

A Hybrid LSTM Autoencoder and Isolation Forest Framework for Anomaly-Based Ransomware Detection in Network Traffic

Qusay J. Shaheen^{1,*}, Esraa Saleh Alomari²

¹ Computer Department, College of Education for Pure Sciences, Wasit University, 52001 Al-Kut, Wasit, Iraq. [ORCID: 0009-0005-2362-1795]

² Computer Department, College of Education for Pure Sciences, Wasit University, 52001 Al-Kut, Wasit, Iraq [ORCID: 0000-0003-4281-8954]

Abstract

In this study, a novel anomaly detection-based hybrid model is realized for the prediction of ransomware attacks by monitoring network traffic. The signature or rule-based traditional approach to combating polymorphic ransomware and zero-day attack is under severe strain, especially in the presence of encrypted network traffic, that requires using more adaptive and flexible approaches that analyse behaviours. The proposed framework exploits temporal patterns of traffic by LSTM autoencoder and identifies statistically anomalous values with Isolation Forest. The outputs from the two models are then combined by a weighted merge mechanism to a final anomaly score to determine if traffic is benign or malicious. The proposed model was tested on an enhanced version of UGRansome_Dataset_2024 dataset having 111,904 records in unbalanced form, and balanced by SMOTE-ENN technique up to 149,197 records containing benign and malicious traffic. The simulation results demonstrate the superiority of the proposed model with 99.66% accuracy, 99.78% precision, 99.85% recall, 99.81% F1-score. These results demonstrate that the combined approach can effectively reduce false alarms, while the ability to detect attacks is significantly improved, and therefore can be used in practice networked environments.

Keywords: Ransomware Detection, Anomaly Detection, LSTM Autoencoder, Isolation Forest, Network Traffic, Hybrid Learning .

1. Introduction

Despite the qualitative leap brought about by the rapid spread of the internet in enhancing the mechanisms of human communication and facilitating the flow of information, at the same time it has created serious challenges related to cybersecurity [1] [2]. With the expansion of global digital connectivity, cybercriminals have taken advantage of the stealth advantage provided by virtual environments, turning it into a springboard for attacks aimed mainly at achieving illicit financial gains [3]. As reported by DataProt, about 560,000 new malware samples are detected every day, resulting in more than one billion malicious programs worldwide [4]. While cyber threats have been greatly diminished by the latest progress of cybersecurity technologies, malicious codes remain as one of the greatest concerns, since attackers look for access to sensitive information, finance-related data, and digital resources.

Among such cyber threats, ransomware has been reported as one of the most destructive types of malware, marking an evolution in the development of malicious software [5]. Ransomware incorporates encryption techniques to prevent access to data, forcing attackers to pay a ransom in exchange for accessing their own data, even though it does not promise any guarantee of data recovery [6]. Over time, several ransomware types, such as TeslaCrypt, CryptoWall, Locky, Cerber, and WannaCry, have been reported, indicating the severity of such attacks [7]. These attacks indiscriminately target anyone, encrypting data in no time. As such, ransomware types have significantly proliferated, increasing by about 600% [8]. Furthermore, recent ENISA reports highlight the severity of ransomware attacks, indicating an increase in data exfiltration from 8 TB in May 2021 to 136 TB in June 2022 [9]. Despite recent advancements in ransomware detection, existing network traffic-based techniques contiguously face significant challenges. Most research works have used self-generated datasets with no well-defined data generation process and no validation for the reliability of the data. Moreover, some datasets have been found to have incorrect label assignments, where some types of malware or anomalous behavior are wrongly classified under ransomware attacks with no well-defined classification and validation methods. Also, existing ransomware detection models have been found to have poor feature representations, thereby resulting in a high false positive rate and a reduction in the efficiency of

security operations. Even a small percentage of false positives can cause a high degree of alert fatigue, thereby compromising the efficiency of security analysts and operations.

That emphasizes the importance of building a more robust and scalable model to accurately distinguish between benign and malicious network activities with a low false alarm rate. The following are the major contributions of this work

- :The hybrid anomaly-based detection framework using LSTM Autoencoder and Isolation Forest model for a ransomware attack in an encrypted network environment overcomes the existing challenges and limitations of detecting ransomware attacks
- .The weighted fusion scheme incorporating a dynamic percentile-based threshold is able to fuse temporal reconstruction error and statistical anomaly score more effectively, which leads to a further reduction of false positive rate
- .New features for financial context such as USD_per_Byte and BTC_per_Cluster are introduced to enhance the discriminatory power of the ransomware behavior in the network
- .The proposed scheme is evaluated with a refined real-world ransomware dataset containing 111,904 clean samples and 149,197 samples applying SMOTE-ENN balancing, in which the efficiency of the scheme is verified .The rest of this paper is organized as follows. Section 2 presents a few related works on ransomware detection and anomaly-based learning methods. Section 3 details the proposed hybrid framework for ransomware detection . Section 4 discusses the experiment setup, datasets, and metrics. Section 5 presents the experiment results and analysis. Section 6 discusses the implications and limitations. Section 7 concludes this paper and provides some suggestions for future work.

2. Related Work

Ransomware represents an escalating security challenge due to its superior ability to hide and bypass traditional defense mechanisms [10]; signature-based methods and static analysis proved to be significantly deficient in front of software variants and "zero-day" attacks, while dynamic analysis in sandbox environments faced obstacles related to resource-intensive consumption and the difficulty of extended deployment [11]. Under this approach, Network Traffic Analysis is seen as a strategic option, whose core idea is to monitor the patterns of communication, not the binary files themselves. This research follows this approach by using anomaly detection algorithms to build the reference models of normal behavior using unsupervised and semi-supervised learning methods. The prior literature, based on a scientifically grounded approach, is divided into four categories, one of which is related to "the supervised learning" approach based on the classification of the already labeled network data. [12] , "unsupervised learning" targeted to detect deviations from the prevailing natural pattern without the need for labeled data [13] , "deep learning" representing the most mature generation for its ability to extract complex patterns from raw data without manual feature engineering [14] , up to "hybrid systems" that unite the advantages of previous tracks to overcome individual shortcomings. This hybrid approach provides a dual ability to accurately generalize known patterns and early detection of unprecedented deviations (Zero-day), even under encrypted traffic or the phenomenon of "concept Drift" caused by temporal behavior change [15] , which the current study seeks to develop in order to address existing research gaps and achieve an optimal balance between detection accuracy and operational efficiency in real-world network environments.

Berrueta et al. (2022) [16] used neural networks and tree clustering to analyze encrypted file sharing traffic patterns to detect ransomware. The study used a large data set of over 70 ransomware samples and thousands of hours of user activity, yielding great accuracy (99.8%) and a low false alarm rate (F1 = 0.9987). The methodology does not require peripheral tool installation and can be applied to multiple protocols, but it can lose data before detection and depends on the time window and analysis characteristics.

Venturini et al. (2025) [17] presented a framework for the detection of ransomware-affected files based on entropy change analysis, which uses Differential Area Analysis (DAA) and its variants (2F, 3F, 4F) to thoroughly investigate the file headers as well as other parts of the files for signs of ransomware encryption. By using a dataset of both uninfected and encrypted ransomware files, DAA demonstrated an accuracy of 98.24%, and an F1 score of 97.10%. The extensions of DAA

further enhance the robustness of the detection technique against entropy modification attacks, with an F1 score of around 93.56%. The technique has the advantage of being computationally inexpensive and easy to apply, but the disadvantage of being applied after the encryption process, which may lead to the loss of some files, and the fact that the effectiveness of the technique depends on the type of files as well as the parameters used.

In their paper presented in Chandler et al. (2024) [18], Multi-Vector Anomaly Profiling (MVAP) is proposed. This method evaluates system behavior through several vectors, including network traffic, file system operations, processes, and resource consumption, using benign and malicious samples of ransomware from three sets of experimental data. The results show that MVAP achieves high levels of accuracy between 95.2% and 97.1%, along with similar ranges for F1 scores (95.2%–97.1%), and low false alarm rates of 2.8%. It is capable of detecting new types of malware without signatures; however, it is computationally expensive and requires constant updates of behavior models and available resources.

Hussein et al. (2024) [19] developed a deep learning framework based on the GN-BiLSTM model, which utilizes graphical representation of behavioral patterns and bidirectional sequential learning for ransomware detection and classification. The authors employed two different CIC-MalMem-2022 datasets and a self-generated dataset based on recent ransomware samples. The developed model has shown promising results in detecting novel ransomware types, as well as evaluating complex inter-behavioral relationships, with an accuracy of 99.99%. The proposed method is efficient, but it requires more time for training, and the results depend on the similarity between the new patterns and existing information. The F1 score is not mentioned, but the results show an appropriate balance between accuracy and retrieval.

An early ransomware detection framework was proposed by Davidian et al. (2024) [20], where deep learning algorithms such as Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), and Deep Neural Networks (DNN) are used to analyze the API calls from benign processes as well as from 62 known ransomware samples. The best performance is obtained at a contextual window size of $W = 7$, where the F1 scores are approximately 0.9903 using CNN on the PARSEC-500 data set and 0.9942 using LSTM on the PARSEC-5000 data set, indicating the efficacy of the detection mechanism for the early detection of ransomware attacks while maintaining high accuracy with limited testing time. However, the mechanism demands a lot of data, high computational power, and is prone to overfitting.

Li et al. (2024) [21] present Semantic Flow Mapping for ransomware detection, which uses graphical models to represent processes and their relationships and anomaly analysis using machine and cluster learning techniques with reference data from multiple Ransomware families and normal system behaviors. With an accuracy of $\approx 98.7\%$ and $F1 \approx 98.7\%$, the method is computationally efficient, scalable, and detects new strains with low false alarm rates ($\sim 1.1\%$) and quick detection time. Its drawbacks include a detection period of 1.8–3.1 seconds, a limited number of undetected cases ($< 1.5\%$), and performance issues with model updates and system behavior changes.

Muhammad S et al. (2025) [22] proposed a hybrid AI-based framework that combines CNN and an automatic encoder to detect ransomware using artificial banking data, achieving an accuracy of 94.3% and $F1 \approx 94.2\%$ with a response time of approximately 1.8 seconds and the ability to reduce false alarms. Despite its effectiveness, its success depends on the availability of high-quality data and sufficient computing resources, as well as challenges related to interpretability and Model Management.

A systematic review of previous studies concludes that there are shortcomings in the current models of countering ransomware, especially in connection with the high rate of false alarms and excessive reliance on artificial data that lacks the complexity of Real Networks. Accordingly, this study proposes a hybrid framework that integrates LSTM Autoencoders to derive temporal patterns, and isolation Forest to enhance the efficiency of anomaly isolation. The added value of this research lies in the use of realistic network traffic (Real-world traffic) instead of simulated data, which ensures a qualitative balance between detection accuracy and operational reliability in dealing with encrypted and unclassified streams.

3. Proposed Hybrid Ransomware Detection Framework

This study proposes a hybrid ransomware detection framework that integrates an LSTM Autoencoder and an Isolation Forest model to enhance detection accuracy in encrypted network traffic. The two models operate in parallel to analyze temporal and statistical patterns of network behavior, enabling effective identification of anomalous activities.

3.1 LSTM Autoencoder for Temporal Anomaly Detection

The LSTM Autoencoder is utilized to capture the temporal behavior of network traffic sequences. It is trained exclusively on benign traffic to learn the normal patterns of network activity. During the detection phase, the model attempts to reconstruct input sequences, and the reconstruction error is computed. Higher reconstruction errors indicate deviations from normal behavior, which are likely associated with ransomware activities.

3.2 Isolation Forest

The Isolation Forest algorithm applies the principle of statistical isolation in order to identify anomalies. It partitions the data space recursively, isolating the points. Outlying data points, such as those associated with ransomware, are isolated very early on compared to ordinary data points. This makes the Isolation Forest both computationally efficient and effective for high-dimensional data, such as network traffic data.

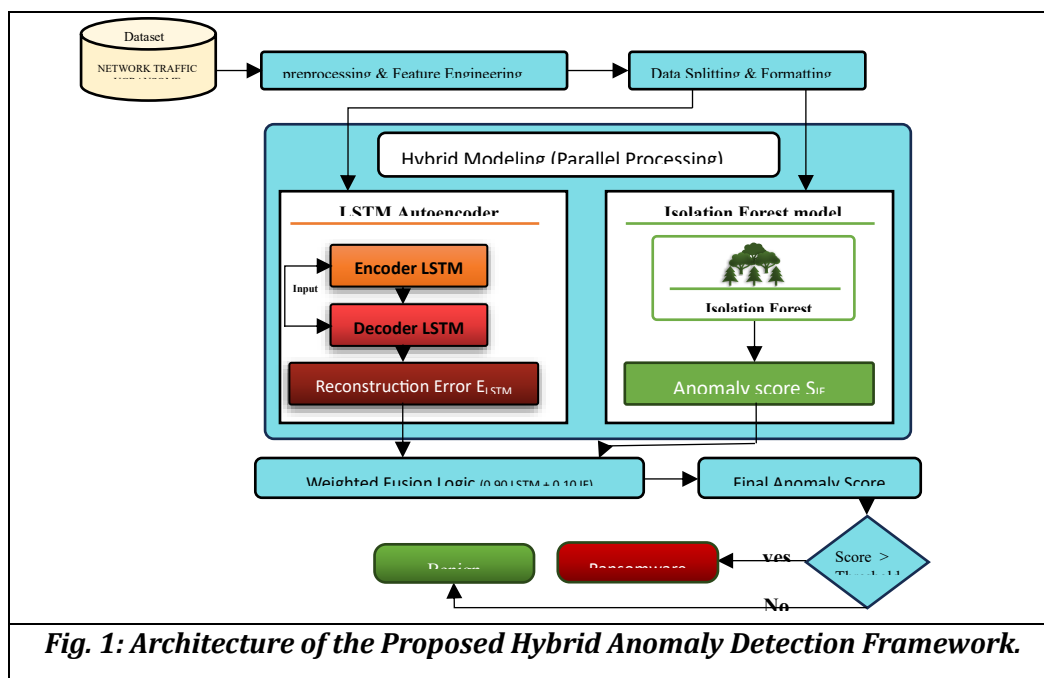
3.3 Weighted Fusion Logic

In order to improve the detection performance, a weighted fusion scheme is introduced to fuse the results of two models.

The normalized reconstruction error obtained by the LSTM Autoencoder and the anomaly score obtained by the Isolation Forest are fused using a predetermined weight. In this research, the LSTM Autoencoder is given a weight of 0.90, and the Isolation Forest is given a weight of 0.10. The hybrid score is calculated as follows:

$$H = (0.90 * E_LSTM) + (0.10 * S_IF)$$

The dynamic threshold is calculated based on the 98th percentile of the scores obtained during the training phase. The samples with scores higher than the threshold are classified as ransomware, and the samples with scores lower than the threshold are classified as benign.



4. Experimental Setup

This section describes the utilized data, the processing steps, and the approach for training and testing the hybrid model to guarantee the trustworthiness of the outcomes.

4.1 Dataset

The UGRansome_Dataset_2024 used in this study is an extension based on the original UGRansome dataset that was made available on the Kaggle platform by Dr. Mike Wa Nkongolo. The initial data were filtered in order to increase the quality and dependability of information, unknown features were removed, inconsistencies in "Time" feature were handled and statistical outliers were treated. Furthermore, feature and property names were harmonized to make them consistent throughout the dataset. The processed version after preprocessing and SMOTE-ENN contains 149,197 network traffic instances each of which has 14 attributes, including a prediction field that can be used for learning. Both normal and attack network traffic is included as realistic network traffic. These are protocol behaviour, volume and financial features (BTC and USD), which have relevance to ransomware payments. Several rake variants are covered in the dataset as well, such as WannaCry, Locky, Cerber, TeslaCrypt, and Ryuk, allowing for testing against various ransomware behaviors

In network traffic, there are three major classes of traffic: Signature (S), Synthetic Signature (SS), and Anomaly (A). The Signature class includes known ransomware patterns, while the Synthetic Signature class includes simulated ransomware attacks, and the Anomaly class may include both benign and possible zero-day attacks. This has created some challenges regarding the reliability of the labels and the realism of the employed dataset, as the existence of synthetic samples may elevate the uncertainty during the training and evaluation of the employed models.

Algorithm 1: Hybrid Ransomware Detection (LSTM-AE + IF)

Input: Dataset D , Sequence Length $L=10$, Threshold Percentile $P = 98$

Output: Prediction $Y \in \{0, 1\}$

- 1: Preprocess data and engineer features
- 2: Select top features using XGBoost
- 3: Normalize features
- 4: Train LSTM Autoencoder on benign data
- 5: Train Isolation Forest on benign data
- 6: Compute anomaly scores (E_LSTM, S_IF)
- 7: Normalize scores
- 8: Compute hybrid score:

$$H = (0.90 \times E_LSTM) + (0.10 \times S_IF)$$
- 9: Determine threshold using percentile
- 10: Classify:
 If $H > \text{Threshold} \rightarrow \text{Attack}$
 Else $\rightarrow \text{Benign}$

TABLE I : SAMPLE ENTRIES FROM UGRANSOME DATASET

Time	Protocol	Flag	Family	Clusters	Sedd	ExpAdd.	BTC	USD	Netflow	IP	Threats	Port	Pred
55	TCP	R	TowerWeb	1	1DA11mPS	1SYStemQ	22	18124	4916	C	Blacklist	5066	S
11	ICMP	AF	TowerWeb	1	17dcMo4V	1DiCeTjB	30	253	1741	C	NerisBonet	5066	SS
46	TCP	AF	Cryptohitman	1	17dcMo4V	1DiCeTjB	22	21345	194	C	NerisBonet	5061	A

TABLE II : Classes of Network Traffic (Prediction Attribute)

Class	Meaning	Includes Benign?	Notes
S	Signature	X	Known ransomware and attack patterns
SS	Synthetic Signature	X	Simulated ransomware behaviors
A	Anomaly	✓ (sometimes)	May include benign traffic and irregular traffic patterns

4.2 Preprocessing

Several steps have been implemented to ensure the quality of the input:

- Purge: remove non-numeric values and deal with missing values by filling them with zero to avoid training failure.
- Normalization: apply Min-Max Normalization to convert values to the range [0, 1].
- Chronology: convert data into time series with length (Sequence Length = 10) to match the LSTM model input.

4.3 Data Splitting Strategy

The "single-class training" (One-Class Training) approach was adopted to enhance the system's ability to detect "zero-day" attacks. The data was divided as follows:

- Training data (64%): limited to natural traffic (Benign) only for learning stable patterns.
- Verification data (16%): to monitor performance during training and activate the "early stopping" mechanism to prevent over-allocation.
- Test data (20% of normal + 100% of attacks): all attack samples were combined at this stage only to measure the sensitivity of the system to previously untrained patterns.

4.4 Evaluation Metrics

The efficiency of the system is assessed using standard performance measures that include: Accuracy, Recall, F1-Score scale, and operating characteristic curve (ROC-AUC).

4.5 Computational Complexity Analysis

The complexity of computation for the hybrid model is found to be appropriate for deployment in a real-world network security environment. Although there is a higher computational cost for the LSTM Autoencoder, particularly during the training process, the overall process of inference is computationally efficient. This allows for deployment in a near real-time environment. On the other hand, the Isolation Forest model has a relatively low computational cost, given its ability to provide efficient anomaly detection even in high-dimensional feature spaces. The overall complexity of computation for the hybrid model is achieved by utilizing the strengths of both models. Additionally, since both models can be executed in parallel, there is no significant impact on the overall latency of deployment for a real-time environment.

5. Results and Analysis

This section offers an extensive evaluation of the proposed hybrid ransomware detection scheme. The performance of the proposed scheme is evaluated by using standard evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC, followed by an extensive evaluation of the confusion matrix and ablation study to evaluate the effectiveness of each component of the proposed models.

5.1 Performance Metrics Analysis

The hybrid framework based on the Long Short-Term Memory Autoencoder and Isolation Forest outperforms the detection capabilities of the separate models used as a reference. In fact, the framework recorded an accuracy of 99.66%, which further confirms the efficiency of the framework in differentiating ransomware traffic from benign traffic. In the same vein, the framework recorded a precision of 99.78%, a recall of 99.85%, which further confirms the effectiveness of the framework in the identification of ransomware traffic while limiting the false alarm rate. In fact, the framework recorded an F1-score of 99.81%, which further confirms the effectiveness of the framework in the identification of ransomware traffic while limiting the false

alarm rate. All these observations confirm the effectiveness of the framework in the identification of ransomware traffic while limiting the false alarm rate.

5.2 Confusion Matrix and Error Distribution

In order to further evaluate the performance of classification in the proposed framework, a confusion matrix was created and is illustrated in Figure 2. In this regard, it is noted that the proposed framework successfully identified 98,517 instances of ransomware and 9,874 instances of benign software (true negatives). At the same time, 220 instances of benign software were incorrectly identified as attacks (false positive), resulting in a false positive rate of 2.18 percent. Furthermore, 160 instances of ransomware were incorrectly identified (false negative), resulting in a false negative rate of 0.16 percent. This demonstrates that the proposed framework maintains high sensitivity in its detection capabilities and low false alarm rates, making it suitable for real-world applications in cybersecurity.

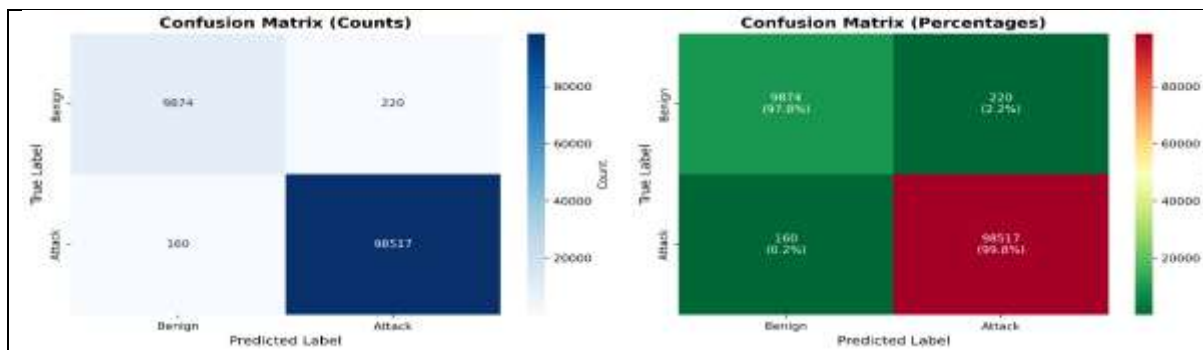


Fig. 2: Confusion matrix of the proposed hybrid LSTM-IF model in terms of sample counts and corresponding percentages.

5.3 Ablation Study

An ablation study is performed to assess the effectiveness of each component of the proposed framework. To achieve this, the performance of the LSTM Autoencoder, the performance of the Isolation Forest, and the performance of the hybrid model are compared. Based on the results presented in Table 2, the LSTM Autoencoder achieves high performance due to the ability to detect temporal dependencies in the network traffic. However, the LSTM Autoencoder is found to have high false positive rates when used independently. On the contrary, the Isolation Forest achieves high robustness in detecting anomalies using the statistical approach, yet the accuracy is compromised. It is evident that the hybrid model is capable of achieving high accuracy while reducing the false positive rates, thereby proving that the proposed approach is more reliable and robust for the detection of ransomware attacks.

5.4 Comparative Analysis

In the above comparative analysis, it can be observed that the hybrid model outperforms the other models as it combines the effectiveness of both the temporal and statistical anomaly detection mechanisms. In the Long Short-Term Memory (LSTM) Autoencoder model, the proficiency of the model in the detection of behavioral patterns of the ransomware can be observed. In the Isolation Forest model, the effectiveness of the statistical anomaly detection mechanism can be observed.

Table 2. Performance Comparison of Proposed Hybrid Model and Baseline Methods					
MODEL	Accuracy	Precision	Recall	F1-Score	ROC-AUC
LSTM-AE	98.92%	98.13%	99.95%	99.03%	99.99%
Isolation Forest	70.57%	74.39%	71.07%	72.69%	78.34%
LSTM-AE + IF (Hybrid) Proposed	99.66%	99.78%	99.85%	99.81%	99.97%

6. Discussion and Practical Implications

The experiment results validate the effectiveness of the suggested hybrid framework in detecting ransomware from encrypted network traffic.

Through deep temporal modeling and a statistical anomaly detection approach, our framework achieves high detection accuracy and low false alarm rate. Actually, LSTM Autoencoder model learns sequential behavioral pattern effectively and Isolation Forest model provides robustness for statistical anomaly. From an application perspective, the proposed scheme can be a practicable one to address real problem of network and host systems in which encrypted traffic is utilized to impede the execution of signature-based scheme. Indeed, the fact that the framework can also detect zero-day ransomware makes it suitable for proactive defense and real-time monitoring of the network.

Limitations of the Study

Nevertheless, there are several limitations of this study: The proposed framework was evaluated based on one ransomware dataset, and hence it is uncertain whether the approach will extend to other network environments as the traffic patterns may differ. Application of the dynamic threshold method may as well entail a further set of calibrations in diverse and evolving environments. The reliance on engineered features, such as financial context, could also make the method sensitive to the particularities of the data, which might not hold in all cases.

7. Conclusion and Future Work

In this paper, We propose a parallel hybrid framework for ransomware detection in network traffic based on deep learning and statistical anomaly detection. Our framework has demonstrated high efficiency in detecting malicious patterns in encrypted network traffic with outstanding results in reducing false alarms and improving the differentiation between normal and ransomware provided traffic features, especially for those with financial dimensions. Experimental results validate that the hybrid anomaly-based detection is a promising approach to mitigate the weaknesses of conventional approaches especially against advanced threats and zero-day attacks. This also increases the robustness of detection systems in real-life scenarios by providing a compromise between accuracy and computational cost. As for future work, the proposed framework can be further extended to more complicated scenarios such as cloud computing and the Internet of things, where the traffic pattern is dramatically different. It is further suggested that the model resistance against adversarial attacks should be enhanced and with the emerging concept of XAI, it can be integrated with XAI techniques to increase solution transparency and enable security analysts to gain a better understanding of the attacks' behavior.

References

- [1] B. Riskhan, A. M. Raufi, and M. H. Usmani, "Physical Security to Cybersecurity (Challenges and Implications in the Modern Digital Landscape)," 2024.
- [2] A. Greubel, D. Andres, and M. Hennecke, "Analyzing Reporting on Ransomware Incidents: A Case Study," *Soc. Sci.*, vol. 12, no. 5, May 2023, doi: 10.3390/socsci12050265.
- [3] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms," *IEEE Access*, vol. 11, pp. 121118–121141, 2023, doi: 10.1109/ACCESS.2023.3328351.
- [4] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput. Secur.*, vol. 111, Dec. 2021, doi: 10.1016/j.cose.2021.102490.
- [5] S. H. Kok, A. Abdullah, and N. Z. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 1984–1999, May 2022, doi: 10.1016/j.jksuci.2020.06.012.
- [6] F. Aldauji, O. Batarfi, and M. Bayousef, "Utilizing Cyber Threat Hunting Techniques to Find Ransomware Attacks: A Survey of the State of the Art," *IEEE Access*, vol. 10, pp. 61695–61706, 2022, doi: 10.1109/ACCESS.2022.3181278.

- [7] T. M. Hassin Mohamed, B. A. Saleh Al-Rimy, and S. A. Almalki, "A Ransomware Early Detection Model based on an Enhanced Joint Mutual Information Feature Selection Method," *Engineering, Technology and Applied Science Research*, vol. 14, no. 4, pp. 15400–15407, Aug. 2024, doi: 10.48084/etasr.7092.
- [8] A. Alexei and A. Alexei, "THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY," *Journal of Engineering Science*, vol. 29, no. 4, pp. 72–83, Jan. 2023, doi: 10.52326/jes.utm.2022.29(4).08.
- [9] G. Nagar, "The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies," *International Journal of Scientific Research and Management (IJSRM)*, vol. 12, no. 06, pp. 1282–1298, Jun. 2024, doi: 10.18535/ijssrm/v12i06.ec09.
- [10] M. Güven, "Dynamic Malware Analysis Using a Sandbox Environment, Network Traffic Logs, and Artificial Intelligence," *International Journal of Computational and Experimental Science and Engineering*, vol. 10, no. 3, pp. 480–490, Jul. 2024, doi: 10.22399/ijcesen.460.
- [11] K. K. Verma, B. M. Singh, and A. Dixit, "A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system," *International Journal of Information Technology (Singapore)*, vol. 14, no. 1, pp. 397–410, Feb. 2022, doi: 10.1007/s41870-019-00364-0.
- [12] N. Christakis and D. Drikakis, "Reducing Uncertainty and Increasing Confidence in Unsupervised Learning," *Mathematics*, vol. 11, no. 14, Jul. 2023, doi: 10.3390/math11143063.
- [13] A. Redhu, P. Choudhary, K. Srinivasan, and T. K. Das, "Deep learning-powered malware detection in cyberspace: a contemporary review," 2024, *Frontiers Media SA*. doi: 10.3389/fpsy.2024.1349463.
- [14] A. Lumazine et al., "Ransomware Detection in Network Traffic Using a Hybrid CNN and Isolation Forest Approach," Oct. 15, 2024. doi: 10.22541/au.172901014.44599790/v1.
- [15] E. Berrueta, D. Morato, E. Magaña, and M. Izal, "Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic," *Expert Syst. Appl.*, vol. 209, Dec. 2022, doi: 10.1016/j.eswa.2022.118299.
- [16] M. Venturini, F. Freda, E. Miotto, M. Conti, and A. Giaretta, "Differential Area Analysis for Ransomware: Attacks, Countermeasures, and Limitations," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 4, pp. 3449–3464, 2025, doi: 10.1109/TDSC.2025.3532324.
- [17] S. Chadler, S. Davis, T. Delacroix, and W. Carrington, "Ransomware Detection Using Multi-Vector Anomaly Profiling for Maximum Security," Nov. 15, 2024. doi: 10.21203/rs.3.rs-5452210/v1.
- [18] A. Hussain, A. Saadia, M. Alhussein, A. Gul, and K. Aurangzeb, "Enhancing ransomware defense: deep learning-based detection and family-wise classification of evolving threats," *PeerJ Comput. Sci.*, vol. 10, pp. 1–44, 2024, doi: 10.7717/peerj-cs.2546.
- [19] M. Davidian, M. Kiperberg, and N. Vanetik, "Early Ransomware Detection with Deep Learning Models," *Future Internet*, vol. 16, no. 8, Aug. 2024, doi: 10.3390/fi16080291.
- [20] E. Li, H. He, C. Huang, J. Zhang, H. Cheng, and Y. Ge, "Anomaly-Driven Crypto-Locking Behavior Analysis for Ransomware Detection through Semantic Flow Mapping," Dec. 12, 2024. doi: 10.36227/techrxiv.173398043.39428308/v1.
- [21] S. Muhammad, "AI-Driven Ransomware Defense Framework for Digital Banking International Journal of Innovative Research in Science Engineering and Technology (IJIRSET) AI-Driven Ransomware Defense Framework for Digital Banking," *Article in International Journal of Innovative Research in Science Engineering and Technology*, 2025, doi: 10.15680/IJIRSET.2025.1406012.