



Enhancing Cyberbullying Detection Systems with Hybrid Machine Learning Models

Abilly Elly, Zakarya Jahin and Zakarya Jesan

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

July 1, 2024

Enhancing Cyberbullying Detection Systems with Hybrid Machine Learning Models

AUTHORS

ABILLY ELLY, ZAKARYA JAHIN, ZAKARYA JESAN

DATA: June 23, 2024

Abstract:

Cyberbullying has emerged as a pervasive issue in the digital age, posing significant challenges to the safety and well-being of individuals, especially among youth. Traditional detection systems often fall short in accurately identifying and mitigating such harmful behavior due to the complex, context-dependent nature of online interactions. This paper explores the enhancement of cyberbullying detection systems through the implementation of hybrid machine learning models, which leverage the strengths of various algorithms to improve detection accuracy and efficiency. By combining supervised learning techniques, such as Support Vector Machines (SVM) and Random Forests, with advanced neural network architectures, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), the proposed hybrid models can capture both linguistic nuances and contextual patterns in textual data. The study involves the collection and preprocessing of a comprehensive dataset from multiple social media platforms, followed by the training and evaluation of the hybrid models. Results demonstrate that hybrid models significantly outperform traditional single-algorithm approaches, achieving higher precision, recall, and F1 scores. The findings underscore the potential of hybrid machine learning models in creating more robust and effective cyberbullying detection systems, ultimately contributing to safer online environments. Future research directions include the integration of real-time detection capabilities and the application of these models across diverse languages and cultural contexts.

Introduction:

The advent of social media and online communication platforms has revolutionized the way people interact, offering unprecedented opportunities for connection and expression. However, these platforms have also become breeding grounds for cyberbullying, a form of harassment that can have severe psychological, emotional, and sometimes physical consequences for victims. Cyberbullying involves the use of digital technologies to deliberately and repeatedly harm others through hostile behavior such as threats, intimidation, and insults. The pervasive and often anonymous nature of cyberbullying makes it a particularly insidious problem, necessitating effective detection and intervention strategies to protect vulnerable individuals.

Traditional approaches to cyberbullying detection rely heavily on rule-based systems and single-algorithm machine learning models, which often struggle to capture the nuanced and context-dependent nature of online abuse. These methods typically involve keyword matching and basic sentiment analysis, which can result in high rates of false positives and false negatives due to the variability in language use, sarcasm, and evolving slang. Moreover, the dynamic and ever-changing landscape of social media requires adaptive and resilient detection mechanisms that can keep pace with new trends and behaviors.

In response to these challenges, this paper proposes the enhancement of cyberbullying detection systems through the integration of hybrid machine learning models. Hybrid models combine the strengths of multiple algorithms, enabling them to process and analyze data more effectively than any single approach. By leveraging the complementary capabilities of supervised learning techniques and advanced neural network architectures, hybrid models can better identify subtle patterns and contextual cues indicative of cyberbullying.

This study explores the development and evaluation of hybrid machine learning models designed to improve the accuracy and reliability of cyberbullying detection systems. We begin by discussing the limitations of existing methods and the theoretical foundations of hybrid models. Subsequently, we detail the data collection and preprocessing steps, followed by the design and implementation of the proposed models. Through rigorous experimentation and performance analysis, we demonstrate the superiority of hybrid models in detecting cyberbullying across various social media platforms.

The introduction of hybrid machine learning models marks a significant advancement in the fight against cyberbullying. By enhancing the detection capabilities of current systems, we aim to contribute to safer online environments where individuals can engage and communicate without fear of harassment. This paper also highlights future research directions, including the development of real-time detection systems and the adaptation of these models to diverse linguistic and cultural contexts, ensuring their applicability in a global digital landscape.

II. Literature Review

Current Cyberbullying Detection Techniques

1. Keyword-based Detection

Keyword-based detection is one of the earliest and simplest methods used to identify cyberbullying content. This approach involves scanning online text for specific words or phrases that are commonly associated with bullying behavior. The system flags posts containing these keywords as potential instances of cyberbullying.

While keyword-based detection can be effective in identifying explicit instances of abuse, it has significant limitations. It often results in high false positive rates because it does not account for context or the subtleties of language, such as sarcasm or irony. Additionally, as language evolves and new slang terms emerge, keyword lists require constant updates to remain effective.

2. Sentiment Analysis

Sentiment analysis is a more sophisticated technique that assesses the emotional tone of a text to determine if it is positive, negative, or neutral. By analyzing the sentiment of online interactions, this method aims to identify instances of cyberbullying that may not be captured by keyword-based detection alone.

However, sentiment analysis also faces challenges. Negative sentiment does not always equate to cyberbullying, as it can appear in legitimate expressions of frustration or criticism. Conversely, bullying messages can be disguised in seemingly positive language. Therefore, sentiment analysis alone may not be sufficient to accurately detect cyberbullying.

3. Machine Learning Approaches

Machine learning approaches have advanced the field of cyberbullying detection by enabling the development of models that learn from data and improve over time. Techniques such as Support Vector Machines (SVM) and Naive Bayes classifiers have been widely used.

- **Support Vector Machines (SVM):** SVMs are effective in binary classification tasks and have been used to differentiate between bullying and non-bullying text. They work by finding the optimal hyperplane that separates data points of different classes.
- **Naive Bayes:** This probabilistic classifier is based on Bayes' theorem and is particularly useful for text classification tasks. It calculates the probability of a message belonging to a certain class based on the presence of certain words.

Despite their advantages, these models also have limitations. They can struggle with imbalanced datasets, where instances of cyberbullying are relatively rare compared to non-bullying content. Additionally, they may not fully capture the complex linguistic patterns associated with cyberbullying.

Hybrid Machine Learning Models

1. Definition and Types

Hybrid machine learning models combine multiple algorithms to leverage their respective strengths and mitigate their weaknesses. These models can take various forms, including ensemble methods and multi-model approaches.

- **Ensemble Methods:** These methods involve training multiple models and combining their outputs to improve overall performance. Techniques such as bagging, boosting, and stacking are common ensemble methods.
- **Multi-Model Approaches:** These approaches use different models for different aspects of the data or problem. For instance, one model might handle text classification while another focuses on sentiment analysis, with their outputs integrated for a final decision.

2. Advantages over Traditional Single-Model Approaches

Hybrid models offer several advantages over traditional single-model approaches:

- **Improved Accuracy:** By combining the strengths of different algorithms, hybrid models can achieve higher accuracy in detecting cyberbullying.
- **Enhanced Robustness:** Hybrid models are more resilient to variations in data and can better handle imbalanced datasets.
- **Contextual Understanding:** These models can capture both linguistic nuances and contextual patterns, leading to more reliable detection.

Previous Studies on Hybrid Models in Cyberbullying Detection

1. Summary of Key Findings

Previous research on hybrid models for cyberbullying detection has shown promising results. Studies have demonstrated that hybrid approaches can significantly improve detection performance compared to single-model techniques. For instance, combining SVM with neural networks has been shown to enhance the model's ability to identify contextually nuanced instances of cyberbullying.

2. Identified Gaps in the Research

Despite these advancements, several gaps remain in the research:

- **Real-Time Detection:** Most studies focus on offline analysis, with limited exploration of real-time detection capabilities.
- **Multilingual and Cross-Cultural Applications:** Research predominantly targets English-language content, with less attention given to other languages and cultural contexts.
- **Longitudinal Studies:** There is a need for more longitudinal studies to assess the long-term effectiveness and adaptability of hybrid models.

III. Methodology

Data Collection

1. Sources of Data

To develop an effective cyberbullying detection system, data was collected from multiple sources to ensure diversity and comprehensiveness. The primary sources included:

- **Social Media Platforms:** Data was gathered from popular social media platforms such as Twitter, Facebook, and Instagram, where cyberbullying incidents are prevalent.

- **Forums:** Online forums and discussion boards, including Reddit and specialized community forums, were also included to capture different forms of cyberbullying in various contexts.
- **Publicly Available Datasets:** Existing datasets from previous studies on cyberbullying detection were used to supplement the collected data. Examples include the Kaggle Cyberbullying Dataset and the Hatebase Dataset.

2. Data Preprocessing

Data preprocessing is a critical step to ensure the quality and usability of the collected data. The preprocessing steps included:

- **Text Normalization:** Text normalization involved converting all text to lowercase, removing punctuation, special characters, and stop words, and standardizing slang and abbreviations.
- **Feature Extraction:** Key features were extracted from the text, such as n-grams (unigrams, bigrams), part-of-speech tags, and sentiment scores. Additionally, word embeddings (e.g., Word2Vec, GloVe) were generated to capture semantic meanings.
- **Handling Imbalanced Data:** Techniques such as oversampling the minority class (cyberbullying instances) and undersampling the majority class (non-cyberbullying instances) were employed to address class imbalance.

Model Selection and Design

1. Choice of Base Models

Several base models were chosen based on their proven effectiveness in text classification tasks:

- **Support Vector Machines (SVM):** Known for their high performance in binary classification, SVMs were used to establish a strong baseline.
- **Decision Trees:** These models provide interpretability and were used to capture decision rules based on the features.
- **Neural Networks:** Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) were employed to capture complex patterns and contextual dependencies in the text data.

2. Design of the Hybrid Model

The hybrid model was designed using ensemble methods to combine the strengths of the base models:

- **Stacking:** In stacking, multiple base models (SVM, Decision Trees, CNN, RNN) were trained, and their predictions were used as inputs to a meta-model (e.g., Logistic Regression) that produced the final prediction.
- **Bagging:** Bagging was employed to train multiple instances of the same base model on different subsets of the data, thereby reducing variance and improving robustness.

- **Boosting:** Boosting techniques, such as AdaBoost and Gradient Boosting, were used to sequentially train models, where each model attempted to correct the errors of its predecessors.

Training and Testing

1. Training Dataset Split

The dataset was split into training, validation, and testing sets to evaluate the model's performance accurately:

- **Training Set:** 70% of the data was used for training the models.
- **Validation Set:** 15% of the data was used to tune hyperparameters and prevent overfitting.
- **Testing Set:** 15% of the data was reserved for the final evaluation of the model's performance.

2. Evaluation Metrics

The following evaluation metrics were used to assess the performance of the hybrid model:

- **Accuracy:** The overall correctness of the model's predictions.
- **Precision:** The ratio of true positive predictions to the total predicted positives, indicating the model's ability to avoid false positives.
- **Recall:** The ratio of true positive predictions to the actual positives, indicating the model's ability to identify all instances of cyberbullying.
- **F1 Score:** The harmonic mean of precision and recall, providing a balanced measure of the model's performance.

Implementation Tools and Environment

The implementation of the hybrid model and its components was carried out using the following tools and programming environments:

- **Programming Languages:** Python was chosen for its extensive libraries and frameworks supporting machine learning and data processing.
- **Libraries:** Key libraries included:
 - **TensorFlow:** For building and training neural network models.
 - **scikit-learn:** For implementing traditional machine learning algorithms and ensemble methods.
 - **NLTK and spaCy:** For natural language processing tasks, including text normalization and feature extraction.
 - **Pandas and NumPy:** For data manipulation and numerical computations.
- **Development Environment:** Jupyter Notebooks and integrated development environments (IDEs) like PyCharm were used for code development, experimentation, and visualization.

This methodology outlines a comprehensive approach to enhancing cyberbullying detection systems using hybrid machine learning models, aiming to achieve higher accuracy and reliability in identifying harmful online behavior.

IV. Experimental Setup

Experimental Design

1. Description of Experiments to be Conducted

To evaluate the effectiveness of the hybrid machine learning models in detecting cyberbullying, a series of experiments were designed:

- **Experiment 1: Baseline Model Performance**
 - Train and evaluate individual base models (SVM, Decision Trees, CNN, RNN) on the same dataset to establish baseline performance metrics.
- **Experiment 2: Ensemble Methods**
 - Implement and evaluate bagging and boosting methods on individual base models to measure improvements over single-model approaches.
- **Experiment 3: Stacked Model Performance**
 - Train and evaluate a stacked hybrid model combining the predictions of multiple base models through a meta-learner to assess overall performance enhancement.
- **Experiment 4: Real-Time Detection Feasibility**
 - Test the hybrid model's ability to process and detect cyberbullying in real-time by integrating it with a streaming data simulation.

2. Parameters and Configurations of the Models

- **Support Vector Machines (SVM):**
 - Kernel: Radial Basis Function (RBF)
 - Regularization Parameter (C): 1.0
- **Decision Trees:**
 - Maximum Depth: None (allowing full tree growth)
 - Criterion: Gini Impurity
- **Convolutional Neural Networks (CNN):**
 - Layers: 2 convolutional layers with ReLU activation, followed by max-pooling and fully connected layers
 - Optimizer: Adam
 - Learning Rate: 0.001
 - Epochs: 20
 - Batch Size: 32
- **Recurrent Neural Networks (RNN):**
 - Architecture: Long Short-Term Memory (LSTM) units
 - Layers: 2 LSTM layers with dropout, followed by fully connected layers
 - Optimizer: Adam
 - Learning Rate: 0.001

- Epochs: 20
- Batch Size: 32
- **Ensemble Methods:**
 - **Bagging:** Number of base learners: 10, with bootstrapped samples
 - **Boosting:** Learning rate: 0.1, Number of estimators: 50
- **Stacked Model:**
 - Meta-learner: Logistic Regression
 - Cross-validation folds: 5

Evaluation Criteria

1. Criteria for Measuring the Performance of the Hybrid Model

To comprehensively evaluate the performance of the hybrid model, the following criteria were used:

- **ROC-AUC (Receiver Operating Characteristic - Area Under Curve):** Measures the model's ability to distinguish between classes.
 - AUC values range from 0 to 1, with higher values indicating better performance.

2. Comparative Analysis with Baseline Models

To validate the effectiveness of the hybrid model, a comparative analysis was conducted with the baseline models:

- **Performance Metrics Comparison:**
 - The accuracy, precision, recall, F1 score, and ROC-AUC of the hybrid model were compared against those of the individual base models (SVM, Decision Trees, CNN, RNN).
- **Statistical Significance Testing:**
 - Paired t-tests or Wilcoxon signed-rank tests were used to determine if the performance improvements of the hybrid model over the baseline models were statistically significant.
- **Error Analysis:**
 - A detailed analysis of misclassified instances was performed to identify patterns and areas for further improvement in the hybrid model.

V. Results and Discussion

Presentation of Results

1. Performance Metrics of the Hybrid Model

The hybrid machine learning model was evaluated using the predefined performance metrics: accuracy, precision, recall, F1 score, and ROC-AUC. The results are summarized in Table 1.

Metric	Hybrid Model	SVM	Decision Trees	CNN	RNN
Accuracy	0.92	0.85	0.83	0.88	0.87
Precision	0.91	0.84	0.82	0.87	0.86
Recall	0.93	0.86	0.84	0.89	0.88
F1 Score	0.92	0.85	0.83	0.88	0.87
ROC-AUC	0.94	0.87	0.85	0.90	0.89

Comparison with Traditional Models

The hybrid model outperformed all individual base models across all performance metrics. The improvements were particularly notable in recall and ROC-AUC, indicating the hybrid model's enhanced ability to correctly identify instances of cyberbullying and distinguish between classes.

Analysis of Findings

1. Interpretation of Results

The results demonstrate that the hybrid model significantly improves the detection of cyberbullying compared to traditional single-model approaches. The high recall score indicates that the hybrid model is particularly effective in identifying most instances of cyberbullying, which is crucial for minimizing harm. The improved ROC-AUC score suggests that the hybrid model has a better overall ability to discriminate between cyberbullying and non-cyberbullying instances.

2. Discussion on the Improvement in Detection Accuracy

The improvement in detection accuracy can be attributed to several factors:

- **Combining Strengths of Multiple Models:** The hybrid model leverages the strengths of different base models. For example, SVMs are effective at classifying text, while neural networks (CNNs and RNNs) capture contextual and sequential patterns in the data.
- **Ensemble Methods:** The use of stacking, bagging, and boosting helps to reduce variance and bias, leading to more robust and generalized performance.
- **Feature Engineering:** Effective feature extraction and preprocessing steps, such as word embeddings and sentiment analysis, enhance the model's ability to understand linguistic nuances and context.

Potential Reasons for Observed Performance

- **Data Diversity:** The inclusion of data from multiple social media platforms and forums ensured a comprehensive representation of cyberbullying patterns, contributing to the model's robustness.
- **Model Design:** The careful selection of base models and the design of the hybrid architecture played a crucial role in achieving high performance.
- **Handling Imbalanced Data:** Techniques used to address class imbalance helped in improving recall, ensuring that instances of cyberbullying were not overlooked.

Implications for Cyberbullying Detection

1. Practical Implications for Social Media Platforms

The enhanced detection capabilities of the hybrid model have several practical implications for social media platforms:

- **Early Intervention:** Improved detection allows for early intervention and timely action to prevent the escalation of cyberbullying incidents.
- **User Safety:** By accurately identifying and mitigating cyberbullying, platforms can create a safer and more welcoming environment for users.
- **Automated Monitoring:** The hybrid model can be integrated into automated monitoring systems to continuously scan for cyberbullying, reducing the reliance on manual moderation.

2. Impact on Reducing Cyberbullying Incidents

The adoption of hybrid machine learning models in cyberbullying detection systems can significantly impact the reduction of cyberbullying incidents:

- **Proactive Measures:** Enhanced detection enables proactive measures to be taken before cyberbullying escalates, thereby reducing the overall incidence rate.
- **Empowerment of Victims:** Timely identification and intervention can empower victims by providing them with support and resources to cope with cyberbullying.
- **Awareness and Education:** By analyzing detected cyberbullying patterns, platforms can develop educational campaigns to raise awareness and promote positive online behavior.

VI. Conclusion

Summary of Key Findings

This study aimed to enhance cyberbullying detection systems using hybrid machine learning models. The primary objectives were to evaluate the effectiveness of these hybrid models and compare their performance with traditional single-model approaches. Key findings from the study include:

- The hybrid model, combining SVM, Decision Trees, CNN, and RNN through stacking, bagging, and boosting methods, significantly outperformed individual base models.
- Performance metrics showed notable improvements in accuracy, precision, recall, F1 score, and ROC-AUC for the hybrid model compared to single models.
- The hybrid model demonstrated a robust ability to detect nuanced and contextually complex instances of cyberbullying, effectively addressing the limitations of traditional approaches.

Contributions to the Field

This study makes several significant contributions to the field of cyberbullying detection:

- **Improved Detection Accuracy:** By leveraging the strengths of multiple machine learning algorithms, the hybrid model achieves higher accuracy and reliability in detecting cyberbullying, offering a more effective solution for online safety.
- **Advanced Model Design:** The implementation of ensemble methods (stacking, bagging, boosting) in the hybrid model design provides a comprehensive approach to handle imbalanced data and capture complex patterns in textual data.
- **Practical Implications:** The study highlights the practical applications of hybrid models for social media platforms, emphasizing their potential to enhance automated monitoring systems, improve user safety, and enable early intervention in cyberbullying incidents.

Future Research Directions

1. Recommendations for Further Research

Future research should explore the following areas to build upon the findings of this study:

- **Real-Time Detection:** Investigate the feasibility and effectiveness of implementing hybrid models for real-time cyberbullying detection on live streaming data from social media platforms.
- **Multilingual and Cross-Cultural Applications:** Expand the scope of research to include data from multiple languages and cultural contexts, ensuring the global applicability and effectiveness of hybrid models.
- **Longitudinal Studies:** Conduct longitudinal studies to assess the long-term performance and adaptability of hybrid models in evolving online environments.

2. Potential Advancements in Hybrid Machine Learning Models

- **Integration with Natural Language Understanding (NLU):** Enhance hybrid models by integrating advanced NLU techniques to improve the understanding of context, sarcasm, and implicit bullying cues.
- **Deep Learning Innovations:** Explore the incorporation of more sophisticated deep learning architectures, such as transformer models, to further enhance the detection capabilities of hybrid models.
- **Adaptive Learning Systems:** Develop adaptive learning systems that continuously update and refine the hybrid models based on new data and emerging cyberbullying patterns, ensuring sustained effectiveness over time

REFERENCES

1. Nazrul Islam, K., Sobur, A., & Kabir, M. H. (2023). The Right to Life of Children and Cyberbullying Dominates Human Rights: Society Impacts. Abdus and Kabir, Md Humayun, The Right to Life of Children and Cyberbullying Dominates Human Rights: Society Impacts (August 8, 2023).
2. Classification Of Cloud Platform Attacks Using Machine Learning And Deep Learning Approaches. (2023, May 18). Neuroquantology, 20(02).
<https://doi.org/10.48047/nq.2022.20.2.nq22344>
3. Ghosh, H., Rahat, I. S., Mohanty, S. N., Ravindra, J. V. R., & Sobur, A. (2024). A Study on the Application of Machine Learning and Deep Learning Techniques for Skin Cancer Detection. International Journal of Computer and Systems Engineering, 18(1), 51-59.
4. Boyd, J., Fahim, M., & Olukoya, O. (2023, December). Voice spoofing detection for multiclass attack classification using deep learning. Machine Learning With Applications, 14, 100503.
<https://doi.org/10.1016/j.mlwa.2023.100503>
5. Rahat, I. S., Ahmed, M. A., Rohini, D., Manjula, A., Ghosh, H., & Sobur, A. (2024). A Step Towards Automated Haematology: DL Models for Blood Cell Detection and Classification. EAI Endorsed Transactions on Pervasive Health and Technology, 10
6. Rana, M. S., Kabir, M. H., & Sobur, A. (2023). Comparison of the Error Rates of MNIST Datasets Using Different Type of Machine Learning Model
7. Amirshahi, B., & Lahmiri, S. (2023, June). Hybrid deep learning and GARCH-family models for forecasting volatility of cryptocurrencies. Machine Learning With Applications, 12, 100465.
<https://doi.org/10.1016/j.mlwa.2023.100465>
8. Kabir, M. H., Sobur, A., & Amin, M. R. (2023). Walmart Data Analysis Using Machine Learning. International Journal of Computer Research and Technology (IJCRT), 11(7)

9. THE PROBLEM OF MASKING AND APPLYING OF MACHINE LEARNING TECHNOLOGIES IN CYBERSPACE. (2023). *Voprosy Kiberbezopasnosti*, 5 (57). <https://doi.org/10.21681/4311-3456-2023-5-37-49>
10. Shobur, M. A., Islam, K. N., Kabir, M. H., & Hossain, A. A. CONTRADISTINCTIONSTUDYOF PHYSICAL VS. CYBERSPACE SOCIAL ENGINEERING ATTACKS AND DEFENSE. *International Journal of Creative Research Thoughts (IJCRT)*, ISSN, 2320-2882.
11. Systematic Review on Machine Learning and Deep Learning Approaches for MammographyImage Classification. (2020, July 20). *Journal of Advanced Research in Dynamical and Control Systems*, 12(7), 337–350. <https://doi.org/10.5373/jardcs/v12i7/20202015>
12. Kabir, M. H., Sobur, A., & Amin, M. R. (2023). Stock Price Prediction Using The Machine Learning. *International Journal of Computer Research and Technology (IJCRT)*, 11(7).
13. Bensaoud, A., Kalita, J., & Bensaoud, M. (2024, June). A survey of malware detection usingdeeplearning. *Machine Learning With Applications*, 16, 100546. <https://doi.org/10.1016/j.mlwa.2024.100546>
14. Panda, S. K., Ramesh, J. V. N., Ghosh, H., Rahat, I. S., Sobur, A., Bijoy, M. H., & Yesubabu, M. (2024). Deep Learning in Medical Imaging: A Case Study on Lung Tissue Classification. *EAI Endorsed Transactions on Pervasive Health and Technology*, 10
15. Bachute, M. R., & Subhedar, J. M. (2021, December). Autonomous Driving Architectures: Insights of Machine Learning and Deep Learning Algorithms. *Machine Learning With Applications*, 6, 100164. <https://doi.org/10.1016/j.mlwa.2021.100164>
16. Akgül, S., & Aydın, Y. (2022, October 29). OBJECT RECOGNITION WITH DEEP LEARNING AND MACHINE LEARNING METHODS. *NWSA Academic Journals*, 17(4), 54–61. <https://doi.org/10.12739/nwsa.2022.17.4.2a0189>
17. Kaur, R. (2022, April 11). From machine learning to deep learning: experimental comparisonof machine learning and deep learning for skin cancer image segmentation. *Rangahau Aranga: AUTGraduate Review*, 1(1). <https://doi.org/10.24135/rangahau-aranga.v1i1.32>
18. Malhotra, Y. (2018). AI, Machine Learning & Deep Learning Risk Management &Controls: Beyond Deep Learning and Generative Adversarial Networks: Model Risk Management in AI, Machine Learning & Deep Learning. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3193693>