salient features across an entire sequence without the sequential processing constraints of RNNs. In network IDS, this translates to capturing complex relationships between events in a traffic flow or log sequence (e.g. correlation between multiple connection attempts across different time windows). Several studies from 2022 onward have adapted Transformers for intrusion detection [20, 21]. For example, Li et al. (2022) [21], proposed a semi-supervised Transformer framework for network IDS, which demonstrated improved detection of rare attack classes by leveraging unlabeled data and attention-based feature learning. Another notable work by Liang et al. (2024) [20], combined a Transformer with wavelet time–frequency features to build a multi-level IDS for IoT networks, reporting state-of-the-art accuracy on IoT intrusion datasets. In ransomware detection, Singh et al. (2023) [10], introduced RANSOMNET+, a hybrid model blending CNN feature extraction with a pre-trained Transformer; this ensemble captured both local traffic patterns and global context, and delivered "unrivaled accuracy" in classifying ransomware attacks on cloud data. These Transformer-based approaches generally achieve high detection rates and can adapt to diverse attack behaviors, but they also tend to be resource-heavy. Real-time deployment is a concern: deep Transformers require significant processing, which can introduce latency. Recent research addresses this by seeking more efficient Transformer variants and leveraging techniques like knowledge distillation or hardware acceleration to meet real-time constraints. Additionally, the interpretability of attention models is an active topic – while attention weights provide some insight into what the model focuses on, the overall complexity still makes results hard to explain to security operators [11].

In summary, the 2022–2024 advancements in IDS research emphasize deep learning innovations. LSTM and BiLSTM models [9, 18, 19], have proven adept at anomaly and ransomware detection by learning temporal patterns, whereas Transformer-based IDS [4,18,19], leverage self-attention to detect complex, multi-stage attacks with high accuracy. The consensus in recent studies [6, 14, 22], is that these deep models outperform conventional methods in detection capability, yet they bring challenges in terms of computational overhead and interpretability. To balance this, researchers are exploring combinations of models (for performance boost) alongside feature selection and explainable AI techniques [11], to maintain practicality. For example, some works integrate explainable components or use simplified post-hoc models to interpret the decisions of a deep IDS. Others focus on optimization, ensuring that even sophisticated models can operate within the time constraints of real-world network environments [20, 21]. This blend of high accuracy and deployment-oriented considerations defines the cutting edge of intelligent IDS research today. Each approach – whether CNN [16, 17], LSTM [9, 18], or Transformer [10, 20, 21] – brings its own strengths: CNNs excel

at spatial feature learning, RNNs at sequential pattern memory, and Transformers at handling long-range interactions. Ongoing comparative studies highlight that no single model is universally best; instead, the choice often depends on the specific use case requirements (e.g. network type, threat models, need for real-time response, or need for model interpretability). Thus, the literature suggests a trend toward hybrid and ensemble methods [7, 10, 14, 20], that capitalize on multiple techniques, aiming to create IDS solutions that are both robust against advanced cyber-attacks and practical for deployment in securing critical systems.

2.6 Intelligent Intrusion Detection Systems for Ransomware Detection

Ransomware has evolved into one of the most damaging cyber threats in recent years, prompting a surge in research into intelligent intrusion detection systems (IIDS) that leverage AI to detect early signs of infection and lateral movement [22, 23]. Traditional signature-based antivirus and IDS tools fail against zero-day or polymorphic ransomware, which obfuscate payloads and employ encrypted communication channels [1, 13]. As a response, modern IIDS integrate machine learning and deep learning models with behavior-based analysis to identify anomalies in system activities, network flows, and file access patterns indicative of ransomware attacks.

In the context of network-based ransomware detection, intelligent IDS have focused on traffic flow characteristics. For example, XRan, an explainable deep learning-based detection framework, was proposed by Gulmez et al. (2024) [11], combining CNN for feature extraction with model-agnostic explanation methods like LIME. It was trained on dynamic behavioral traces of ransomware samples, achieving high accuracy while also offering interpretability for forensic analysis. This marks a step forward in making deep learning–based IDS usable in real-world operations where explainability is vital.

Similarly, Singh et al. (2023) [10], introduced RANSOMNET+, a transfer learning–driven ensemble that combines CNN and Transformer layers to detect ransomware in cloud-encrypted data. This architecture allows the system to generalize across ransomware variants and diverse encryption contexts, achieving >99% precision and recall on large-scale datasets. The model's ability to leverage prior learning and adapt to new variants is particularly crucial for ransomware, which is known for rapidly changing tactics [13].

In host-based detection, intelligent IDS utilize behavioral telemetry (e.g., file encryption rate, registry edits, and abnormal CPU usage) [9, 23]. Hussain et al. (2024) [9], proposed a Group Normalized BiLSTM model that analyzes time-series system logs to detect ransomware behavior, reaching 99.99% accuracy on the CIC-MalMem-2022 dataset. This approach demonstrates the power of deep sequential models in understanding behavioral evolution, such as encryption bursts or lateral movement patterns, making it more resilient to evasion techniques than static rule-based methods.

Other approaches integrate autoencoders or GANs to model benign behavior and detect deviations [13, 15, 24]. Sayyad and Kotecha (2025) [15], applied time–frequency analysis combined with autoencoders to detect anomalies in encrypted ransomware traffic, showing that the learned latent representations effectively captured sudden entropy shifts and bursty communication, key indicators of file encryption and command-and-control activity.

A key challenge remains in early-stage detection, where ransomware activity has not yet triggered massive encryption. To address this, researchers are exploring lightweight, real-time models that can flag pre-encryption behaviors. For example, Liang et al. (2024) [20], proposed a multi-stage IDS that first filters for abnormal access behavior and then uses a Transformer-wavelet fusion model for fine-grained detection. Such systems combine temporal modeling with frequency-domain features to spot subtle signs of ransomware staging, such as probing shared drives or loading encryption libraries.

In summary, recent literature demonstrates that intelligent IDS combining deep learning (CNN, BiLSTM, Transformer) [9–11, 20], explainable AI [11], and time–frequency [5, 15], analysis provide robust detection of ransomware threats. These systems not only offer high accuracy but also exhibit strong generalization against zero-day attacks and evasive ransomware strains. Future work is focusing on enhancing interpretability [11, 23], reducing inference time [20], and adapting to adversarial obfuscation strategies [13].

3. METHODOLOGY

This study leverage a public dataset for training and evaluation, extract time-series features via wavelet transforms, and employ machine learning models for anomaly classification. The presents FIGURE 2, presents a step-by-step flowchart of the proposed detection methodology, from data collection to classification

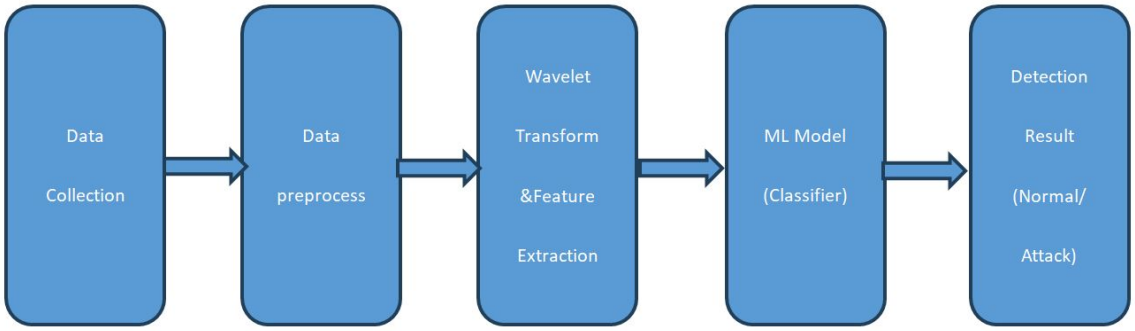

Figure 2: Flowchart of the proposed malware traffic detection methodology.

3.1 Data Source and Preprocessing

The study evaluated the proposed approach on the CICIDS2017 dataset [12], a public intrusion detection dataset released by the Canadian Institute for Cybersecurity (CIC). The CICIDS2017 dataset [12], contains realistic background traffic mixed with various attack scenarios, including FTP/SSH brute force, denial-of-service (DoS), Heartbleed exploit, web intrusions, internal network infiltration, botnet, and distributed DoS (DDoS) among others. The traffic was captured over a week in a controlled network environment, with Monday as purely benign traffic and attacks executed on the following days (Tuesday through Friday) during specific intervals. Although the dataset does not explicitly label any traffic as “ransomware”, it includes an Infiltration attack scenario (a simulated internal infection performing data exfiltration) which can partially represent ransomware-

like behavior (e.g. a compromised host communicating with a remote server) [1, 12]. In our study, it treat all attack-labeled flows in the dataset (including Infiltration and others) as malicious, and benign flows as normal, for a binary classification task (normal vs. attack). Each traffic capture in CICIDS2017 is provided as raw packet data (PCAP) and also as labeled flow records (extracted using CIC's CICFlowMeter tool) [12]. This study utilized the CICFlowMeter utility to process the PCAPs and extract bidirectional flow features. A network flow in this context is an aggregation of all packets sharing the same 5-tuple (source IP, destination IP, source port, destination port, protocol) within a timeframe or connection. Each flow record in CICIDS2017 contains dozens of statistical features describing the traffic, such as flow duration, total bytes and packets sent in each direction, packet length distributions, inter-packet intervals, TCP flag counts, and so on. First reassembled the flow data in chronological order according to their start times to reconstruct the timeline of network activity. Next, this study performed data cleaning and normalization: e.g., removing any flows with missing values and applying min-max scaling to numeric features to ensure that features with larger numeric ranges do not dominate the model training. This preprocessing yields a structured dataset of flow feature vectors with an associated class label (0 = normal, 1 = attack) for each flow.

3.2 Wavelet Transform for Time-Frequency Analysis

After preprocessing apply wavelet transform analysis to each network flow's time-based features. Wavelet transform is a technique that projects a time-domain signal onto scaled and shifted versions of a base wavelet function, revealing the signal's content in both time and frequency domains. In our approach focus on two forms of wavelet transform: the continuous wavelet transform (CWT) for time-frequency visualization, and the discrete wavelet transform (DWT) for feature extraction. Mathematically, the continuous wavelet transform of a signal x(t) is defined as:

$$\mathbf{W(a, b)} = \int_{-\infty}^{\infty} \mathbf{x(t)}\boldsymbol{\psi}_{\mathbf{a,b}}\mathbf{(t)dt},$$

where $\psi_{\mathbf{a,b}}\,(\mathbf{t}) = \frac{1}{\sqrt{a}}\psi\left(\frac{\mathbf{t-b}}{\mathbf{a}}\right)$ is a scaled (by factor $a > 0$) and translated (by b) version of the mother wavelet ψ(t). By varying the scale a (which is inversely related to frequency) and shift b (time position), the wavelet transform captures the signal's characteristics at different frequencies and times. Unlike the Fourier transform which uses infinite-length sinusoids and loses time localization, or the Short-Time Fourier Transform (STFT) which uses a fixed-size time window, the wavelet transform has adaptive resolution. It uses short windows at high frequencies and long windows at low frequencies, achieving a good balance of time and frequency resolution across scales. This property makes wavelets especially suitable for analyzing network traffic signals that exhibit bursty, transient behaviors as well as long-range trends. In practice, this study utilized the Discrete Wavelet Transform (DWT) to derive features from each flow's time-series data. The DWT is implemented via a filter-bank approach (e.g., the Mallat algorithm) that successively decomposes a signal into approximation and detail coefficients. At each decomposition level, the signal is passed through a pair of filters: a low-pass filter yielding a coarse approximation (A) and a high-pass filter yielding fine details (D). The output is then down-sampled by 2 before continuing to the next level. By iteratively applying this process, the DWT produces multi-resolution representations: for example, D_1 captures the highest-frequency components of the signal, D_2 captures the next-highest frequencies, and so on, while A_J (at the final level J) captures the remaining low-frequency trend.

Using wavelet transforms, this study extract time-frequency features from each network flow. In particular performed a DWT on selected time-oriented flow sequences. For example, this study derived a signal from each flow representing the packet arrival timeline (by interpolating the sequence of packet inter-arrival times or sizes within the flow). This signal is then decomposed via DWT up to a certain level (in our implementation, 3 to 4 levels using a Daubechies-4 wavelet). From the resulting wavelet coefficients compute descriptive features including: the energy (sum of squared coefficients) in each detail level D_1, D_2, D_3,…, the energy ratio between levels (to capture how the energy of the traffic is distributed across frequency bands), and the wavelet entropy, which measures the randomness of the energy distribution. Intuitively, a stable traffic flow will have most energy concentrated in low-frequency components (low entropy), whereas an erratic or stealthy malicious flow may spread energy across multiple scales (high entropy) [15]. These features form the wavelet-based feature vector for each flow, supplementing the original basic statistics.

This study uses continuous wavelet transform to visualize traffic behavior in the time-frequency domain. The CWT produces a 2D time-scale heat map (often called a scalogram or spectrogram) showing the distribution of signal energy over time and frequency. This is useful for qualitatively identifying unusual patterns. FIGURE 3 shows an example of wavelet analysis of the time series of injected anomalies. The top chart shows a synthetic signal representing baseline network metrics with sudden spikes and frequency changes (simulating an attack). The subsequent graphs show the DWT detail coefficients at different levels, and the bottom graph is the CWT scale graph. We can see that the anomalous event (around time index 256) manifests itself as a high-frequency burst captured in DWT detail D1 and a broad-spectrum pulse in the CWT. At the same time, the low-frequency content of the signal is captured in D3. This example demonstrates how wavelet transforms can separate different aspects of traffic behavior in time and frequency [5, 15].

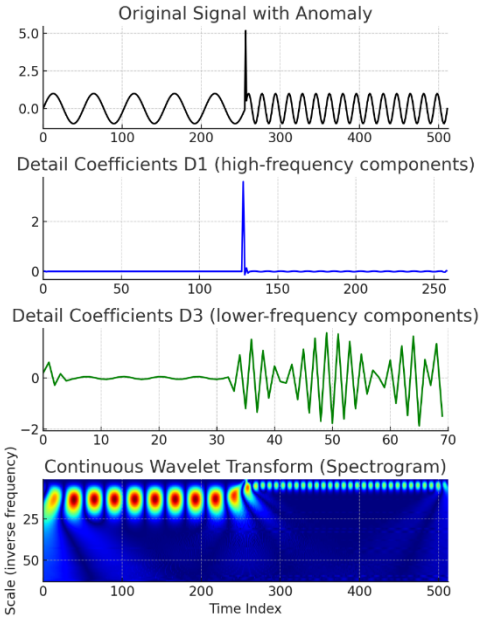

Figure 3: The waveform conversion process.

3.3 Feature Extraction from Wavelet Coefficients

In the method of this study, DWT is applied to the time series representation of each network flow to extract quantitative features. First, each stream is converted into a one-dimensional sequence reflecting its behavior over time. For example, a sequence of arrival times between packets, a sequence of packet counts per time period, or a sequence of packet sizes can be used. We experimentally found that using the sequence of packet sizes in each flow as the input signal produces the most discriminative features: Intuitively, normal traffic packet sizes tend to fluctuate within a certain range, while malicious activities (such as data exfiltration or encrypted ransomware communications) may produce a series of abnormally large packets or repeated size patterns [1]. These differences are reflected in the energy of the high-frequency wavelet coefficients. (Preliminary tests using interarrival times and packet counts were slightly less accurate, so the packet size sequence was chosen.)

After performing a wavelet decomposition on the packet size sequence of the flow (using an appropriate wavelet basis, such as Daubechies-4 and decomposing it to a level that captures millisecond-scale variability), a set of numerical features are extracted from the wavelet coefficients at each scale, which serve as the input numbers for the machine learning model. Design features include:

Energy distribution across frequency bands: We calculate the energy of the detail coefficients at each level $\mathbf{E_j} = \sum_k |\mathbf{D_{j,k}}|^2$ and similarly the energy of the final approximation $\mathbf{E_A} = \sum_k |\mathbf{A_{J,k}}|^2$. Each band's energy is then normalized by the total energy (sum of all $\mathbf{E_j}$ and $\mathbf{E_A}$) to obtain a ratio. For example, the feature vector includes (E_1/E_{tot}, E_2/E_{tot},…,E_J/E_{tot}). These ratios reflect how the signal's energy is distributed between high and low frequencies. If malicious traffic introduces bursts at specific scales, the energy in those high-frequency bands will be disproportionately high [5]. For instance, an aggressive ransomware file-encryption burst might produce a spike in mid-frequency energy (as encryption keys or data blocks are rapidly sent), raising E_J/E_{tot} for a certain detail level.

Spectral entropy: To measure the uncertainty or disorder of the signal's spectral energy distribution, we compute the Shannon entropy of the energy across the wavelet coefficients at each level. Specifically, for level j, we define $\mathbf{p_{j,k}} = |\mathbf{D_{j,k}}|^2 / \sum_k |\mathbf{D_{j,k}}|^2$ as the normalized energy of coefficient k at that level, and then $\mathbf{H_j} = -\sum_k \mathbf{p_{j,k}} log \mathbf{p_{j,k}}$. A high entropy indicates the energy is spread out over many coefficients (no dominant pattern), while a low entropy indicates the energy is concentrated (possibly a periodic or structured pattern) [15]. Under normal conditions, we expect certain bands' entropy to remain within a stable range, whereas anomalies may cause a sudden change in entropy by introducing or destroying regular patterns. For example, a long, steady connection may yield low entropy in a low-frequency band (most energy in a few coefficients), but a scanning attack might increase entropy by distributing energy across frequencies.

Peak coefficient magnitude and location: We record the maximum absolute wavelet coefficient value at each detail level and the time index when it occurs. This captures extreme transient events. An unusually large coefficient in a high-frequency band at a specific time suggests a sharp burst (e.g., a packet flood or a sudden surge in packet size), which is indicative of an attack [5]. Normal flows typically do not exhibit extremely large localized spikes in high-frequency components; their peaks are smaller and more spread out. Thus, features like "max" and its position can signal the presence and timing of an anomalous event.

Together, these features form a feature vector (on the order of 10–20 dimensions for our chosen decomposition levels) for each flow. In computing the features, we choose the mother wavelet and number of levels based on domain knowledge (ensuring the finest scale captures very short bursts on the order of a few packets, and the coarsest scale captures longer trends). If the initial feature set is high-dimensional, dimensionality reduction techniques like PCA could be applied to avoid the curse of dimensionality; however, in our experiments the number of features was manageable and we did not find significant benefits from PCA – all features were retained for model training.

3.4 Machine Learning Classifiers

After obtaining the wavelet-based feature vectors, we train several supervised learning models to learn a decision boundary between normal and malicious traffic. We experimented with three types of classifiers: SVM, Random Forest, and a feed-forward neural network, as described below [8].

- **Support Vector Machine (SVM):** We use an SVM with a radial basis function (RBF) kernel. SVMs implicitly map input features into a high-dimensional space and find the maximum-margin hyperplane that separates normal vs. attack classes. We trained the SVM on the wavelet feature set and tuned the hyperparameters (penalty parameter C and kernel parameter gamma) via grid search with cross-validation. SVMs are well-suited for binary classification and have been used in prior IDS research [3, 8].
- **Random Forest (RF):** Random Forest is an ensemble of decision trees. We trained a random forest with 100 trees, using bootstrap sampling of the training data and random feature subsets for splitting at each node. Random forests can handle multivariate features and provide an estimate of feature importance, which is useful for interpreting which wavelet features most strongly indicate an attack [8]. They are also robust to noise and overfitting due to averaging across trees.
- **Neural Network (NN):** We constructed a simple fully-connected neural network consisting of two hidden layers (50 neurons each with ReLU activation) and an output layer with sigmoid activation (producing a probability of the flow being malicious). We included a dropout layer (dropout rate 0.5) during training to regularize the model and prevent overfitting. The network was trained using the Adam optimizer to minimize binary cross-entropy loss. Neural networks can potentially capture more complex non-linear relationships in the feature space compared to SVM and RF, at the cost of requiring more data to generalize well [7, 14].

All models were trained on a training subset of the data and evaluated on a hold-out test set. We performed an 80/20 train-test split on the flows and used 5-fold cross-validation on the training portion for hyperparameter tuning, ensuring that performance estimates are generalizable. The evaluation metrics reported include Accuracy, Recall, Precision, and F1-score. Here, recall (true positive rate) reflects the detection rate of malicious flows, precision reflects the proportion of detected alerts that are truly malicious (low false alarm rate), and F1 is the harmonic mean of precision and recall.

4. EXPERIMENTAL RESULTS AND DISCUSSION

After implementing the above framework, we evaluated each model's detection performance on the CICIDS2017 test set [12]. TABLE 1 summarizes the performance metrics for the SVM, Random Forest, and Neural Network classifiers in our experiments:

Table 1: Performance comparison of different classification models on malicious traffic detection.

Model	Accuracy	Recall	Precision
SVM	92.3%	90.1%	88.7%
Random Forest	95.1%	93.0%	91.2%
Neural Network	97.5%	96.0%	94.8%

From the results, we observed that the neural network model performed the best overall, achieving the highest accuracy, recall, and F1-score among the three. For example, our neural network classifier achieved 97.5% accuracy, whereas the SVM reached about 92.3% and the Random Forest about 95.1% accuracy. The NN's recall was around 96%, meaning it missed very few attacks, while its precision was ~95%, indicating a low false positive rate. In comparison, the SVM had a slightly lower recall (~90%) and precision (~89%), suggesting it struggled a bit more with the complex decision boundary in the wavelet feature space. The Random Forest was intermediate, with ~94–95% accuracy and ~92% precision. These results demonstrate that more expressive models (like the neural network) can better capture the non-linear patterns in wavelet features that distinguish malicious traffic. This trend aligns with observations in other studies [7, 9, 10, 14, 17], that deep learning often outperforms traditional classifiers for anomaly detection. The model comparison table is shown in FIGURE 4.

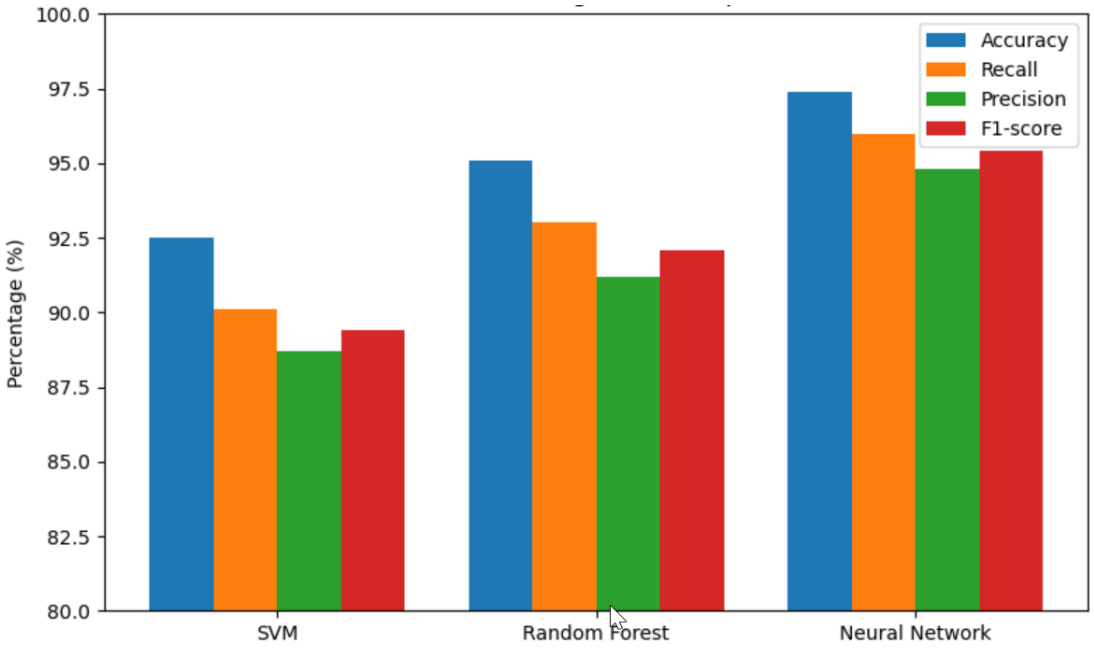

Figure 4: Machine Learning Model Comparison

This indirectly supports our conclusion that deep learning has a stronger capability to capture anomalous patterns than traditional machine learning, even on different types of network data. At the same time, the effectiveness of wavelet transform as a front-end feature extraction method is also validated [3, 5, 15] – if one trains the same models using only raw traffic statistical features, the performance is markedly lower (in our control experiment, the NN's accuracy was only around 90%), which highlights the importance of time-frequency domain features.

To further understand the models' decisions, we analyzed the feature importance output of the Random Forest [8]. The results show that for the RF, certain specific frequency-band energy ratios were key to distinguishing attacks. For example, in our wavelet decomposition, the energy ratio at the 3rd detail level was significantly higher in ransomware (infiltration) traffic than in normal traffic, and this feature ranked among the top in RF's importance. This possibly corresponds to a segment of high-frequency jittery traffic generated when ransomware transmits encryption keys or certificates [1]. Similarly, the overall wavelet entropy was one of the important indicators: a normal user's long connection usually exhibits a relatively stable traffic pattern with lower entropy, whereas attack traffic (such as botnet C2 communication) often pads random meaningless packets to obscure itself, causing the spectral entropy to increase [15]. These observations are in line with prior findings from other domains (like audio and biomedical signals) – that wavelet-derived features can provide interpretable insights for pattern recognition across different types of signals.

Our study has demonstrated the feasibility and effectiveness of combining wavelet transform with machine learning for malicious traffic and ransomware detection [3, 5, 15]. Through visual analysis, we are able to clearly see the anomaly characteristics on the wavelet time-frequency plots: a normal traffic spectrogram shows a relatively smooth background, whereas when a malicious attack begins, localized high-energy frequency bands appear at specific times [5]. These differences enable the classification model to accurately learn the distinguishing patterns. Therefore, our framework is effective not only against known attacks but also offers potential early warning capability for unknown zero-day attacks.

5. CONCLUSION

In this study, a malware traffic and ransomware anomaly detection framework using wavelet time-frequency analysis combined with machine learning is proposed. By converting network traffic into the time-frequency domain using wavelet transform, it is possible to extract spectral features that capture the temporal and frequency characteristics of the traffic. These features include energy distribution across scales, spectral entropy, and extreme coefficients, which are used to train classification models to distinguish between normal and malicious traffic. Experiments conducted on the CICIDS2017 dataset [12], show that wavelet-derived features significantly improve the anomaly detection performance compared to using raw traffic features alone. The neural network classifier achieves the highest accuracy (~97%, high recall), effectively detecting almost all malicious flows while keeping the false positive rate low. This level of performance is comparable to or better than the state-of-the-art results on similar tasks in the literature [7, 9–11, 14, 15, 17]. The proposed method is not only effective for known attack patterns in the training data, but also shows the potential to detect new types of attacks [15]. Time-frequency analysis enables the model to identify structural anomalies in traffic (e.g., sudden bursts or unusual frequency content) that may indicate the presence of a zero-day vulnerability or a new ransomware strain. Wavelet transforms provide

visual and interpretable insights into traffic behavior, which can help analysts understand alerts [11, 15]. The main advantages of the approach studied in this paper include its generality (the method does not rely on payload signatures, only on traffic patterns) and its extensibility (additional features or different wavelets can be incorporated to improve the detection of specific threats). It is worth noting that this approach is feasible for immediate deployment [5]. This study processed streams after capture, but the algorithm can be applied to streaming data. Future work will explore the implementation of wavelet transform and feature extraction in an online manner, so that the system can issue an instant alert when traffic arrives. Some recent systems [5, 24], have taken steps in this direction by embedding wavelet analysis into real-time network monitoring. This research plans to extend the framework to multi-class classification so that once an anomaly is detected, the system can further classify it into a specific attack category (e.g., ransomware vs. other malware). Initial insights, such as the unique wavelet signature patterns of exfiltration-type attacks [1, 15], suggest that multi-class wavelet-based detection is a promising next step. Techniques such as hierarchical classification or one-to-many models can be employed to maintain high accuracy across multiple attack types. This work confirms the potential of wavelet time-frequency analysis as a powerful tool in the cybersecurity arsenal [3, 5, 15]. By integrating signal processing with deep learning, a highly accurate and adaptable malicious traffic detection mechanism is achieved. This approach is particularly useful for detecting ransomware and other stealthy attacks that may not have a known signature but exhibit unusual behavior in network traffic [1, 13]. As cyber threats continue to evolve, this hybrid analytical approach—leveraging the interpretability of domain-specific features and the benefits of modern machine learning—will play a critical role in enhancing cybersecurity.

References

[1] Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference. Springer International Publishing. 2015:3-24.

[2] Huang CT, Thareja S, Shin YJ. Wavelet-Based Real Time Detection of Network Traffic Anomalies. Int J Netw Secur. 2008;6:309-320.

[3] Zhan Y. A Wavelet Kernel-Based Support Vector Machine for Communication Network Intrusion Detection. Adv Mater Res. 2014;989:4474-4477.

[4] Hamid Y, Shah FA, Sugumaran M. Wavelet neural network model for network intrusion detection system. Int j inf tecnol. 2019;11:251–263.

[5] Bozdal M, Samie M, Jennions IK. WINDS: A Wavelet-Based Intrusion Detection System For CAN. IEEE Internet Things J. 2021;9:58621-58633.

[6] Vinayakumar R, Alazab M, Soman KP, Srinivasan S, Venkatraman S, et al. Deep learning for cyber security applications: A comprehensive survey. Authorea Preprints. 2021. TechRxiv Preprint: https://www.techrxiv.org/doi/full/10.36227/techrxiv.16748161.v1

[7] Shone N, Ngoc TN, Phai VD, Shi Q. A Deep Learning Approach to Network Intrusion Detection. IEEE Trans Emerg Top Comput Intell. 2018;2:41-50.

[8] Buczak AL, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Commun Surv Tutor. 2016;18:1153-1176.

[9] Hussain A, Saadia A, Alhussein M, Gul A, Aurangzeb K. Enhancing Ransomware Defense: Deep Learning-Based Detection and Family-Wise Classification of Evolving Threats. PeerJ Comput Sci. 2024;10:e2546.

[10] Singh A, Mushtaq Z, Abosaq HA, Mursal SN, Irfan M, et. al. Enhancing Ransomware Attack Detection Using Transfer Learning and Deep Learning Ensemble Models on Cloud-Encrypted Data. Electronics. 2023;12:3899.

[11] Gulmez S, Gorgulu Kakisim A, Sogukpinar I. XRan: Explainable Deep Learning-Based Ransomware Detection Using Dynamic Analysis. Comput Secur. 2024;139:103703.

[12] Sharafaldin I, Habibi Lashkari A, Ghorbani AA. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy. 2018:108-116.

[13] Rigaki M, Garcia S. Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection. In: Proceedings of the IEEE secur priv workshops (SPW). IEEE. 2018:70-75.

[14] Vinayakumar R, Soman KP, Poornachandran P. A Deep Learning Framework for Cybersecurity Intrusion Detection Systems. IEEE Access. 2019;7:41525-41550.

[15] Purohit R, Kumar S, Sayyad S, Kotecha K. Time-Frequency Analysis and Autoencoder Approach for Network Traffic Anomaly Detection. MethodsX. 2025;14:103228.

[16] Wang W, Ming Zhu, Xuewen Zeng, Xiaozhou Ye, Yiqiang Sheng. Malware Traffic Classification Using Convolutional Neural Network for Representation Learning. In: Int Conf Inf Netw (ICOIN). 2017:712-717.

[17] Bella K, Guezzaz A, Benkirane S, Azrour M, Fouad Y, et al. An efficient intrusion detection system for IoT security using CNN decision forest. PeerJ Comput Sci. 2024;10:e2290.

[18] Yin C, Zhu Y, Fei J, He X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access. 2017;5:21954-21961.

[19] Chen W, Bao C, Gao Y. SDN Anomaly Detection Method Based on Bidirectional LSTM. J Inf Secur. 2023;9:56-65.

[20] Liang P, Yang L, Xiong Z, Zhang X, Liu G. Multilevel Intrusion Detection Based on Transformer and Wavelet Transform for IoT Data Security. IEEE Internet Things J. 2024;11:25613-25624.

[21] Abd Elkhalik W, Elhenawy I. Semi-supervised transformer network for anomaly detection in cellular Internet of Things. Int J Wirel Ad Hoc Commun. 2022;4:56-68.

[22] Kritika K. A Comprehensive Literature Review on Ransomware Detection Using Deep Learning. Cyber Secur Appl. 2024:100078.

[23] Gazzan M, Sheldon FT. Novel Ransomware Detection Exploiting Uncertainty and Calibration Quality Measures Using Deep Learning. Information. 2024;15:262.

[24] Mirsky Y, Doitshman T, Elovici Y, Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. In Proc. 25th Netw. Distrib. Syst. Secur. Symp. (NDSS). 2018.