AI System For MITRE ATT&CK Threat Classification and Organizational Impact Analysis

Prapatsorn Alongkornpradub, Vorameth Reantongcome, and Ekkarat Techanawakarnkul
Department of Computer Science and Information Management
Asian Institute of Technology
Pathumthani, Thailand
{st124846, st124903, st124945}@ait.asia

Abstract

Cybersecurity threats are rapidly evolving, making traditional methods of threat analysis inefficient and time-consuming. This research proposes an AI-powered system that uses Natural Language Processing (NLP) to automatically classify cybersecurity news into MITRE ATT&CK techniques. A fine-tuned BERT model will automate classification, enabling organizations to analyze threat intelligence more efficiently. The experiment involves training and evaluating the BERT model on cybersecurity news articles, assessing its performance using classification metrics. The expected outcome is an accurate system that automates threat intelligence and helps organizations make informed security decisions.

1 Introduction

Cybersecurity threats are evolving at an unprecedented rate, posing significant risks to organizations, governments, and individuals. As cyberattacks become more sophisticated, the ability to quickly analyze and respond to these threats is critical in protecting valuable assets. The MITRE ATT&CK framework, a comprehensive taxonomy of adversarial tactics, techniques, and procedures (TTPs), provides cybersecurity professionals with a structured approach to understanding attacker behaviors and developing defense strategies. However, identifying relevant TTPs from a high volume of cybersecurity news articles remains a challenging task due to the complexity of technical language, inconsistent writing styles, and the sheer amount of threat reports. Manual mapping of security incidents to the ATT&CK framework is inefficient and time-consuming, making it difficult for organizations to keep pace with emerging threats.

To address this challenge, this research proposes an AI-powered system that utilizes Natural Language Processing (NLP) to classify cybersecurity news articles into MITRE ATT&CK techniques. By fine-tuning a BERT model on a labeled dataset of cybersecurity incidents and their corresponding TTPs, this system will automate the process of threat classification. This approach will enable security teams to more efficiently analyze cybersecurity threats, quickly determining which ATT&CK techniques are relevant to specific incidents, and aiding in identifying the affected areas within an organization.

Unlike traditional keyword-based or rule-based threat intelligence systems, which rely on predefined rules and patterns, this system will leverage deep learning-based text classification to significantly enhance both accuracy and scalability. Many existing systems analyze cybersecurity data, but few focus on automatically mapping cybersecurity news to the MITRE ATT&CK framework, which is crucial for a deeper understanding of attacker behaviors. Cybersecurity news articles often contain complex terminology, ambiguous descriptions of attacks, and diverse writing styles, making automated classification a particularly challenging task. By fine-tuning a BERT model specifically on cybersecurity threat intelligence data, this research aims to automate the process of threat classification, reducing the time and effort needed for manual analysis. This will not only enable security teams to respond to emerging threats more quickly but also minimize human error and inconsistencies that arise from manual mapping. Ultimately, the system will empower organizations to make more informed security decisions with greater speed and accuracy, optimizing resource allocation and improving overall threat response efficiency.

1.1 Research Questions

This study aims to answer the following key research questions:

1. How effectively can a fine-tuned BERT model classify cybersecurity news into ATT&CK techniques?

2. How does the performance of the BERT model compare to manual classification approaches in cybersecurity threat analysis?

3. What impact does fine-tuning a transformer model like BERT on a cybersecurity-specific dataset have on the accuracy and relevance of threat classification?

The contributions of this research include the development of an NLP-based system that automates the classification of cybersecurity threats, improving efficiency and reducing the manual effort required in the threat analysis process. By integrating a fine-tuned BERT model, the system will provide structured and actionable threat intelligence, helping organizations improve cybersecurity decision-making and enhance incident response times.

1.2 Rough Idea of the Experiment

The experiment will begin with data preprocessing, where cybersecurity news articles and their corresponding MITRE ATT&CK technique labels will be cleaned and prepared for model training. This involves tokenizing the text, removing any irrelevant information, and formatting the data into a suitable structure for input into the model. A fine-tuned BERT model will be trained on this dataset, using the preprocessed news articles to classify them into the relevant ATT&CK techniques. The dataset will be divided into training, validation, and test sets to ensure that the model generalizes well to new, unseen data. The model's performance will be evaluated using a range of classification metrics, including accuracy, precision, recall, and F1-score.

To evaluate the effectiveness of the fine-tuned BERT model, it will be compared against baseline models that use traditional keyword-based or rule-based methods for threat classification. Additionally, human feedback from cybersecurity professionals will be incorporated during the evaluation process to assess the relevance of the classifications and further refine the model. This feedback loop will help ensure that the model produces practical and useful results for real-world cybersecurity threat analysis.

1.3 Rough Idea of the Expected Results

This research expects to develop an accurate and efficient NLP-based system capable of classifying cybersecurity news articles into MITRE ATT&CK techniques with high precision and low error rates. By fine-tuning the BERT model on a cybersecurity-specific dataset, the system should effectively generalize to new attack reports and maintain high performance across different types of cyber incidents. A comparative analysis will be conducted to evaluate the performance of the fine-tuned BERT model against traditional classification methods, such as keyword-based or rule-based systems.

The expected outcome is that the fine-tuned BERT model will significantly outperform traditional methods in terms of classification accuracy and relevance. By leveraging deep learning, the system will provide a more nuanced understanding of threats, allowing security teams to categorize and analyze cybersecurity incidents more effectively. Ultimately, this research aims to reduce the manual effort involved in threat classification, enhance decision-making in incident response, and improve overall threat intelligence capabilities within organizations.

2 Related Works

2.1 Noise Contrastive Estimation-based Matching Framework for Low-Resource Security Attack Pattern Recognition

With the complexity, long-tailedness and huge number of multi-label classification of Tactics,Techniques and Procedures (TTPs), this could hinder the learning ability of the model. From following problems the authors propose a new learning paradigm on mapping the TTPs in classification problem which consist of introducing ranking-based Noise Contrastive Estimation (NCE) for handling large labelling together with missing labels problems, curating and publicizing an export-annotation dataset, and conducting extensive experiments in their learning methods. The result had shown that proposed NCE-based models outperformed the other baselines model through the comparison, datasets crafting, and hyperparameter tuning. This could help for a new learning paradigm integrated with inductive bias into classification tasks to overkill the other baselines. (Nguyen, Šrndić, & Neth, 2024).

From the new learning model, the time for training took a very long time with current resources.

Consequently, the TTPs had been applied to only one-third of the whole framework in MITRE ATT&CK.

2.2 Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study

Cybersecurity Threat Intelligence (CTI) provides information shared among cybersecurity engineers which will help to spread an indicator of compromise or attack pattern in order to proactive investigate or detect the threat before any attack or incident happens or spreads. Normally, the CTI publishes through a form of unstructured format, i.e., natural language through incident report or threat analysis news. To support cybersecurity proactively, machine learning will be used in order to classify the CTI into the MITRE ATT&CK category. General machine learning and deep learning were being experimented. Eventually, deep learning could outperform general machine learning. In addition, the sentence-level model could outperform the document-level model. From the result, the author concluded that due to the complexity of natural language making such an accurate model could be challenging.

From the experiment, the author provides a dataset which could be used for training the model according to the CTI information aggregation. Moreover, deep learning will be focused according to experiments that the author concluded (Orbinato et al., 2022).

2.3 A Pretrained Language Model for Cyber Threat Intelligence

To digest the information from many Cyber Threat Intelligence reports within a time limit, the authors develop a pre-trained BERT model tailoring for cybersecurity domain for performing extensive experiments on a wide range of tasks and benchmark datasets for the security domain in order to curate a large amount of high quality cybersecurity datasets specifically designed for cyber-threat intelligence analysis. The papers start with data collection from many sources for example academic papers, security wiki, threat reports, and vulnerability. Then, they do the model training and followed with evaluation through applications for example word prediction, MITRE ATT&CK Framework Classification, malware sentence detection, and malware classification. As a result, the authors conclude that the proposed model outperformed the existing general domain (bert-base-uncased and roberta-base) and other cybersecurity domain models (SecBERT and SecRoBERTa) (Park and You, 2023).

Even if the model could outperform the other general or cybersecurity model domain, the limitations are the size of the datasets. With limited size of datasets, the authors still couldn't conclude the performance of the model according to their expectations. This could cause some problems with unknown news or contexts that haven't been trained before. Additionally, the model could support only in the English language, where most of the CTIs are distributed in many languages.

From this paper, the CTI-BERT and SecureBERT could be further extended to support MITRE ATT&CK classification problems. While the original model helps to classify the mitigation and counter-measure of attack according to the model, the proposed model will implement the attack pattern with the MITRE ATT&CK category.

2.4 AnnoCTR: A Dataset for Detecting and Linking Entities, Tactics, and Techniques in Cyber Threat Reports

The AnnoCTR dataset, introduced by Lange et al. (2024), represents a significant advancement in the application of Natural Language Processing (NLP) to cybersecurity. It consists of 400 cyber threat reports (CTRs), 120 of which are annotated by domain experts with named entities, temporal expressions, and cybersecurity-specific concepts, including tactics and techniques from the MITRE ATT&CK knowledge base. Unlike datasets that either provide a single label per document or annotate sentences out of context, AnnoCTR annotates entire documents with a fine-grained level of detail, making it particularly useful for training NLP models for tasks like Named Entity Recognition (NER), temporal tagging, and tactic/technique classification. While AnnoCTR focuses on linking entities and techniques to knowledge bases like MITRE ATT&CK, this project extends these ideas by focusing on the automation of threat classification from cybersecurity news articles. Specifically, this project uses a fine-tuned BERT model to classify incidents into MITRE ATT&CK techniques, improving the efficiency and accuracy of threat intelligence systems. Both approaches aim to reduce manual effort in cybersecurity analysis and enhance real-time decision-making, with AnnoCTR providing a foundation for building models that can be applied to real-world cyber threat reports.

2.5 Introducing a New Dataset for Event Detection in Cybersecurity Texts

Cybersecurity event detection (ED) has been explored in several datasets, although most focus on general-domain events rather than cybersecurity-specific threats. The ACE dataset and TAC KBP are widely used in the general ED domain but fail to capture the domain-specific characteristics of cybersecurity events. The CASIE dataset addressed this gap by introducing a small-scale cybersecurity ED dataset with five event types. However, CASIE's reliance on sentence-level context limits its ability to model complex event dependencies and fails to fully capture the nuances of cybersecurity threats (Duc Trong et al., 2020).

In response to this, the CySecED dataset expanded the scope, offering 30 event types and incorporating document-level context. This advancement allows for more granular event detection and better models the complex relationships between cybersecurity events across entire documents. However, despite these improvements, ED models on CySecED still perform far below human-level accuracy. This demonstrates a clear gap in existing methodologies—while document-level models such as DEEB-RNN (Zhao et al., 2018) have shown some success, they still struggle with accurately capturing long-range dependencies and the contextual nature of cybersecurity event relationships.

In contrast to the traditional ED focus, this work shifts the emphasis from detecting trigger words to improving cyber threat intelligence (CTI) retrieval. Existing ED models and approaches, such as those based on embedding techniques, fail to accurately capture the nuanced relationships between event descriptions in cybersecurity. In this context, the approach aims to bridge this gap by introducing novel methods for improving the accuracy and efficiency of CTI retrieval. Unlike traditional ED methods, this work focuses on refining the search and retrieval of cybersecurity threat intelligence data, moving beyond the limitations of trigger-based detection to address broader contextual and semantic relationships within attack descriptions. The project, by integrating contextual understanding, will enhance the performance of existing systems that rely on simple keyword-based or embedding-based models.

2.6 Full-Stack Information Extraction System for Cybersecurity Intelligence

The paper presents an advanced approach to cybersecurity threat intelligence by focusing on automating the process of extracting and organizing cyber threat information from unstructured sources like news articles, blogs, and threat reports. The system uses several natural language processing (NLP) techniques, such as named entity recognition (NER), to identify cybersecurity-related terms like malware names, attack methods, and profiles of threat actors. By doing this, the system helps turn raw text data into more manageable and useful information, making it easier to monitor and analyze new cybersecurity incidents. The system also uses methods to understand relationships between different entities and extract time-related information, which helps to understand how cyber threats change over time and how different elements are connected, giving a more complete picture of cybersecurity risks (Park & Lee, 2022).

While the study shows an effective system for extracting and organizing threat information, it lacks integration with a standardized framework like MITRE ATT&CK, which classifies different attack techniques. Without such a framework, the extracted data remains disorganized, which makes it harder to provide actionable insights and slow down decision-making and threat prevention. Also, the system does not classify the extracted entities into specific attack techniques, which is important for better understanding the situation. This gap will be addressed in the proposed research, which aims to create an AI system that organizes cybersecurity news into MITRE ATT&CK techniques and evaluates its impact on organizations.

3 Methodology

With the proposed solution, the deep detail will be explained according to the tasks which will be part of the whole system.

3.1 Old Workflow and New Workflow

As a cybersecurity engineer, identifying the threat from news or articles could cost a lot of time for manually processing. From the time consuming problem, the cybersecurity engineers must spend much of their man-day in reading and understanding the news or articles, summarization of threats in paragraphs, identifying the technique and tactics using and mapping into the potential organization resources. After exploring the Natural Language Understanding course, the old workflow could be improved by applying natural language processing, hoping to reduce the time

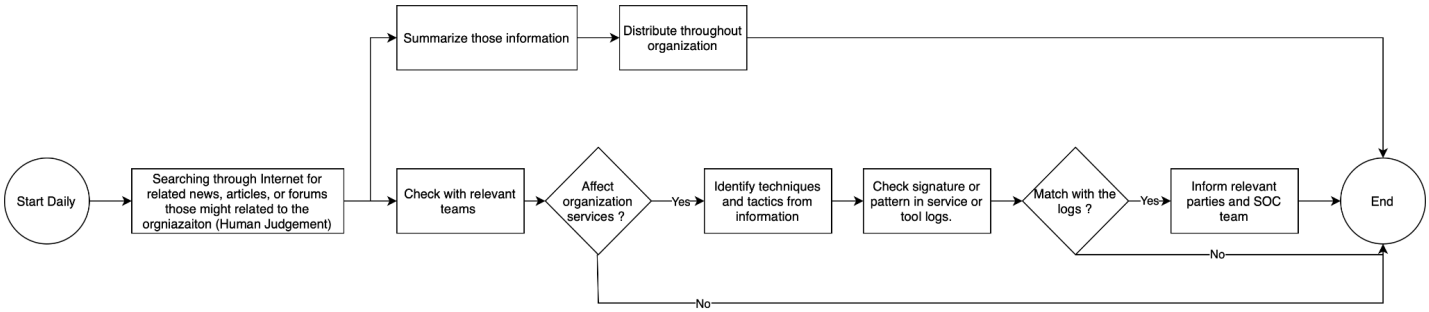

Figure 1: Old Work Flow

consuming problem and help to quickly identify the threats before hackers could attack the organization.

Old Workflow

As shown on Figure 1., The old workflow started with searching through the websites and filtering any threat or cybersecurity incident news, articles, or forums which related to the organization. The process is performed by human judgement. Then, the information will be distributed into two tasks. Firstly, the data will be summarized and shared with executive and other teams for security awareness. The other task is threat identification. The information will be checked against each team in order to identify potential effects of the systems. After verification, the information will be extracted for techniques and tactics which will help to identify the pattern that attacks in organization. If the patterns are matched, the relevant parties and SOC team will be informed for initializing a mitigation plan.

New Workflow

From Figure 2., in the very first step, the security datasets will be pre-processed according to the techniques for the selected pre-trained model. The common pre-processing methods are cleaning text, formatting, or adding marked characters. Additionally, the datasets will be explored for the compatibility and some context on the meaning in order to understand the learnability of the model. After that, the processed datasets will be trained through the pre-trained models available on the Internet. In this preliminary proposal, the BERT model will be chosen as the trained model for specific classification on the MITRE ATT&CK frameworks with cybersecurity context. In the deployment model, the best pre-processing methods will be used for input processing news or articles which could extract the related security information allowing the accurate classification result.

3.2 Datasets

There are three datasets that will be used in this methodology for training the model and using it as a document retrieval. The first potential dataset is tumeteor/Security-TTP-Mapping (tumeteor, n.d.) where the authors show the mapping of the security text with the Tactics, Techniques, and Procedures which could imply that hackers might use this kind of process according to the news to convey the attack. The next potential dataset comes from a paper (Orbinato et al., 2022). They published a dataset which helps to train the model according to the MITRE ATT&CK. The dataset is the aggregation of attack pattern object and relationship in JSON with some of the documents about the incident mapped with MITRE ATT&CK techniques and tactics. The other potential dataset consists of questions and answers regarding the MITRE Frameworks. The last potential dataset is Zainabsa99/mitre_attack (Zainabsa99, n.d.) which translates the MITRE ATT&CK IDs into the consumable datasets through a Huggingface platform consisting of ID, name, description, and detection.

3.3 Data preprocessing

Generalized sentences will be processed at the very first of the model creation. This includes lower case and removing unnecessary characters. During the training of the model, the tokenizer from the model will be used to transform a word into a token and create a word for loading into the model with sentence level including padding, end of sentence tag, and beginning tag. For the real-world implementation, the sentence and clause level will be used in order to evaluate the best accuracy

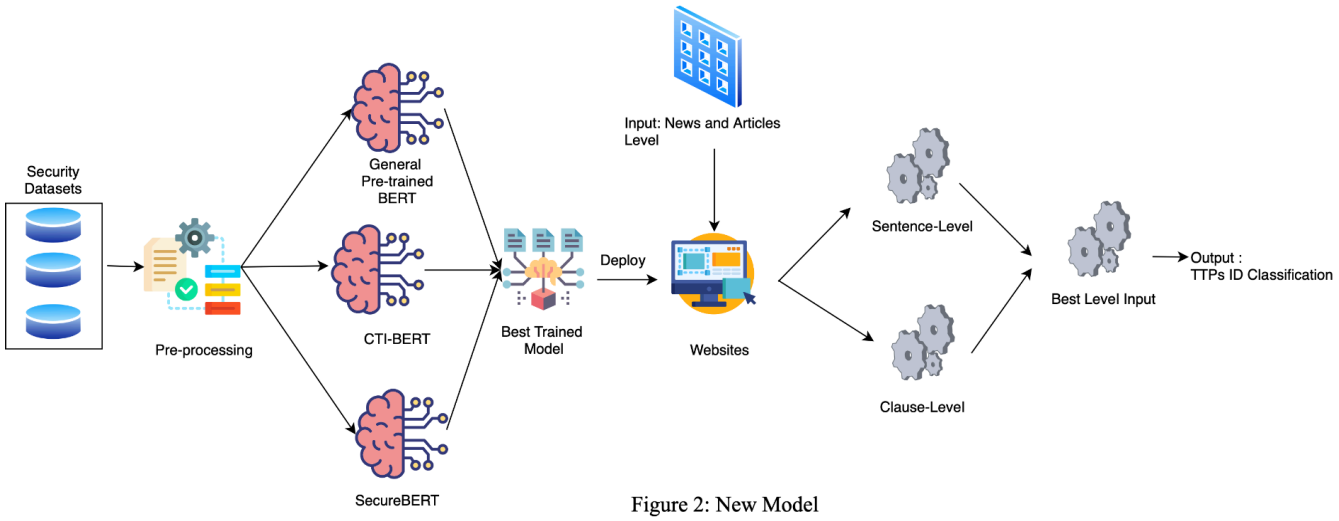

Figure 2: New Model

according to the feed words into the model to predict the correct techniques and tactics IDs.

3.4 Models

With classification problems, BERT will be the main model that will be used in this proposed solution. The model that will be used in this project is the CTI-BERT (Park and You, 2023) which has been trained to specialize in the cybersecurity domain extended from pre-trained SecBert (jackaduma, 2022) model. Secure-BERT (Aghaei et al., 2023) is another model that will be compared with other BERT models which extend from the pre-trained Ro-Bert model. The base model will be bert-base-uncased from Hugginface. These three models will be compared in order to find the best model that will be used in the system.

3.5 Training

From the pre-trained model, the datasets from the cybersecurity context will be applied into the pre-trained model in order to customize the model to specifically expertise at the cybersecurity context. There are three pre-trained model that will be used to compare in order to select the best model that will be used

3.6 Experiment

From the proposed solution, there are two experiments that will be performed in order to find the best model and input pre-processing.

Model Experiment

For the mode experiment, three models as mentioned in Model topic will be used in order to identify the best model for the most accurate classification task. Bert-base-uncased will be used as the base model for comparison with other models. This model will load from the Hugginface repository. The actual models that will be compared are CTI-BERT and Secure-BERT. These three models will use the tokenizer and word embedding from their own model. The hyperparameter will be the default values. These three models will be trained with the same three datasets for initializing the classification task with MITRE ATT&CK scenarios. In the final result, the three models will be compared with evaluation results, i.e., training loss, validation loss, and classification accuracy. Eventually, the best model selected will be selected in order to perform next experiments.

Input Pre-processing Experiment

The input from the news and articles will be processed with two methods for experiment. Each method could give the most accurate results according to the context of the news or articles. The first method is sentence-level which will process the news or articles into a sentence for mapping the relation with the attack pattern from MITRE ATT&CK meaning. In the second method, the clause of sentence will be used for mapping with attack pattern form MITRE ATT&CK. These two methods will be compared through a cybersecurity analyst or engineer to verify the correctness of classification results.

3.7 Evaluation / Metrics

To evaluate the models, two mechanisms will be used. The first method involves calculating performance metrics such as accuracy, precision, recall, and F1-score, which will evaluate how well the model classifies data during the training process with validation datasets. The second method is human evaluation, where cybersecurity experts from each organization will assess the model by answering specific questions to gauge its effectiveness.

4 Preliminary Results

This section presents the preliminary results from the experiments conducted to evaluate the performance of various BERT-based models in classifying cybersecurity news into MITRE ATT&CK techniques. The evaluation involved three models: BERT-base-uncased, CTI-BERT, and Secure-BERT. These models were trained on a cybersecurity-specific dataset and evaluated using standard classification metrics, including training loss, validation loss, accuracy, precision, recall, and F1-score.

4.1 Model Performance

The performance of the three models was evaluated using the metrics above, with training and validation losses, accuracy, precision, recall, and F1-score summarized in Table 1 as follows:

Metrics	BERT-base-uncased	CTI-BERT	SecureBERT
Training loss	3.575500	2.774000	3.579800
Validation loss	3.438241	2.707260	3.307534
Accuracy	0.437643	0.546388	0.444487
Precision	0.292122	0.431662	0.299807
Recall	0.437643	0.546388	0.444487
F1-Score	0.333476	0.466138	0.337116

Table 1: Preliminary Results of BERT-based Models

From Table 1, CTI-BERT outperforms the other models across all metrics. It achieved the lowest training loss (2.77) and validation loss (2.71). With an accuracy of 54.64% which was about 10% higher than BERT-base-uncased. It also had the highest precision (43.17%) and recall (54.64%), resulting in the best F1-score of 46.61%.

4.2 Real-world Impact on Threat Intelligence

The expected outcome of this research is that the fine-tuned BERT model, particularly CTI-BERT, will significantly reduce the time required for threat classification. By automating the process of classifying cybersecurity news articles into MITRE ATT&CK techniques, cybersecurity teams will be able to quickly identify relevant attack patterns, improving response times to emerging threats. This will lead to faster decision-making in incident response, reduce human error, and avoid inconsistencies in manual threat mapping. The automated system will help security teams make better, faster decisions, improve resource use, and strengthen overall cybersecurity.

5 Discussion

The discussion evaluates the effectiveness of the fine-tuned BERT model in classifying cybersecurity news into MITRE ATT&CK techniques, comparing it to manual classification approaches. The findings are addressed in relation to the research questions (RQ1, RQ2, and RQ3), explore the impact of the work, and acknowledge the limitations, along with potential areas for future improvement.

5.1 Effectiveness of the BERT Model for Threat Classification (RQ1)

The preliminary results of this study demonstrate that the BERT-based models, particularly CTI-BERT, are effective in classifying cybersecurity news articles into MITRE ATT&CK techniques. This suggests that the BERT-based model has the capability to understand and categorize complex cybersecurity incidents, even with the challenging terminology and writing styles prevalent in cybersecurity news.

5.2 Comparison to Manual Classification Methods (RQ2)

Manual classification approaches, which rely on human judgment, are often slow, inconsistent, and prone to errors. In comparison, the BERT model—specifically CTI-BERT—offers a substantial improvement in speed

and consistency. While human classifiers are often overburdened with the complexity and volume of cybersecurity reports, the BERT model can process and classify large datasets in a much shorter time.

Human input will still be valuable to ensure classifications align with organizational needs. While expert feedback has not yet been fully incorporated, it will be crucial for fine-tuning the model in future work. Although AI-driven classification accelerates the process, human validation will remain key to ensuring the quality of threat classification.

5.3 Impact of Fine-Tuning a Transformer Model on Accuracy (RQ3)

Fine-tuning a transformer model like BERT on a cybersecurity-specific dataset improved accuracy. The fine-tuned model showed improvements in training and validation loss, as well as a higher F1-score (46.61%) compared to the base BERT model. This suggests that the fine-tuning process on the cybersecurity dataset enhances the model's ability to classify cybersecurity content effectively.

5.4 Impact of the Work

While still in progress, this research has the potential to make a significant impact on how MITRE ATT&CK techniques are classified and analyzed in cybersecurity threats. Automating the classification of cybersecurity news into specific ATT&CK techniques can help security teams save time and reduce the manual effort required to process large volumes of threat data. This allows security professionals to focus more on analyzing and responding to the attack techniques used by adversaries, rather than performing repetitive tasks. Additionally, by improving the speed and accuracy of technique classification, the system can support faster decision-making in incident response, enabling organizations to react to attacks more quickly and effectively.

5.5 Limitations and Challenges

The limitations of the proposed system are the ground truth datasets. Due to the imbalanced data and limited datasets, the ground truth for verifying the correctness of the model in real-world datasets. In addition, the trained dataset is quite limited due to the specialization of the domain in which most of the datasets were processed and collected in a few amounts across the dataset provided platforms. Moreover, the complexity of the MITRE ATT&CK framework could prevent the model from capturing the context and insight of the framework which eventually could cause a new use case to be classified inaccurately.

5.6 Future Work

The main improvement of the model is the experiment method. In order to provide a more comprehensive model, the mechanism of capturing and extracting keywords from the datasets will be extended from the original model in order to provide an insightful and intuitive meaning extraction which will be integrated with a classification task. Moreover, the ground truth datasets will be identified and collected for providing a reliable base scenario allowing the validation of the real-world implementation to be reliable and accurate.

5.7 Conclusion

In conclusion, this research demonstrates the potential of AI-driven NLP systems to improve the efficiency and accuracy of cybersecurity threat classification. Although the system is still in development, the fine-tuned BERT model has shown promising results so far. Continued work will focus on refining the model, incorporating expert feedback, and addressing challenges related to data quality, scalability, and integration into real-world environments. Once fully implemented, the system has the potential to significantly reduce manual effort, minimize human error, and help organizations respond to cybersecurity threats more quickly and effectively.

References

Ehsan Aghaei, Xi Niu, Waseem Shadid, and Ehab AlShaer. 2023. SecureBERT: A Domain-Specific Language Model for Cybersecurity, pages 39–56.

Hieu Man Duc Trong, Duc Trong Le, Amir Pouran Ben Veyseh, Thuat Nguyen, and Thien Huu Nguyen. 2020. Introducing a New Dataset for Event Detection in Cybersecurity Texts. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 5381–5390, Online. Association for Computational Linguistics.

Jackaduma. 2022. SecBERT. https://github.com/jackaduma/SecBERT.

Lukas Lange, Marc Müller, Ghazaleh Haratinezhad Torbati, Dragan Milchevski, Patrick Grau, Subhash Chandra Pujari, and Annemarie Friedrich. 2024. AnnoCTR: A Dataset for Detecting and Linking Entities, Tactics, and Techniques in Cyber Threat Reports. In *Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024)*, pages 1147–1160, Torino, Italia. ELRA and ICCL.

Orbinato, Vittorio, Mariarosaria Barbaraci, Roberto Natella, and Domenico Cotroneo. 2022. Automatic Mapping of Unstructured Cyber Threat Intelligence: An Experimental Study. *Preprint,* arXiv:2208.12144.

Tu Nguyen, Nedim Šrndić, and Alexander Neth. 2024. Noise Contrastive Estimation-based Matching Framework for Low-Resource Security Attack Pattern Recognition. In *Findings of the Association for Computational Linguistics: EACL 2024*, pages 355–373, St. Julian's, Malta. Association for Computational Linguistics.

Tumeteor. Security-TTP-Mapping. https://huggingface.co/datasets/tumeteor/Security-TTP-Mapping.

Youngja Park and Taesung Lee. 2022. Full-Stack Information Extraction System for Cybersecurity Intelligence. In *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing: Industry Track*, pages 531–539, Abu Dhabi, UAE. Association for Computational Linguistics.

Youngja Park and Weiqiu You. 2023. A Pretrained Language Model for Cyber Threat Intelligence. In *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing: Industry Track*, pages 113–122, Singapore. Association for Computational Linguistics.

Zainabsa99. mitre_attack. https://huggingface.co/datasets/Zainabsa99/mitre_attack.