

## Highlights

### **CTISum: A New Benchmark Dataset For Cyber Threat Intelligence Summarization**

Wei Peng,Junmei Ding,Wei Wang,Lei Cui,Wei Cai,Zhiyu Hao,Xiaochun Yun

- To the best of our knowledge, we make the first attempt to build a new benchmark CTISum with the CTIS task and a novel APS subtask in the cybersecurity domain.
- A multi-stage annotation pipeline is designed to obtain the high-quality dataset with the assistance of LLMs while manually controlling the quality.
- Experiments on CTISum demonstrate the challenge of the proposed two tasks, meanwhile indicating a large space for future research.

# CTISum: A New Benchmark Dataset For Cyber Threat Intelligence Summarization\*

Wei Peng<sup>a</sup>, Junmei Ding<sup>b</sup>, Wei Wang<sup>a</sup>, Lei Cui<sup>a</sup>, Wei Cai<sup>a</sup>, Zhiyu Hao<sup>a</sup> and Xiaochun Yun<sup>a</sup>

<sup>a</sup>Zhongguancun Laboratory, Beijing, P.R. China

<sup>b</sup>Beijing University of Posts and Telecommunications, Beijing, China

## ARTICLE INFO

### Keywords:

Information Systems  
Cyber Threat Intelligence  
Summarization  
Dataset and Benchmark

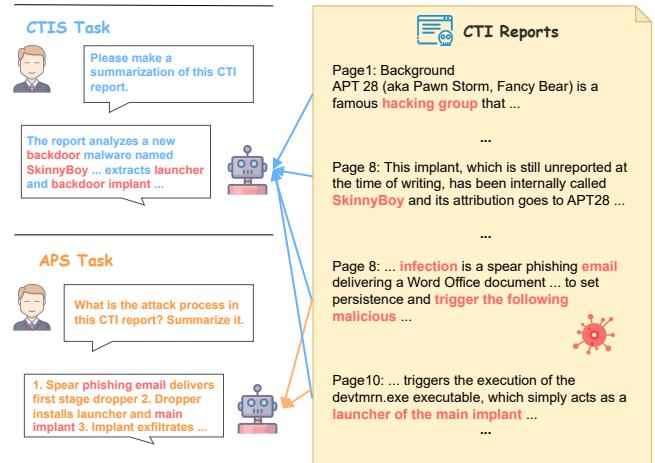
## ABSTRACT

Cyber Threat Intelligence (CTI) summarization involves generating concise and accurate highlights from web intelligence data, which is critical for providing decision-makers with actionable insights to swiftly detect and respond to cyber threats in the cybersecurity domain. Despite that, the development of efficient techniques for summarizing CTI reports, comprising facts, analytical insights, attack processes, and more, has been hindered by the lack of suitable datasets. To address this gap, we introduce CTISum, a new benchmark dataset designed for the CTI summarization task. Recognizing the significance of understanding attack processes, we also propose a novel fine-grained subtask: attack process summarization, which aims to help defenders assess risks, identify security gaps, and uncover vulnerabilities. Specifically, a multi-stage annotation pipeline is designed to collect and annotate CTI data from diverse web sources, alongside a comprehensive benchmarking of CTISum using both extractive, abstractive and LLMs-based summarization methods. Experimental results reveal that current state-of-the-art models face significant challenges when applied to CTISum, highlighting that automatic summarization of CTI reports remains an open research problem. The code and example dataset can be made publicly available at <https://github.com/pengwei-iie/CTISum>.

## 1. Introduction

Cyber Threat Intelligence (CTI), also known as threat intelligence, is knowledge, skills and experience-based information concerning the occurrence and assessment of both cyber and physical threats as well as threat actors [17, 12]. The CTI data often originates from diverse web sources, including forums, blogs, and open-source repositories, making it difficult for analysts to efficiently locate the most relevant and high-value intelligence from the web. Therefore, it becomes crucial to automatically summarize the knowledge contained in CTI reports, which could help analysts simply identify events, patterns, cyber attacks and conclusions. Furthermore, CTI summarization has broad applicability across domains like cybersecurity [36], military intelligence [39], technical alerts, threat modeling, and more, where complicated information needs to be distilled into concise insights.

With the ongoing advancement of summarization techniques, numerous datasets have emerged, such as CNN-DailyMail [28] and XSum [29], among others. In addition, the introduction of these datasets further drives the development of associated technologies like PGNet [37], BART [19], BRIO [23], etc. Furthermore, domain-specific summarization researches have gradually arisen. Examples include biomedicine [46], finance [26], law [38], etc. This further facilitates various applications involving aiding medical decision-making, generating financial reports, and summarizing legal documents. The boom of domain-specific summa-



**Figure 1:** An example in the CTISum. Blue arrow and orange arrow indicate the CTIS and APS tasks, respectively. Red font represents the key words.

rization promotes the understanding of domain terminology and context, which is crucial for generating high-quality summaries for further research.

Despite remarkable progress made in automatic text summarization, effective methods for summarizing CTI reports in the cybersecurity domain remain largely unexplored. This is primarily due to the lack of available dataset. The unique characteristics of CTI reports, such as technical jargon, evolving threat landscapes, longer reports and fragmented data information, make it challenging to create an annotation, which in turn hinders the development of robust models and evaluation benchmarks. However, recent advances in Large Language

\*This document is the results of the research project funded by the Zhongguancun Laboratory.

\*Corresponding author

✉ pengwei@zgclab.edu.cn (W. Peng); wangwei@zgclab.edu.cn (W. Wang); cuilei@zgclab.edu.cn (L. Cui); caiwei@zgclab.edu.cn (W. Cai); haozy@zgclab.edu.cn (Z. Hao); yunxiaochun@zgclab.edu.cn (X. Yun)  
ORCID(s): 0000-0001-8179-1577 (W. Peng)

Models (LLMs) [14, 9, 30, 40, 7, 6] have shown promising text understanding and generation capabilities. Therefore, this raises the question: *How might we construct a high-quality CTI summarization dataset with the assistance of LLMs?*

In this paper, we construct a new benchmark CTISum based on threat intelligence obtained from diverse web sources in the cybersecurity domain. In addition to the CTI Summarization (CTIS) task, considering the importance of attack process, we propose a novel fine-grained subtask, Attack Process Summarization (APS), to enable defenders to quickly understand reported attack behaviors, assess risks and identify security vulnerabilities. Specifically, a multi-stage annotation pipeline is designed to preprocess web CTI reports and obtain annotation data with the assistance of LLMs, which includes the data collection stage, parsing & cleaning stage, prompt schema stage and intelligence summarization stage. To further keep the high quality of the CTISum, we additionally employ expert reviews for double checking (details can be seen in Section 3.1). With proper data, automated systems can help synthesize lengthy CTI reports into concise and accurate summaries for different intelligence analysts. A sampled report and reference summary in CTISum are shown in Figure 1. The system not only requires to make a general summary of the full document (task 1), but also needs the capability to focus on and generate the attack process (task 2). After cleaning and human checking, CTISum obtains 1,345 documents and corresponding summaries.

What makes CTISum a challenging dataset can be presented as follows. First, the average document length is about 2,865 words. Current deep learning techniques are incapable of processing documents surpassing 512/1024 tokens in length (after tokenization), such as GPT1[33], T5[34], BART[19] and so on. Although LLMs can deal with longer input, however, fine-tuning LLMs is resource consuming. Moreover, LLMs are generally pre-trained on generic datasets, so they often fall short when performing zero-shot tasks in specific domains, such as cybersecurity. Second, the document-to-summary compression ratio on the two tasks are 14.32 (2865.60 / 200.04) and 22.23 (2865.60/118.27), respectively (details in Table 1). The high compression ratio shows competitiveness with the current long document summarization datasets, requiring systems to be extremely precise in capturing only the most relevant facts from lengthy documents in a minimal number of words. Finally, CTISum has another subtask, APS, which means the system should be capable of the ability to capture the fine-grained attack process described in CTI reports.

To demonstrate the challenges posed by the proposed CTISum dataset, we conduct comprehensive experiments comparing a range of extractive and abstractive summarization methods. The automatic and human evaluation indicate that existing approaches still have considerable limitations on the CTISum. The extractive methods struggle to identify salient information from lengthy and complex documents. They tend to produce incomplete summaries. Abstractive techniques face challenges in generating coherent and non-

redundant summaries, as well as avoiding hallucinations. Both extractive and abstractive methods achieve low scores on automatic metrics like ROUGE. Our findings highlight the need for continued research to develop summarization techniques that can distill critical information in CTISum. The dataset and baselines will be released for further research.

The contributions can be summarized as follows:

- To the best of our knowledge, we make the first attempt to build a new benchmark CTISum with the CTIS task and a novel APS subtask in the cybersecurity domain, which focuses on summarizing the key facts or attack process from CTI reports.
- A multi-stage annotation pipeline is designed to obtain the high-quality dataset with the assistance of LLMs while manually controlling the quality, which consists of the data collection stage, parsing & cleaning stage, prompt schema stage and intelligence summarization stage.
- Comprehensive experiments on CTISum demonstrate the challenge of the proposed two tasks, meanwhile indicating a large space for future research.

## 2. Related Work

### 2.1. Text Summarization

A considerable amount of existing researches in automatic text summarization [35, 28, 27, 4, 18, 44] have explored to improve summary generation for news articles, using popular datasets such as CNN/DailyMail [28], XSum [29], etc. In addition, scientific document summarization has emerged as another critical area, with datasets based on ArXiv/PubMed [8], and other academic sources. The main approaches cover two aspects. First, extractive methods [13, 5, 45, 21, 22, 44] involve identifying and extracting key sentences or passages from the original text to form the summary. For instance, Liu et al. [22] introduce a document-level encoder based on BERT and propose a general framework for summarization. Second, abstractive techniques focus on generating new sentences to capture the meaning of the source text. For example, sequence-to-sequence models with attention [25, 27, 31] are usually utilized to generate the probability distributions on the vocabulary. In addition, See et al. [37] present a hybrid pointer generator architecture for abstractive summarization. And more recently, transformer-based models like T5 [34], BART [19] and Longformer[3] have shown advanced performance on the summarization task.

Although current general summarization techniques have made some progress, their performance significantly decrease when transferred to CTI summarization tasks due to the lack of domain-specific fine-tuning data. The creation of the CTISum could provide an essential resource for domain adaptation, as well as developing and evaluating domain-specific summarization approaches.

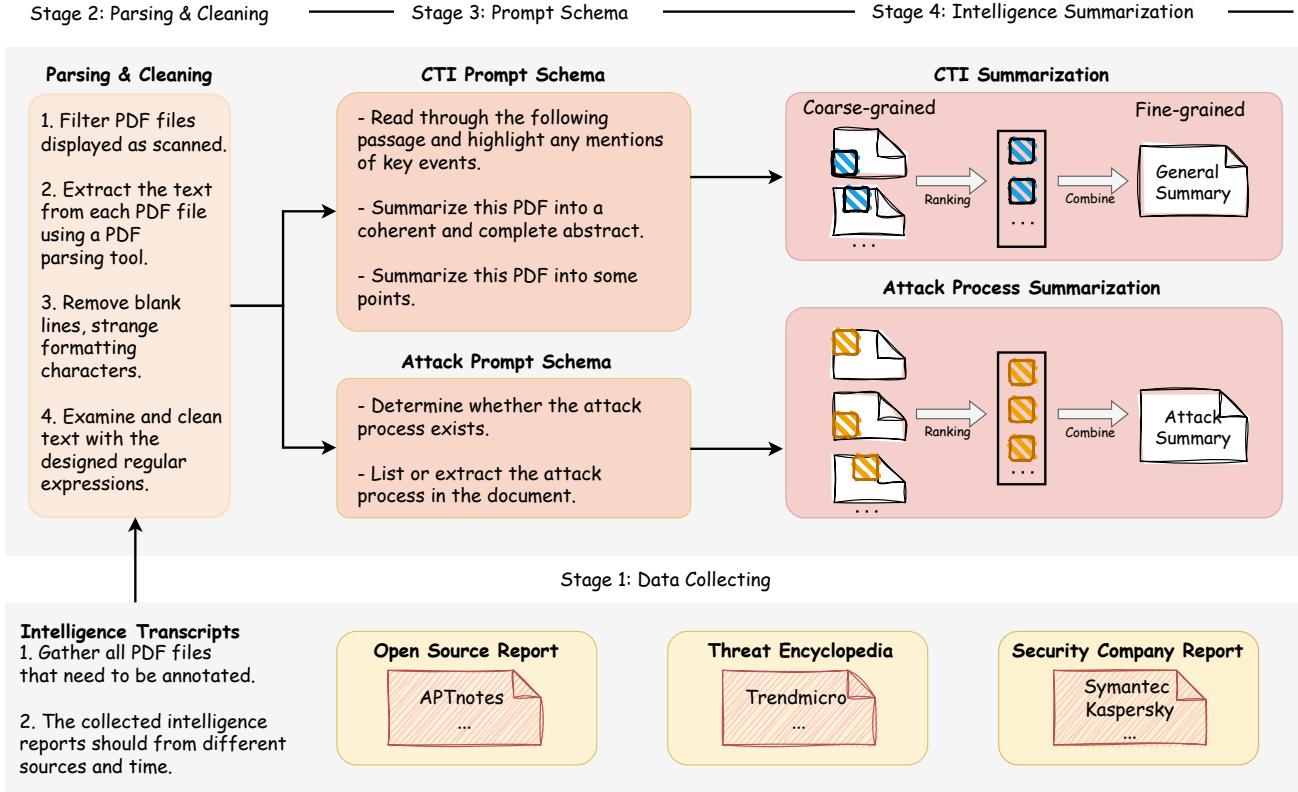


Figure 2: The overview of the proposed multi-stage annotation pipeline for CTISum and APS tasks.

## 2.2. Domain-specific Summarization

For the domain-specific summarization, there are many potential applications across different domains like government [16], finance [26], court rulings [38] and biomedicine [46]. For example, in the government domain, summarization systems can help process large volumes of regulatory text and legal documents. Huang et al. [16] propose a novel efficient encoder-decoder attention with head-wise positional strides to effectively double the processed input sequence size. For the finance industry [26], summarization of earnings reports, financial statements, and news can assist investors and analysts in making decisions. In addition, summarizing court rulings, case law, and litigation documents [38] helps legal professionals in their work. Within biomedicine [46], health-care professionals can make informed decisions by using summaries of clinical trial findings, medical literature, and patient records. Different from the above domains, we make the first attempt to build the CTI summarization dataset in the cybersecurity domain, which helps fill the gap and enables new research into CTI summarization techniques.

## 3. Data Construction

As shown in Figure 2, the proposed multi-stage annotation pipeline consists of four stages. The first stage is collecting data from diverse web sources, namely open source report [10], threat encyclopedia [2], and security company report [1] to ensure the diversity and coverage. The second

stage is parsing and cleaning which aims to parse original PDF reports into readable text, then obtain high-quality input data by manually cleaning and filtering. Next follows the prompt schema stage, where domain experts design various prompts based on different tasks, to fully utilize the powerful text generation capabilities of LLMs and prepare for the annotation. Finally, the intelligence summarization stage. To combine system productivity and expert experience efficiently, we transform the manual annotation process into ranking and classifying, having experts review and rank the outputs of LLMs to obtain the final summary. Next, we first introduce the multi-stage annotation pipeline, and then make a statistics and analysis of the CTISum.

### 3.1. The Multi-stage Annotation Pipeline

The multi-stage annotation pipeline focuses on obtaining the high-quality CTISum dataset, where we attempt to combine the strengths of both expert experience and LLMs (like GPT-4 [30] or Claude2 or 3.5 [6]) to achieve semi-automatic summarization annotation for efficiency in the cybersecurity domain.

**Stage 1: Data Collecting.** To gather relevant CTI reports and build CTISum, we use the reports scraped from diverse web sources, including web open source report like APTnotes<sup>1</sup>, threat encyclopedia like Trendmicro<sup>2</sup>, and security

<sup>1</sup>[https://github.com/blackorbird/APT\\_REPORT](https://github.com/blackorbird/APT_REPORT)

<sup>2</sup><https://www.trendmicro.com>

company report like Symantec<sup>3</sup> to ensure the diversity and coverage of the CTISum. The range of collected data is covered from 2016 to 2024. For the summarization tasks, a balanced dataset of 1,345 documents is sampled and annotated with two categories: CTIS and APS.

*Stage 2: Parsing and Cleaning.* In order to obtain high-quality input data, the second stage focuses more on parsing and further cleaning the parsed text.

Given that CTI reports are currently formatted as PDF files, which have complex structure and cannot be directly used as the input to the system, one necessary step is to parse the PDFs and extract readable text. Specifically, the gathered PDFs are firstly filtered to only include those containing actual text content, rather than scanned documents which cannot be parsed by certain tools like PDFMiner. Then, an off-the-shelf PDF parsing library<sup>4</sup> is leveraged to programmatically extract the readable text from each document, while figures are discarded. Finally, the output text is saved in TXT format, allowing transferability to downstream systems.

After parsing, it is indispensable to clean and filter the extracted text for high-quality input data to the LLMs. This post-processing helps improve the quality and consistency of the textual data. One methodology is to manually review samples of the extracted text to identify issues that need to be cleaned. Some rules are:

- Correcting encoding issues when parsing error.
- Removing blank lines and odd characters that get extracted but provide no value.
- Cleaning up irregular text like ellipses and page numbers that are extracted from tables of contents, lists, etc.
- Removing non-English and useless characters.
- Deduplicating and removing strings like long sequences of consecutive IP addresses, hashes, etc.
- Filtering with regular expressions. Details in Appendix A.2.

The parsing and cleaning stage ensures higher quality input text for the next stage of analysis and annotation.

*Stage 3: Prompt Schema.* The purpose of this stage is to develop a detailed prompt schema to guide the LLMs (Claude2 or 3.5, ChatGLM3, etc.) in producing candidate summaries, such as highlighting key events and summarizing reports, attack processes, some useful annotations, etc. To generate accurate and consistent summaries for the CTIS task and the APS task, CTI experts analyze the parsed and cleaned text and then design the CTI prompt schema and attack process prompt schema, respectively. As shown in Figure 2, several key annotation prompts are defined as follows:

- Key Events: The instruction, **read through the following passage and highlight any mentions of key events**, will focus on important cyber threat events like new malware campaigns, critical vulnerabilities, or notable hacks.

<sup>3</sup><https://www.broadcom.com/support/security-center>

<sup>4</sup><https://github.com/euske/pdfminer/tree/master>

- Coherent Summary: To obtain the complete and coherent abstract, the instruction, **summarize this PDF into a coherent and complete abstract**, is leveraged.
- Additional Points: The purpose of the instruction **summarize this PDF into some points** is to generate some additional aspects for supplementary.
- Determination: Considering some reports do not contain the attack process, the instruction **determine whether the attack process exists** is designed.
- Attack Process: The instruction, **list or extract the attack process in the document**, is utilized for the APS task.

The prompt schema outlines each annotation prompt in detail, which is a critical component that will guide the LLMs to produce useful, accurate, and consistent summaries.

*Stage 4: Intelligence Summarization.* To combine system productivity and expert experience more efficiently, we transform the manual annotation process into ranking and classifying model-generated results, having three experts review and rank the outputs into overall summaries. Specifically, LLMs like GPT-4o [30], Claude2 or 3.5 [6], ChatGLM3 [42] are leveraged to generate multiple coarse-grained summaries for the proposed two tasks. Then, three domain experts are involved in reviewing and ranking the candidate summaries, discussing and selecting the better content to combine into a final gold summary. If the generated summaries turn out to be inadequate, the example would be discarded. The domain experts play a key role in evaluating and improving the model-generated summaries to produce a high-quality benchmark. Their human judgment and domain expertise complement the capabilities of LLMs. This collaborative human-AI approach allows the creation of abstractive summaries that are coherent, relevant, and accurate.

### 3.2. Data Statistics

Table 1 describes the statistics of the CTISum dataset and existing summarization datasets from different domains. The datasets are divided into general and specific domain categories, with the latter attracting substantial interest in recent years from 2021 to 2024. And we make the first attempt to build the CTI summarization dataset in the cybersecurity domain. Specifically, CTISum has 1,345 documents from diverse web sources, with an average document length of 2,865 words, with an average CTI summary length of 200 words, and with a high compression ratio of 14.32. Notably, CTISum is the only dataset with the subtask, while other datasets simply make a general summary of the document. The average length of the attack process summaries is about 118 words, which is shorter than the general summaries. This highlights the challenging nature of generating focused summaries that capturing the attack process from long documents. In addition, the Fleiss Kappa evaluation of the dataset can be seen in Sec. 5.5.

In summary, the table highlights that CTISum is a challenging dataset for summarization in the cybersecurity domain, with a novel subtask (attack process summarization) and high abstraction requirements. The CTISum dataset helps

**Table 1**

Statistics of CTISum dataset and existing different domain summarization datasets. Numbers which are not reported are left blank. The numbers for the datasets marked with \* are copied from the paper [26], whereas the ones marked with † are copied from the work [29]. Doc.: document, Avg.: average, Len.: length, APS: attack process summarization.

Dataset	# Doc.	Avg. Doc. Len.	Avg. Sum. Len.	Avg. APS Len.	Has Subtask	Domain
General Domain						
ARXIV/PUBMED [8]*	346,187	5,179.22	257.44	-	No	Academic
CNN [28]†	92,579	760.50	45.70	-	No	News
DAILYMAIL [28]†	219,506	653.33	54.65	-	No	News
XSUM [29]†	226,711	431.07	23.26	-	No	News
BOOKSUM Chapters [26]*	12,630	5,101.88	505.42	-	No	Books
Specific Domain						
GOVREPORT [16]	19,466	9,409.40	553.40	-	No	Government
DISCHARGE [46]	50,000	2,162.29	28.84	-	No	Biomedicine
ECHO [46]	162,000	315.30	49.99	-	No	Biomedicine
ECTSUM [26]	2,425	2,916.44	49.23	-	No	Finance
IN-EXT [38]	50	5,389	1,670	-	No	Court Rulings
UK-ABS [38]	793	14,296	1,573	-	No	Court Rulings
CTISUM	1,345	2,865.60	200.04	118.27	Yes	Cybersecurity

fill the gap and enables new system design in future work.

## 4. Problem Formulation

Existing approaches usually define the summarization task as a sequence-to-sequence task. Specifically, the problem formulation can be formulated as follows. Given a document  $D = (x_1, \dots, x_N)$  that consists of  $N$  words, with  $Y = (y_1, \dots, y_M)$  being the corresponding summary. For the proposed CTISum, there are two tasks, including CTIS task and APS task. For CTIS task, the object is to output a general summary of the CTI report. Similarly, the object of the APS task is to generate a summary of the attack process.

## 5. Experiments

### 5.1. Evaluation Metrics

In this section, the automatic and human A/B evaluation are considered to validate the performance of the current SOTA models.

Following papers [15, 26], BERTScore [43] and ROUGE- $n$  (R- $n$ ) [20] are taken as evaluation metrics, which are widely used for evaluating the quality of summarization. BERTScore is a metric for evaluating text generation models, which measures the similarity between the generated text and reference text using contextual embeddings from pre-trained BERT. ROUGE- $n$  refers to the overlap of  $n$ -grams between the generated and reference summaries. Specifically, ROUGE-1 evaluates unigram overlap, ROUGE-2 measures bigram overlap, and ROUGE-L calculates longest common subsequence overlap. These metrics compare matching units such as words and phrases between the generated and reference summaries, with higher scores indicating better summarization quality. Among the ROUGE metrics, ROUGE-L generally corresponds best with human judgments of summary quality.

In previous studies, human evaluation is usually conducted by crowdsourcing workers who rate responses on a scale from 1 to 5 from the aspects of correctness, relevancy, etc. However, the criteria can vary widely between different individuals. Therefore, this study adopts the human A/B evaluation for a high inter-annotator agreement. Given the generated summaries of two models A and B, three analysts are prompted to go through an entire CTI report and choose the better one for each of the 80 randomly sub-sampled test instances. For objectivity, annotators include those with and without background knowledge (task-related). The final results are determined by majority voting. If the three annotators reach different conclusions, the fourth annotator will be brought in. We adopt the same human evaluation with paper [26]: 1) Factual Correctness: which summary can be supported by the source CTI report? 2) Relevance: which summary captures pertinent information relative to the CTI report? 3) Coverage: which summary contains the greatest coverage of relevant content in the CTI report?

### 5.2. Experimental Setting

The implementation of baselines is based on the Hugging-Face framework. The AdamW optimizer [24] with  $\beta_1 = 0.9$  and  $\beta_2 = 0.99$  is used for training, with an initial learning rate of  $3e - 5$  and a linear warmup with 100 steps. The batch size is set to 16 for training, and we use a batch size of 1 and a maximum of 128 decoding steps during inference. Top- $p$  sampling is set to 0.9, temperature  $\tau = 0.7$ . The epoch is set to 5. For preprocessing, we randomly split the dataset into train, validation and test set with a ratio of 8:1:1.

### 5.3. Baselines

Several SOTA approaches are illustrated for comparison. The models can be mainly divided into extraction-based, abstraction-based and long-document-based methods.

**Table 2**

Performance of automatic evaluation on CTIS and APS tasks. LLAMA2 is in the zero-shot setting because of the lack of resources. The best results are highlighted in **bold**.

Model	CTIS Validation				CTIS Test			
	BERTScore↑	R-1↑	R-2↑	R-L↑	BERTScore↑	R-1↑	R-2↑	R-L↑
<b>Extractive</b>								
BertSumExt [22]	82.15	26.91	5.91	13.09	81.36	20.43	3.52	11.76
MatchSum [44]	<b>83.91</b>	39.31	13.39	20.60	<b>83.75</b>	33.76	9.34	18.91
<b>Abstractive</b>								
Transformer [41]	45.83	34.15	12.05	19.88	45.17	32.94	10.37	18.55
T5 [34]	70.48	43.75	16.58	28.06	69.21	42.41	14.35	27.32
BART-base [19]	70.36	44.45	16.26	27.24	69.24	42.48	14.30	26.23
BART-large [19]	71.21	<b>47.11</b>	<b>18.32</b>	<b>29.20</b>	70.41	<b>45.76</b>	<b>16.88</b>	<b>29.03</b>
<b>Long-document-based</b>								
Longformer[3]	71.06	46.97	17.21	28.22	70.31	45.39	15.66	27.09
LLAMA2 [40] (zero-shot)	33.87	21.35	5.93	20.51	32.15	20.89	5.66	19.22
GPT-4o (zero-shot)	65.82	40.18	13.22	24.33	64.31	38.70	12.71	22.98
Model	APS Validation				APS Test			
	BERTScore↑	R-1↑	R-2↑	R-L↑	BERTScore↑	R-1↑	R-2↑	R-L↑
<b>Extractive</b>								
BertSumExt [22]	81.38	20.67	3.06	11.87	81.38	20.35	3.46	11.73
MatchSum [44]	<b>83.93</b>	33.86	9.86	19.17	<b>83.75</b>	33.73	9.35	18.88
<b>Abstractive</b>								
Transformer [41]	40.43	28.22	7.86	16.50	39.15	27.03	6.21	15.48
T5 [34]	68.41	36.20	10.27	24.70	66.06	32.09	7.62	21.78
BART-base [19]	70.47	40.47	12.33	25.28	70.70	39.42	11.13	24.45
BART-large [19]	71.31	<b>41.88</b>	<b>12.76</b>	<b>26.54</b>	70.32	<b>40.25</b>	<b>11.65</b>	<b>25.06</b>
<b>Long-document-based</b>								
Longformer[3]	70.98	41.35	11.77	25.36	70.41	39.91	9.78	23.93
LLAMA2 [40] (zero-shot)	21.06	15.68	2.23	13.14	20.38	14.66	2.02	12.28
GPT-4o (zero-shot)	48.77	32.06	9.11	18.69	45.39	30.55	8.61	17.75

**Extractive Model** Extractive summarization involves selecting a subset of salient sentences, phrases, or words from the original document to form the summary. The key idea is to identify and extract the most important content, and then arrange extracted content to flow logically. We simply introduce some methods as follows.

BertSumExt [22] is a neural extractive summarization model based on BERT [11], which takes BERT as the sentence encoder and a Transformer layer as the document encoder. A classifier is utilized to perform sentence selection, then the model outputs the final summary.

MatchSum [44] formulates the extractive summarization task as a semantic text matching problem and develops a novel summary-level framework MatchSum, which generates a collection of possible candidate summaries from the output of BertSumEXT. The candidate that matches best with the document is selected as the final summarized version.

**Abstractive Model** Abstractive summarization involves generating new phrases and sentences that convey the most important information from the source document, which uses semantic understanding and language generation technology to make a summarization. Hence, we fine-tune BART [19] and T5 [34] from the HuggingFace library.

BART [19] is an encoder-decoder language model based on a sequence-to-sequence architecture, which achieves strong performance on a variety of NLP tasks like summarization, question answering and text generation after fine-tuning.

T5 [34] uses a standard Transformer encoder-decoder architecture, which converts all NLP tasks into a unified text-to-text format where the input and output are always text strings. T5 comes in several sizes including T5-Small, T5-Base, T5-Large, etc. In this paper, the setting is based on T5-Base.

**Long-document-based Model** Long-document-based summarization refers to generating summaries for documents that

**Table 3**

Results for the human evaluation of model-generated summaries by three intelligent analysts.

Model	CTIS Task			APS Task		
	Correctness	Relevance	Coverage	Correctness	Relevance	Coverage
<b>Summary-level scores (about 80 summaries)</b>						
<b>BART better</b>	33.33	26.67	46.67	40.00	33.33	46.67
<b>Longformer better</b>	26.67	20.00	20.00	26.67	26.67	20.00
<b>Both equally good</b>	40.00	53.33	33.33	33.33	40.00	33.33

are significantly longer than typical texts, e.g. 1,024 tokens, like Longformer[3], LLAMA2 [40], etc.

Longformer[3] is an extension to the Transformer architecture, which leverages an attention mechanism whose computational complexity grows linearly as the length of the input sequence increases, making it easy to process thousands of tokens or more. LLAMA2 [40] is a Transformer-based large language model, which is trained on massive text datasets to learn natural language patterns and generate human-like text. The context length of LLAMA2 can extend up to 4096 tokens, allowing it to understand and generate longer texts. In this paper, the 7 billion LLAMA2 is utilized to compare against fine-tuned models in zero-shot setting.

#### 5.4. Main Results

*Automatic Evaluation.* We compare the performance of extractive models, abstractive models and long-document-based models on CTIS and APS tasks. As depicted in Table 2, extractive models perform the almost worst on both tasks, demonstrating that intelligence summarization in cybersecurity involves more than just extracting sentences. Interestingly, they obtain the best BERTScore, one possible reason is that these two models are based on BERT, leading to high BERTScore. Compared with MatchSum, abstractive model like BART-large (about 374M) achieves better result, about 10.12% and 6.18% gain on ROUGE-L on two tasks, which shows that the abstractive models are more suitable for these two tasks. Then, long-document-based model like Longformer (102M) obtains similar results compared with BART-base (about 121M). Notably, LLAMA2-7B and GPT-4o (zero-shot) do not attain further improvement on all the evaluation metrics, leaving noticeable room for future work on domain LLMs fine-tuning and few-shot learning on the benchmark. Finally, we find that performance is worse on the APS task, likely because the attack process exhibits properties like variability, concealment and complexity, making APS more challenging than general summarization. Enhancing models for APS task remains an important direction for future research.

*Human A/B Evaluation.* In addition to the automatic evaluation, human A/B evaluation [32] is conducted to validate the effectiveness of current SOTA models that BART-large and Longformer are compared. The results in Table 3 demonstrate the consistent conclusion with automatic evaluation. It can be seen that the summaries from BART-large are much

**Table 4**  
Fleiss Kappa evaluation of CTISum dataset.

Score	1	2	3	4	5	Fleiss Kappa
Result	0	9	58	129	54	0.37
Score	1 and 2	3	4 and 5			Fleiss Kappa
Result	9	58	183			0.61

more preferred than those of the baselines in terms of the three aspects. For example, compared with Longformer, BART is superior in terms of the coverage metric, indicating that the larger the number of parameters, the better the generated summaries. Besides, it is noted that BART does not significantly outperform Longformer in the relevance metric, and this is probably attributed to the powerful understanding ability of the PLMs, but BART still obtains decent improvements.

#### 5.5. Fleiss Kappa Analysis

To verify the consistency of the final summary generation quality, we select 5 experts to execute a consistency evaluation of 50 sampled summaries using Fleiss Kappa, where the scores are rated from 1 to 5, with 1 very negative, 2 negative, 3 neutral, 4 positive, and 5 very positive. As shown in the Table 4, the final Fleiss Kappa score is 0.37, indicating relatively low agreement. This can be attributed to the fact that summary generation belongs to language generation task, where different experts tend to have subjective views on summary quality (e.g., examples that annotated as positive or very positive are inconsistent, but they are all good), which differs greatly from the objectivity of classification tasks. However, we also analyze the score distribution of all experts, finding that summaries rated 3 or above account for 96.4% (241/250) of the total, demonstrating that the quality of the annotated dataset is controllable and accurate. Moreover, we have conduct another round of Fleiss Kappa Analysis on the previous annotation scores from multiple raters. Specifically, we combine score 1 and 2 into one bin, keep score 3 as a separate bin, and combine score 4 and 5 into another bin. This result in a Fleiss Kappa score of 0.613184, which indicate the consistency evaluation.

#### 5.6. Input Length Analysis

In this section, the input length analysis is performed to study the model’s sensitivity to input length. We evaluate

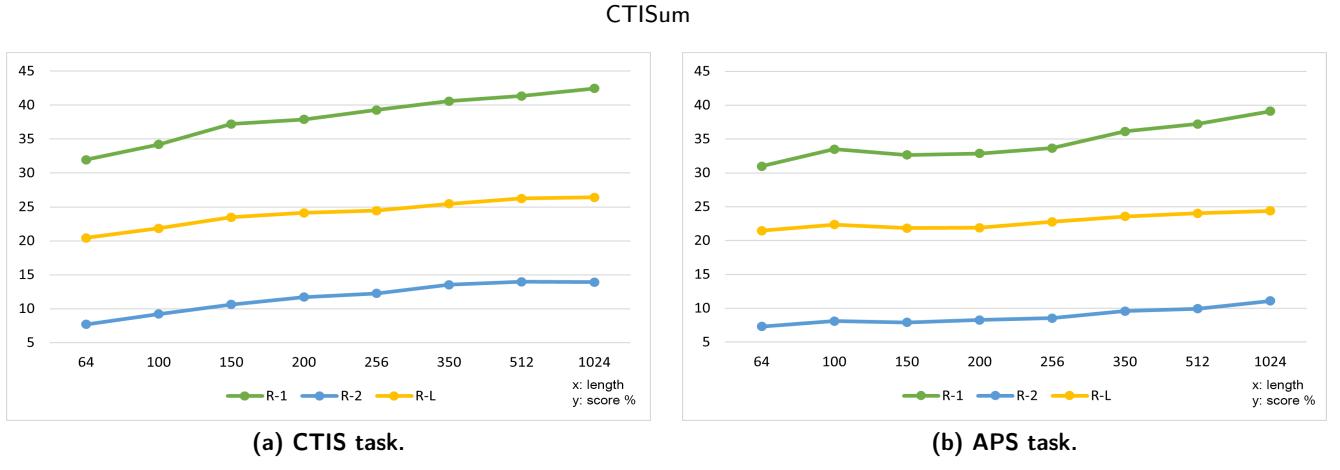


Figure 3: Input length analysis of two tasks.

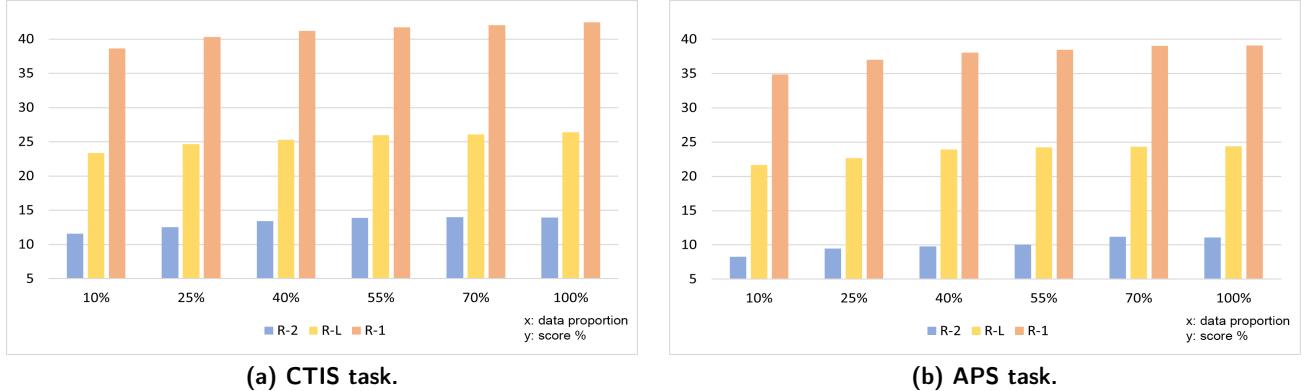


Figure 4: Few shot experiments of the proposed two tasks.

the impact of different input lengths on the BART-base (the purpose of using base model is to train the model quickly on CTI and APS tasks. We divide the different length to get better insight into the current models. As shown in Figure 3, where the x-axis represents the input length and the y-axis denotes the measure value of evaluation metrics. The conclusions can be drawn: 1) As the input length increases, the model performance improves steadily, highlighting the model’s ability to process and summarize longer sequences. 2) As the length of BART reaches 1024 tokens, performance on our tasks continues to improve. To further investigate the impact of longer length, we increase the size of Longformer and find that lengthening to 3500 tokens (75th percentile of length distribution) results in optimal performance, which suggests the advantage of long-distance modeling. 3) The model achieves poorer performance on the APS task compared to the CTIS task, indicating it struggles more with summarizing technical attack details than threat intelligence reports. In summary, the experiments provide insight into current models’ ability to capture long-distance dependencies in documents and summarize essential information as the input size varies. Further work could focus on improving the model’s ability of length to boost performance on lengthy, technical summarization tasks.

## 5.7. Few-shot Analysis

Analyzing the impact of data size can help to understand the relationship between data size and summarizing performance. To demonstrate such a relationship, in this section, few-shot analysis experiments on BART-base are conducted to study model’s sensitivity in different training data sizes. We experiment with 10%, 25%, 40%, 55%, 70%, and 100% of the total training data to analyze the impact on CTIS task and APS task. The experimental results are shown in the Figure 4 with several conclusions: 1) Performance of BART-base improves as the training data size increases, indicating that model quality benefits from more abundant training data. Furthermore, the result in the figure is still growing, which suggests further improvements with larger training data size. 2) Performance on the APS task is worse than the CTIS task, especially in few shot setting (e.g., 10%, 25%). Therefore, how to improve the performance of summarization models in few-shot setting for cybersecurity domain will be an important future research track. And data augmentation is also another area worth researching.

## 5.8. Case Analysis

Qualitatively, we observe interesting examples on the BART-base from CTIS and APS tasks in Table 5. In case one on CTIS task, the model generates hallucination about

**Table 5**

Case analysis on CTIS and APS tasks. **Orange words** mean the hallucination generated by the baseline. **Blue words** present the correct result. **Red words** indicate some of the key information that needs to be extracted.

Task	CTIS Task
Document	ShadowGate Returns to Worldwide Operations With Evolved <b>Greenflash Sundown</b> ... After almost two years of sporadic restricted activity, the <b>ShadowGate campaign</b> has started delivering cryptocurrency miners with a newlyupgraded version of the Greenflash Sundown exploit kit ... <b>ShadowGate was active since 2015</b> but restricted operations after a takedown <b>in 2016</b> ... <b>In April 2018</b> , ShadowGate was spotted spreading ...
BART	The PDF describes the activities of a threat actor group called ShadowGate ... <b>The campaign has been actively evolving its exploit kit since 2016</b> ... ShadowGate started distributing cryptocurrency miners using a new version of <b>Green_Sundown</b> , likely to avoid ... The Monero
Ground truth	The report analyzes the resurgence of a cybercrime campaign called ShadowGate, which is using an upgraded version of its custom exploit kit, Greenflash Sundown, to infect victims worldwide with cryptocurrency mining malware. ShadowGate was active <b>since 2015</b> but restricted operations after a takedown <b>in 2016</b> . It recently resumed attacks using compromised ...
Task	APS Task
Document	Staring at a major financial resource crunch, MSME's are worst affected due to the ongoing COVID-19 pandemic. We observed one similar wave on MSME in late April 2020 — it was a phishing campaign luring victims with <b>COVID-19 themed maldocs</b> ... Victims <b>received an email</b> with attached zip“face mask order.zip” which contained the <b>aforementioned maldoc</b> ... The attack begins <b>after opening “face mask order.doc”</b> . This RTF is weaponized with exploit which triggers <b>CVE-2017-11882</b> vulnerability to execute arbitrary code ... injected Agent Tesla payload in <b>RegAsm.exe</b> ...
BART	1. The phishing email contains a malicious RTF file titled “face mask order.zip” 2. The RTF contains an exploit that triggers <b>CVE-2017-11882</b> to execute arbitrary code. 3. The exploit extracts the <b>OLE</b> objects from RTF files. 4. The OLE object contains a VBScript script that executes an <b>Equation Editor</b> payload. 5. The Equated Editor payload connects to a command and control server to receive commands. 6. Command server sends commands to the C2 server to execute additional payloads. 7. Additional payloads are delivered to the infected ...
Ground truth	1. Gorgon APT sends phishing emails with COVID-19 themed Word documents to targets in the MSME sector. 2. The documents contain an exploit for <b>CVE-2017-11882</b> to execute malicious code. 3. The code drops a visual basic script named <b>ServerEncrypted.vbs</b> . 4. The VBScript executes a <b>PowerShell command</b> to download additional payloads. 5. The first payload is an injector DLL. 6. The second payload is the Agent Tesla Remote Access Trojan. 7. The injector DLL loads itself into memory using PowerShell. 8. Agent Tesla is injected into the <b>RegAsm.exe</b> process. 9. Agent Tesla ...

time **since 2016**, leading to incorrect time information in the summary. This phenomenon likely occurs because if the source document contains multiple time details, the model may confuse about which time points are being referenced. Therefore, addressing this challenge will be critical for future improvements. In case two on APS task, while generated attack process summary can include some factual information **CVE-2017-11882**, many factual inconsistencies errors exist, such as **OLE** and **Equation Editor**. This stems from attack behaviors that exhibit properties of complexity, diversity, and contextual dependence, which makes the APS task difficult. Thus, adapting appropriate methods to better capture the intricacies of attack behaviors represents a promising research direction. Overall, these cases highlight important limitations, but also provide exciting opportunities to advance CTIS and APS tasks through innovations targeting core summarize-ability challenges in the cybersecurity domain.

## 6. Conclusion

With a lack of publicly available intelligence data, in this paper, we make the first attempt to propose CTISum benchmark which provides a valuable resource to spur innovation in this critical but unobserved cybersecurity domain. The creation of this intelligence-focused summarization benchmark represents an important step toward developing AI systems that can effectively process and synthesize CTI reports. To combine system productivity and expert experience more efficiently, a multi-stage annotation pipeline is designed for obtaining the high-quality dataset. Our experiments reveal that while current models can produce decent summaries, there is significant room for improvement in capturing key details accurately. The technical cybersecurity terminology and complex contextual concepts present in the reports pose great challenges for generating intelligence summaries. In the future work, leveraging transfer learning and LLMs to the

cybersecurity domain can provide a starting point, as well as exploring adaptations of summarization techniques to address the unique characteristics of the cyber threat intelligence field. Ethical statement is in Appendix A.1.

## Acknowledgments

We thank all anonymous reviewers for their constructive comments. This work is supported by the Zhongguancun Laboratory.

## A. Appendix

### A.1. Ethical Statement

All data in CTISum dataset has been double checked by experts that major in intelligence analysis, and manually checked to ensure the absence of any ethical or political inaccuracies.

### A.2. Details of Regular Expression

During the process of filtering and cleaning the parsed PDF data, in order to reduce the burden of manual checking by annotators, we first sample and observe 50 examples, and then extract some common features to formulate into regular expressions for automatically cleaning the data. Specifically, details of regular expression are in the following:

- Removing consecutive dots (table of contents)
- Deleting redundant newlines/carriage returns
- Removing extra whitespace between characters
- Deleting multiple consecutive lines of IP addresses, hashes, etc.
- Removing website links starting with “http”
- Removing Thai, Korean and other non-English characters

By automating the cleaning of patterns and noise with regex, we aim to improve efficiency and reduce manual effort. The regular expressions are tuned iteratively based on continuously sampling and inspecting. This method allows us to programmatically clean a significant portion of repetitive issues in parsed PDF data before manual review. In the future, we can continue refining the regex and identifying new patterns to clean the data. The goal is to minimize the amount of manual effort while ensuring high-quality cleaned data. Some utilized code of regular expression (Python) can be seen as follows:

```
r '\.{ 2 , } '
r '\{ 2 , } '
r '\s\s+'
r '(\d{ 1 , 3 }\.){ 3 }\d{ 1 , 3 }|[ a-f0 -9]{ 32 , 64 }'
r '^( $ .+[ \n ] )+|^\\w+\\([ ^\\ ]) +\\)( [ \\s\\S ] { 1 } ){ [
\\r ] \\s.+'
r 'https ://(?:[ -\\w . ]|(? :% [ \\da-fA-F ] { 2 } ))+ '
```

## References

- [1] , 2020. Symantec security center .
- [2] , 2020. Threat encyclopedia .
- [3] Beltagy, I., Peters, M.E., Cohan, A., 2020. Longformer: The long-document transformer. arXiv preprint arXiv:2004.05150 .
- [4] Celikyilmaz, A., Bosselut, A., He, X., Choi, Y., 2018. Deep communicating agents for abstractive summarization. arXiv preprint arXiv:1803.10357 .
- [5] Cheng, J., Lapata, M., 2016. Neural summarization by extracting sentences and words, in: Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, ACL 2016, August 7-12, 2016, Berlin, Germany, Volume 1: Long Papers, The Association for Computer Linguistics. URL: <https://doi.org/10.18653/v1/p16-1046>, doi:10.18653/V1/P16-1046.
- [6] Claude, A., 2023a. 2. anthropic blog 2023, july 11.
- [7] Claude, A.I., 2023b. Anthropic blog 2023 march 14.
- [8] Cohan, A., Dernoncourt, F., Kim, D.S., Bui, T., Kim, S., Chang, W., Goharian, N., 2018. A discourse-aware attention model for abstractive summarization of long documents, in: Walker, M.A., Ji, H., Stent, A. (Eds.), Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT, New Orleans, Louisiana, USA, June 1-6, 2018, Volume 2 (Short Papers), Association for Computational Linguistics. pp. 615–621. URL: <https://doi.org/10.18653/v1/n18-2097>, doi:10.18653/V1/N18-2097.
- [9] Cui, T., Wang, Y., Fu, C., Xiao, Y., Li, S., Deng, X., Liu, Y., Zhang, Q., Qiu, Z., Li, P., et al., 2024. Risk taxonomy, mitigation, and assessment benchmarks of large language model systems. arXiv preprint arXiv:2401.05778 .
- [10] CyberMonitor, R.H., et al., 2019. Apt and cybercriminals campaign collection .
- [11] Devlin, J., Chang, M., Lee, K., Toutanova, K., 2019. BERT: pre-training of deep bidirectional transformers for language understanding, in: Burstein, J., Doran, C., Solorio, T. (Eds.), Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT 2019, Minneapolis, MN, USA, June 2-7, 2019, Volume 1 (Long and Short Papers), Association for Computational Linguistics. pp. 4171–4186. URL: <https://doi.org/10.18653/v1/n19-1423>, doi:10.18653/V1/N19-1423.
- [12] of England, B., 2016. Cbest intelligence-led testing: Understanding cyber threat intelligence operations.
- [13] Erkan, G., Radev, D.R., 2004. Lexrank: Graph-based lexical centrality as salience in text summarization. J. Artif. Intell. Res. 22, 457–479. URL: <https://doi.org/10.1613/jair.1523>, doi:10.1613/JAIR.1523.
- [14] Hsiao, E.S., Collins, E., 2023. Try bard and share your feedback.
- [15] Hsu, T., Suhara, Y., Wang, X., 2022. Summarizing community-based question-answer pairs, in: Goldberg, Y., Kozareva, Z., Zhang, Y. (Eds.), Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing, EMNLP 2022, Abu Dhabi, United Arab Emirates, December 7-11, 2022, Association for Computational Linguistics. pp. 3798–3808. URL: [https://doi.org/10.18653/v1/2022.EMNLP-MAIN.250](https://doi.org/10.18653/v1/2022.emnlp-main.250), doi:10.18653/V1/2022.EMNLP-MAIN.250.
- [16] Huang, L., Cao, S., Parulian, N.N., Ji, H., Wang, L., 2021. Efficient attentions for long document summarization, in: Toutanova, K., Rumshisky, A., Zettlemoyer, L., Hakkani-Tür, D., Beltagy, I., Bethard, S., Cotterell, R., Chakraborty, T., Zhou, Y. (Eds.), Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT 2021, Online, June 6-11, 2021, Association for Computational Linguistics. pp. 1419–1436. URL: [https://doi.org/10.18653/v1/2021.NAACL-MAIN.112](https://doi.org/10.18653/v1/2021.naacl-main.112), doi:10.18653/V1/2021.NAACL-MAIN.112.
- [17] Jo, H., Lee, Y., Shin, S., 2022. Vulcan: Automatic extraction and analysis of cyber threat intelligence from unstructured text. Comput. Secur. 120, 102763. URL: [https://doi.org/10.1016/j.COSE.2022.102763](https://doi.org/10.1016/j.cose.2022.102763), doi:10.1016/J.COSE.2022.102763.
- [18] Lebanoff, L., Song, K., Dernoncourt, F., Kim, D.S., Kim, S., Chang, W., Liu, F., 2019. Scoring sentence singletons and pairs for abstractive

- summarization. arXiv preprint arXiv:1906.00077.
- [19] Lewis, M., Liu, Y., Goyal, N., Ghazvininejad, M., Mohamed, A., Levy, O., Stoyanov, V., Zettlemoyer, L., 2020. BART: denoising sequence-to-sequence pre-training for natural language generation, translation, and comprehension, in: Jurafsky, D., Chai, J., Schluter, N., Tetreault, J.R. (Eds.), Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, ACL 2020, Online, July 5-10, 2020, Association for Computational Linguistics. pp. 7871–7880. URL: <https://doi.org/10.18653/v1/2020.acl-main.703>, doi:10.18653/V1/2020.ACL-MAIN.703.
- [20] Lin, C.Y., 2004. Rouge: A package for automatic evaluation of summaries, in: Text summarization branches out, pp. 74–81.
- [21] Liu, Y., 2019. Fine-tune BERT for extractive summarization. CoRR abs/1903.10318. URL: <http://arxiv.org/abs/1903.10318>, arXiv:1903.10318.
- [22] Liu, Y., Lapata, M., 2019. Text summarization with pretrained encoders, in: Inui, K., Jiang, J., Ng, V., Wan, X. (Eds.), Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, EMNLP-IJCNLP 2019, Hong Kong, China, November 3-7, 2019, Association for Computational Linguistics. pp. 3728–3738. URL: <https://doi.org/10.18653/v1/D19-1387>, doi:10.18653/V1/D19-1387.
- [23] Liu, Y., Liu, P., Radev, D.R., Neubig, G., 2022. BRIO: bringing order to abstractive summarization, in: Muresan, S., Nakov, P., Villavicencio, A. (Eds.), ACL 2022, Association for Computational Linguistics. pp. 2890–2903. URL: <https://doi.org/10.18653/v1/2022.acl-long.207>, doi:10.18653/V1/2022.ACL-LONG.207.
- [24] Loshchilov, I., Hutter, F., 2017. Fixing weight decay regularization in adam. ArXiv abs/1711.05101.
- [25] Luong, T., Pham, H., Manning, C.D., 2015. Effective approaches to attention-based neural machine translation, in: Màrquez, L., Callison-Burch, C., Su, J., Pighin, D., Marton, Y. (Eds.), Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing, EMNLP 2015, Lisbon, Portugal, September 17-21, 2015, The Association for Computational Linguistics. pp. 1412–1421. URL: <https://doi.org/10.18653/v1/d15-1166>, doi:10.18653/V1/D15-1166.
- [26] Mukherjee, R., Bohra, A., Banerjee, A., Sharma, S., Hegde, M., Shaikh, A., Shrivastava, S., Dasgupta, K., Ganguly, N., Ghosh, S., Goyal, P., 2022. Ectsum: A new benchmark dataset for bullet point summarization of long earnings call transcripts, in: Goldberg, Y., Kozareva, Z., Zhang, Y. (Eds.), Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing, EMNLP 2022, Abu Dhabi, United Arab Emirates, December 7-11, 2022, Association for Computational Linguistics. pp. 10893–10906. URL: <https://doi.org/10.18653/v1/2022.emnlp-main.748>, doi:10.18653/V1/2022.EMNLP-MAIN.748.
- [27] Nallapati, R., Zhai, F., Zhou, B., 2017. Summarunner: A recurrent neural network based sequence model for extractive summarization of documents, in: Proceedings of the AAAI conference on artificial intelligence.
- [28] Nallapati, R., Zhou, B., Gulcehre, C., Xiang, B., et al., 2016. Abstractive text summarization using sequence-to-sequence rnns and beyond. arXiv preprint arXiv:1602.06023 .
- [29] Narayan, S., Cohen, S.B., Lapata, M., 2018. Don't give me the details, just the summary! topic-aware convolutional neural networks for extreme summarization, in: Riloff, E., Chiang, D., Hockenmaier, J., Tsujii, J. (Eds.), Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing, Brussels, Belgium, October 31 - November 4, 2018, Association for Computational Linguistics. pp. 1797–1807. URL: <https://doi.org/10.18653/v1/d18-1206>, doi:10.18653/V1/D18-1206.
- [30] OpenAI, 2023. Gpt-4 technical report. ArXiv .
- [31] Peng, W., Hu, Y., Yu, J., Xing, L., Xie, Y., 2021. APER: adaptive evidence-driven reasoning network for machine reading comprehension with unanswerable questions. Knowl. Based Syst. 229, 107364. URL: <https://doi.org/10.1016/j.knosys.2021.107364>, doi:10.1016/J.KNOSYS.2021.107364.
- [32] Peng, W., Qin, Z., Hu, Y., Xie, Y., Li, Y., 2023. FADO: feedback-aware double controlling network for emotional support conversation. Knowl. Based Syst. 264, 110340. URL: <https://doi.org/10.1016/j.knosys.2023.110340>, doi:10.1016/J.KNOSYS.2023.110340.
- [33] Radford, A., Narasimhan, K., Salimans, T., Sutskever, I., et al., 2018. Improving language understanding by generative pre-training .
- [34] Raffel, C., Shazeer, N., Roberts, A., Lee, K., Narang, S., Matena, M., Zhou, Y., Li, W., Liu, P.J., 2020. Exploring the limits of transfer learning with a unified text-to-text transformer. The Journal of Machine Learning Research 21, 5485–5551.
- [35] Rush, A.M., Chopra, S., Weston, J., 2015. A neural attention model for abstractive sentence summarization. arXiv preprint arXiv:1509.00685 .
- [36] Schatz, D., Bashroush, R., Wall, J.A., 2017. Towards a more representative definition of cyber security. J. Digit. Forensics Secur. Law 12, 53–74. URL: <https://doi.org/10.15394/jdfs1.2017.1476>, doi:10.15394/JDFSL.2017.1476.
- [37] See, A., Liu, P.J., Manning, C.D., 2017. Get to the point: Summarization with pointer-generator networks, in: Barzilay, R., Kan, M. (Eds.), Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, ACL 2017, Vancouver, Canada, July 30 - August 4, Volume 1: Long Papers, Association for Computational Linguistics. pp. 1073–1083. URL: <https://doi.org/10.18653/v1/P17-1099>, doi:10.18653/V1/P17-1099.
- [38] Shukla, A., Bhattacharya, P., Poddar, S., Mukherjee, R., Ghosh, K., Goyal, P., Ghosh, S., 2022. Legal case document summarization: Extractive and abstractive methods and their evaluation, in: He, Y., Ji, H., Liu, Y., Li, S., Chang, C., Poria, S., Lin, C., Buntine, W.L., Liakata, M., Yan, H., Yan, Z., Ruder, S., Wan, X., Arana-Catania, M., Wei, Z., Huang, H., Wu, J., Day, M., Liu, P., Xu, R. (Eds.), Proceedings of the 2nd Conference of the Asia-Pacific Chapter of the Association for Computational Linguistics and the 12th International Joint Conference on Natural Language Processing, AACL/IJCNLP 2022 - Volume 1: Long Papers, Online Only, November 20-23, 2022, Association for Computational Linguistics. pp. 1048–1064. URL: <https://aclanthology.org/2022.aacl-main.77>.
- [39] van Tilborg, H.C.A. (Ed.), 2005. Encyclopedia of Cryptography and Security. Springer. URL: <https://doi.org/10.1007/0-387-23483-7>, doi:10.1007/0-387-23483-7.
- [40] Touvron, H., Martin, L., Stone, K., Albert, P., Almahairi, A., Babaei, Y., Bashlykov, N., et al., 2023. Llama 2: Open foundation and fine-tuned chat models. arXiv preprint arXiv:2307.09288 .
- [41] Vaswani, A., Shazeer, N., Kaiser, L., Polosukhin, I., et al., 2017. Attention is all you need, in: NIPS.
- [42] Zeng, A., Liu, X., Du, Z., Wang, Z., Lai, H., Ding, M., Yang, Z., Xu, Y., Zheng, W., Xia, X., et al., 2022. Glm-130b: An open bilingual pre-trained model. arXiv preprint arXiv:2210.02414 .
- [43] Zhang, T., Kishore, V., Wu, F., Weinberger, K.Q., Artzi, Y., 2020. Bertscore: Evaluating text generation with BERT, in: 8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia, April 26-30, 2020, OpenReview.net. URL: <https://openreview.net/forum?id=SkeHuCVFDr>.
- [44] Zhong, M., Liu, P., Chen, Y., Wang, D., Qiu, X., Huang, X., 2020. Extractive summarization as text matching, in: Jurafsky, D., Chai, J., Schluter, N., Tetreault, J.R. (Eds.), Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, ACL 2020, Online, July 5-10, 2020, Association for Computational Linguistics. pp. 6197–6208.
- [45] Zhou, Q., Yang, N., Wei, F., Huang, S., Zhou, M., Zhao, T., 2018. Neural document summarization by jointly learning to score and select sentences, in: Gurevych, I., Miyao, Y. (Eds.), Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics, ACL 2018, Melbourne, Australia, July 15-20, 2018, Volume 1: Long Papers, Association for Computational Linguistics. pp. 654–663. URL: <https://aclanthology.org/P18-1061/>, doi:10.18653/V1/P18-1061.
- [46] Zhu, Y., Yang, X., Wu, Y., Zhang, W., 2023. Leveraging summary guidance on medical report summarization. IEEE J. Biomed. Health Informatics 27, 5066–5075. doi:10.1109/JBHI.2023.3304376.



Wei Peng received the B.S. degree in Computer Science and Technology from Chang'an University, Xi'an, China, in 2018 and his PhD degree in Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, in 2023. He has published his research in high quality journals and conferences in the area, including KBs, Neurocomputing, IJCAI, SIGIR, AAAI, EMNLP, etc. His research interests include summarization, natural language generation and question answering.



Lei Cui is an associate professor of Zhongguancun Laboratory, Beijing. He received his Doctor's degree in Computer Software and Theory from Beihang University in 2015. His research interests include operating system, system security, and system virtualization. He has published over 40 papers in journals and conferences including TPDS, TIFS, TSC, ISSTA, ICCD, RAID, VEE, LISA, DSN.



Junmei Ding is a doctoral candidate at the School of Cyberspace Security, Beijing University of Posts and Telecommunications, holding a Master's degree in Software Engineering from Shanxi University. Her main research directions are anomaly behavior detection, threat detection, and cyber threat intelligence summarization.



Wei Cai is an assistant research scientist in the Network Connection Security Department at Zhongguancun Laboratory. He holds a PhD from the Institute of Information Engineering at the Chinese Academy of Sciences. His research primarily focuses on mobile encrypted traffic analysis and adversarial machine learning.



Wei Wang received the doctor's degree in Institute of Information Engineering, School of Cyber Security, University of Chinese Academy of Sciences. She is currently a research assistant of Zhongguancun Laboratory. Her research interests include system virtualization and network security. She has published several papers in journals and conferences including TSC, ICCD, VEE.



Zhiyu Hao is currently a professor of Zhongguancun Laboratory, Beijing. He received his Ph.D degree in Computer System Architecture from Harbin Institute of Technology in 2007. His research interests include network security, system virtualization. He has published over 50 papers in journals and conferences including TPDS, ICPP, IEEE S&P, ICA3PP and CLUSTER.



Xiaochun Yun is the Deputy Director of the National Computer Network Emergency Response Technical Team/Coordination Center of China. He obtained a Bachelor's degree in Computer Science and Application from Harbin Institute of Technology, and a Ph.D. degree in Computer System Architecture from the same university. His research areas include network malware detection and prevention technology, security analysis, and content security. He has published over 100 academic papers.