Proceedings of the 4th International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/2026.33193

Fusion and Credibility Evaluation of Open-source Threat Intelligence Based on Machine Learning Algorithms

Ruofan Li

City University of Macau, Faculty of Data Science, Macau, China
D24091101091@cityu.edu.mo

Abstract. The situation of cyber threats is becoming increasingly complex and changeable. The traditional cyber threat intelligence system, due to its excessive reliance on closed data sources, has problems such as lagging updates and limited coverage. It is not only difficult to meet the real-time defense requirements but also unable to comprehensively capture new attack methods and potential threat trends. Open-source threat intelligence, with its advantage of multiple sources, can expose attack trends in advance and has become an important force to supplement the traditional intelligence system. However, the existing single machine learning algorithm has obvious shortcomings in the classification and evaluation of open-source threat intelligence and is difficult to take into account the multi-dimensional data features. To this end, this paper proposes the LSTM-KELM-Transformer classification algorithm. Firstly, data mining is carried out through correlation analysis and violin graph analysis, and then comparative experiments are conducted with multiple machine learning algorithms. The results show that this algorithm achieves 99% in accuracy, recall rate, precision rate and F1 score, with an AUC value of 99%. All evaluation indicators significantly outperform other algorithms, demonstrating excellent classification performance. This research provides a new technical solution for the efficient classification of open-source threat intelligence, which is of great practical significance for strengthening the real-time defense capability against network threats and improving the threat intelligence system construction.

Keywords: cyber threats, LSTM, KELM, Transformer.

1. Introduction

The current situation of cyber threats is becoming increasingly complex and changeable. The traditional cyber threat intelligence system overly relies on closed data sources and is difficult to meet the real-time defense requirements [1]. Such closed data sources often have the problem of lagging updates and limited coverage, making it impossible to comprehensively capture new attack methods and potential threat trends [2]. In contrast, open-source threat intelligence, with its advantage of diverse sources, can expose attack trends in advance and has become an important force to supplement the traditional intelligence system. However, open-source threat intelligence is confronted with numerous inherent challenges. The data noise content is high, the credibility of information from different sources varies greatly, and some contents are repetitive or even

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.33193

contradictory. There is a lack of a systematic integration and trust evaluation framework within the industry, which seriously restricts its application value in actual security defense. Building a scientific open-source threat intelligence trusted evaluation system has become an urgent need in the field of cyber security [3].

Machine learning algorithms provide core technical support for solving the problem of open-source threat intelligence assessment. The traditional assessment method relies on manual screening and judgment, which is inefficient and highly subjective, and is difficult to deal with massive heterogeneous open-source data [4]. Machine learning algorithms can automatically process large-scale open-source intelligence data. Through feature extraction and pattern recognition, they can mine the potential correlations behind the data and achieve quantitative assessment of intelligence credibility [5]. Classification algorithms can precisely divide intelligence into different credibility levels, providing a basis for subsequent data fusion. At the same time, it has adaptive learning capabilities, which can optimize the assessment model in response to changes in the threat situation, effectively reducing the cost of manual intervention, enhancing the objectivity and timeliness of assessment results, and providing an efficient and stable technical solution for the screening, integration, and trusted assessment of open-source threat intelligence [6].

The existing single machine learning algorithm has obvious shortcomings in the classification and evaluation of open-source threat intelligence and is difficult to take into account the multi-dimensional data features. Some algorithms are good at handling temporal features but fail to capture global correlations adequately. Some algorithms perform well in nonlinear data fitting but have weak temporal sensitivity, and thus cannot fully adapt to the complex features of open-source intelligence that combine temporal, nonlinear and relational characteristics. For this purpose, this paper proposes the LSTM-KELM-Transformer classification algorithm. This algorithm integrates the core advantages of long short-term memory networks, kernel extreme learning machines, and Transformer models. It captures the temporal characteristics of intelligence release and dissemination with LSTM, enhances the fitting ability of nonlinear credibility correlations through KELM, and precisely captures the global dependency relationships among multiple sources of intelligence with Transformer. The three work in synergy to make up for the shortcomings of a single algorithm, achieve precise classification of the credibility of open-source threat intelligence, and provide key algorithmic support for the construction of an open-source threat intelligence system.

2. Data sources

The dataset used in this article contains 920 pieces of data and 15 variables, specifically including the source, type, release time, content length, author credibility, completeness of technical details, verification links, whether there is social dissemination and community feedback, the number of cross-source confirmations of data, the proportion of repetitive and contradictory content, language clarity and timeliness of open-source intelligence, and other indicators. The prediction metrics of the dataset are classified labels with three credibility levels: low, medium and high. First, conduct a correlation analysis on each data point and draw a correlation heat map, as shown in Figure 1.

DOI: 10.54254/2755-2721/2026.33193

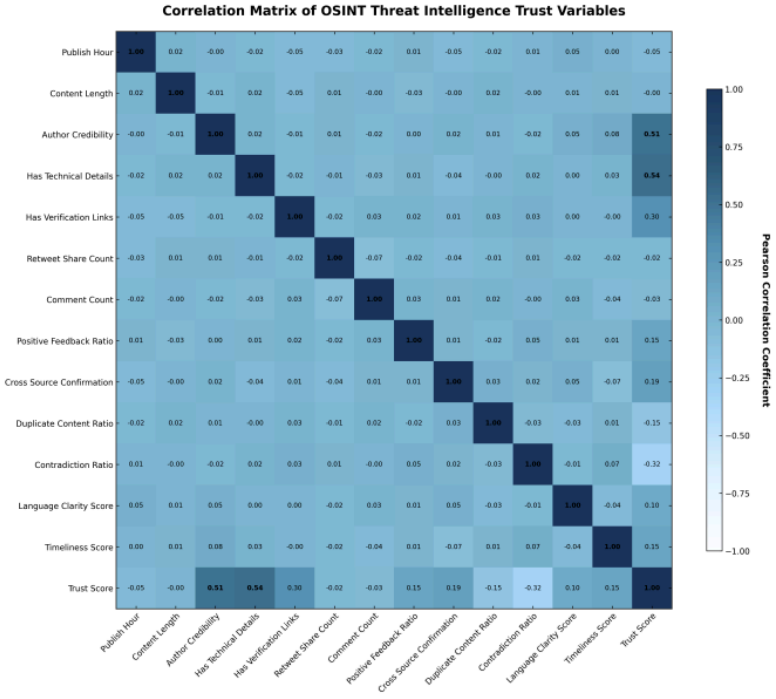

Figure 1. The correlation heat map

By conducting violin plot analysis on each variable and drawing the violin plots of each variable, the distribution of each variable can be observed. As shown in Figure 2.

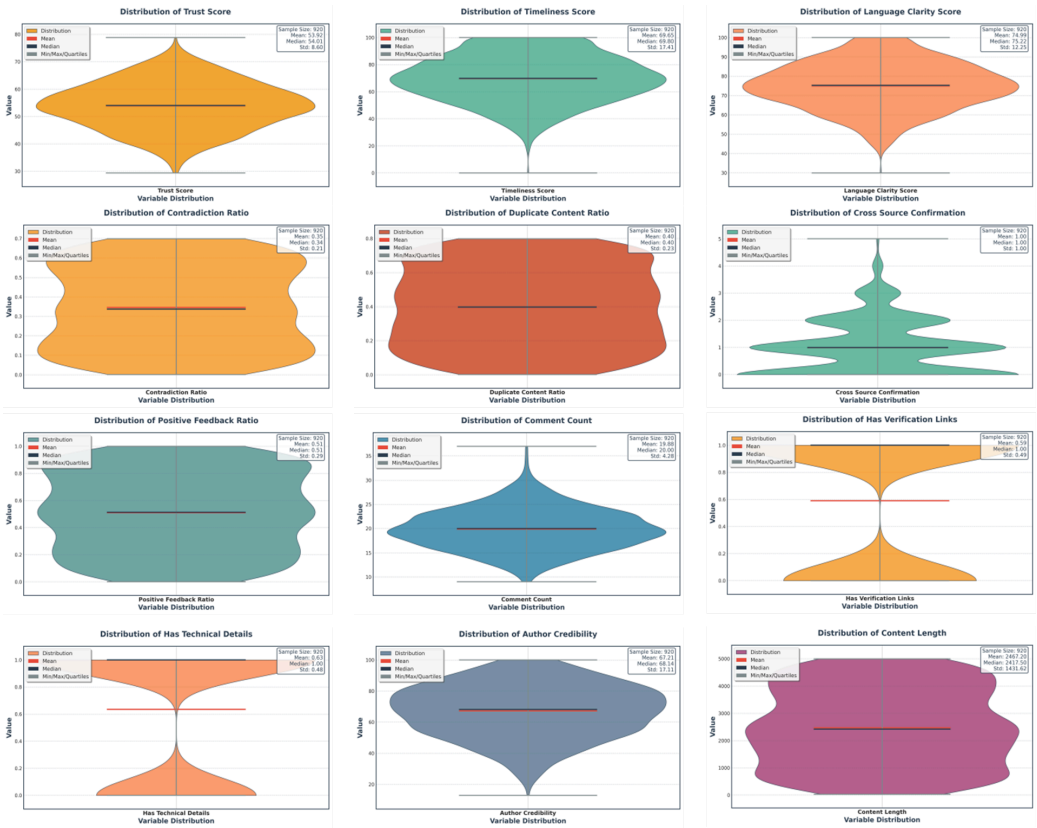

Figure 2. The violin diagrams of each variable

DOI: 10.54254/2755-2721/2026.33193

3. Method

3.1. LSTM

Long short-term memory networks are an improved model of recurrent neural networks. The core lies in solving the vanishing or exploding gradient problems of traditional recurrent neural networks through gating mechanisms. It consists of three core structures: the forget gate, the input gate, and the output gate. The forget gate determines whether historical information is retained, the input gate controls the reception and storage of new information, and the output gate regulates the output intensity of the current information [7]. The algorithm conveys long-term dependency information through cell states, and the gating structure dynamically adjusts the retention and discarding of information based on the input data, which can effectively capture the temporal features in sequence data. The network structure of LSTM is shown in Figure 3.

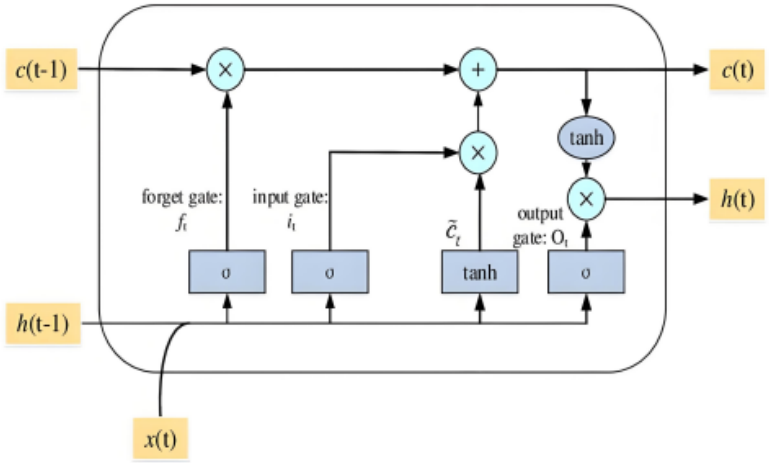

Figure 3. The network structure of LSTM

3.2. KELM

The kernel extreme learning machine is an improved algorithm combining the extreme learning machine and the kernel function. It retains the advantages of the extreme learning machine, such as its simple structure and fast training speed, while enhancing the nonlinear fitting ability through kernel function mapping [8]. The algorithm does not require adjusting the weights of the hidden layer. It only needs to randomly initialize the connection weights and biases between the input layer and the hidden layer, then map the input features to the high-dimensional feature space through the kernel function, and finally solve the output weights by using the least square method [9]. The core logic is to simplify the computation in high-dimensional Spaces through kernel techniques, avoid complex iterative training processes, and enhance the model's ability to capture nonlinear relationships while ensuring computational efficiency.

3.3. Transformer

The Transformer algorithm is constructed based on the self-attention mechanism, completely breaking away from the dependence of recurrent neural networks on sequence order and achieving parallel computing. The self-attention mechanism can directly capture the dependencies within the global scope by calculating the association weights of each position in the input sequence with all

DOI: 10.54254/2755-2721/2026.33193

other positions, without having to traverse the sequence in sequence [10]. The algorithm consists of an encoder and a decoder structure. The encoder is responsible for global feature extraction of the input features, while the decoder handles the task of generating the output sequence. The design of layer normalization and residual connection further enhances the stability and training effect of the model. The network structure of the Transformer is shown in Figure 4.

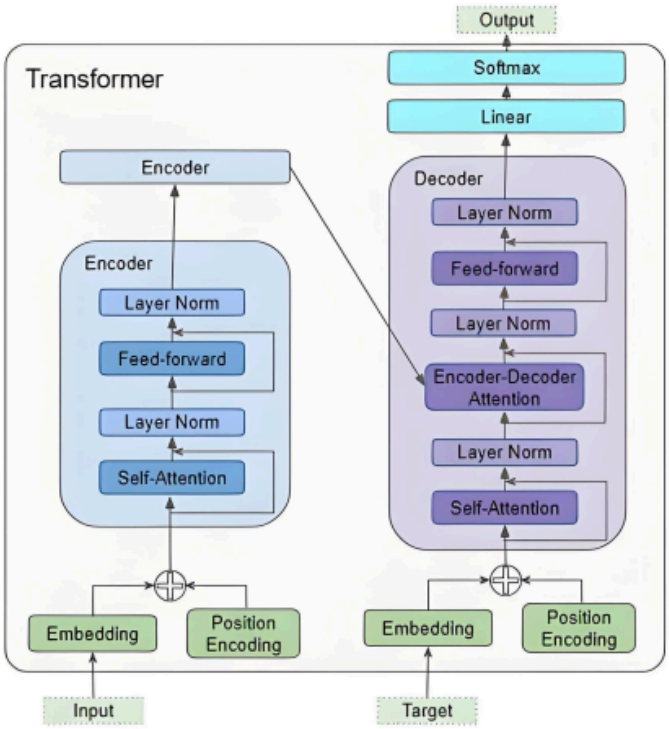

Figure 4. The network structure of the Transformer

3.4. LSTM-KELM-Transformer

The LSTM-KELM-Transformer algorithm adopts a modular fusion architecture, organically combining the core advantages of the three algorithms. Firstly, the time series data of open-source threat intelligence is processed through the LSTM module to extract the time series dependency features during the intelligence release and dissemination process, laying the foundation for subsequent analysis. Subsequently, the temporal features and features of other dimensions are input into the KELM module. By leveraging the mapping capability of the kernel function, the fitting of nonlinear feature relationships is strengthened, enabling rapid processing of high-dimensional heterogeneous intelligence feature data. Finally, through the self-attention mechanism of the Transformer module, the global dependency relationship among multi-source intelligence is captured, and the analysis results of temporal features and nonlinear features are integrated.

4. Result

In terms of parameter Settings for this project, the dataset is divided into the training set and the test set at a ratio of 70%. When building the Transformer-LSTM model, the input channel number matches the feature dimension. The maximum position encoding is set to 512, the number of heads

DOI: 10.54254/2755-2721/2026.33193

of the self-attention mechanism is 4, the number of key channels of each head is 32, and the total number of key channels reaches 128. The model consists of a sequence input layer, a position embedding layer, an addition layer, a two-layer self-attention layer, a 6-dimensional LSTM layer, a ReLU activation layer, a dropout layer (with a discard probability of 0.01), an index layer, a fully connected layer corresponding to the number of categories, a softmax layer, and a classification layer. The Adam optimizer was selected for model training. The maximum number of training rounds was 800, and the batch size was set to 256. The dataset was shuffled in each round of training. The initial learning rate was 0.01, the learning rate decline factor was 0.1, the decline period was 650, the L2 regularization coefficient was 0.001, the gradient clipping threshold was 10, and the execution environment was automatically adapted. In the Transformer-LSTM-KELM module, the regularization coefficient is set to 20, the kernel parameter is 6, and the radial basis function is selected as the kernel function type.

Output the results of each algorithm as shown in Table 1. Output the comparison results of each indicator, as shown in Figure 5.

Table 1. The results of the comparative experiment

Model	Accuracy	Recall	Precision	F1	AUC
CatBoost	0.967	0.967	0.967	0.967	0.975
Decision tree	0.949	0.949	0.955	0.952	0.962
ExtraTrees	0.957	0.957	0.957	0.956	0.967
Random Forest	0.978	0.978	0.975	0.977	0.975
BP neural network	0.732	0.732	0.536	0.619	0.799
GBDT	0.953	0.953	0.953	0.952	0.988
SVM	0.833	0.833	0.887	0.852	0.953
XGBoost	0.975	0.975	0.978	0.976	0.986
Linear regression	0.899	0.899	0.896	0.897	0.978
LSTM-KELM-Transformer	0.989	0.989	0.989	0.989	0.993

The LSTM-KELM-Transformer algorithm proposed in this paper demonstrates significant advantages in all evaluation indicators. Its accuracy rate, recall rate, precision rate and F1 score all reach 99%, and the AUC value is 99%, comprehensively surpassing all other machine learning algorithms. In contrast, the random forest performs more outstandingly, with an accuracy rate and recall rate of 98%, an F1 score of 98%, and an AUC value of 98%. However, all these indicators are still lower than those of the LSTM-KELM-Transformer algorithm. The accuracy recall rate of XGBoost is 98%, the precision rate is 98%, the F1 score is 98%, and the AUC value is 99%. In terms of the AUC metric, it is close to the proposed algorithm, but the other metrics are slightly insufficient. The various indicators of CatBoost ExtraTrees and GBDT are all between 95% and 98%. The overall performance is good, but there is a certain gap compared with the LSTM-KELM-Transformer algorithm. The accuracy recall rate of Linear regression is 90%, the precision rate is 90%, the F1 score is 90%, and the AUC value is 98%. The performance is moderate. The various indicators of SVM range from 83% to 89%, which is at a moderately lower level. The performance of the BP neural network is the worst, with an accuracy recall rate of only 73%, an precision rate of 54%, an F1 score of 62%, and an AUC value of 80%. The gap with the LSTM-KELM-Transformer algorithm is the most obvious. This fully demonstrates that the LSTM-KELM-Transformer algorithm proposed in this paper has stronger superiority and stability in classification performance.

DOI: 10.54254/2755-2721/2026.33193

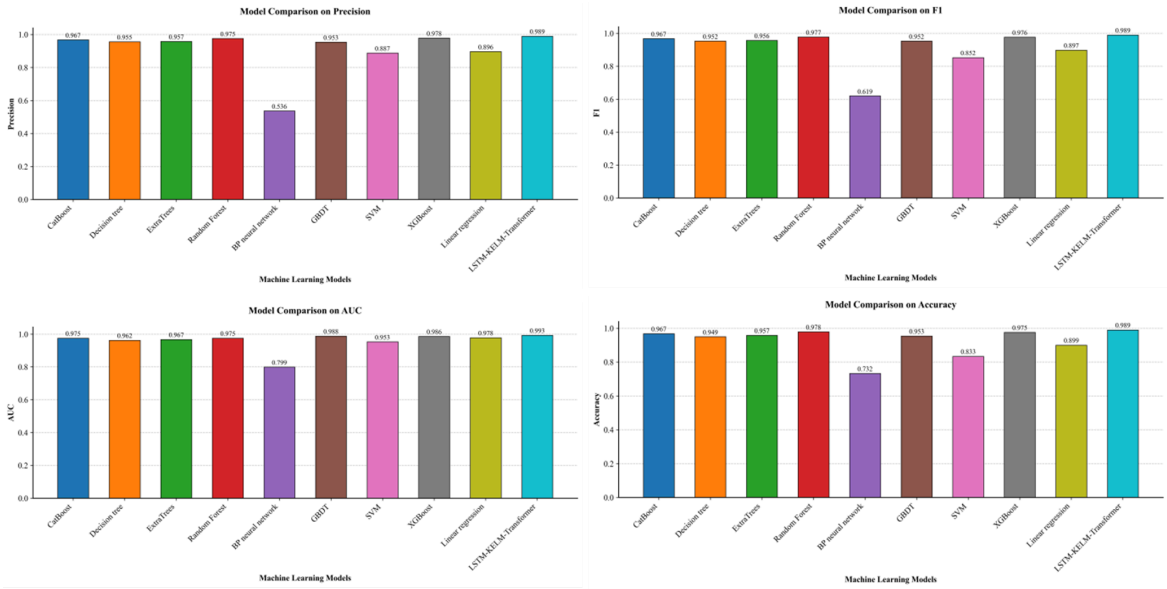

Figure 5. The bar comparison charts of each indicator

Output the confusion matrix of the test set of LSTM-KELM-Transformer, as shown in Figure 6.

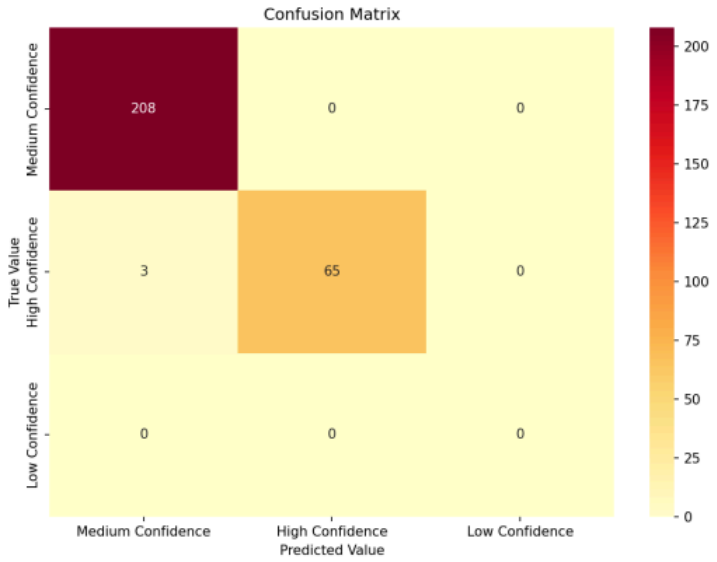

Figure 6. The confusion matrix of the test set of LSTM-KELM-Transformer

5. Conclusion

Nowadays, the situation of cyber threats is becoming increasingly complex and changeable. The traditional cyber threat intelligence system relies heavily on closed data sources and is no longer able to meet the real-time defense requirements. Such closed data sources generally have the problem of lagging updates and a relatively narrow coverage, making it impossible to comprehensively capture new attack methods and potential threat trends. In contrast, open-source threat intelligence, with its advantage of diverse sources, can expose attack trends in advance and has become a key force to supplement the traditional intelligence system. However, the existing single machine learning algorithm has obvious deficiencies in the classification and evaluation of

DOI: 10.54254/2755-2721/2026.33193

open-source threat intelligence and is difficult to take into account the multi-dimensional data features. To this end, this paper proposes the LSTM-KELM-Transformer classification algorithm. Firstly, correlation analysis and violin graph analysis are carried out, and then comparison and verification are conducted through multiple machine learning algorithms. The results show that this algorithm performs outstandingly in all evaluation indicators, with accuracy, recall rate, precision rate and F1 score all reaching 99%, and the AUC value is also 99%. It comprehensively surpasses other types of machine learning algorithms. This achievement provides an efficient and reliable technical solution for the precise classification and evaluation of open-source threat intelligence. Help enhance the intelligence and real-time performance of network security defense.

References

[1] Tundis, Andrea, Samuel Ruppert, and Max Mühlhäuser. "On the automated assessment of open-source cyber threat intelligence sources." International Conference on Computational Science. Cham: Springer International Publishing, 2020..

[2] Adewopo, Victor, Bilal Gonen, and Festus Adewopo. "Exploring open source information for cyber threat intelligence." 2020 IEEE International Conference on Big Data (Big Data). IEEE, 2020.

[3] Obioha Val, Onyinye, et al. "Investigating the feasibility and risks of leveraging artificial intelligence and open source intelligence to manage predictive cyber threat models." Temitope and Olaniyi, Oluwaseun Oladeji and Gbadebo, Michael Olayinka and Olisa, Anthony Obulor, Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models (January 23, 2025) (2025).

[4] Pedersen, Tore, and Pia Therese Jansen. "Seduced by secrecy–perplexed by complexity: effects of secret vs open-source on intelligence credibility and analytic confidence." Intelligence and National Security 34.6 (2019): 881-898.

[5] Gioti, Angeliki. Advancements in Open Source Intelligence (OSINT) Techniques and the role of artificial intelligence in Cyber Threat Intelligence (CTI). MS thesis. Πανεπιστήμιο Πειραιώς, 2024.

[6] Khurana, Nitika, et al. "Preventing poisoning attacks on AI based threat intelligence systems." 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP). IEEE, 2019.

[7] Liao, Xiaojing, et al. "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.

[8] Tang, Fengxiao, et al. "LRCTI: A Large Language Model-Based Framework for Multi-Step Evidence Retrieval and Reasoning in Cyber Threat Intelligence Credibility Verification." arXiv preprint arXiv: 2507.11310 (2025).

[9] Ranade, Priyanka, et al. "Generating fake cyber threat intelligence using transformer-based models." 2021 International Joint Conference on Neural Networks (IJCNN). IEEE, 2021.

[10] Wright, Edward J., and Kathryn Blackmond Laskey. "Credibility models for multi-source fusion." 2006 9th International Conference on Information Fusion. IEEE, 2006.