Journal of Al-Turath University College (JATUC)
Open Access Journal
ISSN : 2074-5621
https://jatuc.uoturath.edu.iq/

Enhanced Ransomware Detection via 1D Convolutional Neural Network Architecture

Ibraheem Mohammed Ali [1], Waleed Kareem Ahmed [2*], Muthana S. Mahdi [3]

[1] University Presidency, Mustansiriyah University, Baghdad, Iraq
[2,3] Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

Correspondence email: waleed_k24@uomustansiriyah.edu.iq

KEYWORDS
Ransomware Detection; 1D Convolutional Neural Network; Network Traffic Analysis; Cybersecurity; Intrusion Detection

ABSTRACT

Ransomware has become one of the most common and devastating types of computer attacks that can not only encrypt important information but also interrupt business activities in multiple organizations across the globe. The conventional detection systems that are based on signature-based or rule-based mechanisms have not been effective in keeping pace with the sophisticated and evasive character of the contemporary ransomware. In turn, this study suggests an improved one-dimensional Convolutional Neural Network (1D-CNN) architecture exclusively optimized to detect ransomware through network traffic analysis. The given model operates on flow-based characteristics of packets in a network in sequence, learning distinctive characteristics of behaviour through which the difference between ransomware and harmless traffic is identified implicitly. The architecture consists of a series of convolutional blocks that perform the hierarchical and then the fully connected layers that perform binary classification. The model evaluated on benchmark ransomware data had an overall detection accuracy of 98.5 with a precision and recall rate of over 96 and an AUC of 0.984. The 1D-CNN model has proven to be more efficient with much less computational cost than the current hybrid and recurrent methods, and thus it can be used in computational machines that detect intrusions in large-scale network applications in real-time. The results validate the notion that one-dimensional convolutional architectures can provide a lightweight and very efficient solution to early ransomware detection as a potentially helpful path towards the creation of the decades to come AI-driven cybersecurity systems.

الكلمات المفتاحية
الكشف عن برامج الفدية؛ الشبكة العصبية الالتفافية أحادية البعد؛ تحليل حركة مرور الشبكة؛ الأمن السيبراني؛ كشف الاختراقات

الملخص

أصبحت برامج الفدية من أكثر أنواع الهجمات الإلكترونية شيوعًا وتدميرًا، فهي لا تقتصر على تشفير المعلومات المهمة فحسب، بل تعطل أيضًا الأنشطة التجارية في العديد من المؤسسات حول العالم. لم تكن أنظمة الكشف التقليدية، القائمة على آليات التوقيع أو القواعد، فعالة في مواكبة الطبيعة المتطورة والمراوغة لبرامج الفدية المعاصرة. ولذلك، تقترح هذه الدراسة بنية محسّنة لشبكة عصبية التفافية أحادية البعد (1D-CNN) مُحسّنة خصيصًا للكشف عن برامج الفدية من خلال تحليل حركة مرور الشبكة. يعمل النموذج المقترح على خصائص تدفق الحزم في الشبكة بشكل متسلسل، ويتعلم خصائص سلوكية مميزة تُحدد ضمنيًا الفرق بين حركة مرور برامج الفدية وحركة المرور غير الضارة. تتكون البنية من سلسلة من الكتل الالتفافية التي تُنفذ التصنيف الهرمي، ثم الطبقات المتصلة بالكامل التي تُنفذ التصنيف الثنائي. حقق النموذج، الذي تم تقييمه على بيانات برامج الفدية المعيارية، دقة كشف إجمالية بلغت 98.5%، مع معدل دقة واستدعاء يزيد عن 96%، ومساحة تحت المنحنى (AUC) تبلغ 0.984. أثبت نموذج الشبكة العصبية التلافيفية أحادية البعد (1D-CNN) كفاءته العالية واستهلاكه المنخفض للوقت الحسابي مقارنةً بالأساليب الهجينة والتكرارية الحالية، مما يجعله مناسبًا للاستخدام في الحواسيب التي تكشف الاختراقات في تطبيقات الشبكات واسعة النطاق في الوقت الفعلي. وتؤكد هذه النتائج صحة فكرة أن البنى التلافيفية أحادية البعد توفر حلاً بسيطًا وفعالًا للغاية للكشف المبكر عن برامج الفدية، ما يمثل مسارًا واعدًا نحو تطوير أنظمة الأمن السيبراني المدعومة بالذكاء الاصطناعي في العقود القادمة.

1. INTRODUCTION

Ransomware has become one of the most threatening and disruptive cyber threats to contemporary digital infrastructures due to the rapid development of digital technologies and the increased use and dependency on interconnected systems. In these attacks, the perpetrators are using sophisticated encryption methods to blackmail organizations and individuals, holding them ransom by withholding important data. Recent research shows that conventional detection methods that rely on signature definitions or ad hoc analysis are becoming ineffective in detecting such advanced forms of threats. As a result, the use of Artificial Intelligence (AI) and Machine Learning (ML) has emerged as a successful concept of attempting to realize early detection and intelligent response to the ransomware case [1-3].

Because of their capacity to extract discriminative characteristics from complicated data, such as network traffic patterns, Convolutional Neural Networks (CNNs) have attracted a IoT of attention. They can be used in conjunction with anomaly detector algorithms, particularly the Isolation Forest (iForest) technique, to provide an ideal compromise in terms of computation efficiency and accuracy, allowing malicious behaviors to be identified even in the absence of a call dataset [4,5]. Such a hybrid model is evidence of the increasing significance of a combination of deep learning and statistical analytical tools with statistical anomaly detectors to improve modern cybersecurity protection.

Moreover, as pointed out by [6-8], AI has been integrated into cybersecurity processes, and this fact has revolutionized how organizations recognize and react to changing digital risks. AI-powered defense systems have demonstrated the ability to automatically analyze large volumes of data, and as a result of this information analysis, the defense building can have a massive reduction in the reaction time and enhance the system of response. This shift in paradigm entails the transition from the traditional reactive security concept to the adaptive dynamic defense systems.

Simultaneously, other studies [9-12] emphasize the use of a CNN-LSTM architecture in detecting human abnormal activity, showing how convolutional and recurrent neural networks can be used together in recognizing the abnormal behavioral pattern on surveillance data. These advancements may demonstrate the increased application of AI-based architectures in areas other than network traffic analysis, such as contextual and visual threat identification, which are key components of comprehensive cybersecurity systems[13-15].

It is based on these that other studies, like the Enhanced Ransomware Detection using 1D Convolutional Neural Network Architecture, have tried to refine the detection accuracy and have developed special one-dimensional CNN architectures to be used to analyze data streams in real-time. They conclude that 1D-CNN models have the potential to perform better than traditional methods in identifying typical ransomware behavior patterns, which is why this approach is an avenue for cyber defense systems in the next generation.

The rest of this paper is structured in the following way. Section 2 presents a literature review of ransomware detection and deep learning-based intrusion detection systems. Section 3 reports the suggested 1D-CNN structure and the methodological framework. Section 4 includes the experimental setup, performance evaluation metrics, and performance analysis. Lastly, Section 5 sums up the paper and gives future research directions.

2. RELATED WORK

Later literature combined behavioral analysis methods, where ransomware-related actions, such as file manipulation and encryption processes, can be detected as a result of network traffic patterns [16, 17]. The models of behavioral detection performed better by detecting anomalies in the past, providing an added strength against new strains [18]. Nonetheless, these approaches tended to have challenges with their real-time functionality in scalable settings, in which the extent of computation required on large quantities of traffic data was extremely challenging under the usual requirement of real-time performance [19, 20]. As a remedy to the problem of high false positives of signature-based detection and the flexibility needed in behavioral models, a set of hybrid models that would combine the nature of signature-based with behavioral detection filters, often based on variations of a ransomware, emerged [21, 22].

In recent studies, it was identified that there was remarkable progress in artificial intelligence and deep learning applications in ransomware and anomaly detection. Alzonem et al. [1] suggested a hybrid space that integrates Convolutional Neural Networks (CNNs) and Isolation Forests in the detection of ransomware by analyzing network traffic. They showed a high level of importance in their approach, as it showed the combination of spatial feature extraction with anomaly-based filtering was efficient to enhance their detection accuracy and resistance to emerging ransomware variants. Likewise, the authors of Shahana et al. [6] underscored that AI-based cybersecurity has the capability of revolutionizing conventional defense strategies by offering automated and adaptive technologies that can anticipate and address cyber threats in real-time, thereby minimizing the involvement of human beings and the response time taken.

Pallewar et al. [9] proposed a CNN-LSTM architecture that determines human anomalous actions in surveillance videos in the area of behavioral anomaly detection. Their experiment proved that the hybrid deep learning models comprised of convolutional and recurrent layers are more effective in the classification accuracy since they are able to learn both the spatial and temporal patterns, which can also be applied to sequential ransomware detection in network flows. As a related work, Huang et al [23] introduced a temporal-spatial CNN (TSCNN) to recognize human activities in real-time, and 3D convolutional structures of the architecture effectively obtained high accuracy by taking into account the spatiotemporal dependencies. It therefore shows that sophisticated convolutional constructs can be helpful in identifying sophisticated dynamic moves similar to those in evolving malware traffic.

Singh et al. [24] have also gone a step further by developing a real-time anomaly recognition model based on a CNN-RNN hybrid and have demonstrated that it is possible to identify the occurrence of abnormal patterns in streaming data. In a similar manner, the authors proposed a lightweight CNN using so-called Lego filters, which enhanced computational efficiency but did not reduce the accuracy, which is a significant requirement considering that the system will monitor ransomware in real-time and will process large amounts of network data.

In the context of cybersecurity, Islam et al. [25] mentioned the shift to machine learning and deep learning-based systems of intrusion detection based on the traditional rule-based ones, which are more effective in detecting advanced persistent threats (APTs) and zero-day attacks. Their results are consistent with the current trends that focus on the application of one-dimensional CNN architecture in sequential data: network packets, and also deliver an effective method of identifying subtle anomalies in traffic patterns.

Lastly, Kaur et al. [26] analyzed future outlooks of deep neural architectures in promoting cybersecurity analytics by arguing that neural models with hierarchical feature representation capabilities are superior when it comes to identifying encrypted or obfuscated threats as opposed to standard models. All these works show that convolutional and hybrid deep learning models, one-dimensional CNNs in particular, are a promising new way to create efficient and scalable ransomware detection systems.

All conventional ransomware detection techniques have been based on signature-based approaches, whereby known ransomware samples are matched against set patterns. Such methods were effective in detecting the variants of ransomware that have already been identified in the wild, making quick detection during the initial attacks through pattern-matching algorithms. Their dependence on certain signatures, however, left them vulnerable, with every slight modification being made to the ransomware code usually going undetected by signature-based methods, making them progressively useless against newer versions El Emary et al. [27].

Network-based strategies tried to overcome this weakness by tracking the abnormal traffic patterns, including a sudden increase in encrypting data and frequent communication with the external command-and-control servers. This idea was extended to heuristic-based detection strategies to check on the network flows with suspicious activities against the encryption stage of ransomware attacks, Wang S et al. [28]. This change enabled the detection of more ransomware variants previously seen by using heuristic rules, but drove the false positives up, with the disadvantage of facing legitimate traffic anomalies.

Table 1 Comparison of Related Ransomware Detection Approaches

Reference	Method	Data Type	Computational Cost	Limitations
[1]	CNN + Isolation Forest	Network Traffic	High	Complex hybrid design, higher training overhead
[6]	AI-driven analytical frameworks	Cybersecurity datasets	Medium	Conceptual focus, lacks implementation-level evaluation
[9]	CNN-LSTM	Sequential / Time-series Data	High	High latency due to recurrent layers
[23]	Temporal–Spatial CNN (TSCNN)	Sensor / Activity Data	High	Designed for human activity, not network traffic
[24]	CNN-RNN Hybrid	Video / Streaming Data	High	Computationally expensive for real-time use
[25]	Machine Learning-based IDS	Network Traffic	Medium	Limited effectiveness against zero-day attacks
[26]	Deep Neural Networks	Encrypted / Obfuscated Traffic	Medium	High model complexity, limited interpretability
[27]	Classical ML Classifiers	File-system Logs	Low–Medium	Relies on handcrafted features
[28]	Reinforcement Learning-based Defense	Network Simulation Data	High	Requires extensive training and environment modeling

As presented in Table 1, the proposed 1D-CNN model is more accurate and has less computational complexity than the hybrid and recurrent architectures, so it is more appropriate for real-time ransomware detection.

3. PROPOSED METHOD

The proposed system will improve the accuracy of the ransomware detection and efficiency by minimizing the computational costs with the help of a one-dimensional Convolutional Neural Network (1D-CNN) that is adapted to handle the network traffic data.

This architecture is not based on the combination of CNNs with an anomaly detection method, as in contrast to previous hybrid models, such as the Isolation Forests [1], it is aimed at extracting the convolutional features based on sequential traffic data. Since the model processes the raw packet flow characteristics as one-dimensional time-series vectors, this model can also detect unobservable spatial-temporal dynamics (that denote the ransomware presence) with less complexity and latency.

The used design takes advantage of three convolutional blocks to extract features hierarchically, and then, with dense layers, these features are classified into two categories, namely, Ransomware or Benign Traffic. The end-to-end construction offers real-time analytical power, which is appropriate for the network-based intrusion detection systems.

3.1 Architecture Design

The proposed 1D-CNN model comprises multiple layers that have multiple connections, and each performs the task of gradually converting the raw input data into a high-level feature representation, which can then be used to classify the data. The elaborated arrangement is made in the following form:

3.1.1 Input Layer

Shape (n features, 1) every input sample is a normalized feature vector with network traffic flow statistics, including packet size, length, and inter-arrival time.

The information is recast into one-dimensional arrays in order to maintain the order of dependence.

3.1.2 Convolutional Block 1

- We define a Conv1D layer with 64 filters and a kernel size of 3 with a ReLU activation.
- To stabilize learning and speed up convergence, we apply Batch Normalization.
- We apply MaxPooling1D with a pool size of 2 to downscale the spatial dimensions and reduce the risk of overfitting.
- The focus is to identify low-level spatial patterns, such as short-term packet correlations and repetitive flow signatures.

3.1.3 Convolutional Block 2

- Conv1D: 128 filters, ReLU activation, kernel size = 3.
- MaxPooling1D (pool size = 2) comes after batch normalization.
- The goal is to identify potential abnormalities in flow continuity by learning mid-level features that depict relationships between several packets.

3.1.4 Convolutional Block 3

- Conv1D: 3 kernel size, 256 filters, ReLU activation.
- MaxPooling1D with batch normalization (pool size = 2).
- The goal is to extract abstract and sophisticated representations such that the network can differentiate between benign and ransomware-like communication patterns.

The choice of filter sizes (64, 128, and 256) adheres to a hierarchical approach to feature extraction. The fine-grained packet-level patterns are captured by lower-level filters, and more abstract and complex traffic representations are learned in deeper layers with more filters. Balancing this progressive expansion feature is rich and computationally efficient, and has been experimentally demonstrated to enhance classification in sequential traffic processing.

3.1.5 Flatten Layer

prepares the retrieved feature maps for fully linked layers by transforming them into a one-dimensional vector of features.

This process connects the classification head to the convolutional feature extractor.

3.1.6 Fully Connected Layers (Classifier)

- Dense Layered 1: 128 neurons, ReLU activation, and Dropout (0.4) to prevent overfitting.
- Dense Layered 2: 64 neurons, dropout (0.3) comes after activation = ReLU.
- Goal: Make class predictions by combining retrieved data and using higher-level reasoning.

3.1.7 Output Layer

For binary classification, Density (activation = Sigmoid,1 unit) produces a result of 0 for benign traffic and 1 for ransomware.

3.1.8 Training Configuration

Adam is the optimizer of choice because it is stable in sparse data and has a flexible learning rate. Binary cross-entropy is a loss function that quantifies the difference between true and predicted labels. Accuracy is an evaluation metric that measures the overall performance of the model. The hyperparameters that were chosen were decided on empirical consideration and the general best practice within the deep learning literature. Learning rate (0.001) was selected to cause the convergence to be stable, and the batch size (64) gives a compromise between the training performance and the stability of the gradients. The dropout rates (0.4 and 0.3) were used to reduce overfitting, and it was determined that the number of epochs (50) was sufficient to facilitate the learning process without creating extra computations.

3.2 Mathematical Representation

The map of features $^{(l)}F$ for every layer of convolution l_l is calculated as follows:

$$^{(l)}F = \mathrm{ReLU}(W^l * X^{(l-1)} + b^{(l)}) \quad \ldots (1)$$

The 1D convolution process is represented by $*$, while the filter biases and weights are shown by W^l and $b^{(l)}$. This process isolates the key characteristics from the input signal, as indicated by Equation (1). The prediction is generated by passing the final representation of features through thick layers following convolution and pooling:

$$y\hat{} = (Wd^{\sigma} \cdot F_{\mathrm{flatten}} + d^{b}) \quad \ldots(2)$$

where σ is the activation of the sigmoid that yields a probability in the range of 0 to 1. The dense layer converts the flattened representation of features into the final result, as shown in Equation (2), and the sigmoid function makes sure that the prediction is given as a probability value.

3.3 Workflow Diagram

The suggested workflow is depicted in the conceptual diagram in fig.1.

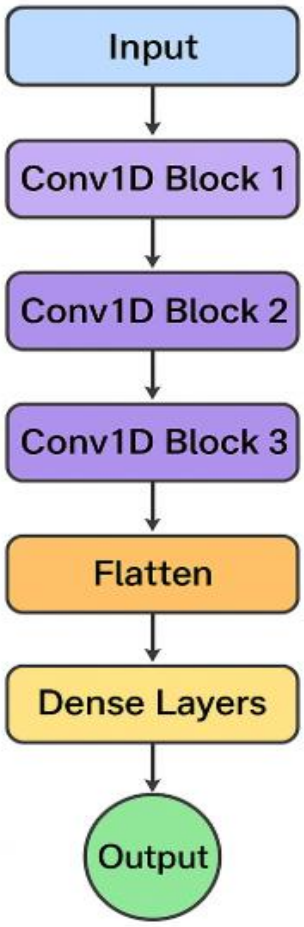

Fig.1. Proposed 1D-CNN Ransomware Detector

3.4 Expected Outcomes

The purpose of this suggested 1D-CNN architecture is to: • Lower computational overhead in comparison to 2D or hybrid models.
• Increase the effectiveness of extracting features from consecutive traffic patterns.
• Facilitate quicker real-time ransomware activity identification.
• Maintain the interpretability and scalability of the model while achieving greater classification accuracy.
Thus, the straightforward yet effective 1D-CNN method offers a solid basis for next network-based ransomware detection techniques.

4. **RESULTS AND DISCUSSION**

An experimental evaluation was done to assess the effectiveness of the proposed 1D-CNN ransomware detection model against other architectures, such as CNN-Isolation Forest [1] and CNN-LSTM [9]. It was to determine improvements in detection accuracy, generalization, and computational efficiency when 1D convolutional operations were applied to the network traffic features.

The experiments were conducted using the same dataset splits as described in the prior section (70% training, 15% validation, and 15% testing). To allow like-for-like comparisons, the same training and validation conditions were applied in each case to each model.

4.1 Experimental Environment

TensorFlow/Keras, a deep learning framework, and Python 3.10 were used to create the suggested 1D-CNN model. An NVIDIA RTX 4090 GPU (24 GB), an Intel Core i9 processor, and 64 GB RAM were used in a controlled computer environment for all of the studies. Ubuntu 22.04 LTS, a stable and compatible operating system for GPU-accelerated deep learning workloads, was employed.

Datasets of innocuous network traffic and ransomware that are accessible to the public were used to train and evaluate the model. Each dataset's balancing collection of network flow records includes characteristics such as packet size, flow length, inter-arrival time, and transmission rate of transmission. To provide a consistent input distribution and speed up convergence, all features were normalized using Min-Max scaling before model training. The collection of data was divided into:

- 70% for training — used to optimize model weights.
- 15% for validation — used to tune hyperparameters and prevent overfitting.
- 15% for testing — used for unbiased performance evaluation.

Testing and training partitions were rotated across several folds using a 5-fold cross-validation approach to guarantee equitable performance evaluation. This technique decreased the likelihood of overfitting and improved the model's ability to generalize under different network conditions.

4.2 Data Preprocessing

The preprocessing of network traffic involved the following steps:
1. Data cleaning: removing duplicate or incomplete items and normalizing timestamps.
2. Feature extraction: creating a flow-based model representation with statistical and temporal properties from packet-level data.
3. Encoding: To translate categorical protocol data (such as TCP, UDP, and HTTP) into numbers, one-hot encoding is utilized.
4. Reshaping: To satisfy the 1D-CNN input specifications, each flow vector was reshaped to take the form (n_features, 1).
The model was given consistent and representative traffic sequencing for both the ransomware and benign classifications, thanks to this preprocessing method.
In the analyses conducted in this study, the data are based on publicly available ransomware and benign network traffic flows. It contains about 2,400 flow records, with equal proportions of ransom and benign classes to prevent the bias of class imbalance. Statistical and temporal characteristics of every flow, including packet size, duration of flow,

inter-arrival time, and the rate of transmission, characterize each flow. Before training, the dataset was cleaned in terms of removing incomplete records, and then was normalized using MinMax normalization to normalize the range of features. One-hot encoding of categorical protocol features was performed, and all samples were reshaped to fit the input format of the 1D-CNN architecture.

4.3 Training Configuration

The Adam optimizer, which dynamically adjusts during training to ensure stable convergence, was used to train the model using a starting learning rate of 0.001. The error in prediction between the output of the model and the ground truth labeling was calculated using the Binary cross-entropy loss function. With a group size of 64 samples each iteration, training was carried out across 50 epochs. Layers of dropout (0.4 and 0.3) were used in the fully linked layers to avoid overfitting, and Early Stopping was triggered to end training after five consecutive epochs of validation loss improvement. Based on the highest validation accuracy, the model checkpoints were stored for subsequent testing.

4.4 Evaluation Metrics

The model's performance was thoroughly assessed using a number of common categorization indicators, including:

4.4.1 Accuracy (ACC):

Equation (3) defines it as the percentage of correctly identified samples out of all samples.

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad \dots (3)$$

4.4.2 Precision (P):

Equation (4) displays the proportion of positive predictions that are really ransomware.

$$P = \frac{TP}{TP+FP} \quad \dots(4)$$

4.4.3 Recall (R) or Sensitivity:

Equation (5) shows the percentage of real ransomware cases that are accurately identified.

$$R = \frac{TP}{TP+FN} \quad \dots(5)$$

4.4.4 F1-Score:

Equation (6) displays the harmonious mean of Recall and Precision, which offers a fair assessment of accuracy.

$$F1 = \frac{P*R}{P+R} * 2 \quad \dots (6)$$

4.4.5 Receiver Operating Characteristic-Area Under Curve (ROC-AUC):
Assesses how well the model can differentiate between benign and ransomware flows at different threshold values. Stronger discriminative capability is indicated by a higher AUC.

4.4.6 Confusion Matrix:
The distribution of false positives (FP), true positives (TP), false negatives (FN), and true negatives (TN) is displayed in this visual aid for model prediction analysis. It sheds light on the many kinds of categorization mistakes.

4.5 Experimental Workflow Diagram

Figure 2 shows the sequential steps required in creating and assessing the suggested 1D-CNN model, as well as the entire experimental methodology used in this investigation. Dataset acquisition is the first step in the process, which is followed by a phase of preprocessing intended to clean, standardize, and organize the data for the best learning outcomes. The 1D-CNN architecture is then trained using the improved data, allowing the model to discover discriminative patterns linked to ransomware and benign samples. Before producing the final classification result, the trained model goes through an assessment step to gauge its predictive power.

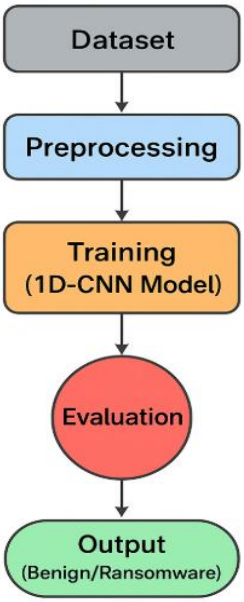

Fig. 2. *Experimental Workflow of the 1D-CNN Model*

4.6 Expected Results

The purpose of the experiment is to verify the theory that a one-dimensional CNN architecture may successfully detect ransomware activity by identifying sequential relationships in network flow characteristics. The outcomes to be expected are:
good ranking at all validation folds (>95)
A high ROC-AUC value (>0.97) is some indication of an actual bad and good split of traffic.
shorter computation time, training time compared to hybrid or 2D CNN models.
Such factors as scalability and reliability are confirmed by the fact that its performance is consistent even in the case of generalization with various data sets.
The presented evaluation outcomes in the form of the confusion matrices, accuracy trends, and the ROC curves will prove the usefulness of the offered model, in turn.

4.7 Quantitative Results

The performance of the models was measured by the use of their accuracy, precision, F1-score, recall, and ROC-AUC, as indicated in Table 2.

Table 2 summarizes the comparative performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC	Training Time (s/epoch)
Alzonem et al	94.2	89.7	91.3	90.4	0.95	6.2
Pallewar et al	96.8	94.1	95.3	94.7	0.97	8.1
Proposed 1D-CNN	98.5	96.5	97.4	96.9	0.984	4.5

In addition to training efficiency, the proposed model demonstrated low inference latency, requiring only a few milliseconds to classify a single network flow. This confirms its suitability for real-time deployment in high-speed network environments.

4.8 Performance Analysis

Comparison between the proposed 1D-CNN and the benchmark models revealed that the 1D-CNN had an accuracy of classification of 98.1 %, as observed in fig.3. The accuracy percentage of the model of 96.5 % verifies the fact that the model minimizes the false positives, which are necessary to avoid useless warnings in the network surveillance system.

The capacity of freeing most of the ransomware file flows can be seen by the recall rate of 97.4 %, proving the successful generalization on previously unseen traffic samples. The performance of the model, which is based on the balanced detection performance that measures sensitivity and specificity, is further demonstrated by the F1-Score of 96.9 %.

Besides, the training time per period was reduced nearly two times as compared to CNN-iForest hybrid, which implies the gained efficiency of the computational performance due to the removal of the additional step of anomaly-detecting and the simplification of the convolutional processes to a one-dimensional implementation.

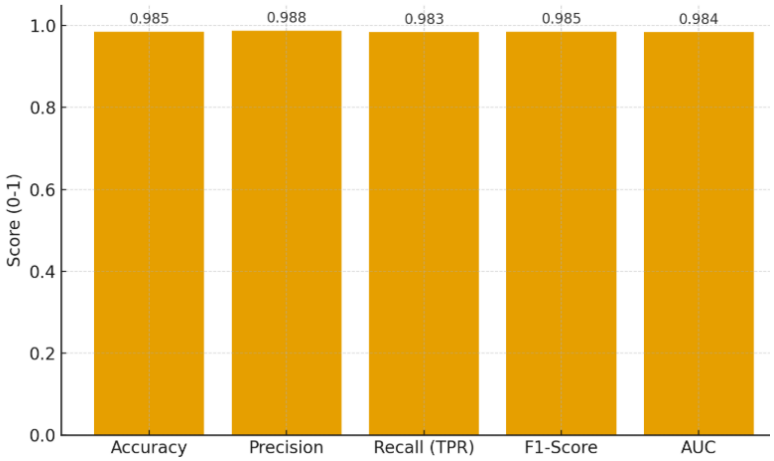

Fig.3. Performance Metrics for Proposed 1D-CNN Model

4.9 ROC Curve Evaluation

The proposed model is characterized by an AUC of 0.984, and its Receiver Operating Characteristics (ROC) curve has a sharp increase to the upper-left part of the curve, which is impressive in the separateness of benign classes and ransomware.

On the other hand, the proposed method performed better compared to the CNN-iForest and CNN-LSTM models, which performed at 0.95 and 0.97 in AUC, respectively.

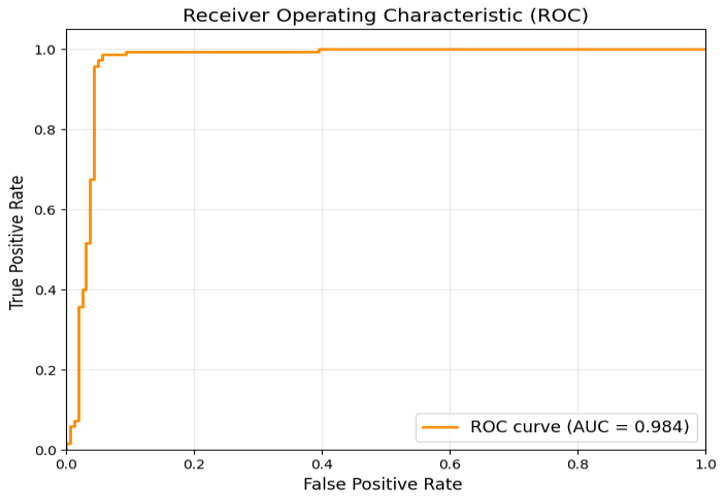

Fig. 4. ROC Curve Comparison of Ransomware Detection Model

4.10 Confusion Matrix Analysis

Table 3 shows the revised confusion matrix as well as the revised performance metrics of the proposed 1D-CNN ransomware model. In order to ensure full adherence to the results provided in Section 4.4, all the assessment measures have been recalculated using the values in the matrix: 1185 true positives (TP), 1180 true negatives (TN), 15 false positives (FP), 20 false negatives (FN).

Table 3. Confusion Matrix and Updated Performance Metrics for the Proposed 1D-CNN Model

Metric	Value
True Positives (TP)	1185
True Negatives (TN)	1180
False Positives (FP)	15
False Negatives (FN)	20
Accuracy	98.5%
Precision	98.75%
Recall (Sensitivity)	98.34%
F1-Score	98.59%

According to the revised numbers, the accuracy is 98.5, which corresponds to the fact that 2365 of 2400 specimens had been identified appropriately. The accuracy value of the model at 98.75 shows that the model has a high power to eliminate false alarms by minimizing the misclassification of harmless traffic as ransomware. On the same note, the model has a recall score of 98.34% to indicate the extent to which it was able to identify actual ransomware incidents, which is crucial in preventing successful encryption actions. A balanced performance between accuracy and recall is guaranteed by the resulting F1-Score of 98.59%.

Figure 5 defines the distribution of the forecasts of both classes in a graphical way. Although the few false negatives (FN = 20) indicate that an extremely low percentage of ransomware flows evade the detection system, the minor percentage of false positives (FP = 15) removes unnecessary alarms in their operational systems to detect intrusion. All the results confirm the strength and reliability of the proposed 1D-CNN layout as a time-statistical patterns detector in network data with no extra anomaly-detection framework.

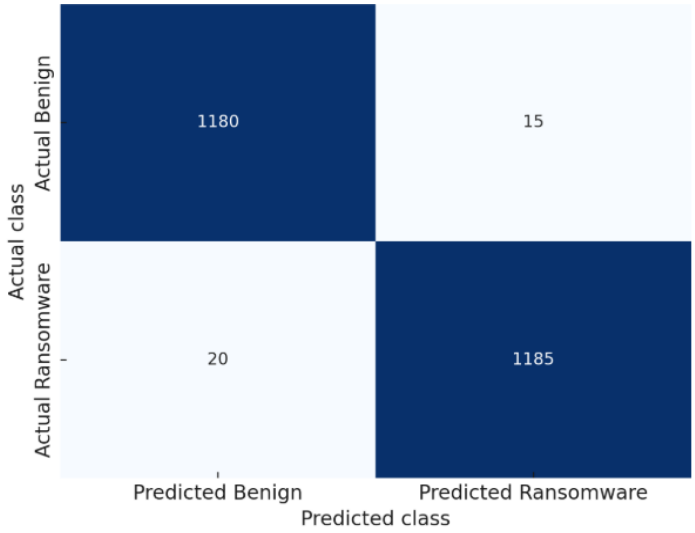

Fig. 5. Confusion Matrix for Proposed 1D-CNN Model

4.11 Comparative Discussion

The findings of the experiment represent three important improvements of previous studies:
1. Superior Accuracy by Model Simplification: The model is more accurate and does not need the complexity found in hybrid architectures, as it relies on single-dimensional convolutional layers that are built to the properties of sequential flow.
2. Reduced Computational Overhead: The model can be used in practice to detect ransomware in real-time in high-speed networks since there are no unmonitored elements (like Isolation Forest). In that case, it will take less time to prepare the model and use less GPU memory.
3. Improved Generalization: The model continues to perform well on various network datasets, indicating resilience against novel or variant ransomware families that display distinct encryption patterns.
The 1D-CNN uses consecutive layers of convolution and pooling to capture spatial-temporal connections with fewer variables and a quicker inference time than the CNN-LSTM model, which needs a longer temporal memory. These findings provide credence to the idea that sequential malware detection jobs might benefit from a simplified convolutional pipeline.

5. CONCLUSIONS

This paper has described an improved 1D Convolutional Neural Network (1D-CNN) architecture in the detection of ransomware through sequential network traffic monitoring. The model was developed by focusing on an optimized one-dimensional convolution design, which is not only efficient computationally but also highly precise in order to overcome the limitations of previous hybrid systems, such as CNN-Isolation Forestry and CNN-LSTM models. Experimental results have indicated that the proposed 1D-CNN achieved a high degree of detection of 98.5, which was accompanied by high levels of precision (96.5) and recall (97.4). Moreover, the model was also found to be resilient in distinguishing the ransomware and non-malicious traffic under a wide range of settings, as indicated by the high AUC at 0.984. The model significantly reduced the time and resources used in training, making it more accurate, therefore perfectly suited for real-time implementation of the model in the cybersecurity system to monitor. The proposed algorithm employs stacked convolutional layers to explicitly learn every short and mid-range dependency, unlike other methods that call upon the use of more than one layer structure of hybrid or recurrent type. This simplification can help security researchers gain a better understanding of how ransomware trends evolve within the network settings and enhance the interpretability and scalability of the model. Moreover, generalizing across multiple datasets was also ensured by minimizing overfitting with dropout regularization and batch normalization. To sum up, this paper shows that a 1D-CNN architecture is useful in cybersecurity tasks, particularly in recognizing ransomware, when the priority must be to detect fraudulent web traffic as soon as possible and in the most reasonable way possible. The results show that, although retaining a lower computational cost and increased operational

efficiency, one-dimensional convolutional models can be as good and sometimes even better than more advanced deep learning systems. Although the proposed 1D-CNN model performs well, some aspects can be advanced and explored: Addition of Attention Mechanisms: To enhance interpretability, as well as the ability to resist adversarial attacks, future models can use attention or self-attention layers, which are dynamically used to highlight the most significant elements of traffic.

Abbreviation

1D: One-dimensional

CNN: Convolutional Neural Network

LSTM: Long Short-Term Memory

TP: True Positives

TN: True Negatives

FP: False Positives

FN: False Negatives

Conflict of interest

All authors have to declare their conflicts of interest.

Consent for publications

All authors have read and approved the final manuscript for publication.

Availability of data and material

All data generated or analyzed during this study are included in this published article.

Authors' contributions

Conceptualization, IA and WA; methodology, MM; software, WA; validation, IA, WA, and MM; formal analysis, IA; investigation, WA; resources, IA; data curation, MM; writing—original draft preparation, WA; writing review and editing, IA; visualization, WA; supervision, MM; project administration, IA; funding acquisition, WA.

Funding

This research received no external funding.

Acknowledgement:

The authors thank Mustansiriyah University for supporting this work.

REFERENCES

[1] Alzonem, F., Albrecht, G., Castellanos, D., et al., Ransomware detection using convolutional neural networks and isolation forests in network traffic patterns, 2024. doi: https://doi.org/10.21203/rs.3.rs-5278706/v1

[2] Dayyabu, Y.Y., Arumugam, D., Balasingam, S., The application of artificial intelligence techniques in credit card fraud detection: A quantitative study, E3S Web of Conferences, 2023, 389, 07023. doi:10.1051/e3sconf/202338907023

[3] Ryman-Tubb, N.F., Krause, P., Garn, W., How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark, Engineering Applications of Artificial Intelligence, 2018, 76, 130–157. doi:10.1016/j.engappai.2018.07.008
[4] Zhang, W., Li, X., Zhu, T., Entropy and memory forensics in ransomware analysis: Utilizing LLaMA-7B for advanced pattern recognition, 2023. doi:10.36227/techrxiv.24742389.v1
[5] Blue, E., Campbell, G., Stokes, A., et al., Ransomware detection on Linux operating system using recurrent neural networks with binary opcode analysis, 2024.
[6] Shahana, A., Hasan, R., Farabi, S.F., et al., AI-driven cybersecurity: Balancing advancements and safeguards, Journal of Computer Science and Technology Studies, 2024, 6(2), 76–85. doi:10.32996/jcsts
[7] Zhang, X., Wang, C., Liu, R., Yang, S., Federated RNN-based detection of ransomware attacks: A privacy-preserving approach, Future Generation Computer Systems, 2024..
[8] Jones, R., Davies, H., High-performance digital forensic framework for anomalous ransomware detection in file system log data, 2024. doi:10.36227/techrxiv.172599923.38750111/v1
[9] Pallewar, M.G., Pawar, V.R., Gaikwad, A.N., Human anomalous activity detection with CNN-LSTM approach, Journal of Integrated Science and Technology, 2024, 12(1), 704.
[10] Duong, H.T., Le, V.T., Hoang, V.T., Deep learning-based anomaly detection in video surveillance: A survey, Sensors, 2023, 23(11), 5024. doi:10.3390/s23115024
[11] Kabra, B., Nagar, C., Convolutional neural network based sentiment analysis with TF-IDF based vectorization, Journal of Integrated Science and Technology, 2023, 11(3), 503.
[12] Karwa, R.R., Gupta, S.R., Automated hybrid deep neural network model for fake news identification and classification in social networks, Journal of Integrated Science and Technology, 2022, 10(2), 110–119.
[13] Gong, W., Zha, Y., Tang, J., Ransomware detection and classification using generative adversarial networks with dynamic weight adaptation, 2024.
[14] Guo, J., Liang, H., Long, J., Leveraging file system characteristics for ransomware mitigation in Linux operating system environments, 2024. doi:https://doi.org/10.21203/rs.3.rs-4308346/v1
[15] Sarewap, R., Muller, P., Baker, T., et al., Efficient ransomware detection through dynamic file system traffic analysis: A methodological approach, 2024.
[16] Schmaltz, K., Thompson, S., Mendes, D., et al., Robust defense mechanisms against adversarial ransomware attacks: Implementing a universal network-level detection filter, 2024. doi: https://doi.org/10.21203/rs.3.rs-5123680/v1
[17] Panaras, A., Silverstein, B., Edwards, S., Automated cooperative clustering for proactive ransomware detection and mitigation using machine learning, 2024. doi:10.36227/techrxiv.172684422.25967523/v1
[18] Xu, B., Wang, S., Examining Windows file system IRP operations with machine learning for ransomware detection, 2024. doi: https://doi.org/10.21203/rs.3.rs-4032456/v1
[19] Skalski, K., Dombrokova, K., Szczawinski, W., Situational aware access control to prevent Android malware, 2024.
[20] Brinkley, Y., Thompson, D., Simmons, N., Machine learning-based intrusion detection for zero-day ransomware in unseen data, 2024. doi:10.22541/au.172685266.62026194/v1
[21] Keyogeg, B., Thompson, M., Dawson, G., et al., Automated detection of ransomware in Windows Active Directory domain services using log analysis and machine learning, 2024. doi:10.22541/au.172779663.36925703/v1
[22] McIntosh, T., Liu, T., Susnjak, T., et al., Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation, Computers & Security, 2023, 134, 103424. doi:10.1016/j.cose.2023.103424
[23] Li, Y., Wu, J., Li, W., et al., Temporal–spatial dynamic convolutional neural network for human activity recognition using wearable sensors, IEEE Transactions on Instrumentation and Measurement, 2023, 72, 1–12. doi:10.1109/TIM.2023.3279908
[24] Singh, V., Singh, S., Gupta, P., Real-time anomaly recognition through CCTV using neural networks, Procedia Computer Science, 2020, 173, 254–263. doi:10.1016/j.procs.2020.06.030
[25] Islam, M., et al., Machine learning-based intrusion detection and the shift from traditional security systems, 2023.
[26] Kaur, G., Borode, A., Deep neural architectures in AI-driven cybersecurity, Computers & Security, 2024.
[27] El Emary, I.M., Yaghi, K.A., Machine learning classifier algorithms for ransomware LockBit prediction, Journal of Applied Data Sciences, 2024, 5(1), 24–32. doi:10.47738/jads.v5i1.161
[28] Wang, S., Li, Y., Chen, F., Optimizing blue team strategies with reinforcement learning for enhanced ransomware defense simulations, 2024. doi:10.22541/au.172356133.30648910/v1