electronics

MDPI

Article

Text Command Intelligent Understanding for Cybersecurity Testing

Junkai Yi [1], Yuan Liu [1,*], Zhongbai Jiang [2] and Zhen Liu [1]

[1] Key Laboratory of Modern Measurement and Control Technology Ministry of Education, Beijing Information Science and Technology University, Beijing 102206, China; yijk@bistu.edu.cn (J.Y.); liuz@bistu.edu.cn (Z.L.)
[2] China Information Technology Security Evaluation Center, Beijing 100085, China; jianzb@itsec.gov.cn
* Correspondence: 2023020399@bistu.edu.cn

Abstract: Research on named entity recognition (NER) and command-line generation for network security evaluation tools is relatively scarce, and no mature models for recognition or generation have been developed thus far. Therefore, in this study, the aim is to build a specialized corpus for network security evaluation tools by combining knowledge graphs and information entropy for automatic entity annotation. Additionally, a novel NER approach based on the KG-BERT-BiLSTM-CRF model is proposed. Compared to the traditional BERT-BiLSTM model, the KG-BERT-BiLSTM-CRF model demonstrates superior performance when applied to the specialized corpus of network security evaluation tools. The graph attention network (GAT) component effectively extracts relevant sequential content from datasets in the network security evaluation domain. The fusion layer then concatenates the feature sequences from the GAT and BiLSTM layers, enhancing the training process. Upon successful NER execution, in this study, the identified entities are mapped to pre-established command-line data for network security evaluation tools, achieving automatic conversion from textual content to evaluation commands. This process not only improves the efficiency and accuracy of command generation but also provides practical value for the development and optimization of network security evaluation tools. This approach enables the more precise automatic generation of evaluation commands tailored to specific security threats, thereby enhancing the timeliness and effectiveness of cybersecurity defenses.

Keywords: cybersecurity testing; KG-BERT-BiLSTM-CRF; bidirectional long short-term memory networks; conditional random fields

check for updates

Citation: Yi, J.; Liu, Y.; Jiang, Z.; Liu, Z. Text Command Intelligent Understanding for Cybersecurity Testing. *Electronics* **2024**, *13*, 4330. https://doi.org/10.3390/electronics13214330

Academic Editor: Aryya Gangopadhyay

Received: 15 October 2024
Revised: 1 November 2024
Accepted: 3 November 2024
Published: 4 November 2024

1. Introduction

In the field of network security, the utilization of automated tools [1] is crucial for enhancing system defense and response times. Specifically, cybersecurity testing tools such as penetration testing software and vulnerability scanners play an important role by automatically generating test commands to simulate attacker actions, thereby detecting and mitigating potential security vulnerabilities [2]. As automation levels advance, the efficiency and precision of these tools have become focal points of research and development.

Advances in artificial intelligence and machine learning have further enabled these tools to process complex data inputs more effectively, with named entity recognition (NER) [3,4] being one of the key technologies driving improvements. NER swiftly identifies key informational entities from complex security incident reports or network logs, such as IP addresses, domain names, and protocol types. This entity information is particularly crucial for generating targeted test commands, as they directly relate to the network components that will be tested or monitored. To better meet the needs of cybersecurity, optimizing NER technology is paramount. This involves training specialized models to recognize specific entities within the cybersecurity domain, such as vulnerability identifiers (e.g., CVE tags) [5] and malware names [6]. Additionally, the development of more precise test command generation algorithms is necessary. These algorithms can utilize identified entities and related contextual information from the text to automatically construct and adjust test commands. In generating these commands, it is essential to consider security policies, the latest security threat intelligence, and the actual architecture of the system to ensure the specificity and effectiveness of the test commands.

Despite advances in NER technology across domains such as healthcare, education, and the military, the cybersecurity field faces unique challenges due to the scarcity of specialized, publicly available corpora. This limitation restricts the precision and effectiveness of NER models in identifying cybersecurity-specific entities, as traditional NER models often lack the adaptability required for dynamic and complex cybersecurity contexts. To address these issues, this study employs a novel approach that combines data scraping from the official documentation of cybersecurity tools with a knowledge graph-based automatic annotation process. The knowledge graph [7,8], combined with Transformer-based validation [9] using information entropy [10], supports the construction of a specialized corpus tailored for NER in cybersecurity evaluation tools. Furthermore, in this study, a KG-BERT-BiLSTM-CRF model is introduced, designed to integrate the knowledge graph with sequence processing, enhancing recognition accuracy for entities specific to cybersecurity.

The main contributions of this paper are as follows:

- Novel corpus construction: A unique corpus specifically tailored for cybersecurity, NER was constructed by utilizing data scraping from official tool documentation combined with a knowledge graph-based automatic annotation process.
- Development of KG-BERT-BiLSTM-CRF model: The proposed model innovatively integrates knowledge graph-based features and BERT with BiLSTM-CRF, significantly enhancing the accuracy of entity recognition in cybersecurity contexts.
- Transformer-based validation using information entropy: A validation process incorporating transformers and information entropy was implemented, ensuring high-quality annotation and robust model performance in dynamic cybersecurity contexts.

The structure of this paper is as follows: Section 2 presents the related work and a comparative analysis of recent NER techniques. Section 3 details the proposed KG-BERT-BiLSTM-CRF model, followed by Section 4, which covers the experimental setup, dataset construction, and model evaluation. Section 5 discusses the findings and limitations. Finally, Section 6 concludes with insights on the practical implications and directions for future research on cybersecurity testing tools.

2. Related Work

In this context, named entity recognition (NER) technology in natural language processing plays an important role in cybersecurity testing, offering robust support.

Xu et al. [11] proposed a BERT-CNN-BiLSTM model that enhances text classification performance on small datasets and effectively addresses overfitting by integrating BERT's deep semantic understanding, CNN's feature extraction, and BiLSTM's sequence processing capabilities. Zhang et al. [12] developed the MGBERT-Pointer model, which leverages a multi-granularity BERT adapter and an efficient global pointer to significantly improve the accuracy of Chinese named entity recognition, especially in handling nested entities and entities with ambiguous boundaries.

Arslan [13] explored the automatic recognition of product names in unstructured Turkish texts using a BiLSTM-CRF model combined with various embedding techniques. Wei et al. [14] demonstrated the effectiveness of the BERT-BiLSTM-CRF model in the domain of educational emergencies, showing how deep learning technologies handle complex entities effectively within specific domains. Li et al. [15] proposed a model combining BERT, BiLSTM, and CRF for the heterogeneous recognition of military entities, significantly enhancing the model's performance in handling complex military terminology. Li et al. [16] explored methods for identifying urban underground space disaster entities using text information extraction techniques. Their study proposed a model combining ALBERT, BiLSTM, and CRF for entity recognition in text information about urban underground space disasters.

Chu et al. [17] proposed a multi-feature fusion transformer (MFT) that significantly improves the accuracy of named entity recognition in aerospace domain texts by integrating language features at different levels. Zhang et al. [18] developed an entity recognition classification framework that systematically examines the diversity of named entity recognition datasets. Wang et al. [19] proposed a named entity recognition model based on entity trigger reinforcement learning, combining word2vec, BiLSTM, and CRF technologies, specifically designed for automated Chinese entity recognition.

Shishehgarkhaneh et al. [20] explored the application of transformer models such as RoBERTa in Australian construction supply chain risk management, demonstrating the potential of deep learning technologies in handling complex text data. Jeong et al. [21] showcased the application of deep learning models for information extraction tasks by combining BERT with Korean modifier relations. Mao et al. [22] introduced a span-level tagging method to enhance the recognition performance of discontinuous named entities, employing a simplified tagging scheme and graph convolutional network to boost model performance. Wang et al. [23] developed RSRNeT, a multimodal network framework for named entity recognition and relation extraction, showcasing a new approach to integrating visual and textual information.

Ma et al. [24] introduced a decomposition-based meta-learning framework for few-shot sequence labeling, significantly enhancing performance in cross-domain few-sample environments by decomposing tasks into mention detection and type classification, and processing them sequentially through a meta-learning strategy. Tian et al. [25] introduced a pre-trained stride detector and entity-type reference based on large-scale language models in their improved few-shot named entity recognition model, demonstrating superior performance across various datasets.

He et al. [26] proposed a method for text sentiment analysis of Douban movie reviews using a BERT-CNN-BiLSTM-Att model, effectively improving the accuracy of sentiment classification. Han et al. [27] introduced a new named entity recognition model for the long-term COVID literature, named BERT-BiLSTM-IDCNN-ATT-CRF (BBIAC). Zheng et al. [28] focused on named entity recognition in Chinese medical texts, presenting an improved deep learning model incorporating BERT, BiLSTM, improved convolutional networks (imConvNet), and CRF, named BERT-imConvNet-BiLSTM-CRF. Tikhomirov et al. [29] applied a BERT-based model with data augmentation techniques for named entity recognition in the Russian cybersecurity domain, achieving enhanced results by training on a specialized cybersecurity text collection.

The studies outlined above highlight a variety of named entity recognition (NER) models, each tailored to meet specific challenges across diverse application domains. To provide a clearer overview, Table 1 summarizes key models, their application fields, and the strengths and limitations associated with each approach.

Table 1. Summary of models and their performance characteristics.

Model Method	Application Domain	Advantages	Limitations
BERT-CNN-BiLSTM	Small dataset text classification	Effectively reduces overfitting in small datasets, improving accuracy.	Complex structure, high computational cost.
MGBERT-Pointer	Chinese named entity recognition	Improves accuracy for nested and ambiguous boundary entities.	Requires high annotation accuracy, limited generalizability to other languages.
Bi-LSTM-CRF	Non-English language product name recognition	Adapts well to linguistic irregularities.	Difficult to generalize to other languages or domains.

Table 1. *Cont.*

Model Method	Application Domain	Advantages	Limitations
BERT-BiLSTM-CRF	Specialized domain entity recognition (e.g., education, military)	Handles complex terms, robust in specialized contexts.	Strong dependency on specific domains, limited transferability.
Multi-Feature Fusion Transformer (MFT)	Aerospace text recognition	Enhances recognition accuracy for entities in specialized fields.	High computational complexity, long processing times.
Graph Convolutional Network + Span-Level Tagging	Discontinuous entity recognition	Improves recognition for discontinuous entities.	Challenging to process semantically disjointed contexts.
Decomposition-Based Meta-Learning	Cross-domain, low-resource environments	Enhances tagging accuracy in low-resource scenarios.	Limited adaptability to new domains.
RSRNeT Multimodal Network	Entity recognition and relation extraction	Combines visual and textual data, enhancing cross-modal recognition.	High annotation requirements, high model complexity.
BERT-BiLSTM-IDCNN-ATT-CRF	Long-text entity recognition (e.g., the COVID literature)	Improves entity recognition in lengthy texts.	High memory requirements when processing long documents.

Despite advancements in the fields of named entity recognition and command generation, how to effectively combine these technologies to enhance the intelligence and adaptability of automated testing tools [30] remains a hot topic in the current research. Additionally, handling and protecting sensitive information generated and used in automated testing is a key aspect of ensuring the reliability of cybersecurity tools. These studies not only push the boundaries of technology but also have a profound impact on practical cybersecurity measures.

3. KG-BERT-BiLSTM-CRF Model

This section primarily introduces the structure of the KG-BERT-BiLSTM-CRF model and provides a detailed explanation of the roles and functions of its various components.

3.1. KG-BERT-BiLSTM-CRF

The KG-BERT-BiLSTM-CRF model, as shown in Figure 1, is a composite model that integrates BERT [31], graph attention network (GAT) [32], bidirectional long short-term memory (BiLSTM) [33], and conditional random fields (CRF) [34]. In this model, the GAT component utilizes a knowledge graph (KG) to construct the adjacency matrix, which enhances the model's ability to leverage relational information between entities. This adjacency matrix is critical for effectively applying the attention mechanism across different nodes (entities) within the graph, enabling more precise entity recognition. Primarily employed for named entity recognition (NER), the model combines these four distinct techniques to address various aspects of sequence data, thereby enhancing overall performance and accuracy.

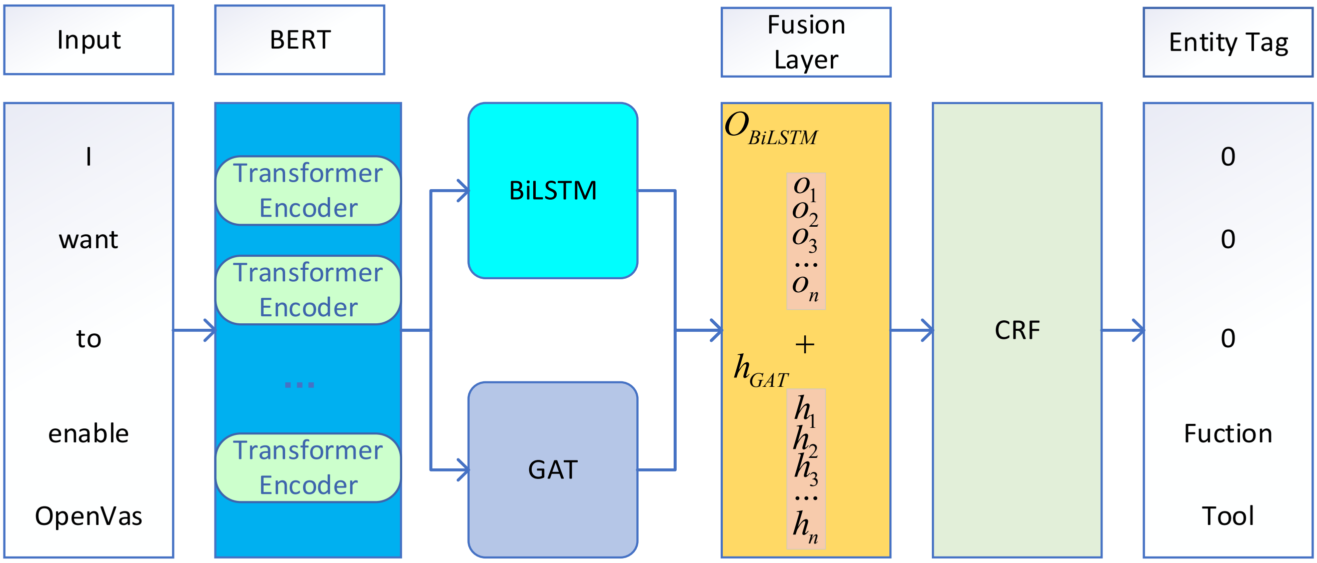


Figure 1. Structure diagram of KG-BERT-BiLSTM-CRF model.

In the KG-BERT-BiLSTM-CRF model, BERT, BiLSTM, GAT, and CRF each play different roles.

- BERT acts as the frontend of the model, utilizing its transformer-based mechanism to deeply encode the input data related to network security evaluation tools, generating sub-vector sequences for the text.
- The GAT layer receives the vectors generated by the BERT layer and combines them with the knowledge graph constructed in this study to calculate entity embeddings.
- The BiLSTM model also processes the output from BERT further, using forward and backward LSTM networks to encode and capture the semantic information and contextual relationships of words in the sequence.
- A specially designed fusion layer concatenates the output vectors from both the GAT and BiLSTM layers.
- The CRF layer performs labeling based on the output from the fusion layer, leveraging the learned contextual information to make accurate label predictions for each word or character, ultimately producing the named entity recognition results.

3.2. The BERT Pretrained Model

In the KG-BERT-BiLSTM-CRF model, BERT serves as the frontend, responsible for understanding and encoding the meaning of the input text, providing deep, context-aware word vector representations. Through its pre-trained deep bidirectional transformer network, BERT generates different word vectors for the same word depending on its context, offering greater flexibility and accuracy, particularly in handling polysemy.

This section focuses on fine-tuning the BERT model using proprietary data from the network security evaluation domain. As shown in Figure 2, data were collected from official websites, academic papers, professional blogs, and the patent literature related to network security. These data were used to perform the customized fine-tuning of the BERT model. The aim of this process was to enhance BERT's accuracy in processing and understanding security-specific terminology and contexts. Through this fine-tuning, the performance of the BERT model was significantly improved, particularly in supporting automated text processing and analysis tasks for network security evaluation tools, demonstrating greater adaptability and accuracy.

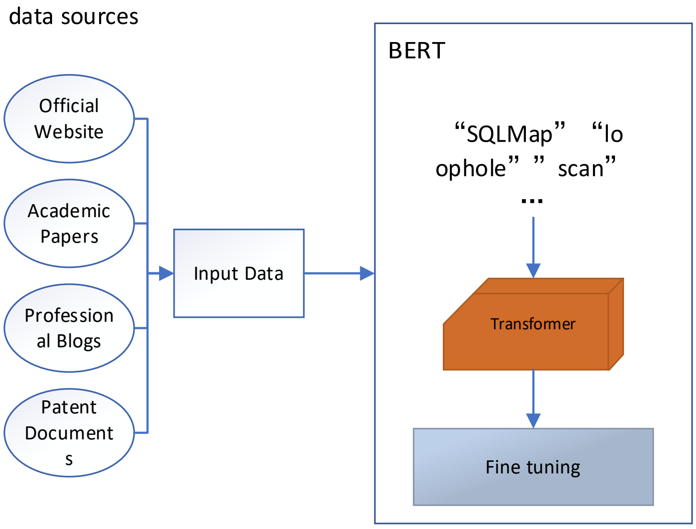


Figure 2. Fine tuning of BERT.

3.3. GAT Model

The core of the GAT lies in its use of the self-attention mechanism [35] to explicitly learn the weights between nodes, allowing GAT to not only adapt to different types of graph structures but also handle the heterogeneity of node connections within the graph.

In this study, based on each entity in the knowledge graph constructed during the auxiliary annotation process, the GAT model updates the feature representation of each entity using the contributions of its neighboring entities and the attention mechanism, as shown in Equation (1).

$$h'_v = \sigma(\sum_{u \in N(V)} \alpha_{vu} w h_u) \tag{1}$$

In this context, h_u represents the feature vector of entity u, w is the learnable linear transformation matrix, $N(v)$ denotes the set of neighboring entities of entity v, and σ is the ReLU [36] activation function. The attention coefficient between entity v and entity u, denoted as α_{vu}, is computed using Equation (2).

$$\alpha_{vu} = \frac{\exp(LeakyReLU(a^T[wh_v||wh_u]))}{\sum_{k \in N(v)} \exp(LeakyReLU(a^T[wh_v||wh_u]))} \tag{2}$$

3.4. BiLSTM Model

In the KG-BERT-BiLSTM-CRF model, the BiLSTM network processes and refines the outputs generated by BERT, enhancing the model's ability to handle sequential data and capture long-term dependencies. The bidirectional LSTM consists of two LSTMs—one processing the sequence forward and the other backward, as shown in Equations (3) and (4). The outputs from both directions are concatenated to form a comprehensive representation, as illustrated in Equation (5).

$$\overrightarrow{h_t} = LSTM(\overrightarrow{x_t}, \overrightarrow{h_{t-1}}) \tag{3}$$

$$\overleftarrow{h_t} = LSTM(\overleftarrow{x_t}, \overleftarrow{h_{t-1}}) \tag{4}$$

$$h_t = [\overrightarrow{h_t}, \overleftarrow{h_t}] \tag{5}$$

LSTM, a special type of RNN (Recurrent Neural Network), includes an input gate, a forget gate, and an output gate. The forget gate determines which information to discard, the input gate decides what information to update into the cell state, and the output gate determines what information to output.

Through the aforementioned calculations, the final output sequence is obtained as $O = \{o_1, o_2, o_3, \ldots, o_n\}$.

3.5. Fusion Layer

In the KG-BERT-BiLSTM-CRF model, the fusion layer plays a critical role by effectively concatenating the outputs from both the GAT layer and the BiLSTM layer, generating a comprehensive feature representation. This operation leverages the strengths of both techniques, resulting in a richer and more informative feature set, which is crucial for the subsequent Named Entity Recognition (NER) tasks.

Specifically, the GAT layer captures the structural relationships between entities using a knowledge graph and produces a sequence of feature representations. The output from the GAT layer can be denoted as $H = [h_1{}', h_2{}', h_3{}', \ldots, h_n{}']$, where each h'_v represents the feature representation of the i-th entity. On the other hand, the BiLSTM layer processes the input sequence and captures contextual dependencies within the text, resulting in an output sequence $O = \{o_1, o_2, o_3, \ldots, o_n\}$.

As shown in Figure 3 and Equation (6), the primary objective of the fusion layer is to concatenate h'_v and O, forming a fused feature sequence $h_i{}'$.

$$h_i{}' = [o_i||h'_{vi}] \tag{6}$$

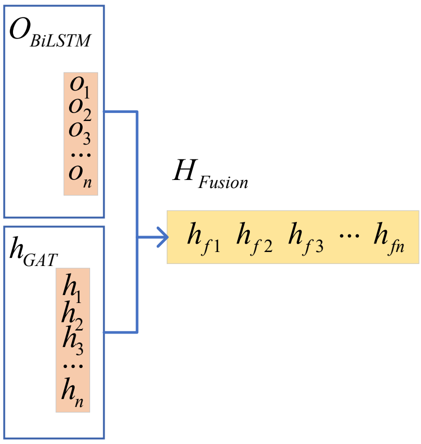


Figure 3. Fusion Layer.

Here, the symbol "||" represents the concatenation operation, which connects the output vectors from the GAT and BiLSTM layers along their dimensions. This concatenated vector $h_i{}'$ contains both the entity relationship information from the GAT layer and the contextual information from the BiLSTM layer.

This fusion mechanism is of significant importance. The feature representations from the GAT layer capture the structural relationships between entities, while those from the BiLSTM layer capture the sequential and contextual information within the text. By concatenating these two types of information, the model can develop a more holistic understanding of each word or entity in the text and its relationship with other entities. This fusion method is particularly beneficial in handling tasks that involve polysemous words or complex dependencies between entities and their contexts, thereby improving the model's overall performance.

3.6. The Conditional Random Field

In the KG-BERT-BiLSTM-CRF model, the CRF layer plays a crucial role in the sequence labeling task, particularly during the final labeling decision stage. The primary function of the CRF layer is to optimize and refine the label sequence at the model's output, ensuring that the final labeling results are both accurate and consistent across the entire sequence.

Unlike classification models that evaluate each label independently, the CRF layer employs a global optimization approach. By learning the transition probabilities between labels, it enables optimal labeling decisions at the sequence level.

By receiving the output sequence H from the fusion layer, the CRF defines the conditional probability of the label sequence Y, as shown in Equation (7).

$$P(Y|H) = \frac{\exp(s(H,Y))}{\sum Y'^{\exp(s(H,Y'))}} \tag{7}$$

Here, $s(H,Y)$ represents the score of sequence H and its corresponding label sequence Y, with the calculation formula provided in Equation (8).

$$s(H,Y) = \sum\nolimits_{i=1}^{n} \left(w_{y_i} h_i{}' + b_{y_i} + T_{y_{i-1},y_i}\right) \tag{8}$$

Here, w_{y_i} and b_{y_i} are the weight and bias corresponding to label v_i in the CRF layer, and $T_{y_{\mathrm{i}-1},y_i}$ represents the transition score, indicating the score for transitioning from label y_{i-1} to label y_i.

3.7. Model Optimization

In this study, an enhanced approach based on the BERT model was employed by adding GAT, BiLSTM, and CRF layers on top of the initial BERT model to further improve the model's recognition capability and accuracy in sequence labelling tasks. BERT, as a powerful language representation model, has demonstrated outstanding performance across various natural language processing tasks by capturing rich linguistic features through pre-training. However, when faced with specific sequence labelling tasks, relying solely on features extracted by BERT may not fully meet the high precision requirements. Therefore, GAT, BiLSTM, and CRF layers were introduced in this study. The GAT layer effectively leverages the knowledge graph constructed in this research to capture relationships between different entities. The BiLSTM layer captures contextual information within the sequence, while the CRF layer optimizes the model's labelling decisions across the entire sequence, particularly by handling dependencies between labels, thus avoiding illogical label sequences.

Moreover, to further enhance the model's performance, a meticulous adjustment of the learning rate was implemented. The learning rate is a crucial hyperparameter that controls the speed of parameter updates during model training, and an appropriate learning rate setting is essential for achieving better training outcomes. In the experimental process, various learning rate adjustment strategies were explored, including fixed learning rates, dynamic learning rate adjustments, and learning rate warm-ups, to find the optimal configuration. The introduction of these strategies not only accelerated the model's convergence but also mitigated the issue of overfitting to some extent, resulting in higher accuracy across multiple sequence labelling tasks.

4. Experiment

This section primarily introduces the construction of the command-line dataset for cybersecurity testing tools and provides a detailed analysis of the model performance experiments, model comparison experiments, dataset comparison experiments, and command generation experiments conducted.

4.1. Dataset

A key challenge in cybersecurity entity recognition is the limited availability of specialized, publicly accessible corpora, especially for entity data specific to cybersecurity evaluation tools. To address this, in this study, the Scrapy framework was utilized to systematically scrape data from official documentation of widely used cybersecurity tools, aiming to construct a corpus tailored for entity recognition in cybersecurity contexts. This data scraping process involved the following steps:

- Selecting Target URLs: official documentation pages of prominent tools, including OpenVAS, Metasploit, OWASP, Tcpdump, and SQLMap, were identified to ensure comprehensive coverage of usage guidelines, configuration details, and command syntax.
- Extracting and Filtering Data: using Scrapy's 3.6.1 CSS selectors and XPath, in this study, relevant content was selectively retrieved while filtering out non-essential elements, such as navigation bars and ads, to ensure data quality.
- Cleaning and Formatting Data: the extracted content was processed to remove HTML tags and irrelevant text, then structured into machine-readable formats suitable for NER tasks.

The selection of these cybersecurity evaluation tools was based on a structured process to ensure their relevance, functionality, and documentation adequacy for research objectives. Tools were chosen to support diverse cybersecurity testing scenarios, including vulnerability scanning, penetration testing, and log analysis. The selection criteria included the following:

- Functionality Coverage: each tool needed to support essential tasks across multiple cybersecurity testing scenarios.
- Reputation and Industry Usage: only tools widely recognized in both industry and academic research were prioritized to ensure alignment with established cybersecurity practices.
- Documentation Accessibility: comprehensive, publicly accessible documentation was essential, facilitating effective data scraping and high-quality corpus construction.

By following the aforementioned steps, this research successfully developed a specialized corpus tailored for cybersecurity entity recognition within cybersecurity evaluation tools. The corpus comprised six hundred entries each from OpenVAS, Metasploit, OWASP, Tcpdump, and SQLMap, ensuring an equal distribution of data across different tools. This consistent number of entries across all tools was intentionally designed to enhance the fairness of model construction and validation, minimizing bias that could arise from data imbalance. Consequently, this balanced dataset provides a robust foundation for fair comparison and experimental validation of the entity recognition models.

4.2. Construction of Knowledge Graph

Data were collected from official websites, academic papers, blogs, and patents in the field of network security evaluation, focusing primarily on the five commonly used security assessment tools of OpenVAS, Metasploit, Nikto, Tcpdump, and SQLMap. In this study, the aim was to extract relevant information from these data sources, such as tool names, functional features, and certain IP addresses, and to systematically categorize and organize this information. A targeted knowledge graph was constructed by establishing relationships between different types of entities, aiding in subsequent manual annotation processes.

Table 2 below shows the initially constructed entity types and the number of distinct entities within each type.

There are instances of functional overlap or similarities in parameter formats among multiple security tools, which may create challenges during the information extraction process. To resolve this issue, in this study, a comprehensive entity relationship model was carefully designed. Through defining and refining entity relationships, in this study, tool features with similar functions or parameter formats were effectively differentiated and managed. Moreover, the established entity relationship model not only optimized the data organization and structuring but also provided robust support for subsequent automated annotation and entity recognition, greatly enhancing the utility and practical value of the knowledge graph.

Table 3 below presents the specific entity relationship settings.

Table 2. Entity types and quantity of types table.

Entity	Entity Type
Tool	5
Function	84
IP	50
Configuration	50
Module	300
RHOSTS	50
LHOST	50
Interface	10
Data_packet	20
File	50
Source port	30
URL	30
Database	20
Data_table	20
Port	30
Report	50

Table 3. Special entity relationship table.

Entity 1	Entity 2	Entity Relationship
Tcpdump	Port	Tcpdump-Port
Sqlmap	UR	Sqlmap-URL
Nikto	URL	Nikto-URL
Nikto	Port	Nikto-Port
Openvas	Function	Openvas-Function
Metasploit	Function	Metasploit-Function
Tcpdum	Function	Tcpdum-Function
Nikto	Function	Nikto-Function
SQLMap	Function	SQLMap-Function

4.3. Entity Tagging

As shown in Figure 4, the basic architecture and workflow of the automatic entity annotation system are presented. The process is divided into the two main stages of entity annotation and entity annotation verification.

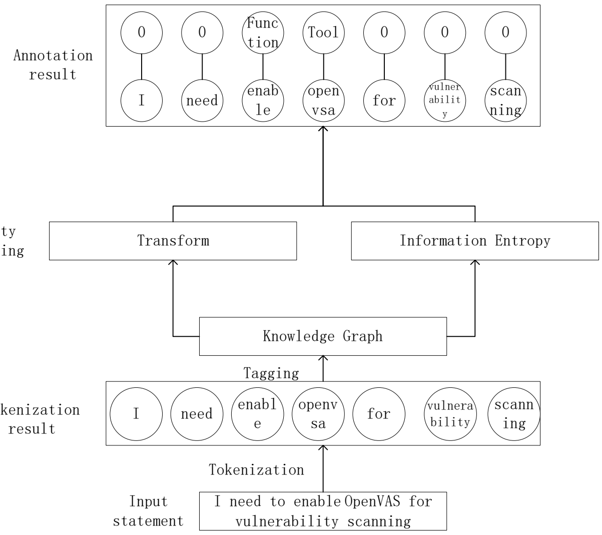


Figure 4. Automatic entity annotation workflow diagram.

In this study, the constructed knowledge graph for a network security assessment tool is used to automatically annotate entities in a corpus related to network security assessment tools. In this process, the knowledge graph serves as a foundational resource, enabling the automatic identification and annotation of entities in the corpus text. This method effectively utilizes the information stored in the knowledge graph, such as tool names, parameters, and operational functions, to assist in identifying corresponding entities in the corpus text, thereby automating the annotation process. This automation not only improves annotation efficiency but also enhances the consistency and accuracy of the dataset, providing essential data for enhancing the development and optimization of future network security assessment tools.

After the entity annotation, auxiliary verification using transformation and information entropy is conducted to ensure the accuracy of the entity annotations. Initially, a pretrained transformer model is used to generate contextually relevant embedding vectors for the annotated entities within the input text. Embedding vectors v_i for the entity words w_i in the input text are generated using Equation (9). If an entity consists of multiple words $w_1, w_2, \ldots\ldots, w_n$, Equation (10) is used to aggregate these word vectors into a single vector through an aggregation method.

$$v_i = Transformer\ Model(w_i) \tag{9}$$

$$v_E = \frac{1}{n}\sum_{i=1}^{n} v_i \tag{10}$$

After obtaining the entity embedding vectors, they are compared with the embeddings of each entity category in the knowledge graph. The similarity s_c between the entity embedding vectors v_i or v_E and each category embedding vector μ_c is calculated using Equation (11).

$$s_c = \frac{v_E \cdot \mu_c}{\parallel v_E \parallel \parallel \mu_c \parallel} \tag{11}$$

After obtaining the similarity s_c, it is converted into the probability $p(c|v_E)$ using Equation (12).

$$p(c|v_E) = \frac{\exp(s_c)}{\sum_{k \in C} \exp(s_k)} \tag{12}$$

Here, C is the set of all categories. Finally, based on the probabilities obtained, the information entropy for each entity is calculated using Equation (13) to evaluate the uncertainty of the classification. Higher information entropy indicates greater uncertainty.

$$H(X) = -\sum_{c \in C} p(c|v_E) \log p(c|v_E) \tag{13}$$

Considering that the errors introduced during the automated annotation process may affect the quality of the dataset, in this study, an important follow-up step—manual review—is also included. Manual review ensures the final quality of the dataset, thereby guaranteeing the reliability of the research outcomes and the effectiveness of its applications.

4.4. Experimental Setup

In this study, our proposed method on the Python 3.8 simulation platform was simulated. Our model was constructed using PyTorch 2.2.1 and runs on a single Nvidia GeForce RTX 2060 GPU. In this study, the Adam optimizer was used for model optimization. The simulation parameters are provided in Table 4.

Table 4. KG-BERT-BiLSTM-CRF model hyperparameter table.

Parameter Name	Parameter Values
dropout	0.1
LSTM_size	256
batch_size	32
Learning_tate	5×10^{-5}
max_sep_len	128

Additionally, early stopping measures were introduced to prevent overfitting, terminating training if the validation loss did not improve for 50 consecutive epochs.

4.5. Evaluation Metrics

The evaluation of entity recognition models involves the following three core performance metrics as standard benchmarks: precision, recall, and the F1 score, which combines precision and recall into a single measure. The F1 score is particularly important because it balances precision and recall, providing a comprehensive measure of the model's effectiveness. The mathematical definitions of these metrics are provided below.

(a) Precision

Precision [37] calculates the ratio of correctly identified entities to the total number of entities that the model identified (correctly and incorrectly). It reflects the accuracy with which the model identifies entities as being relevant.

$$P = \frac{T_P}{T_P + F_P} \tag{14}$$

(b) Recall

Recall [38] measures the proportion of actual entities that were correctly identified by the model, accounting for the sensitivity of the model towards capturing relevant entities.

$$R = \frac{T_P}{T_P + F_N} \tag{15}$$

(c) F1 Score

The F1 score [39] is the harmonic mean of precision and recall, offering a balance between the precision and recall metrics. It is particularly useful when the classes are imbalanced, providing a more realistic measure of model performance.

$$F = \frac{2 \times P \times R}{P + R} \tag{16}$$

These metrics together furnish a robust framework for assessing the performance of named entity recognition systems, allowing for nuanced insights into their operational effectiveness.

4.6. Experimental Results

- Experiment I: KG-BERT-BiLSTM-CRF Model Training Experiment

The corpus constructed for evaluating cybersecurity testing tools is stratified and divided, with 10% each allocated for validation and testing, and the remaining 80% for training. This ensures an even distribution of annotated entities across the training, validation, and testing sets, and the model is set to run for 100 epochs.

Figures 5–7 show that the KG-BERT-Bi-LSTM-CRF model achieves superior precision, recall, and F1-score metrics, with respective values of 99.91%, 99.96%, and 99.97%. These improvements validate the model's efficacy and precision in relevant tasks. The results further demonstrate that the model excels across all evaluation metrics, maintaining a balanced performance in precision and recall and yielding a high F1-score as a comprehensive metric.

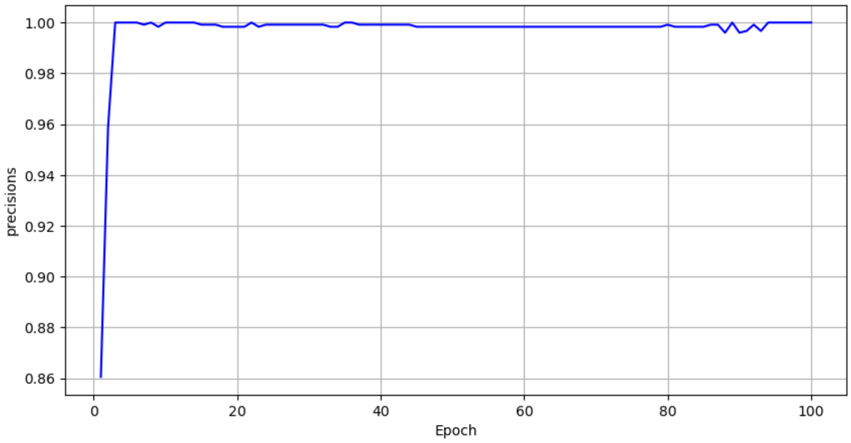


Figure 5. KG-BERT-BiLSTM-CRF model precision variation diagram.

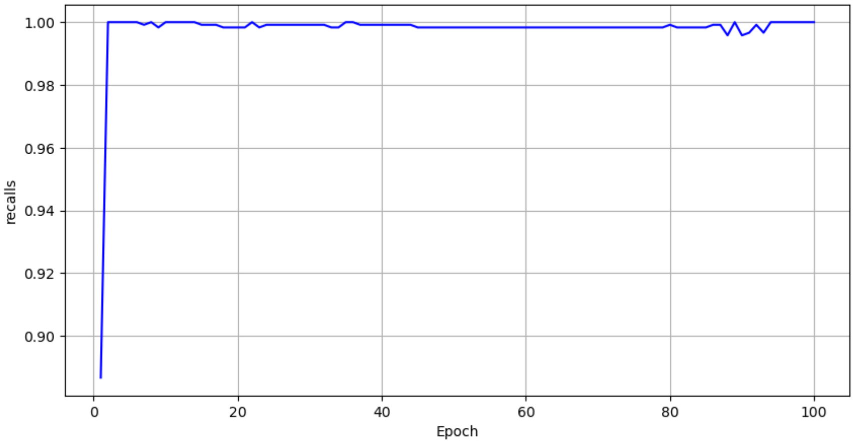


Figure 6. KG-BERT-BiLSTM-CRF model recall variation diagram.

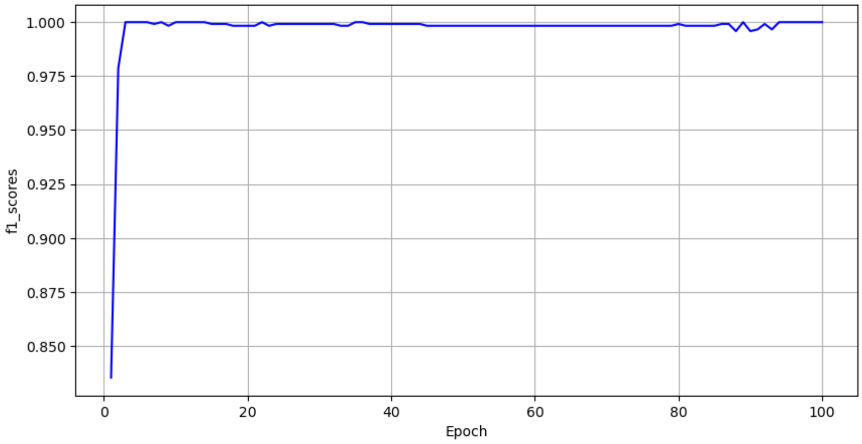


Figure 7. KG-BERT-BiLSTM-CRF model F1 variation diagram.

Table 5 provides detailed precision, recall, and F1-score values across various annotated entity types, supporting the model's robust performance.

Table 5. Experimental result 1 (partial entity results only).

Entity Type	P	R	F_1
Tool	0.9991	0.9992	0.9993
Ip	0.9961	0.9963	0.9965
Function	0.9998	0.9994	0.9996
Configuration	0.9981	0.9995	0.9987

- Experiment II: Model control experiment

In this study, the proposed model is compared with other relevant named entity recognition models. The first control experiment uses a standalone BERT-based NER model, while the second employs a BERT-BiLSTM NER architecture.

Table 6 and Figure 8 present the results of the comparative studies. Notably, the KG-BERT-BiLSTM-CRF model shows significant performance improvements over the conventional BERT and BERT-BiLSTM architectures.

Table 6. Experimental result 2.

Identification Model	P	R	F_1
BERT	0.7995	0.7998	0.7997
BERT-Bi-LSTM	0.9564	0.9316	0.9585
KG-BERT-Bi-LSTM-CRF	0.9991	0.9996	0.9997

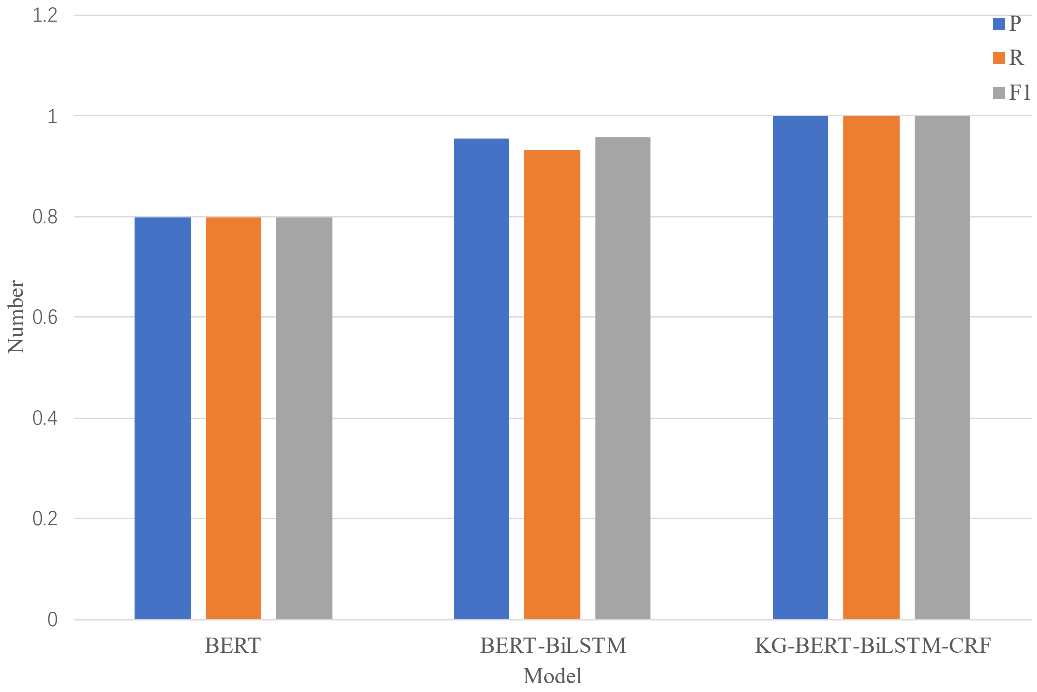
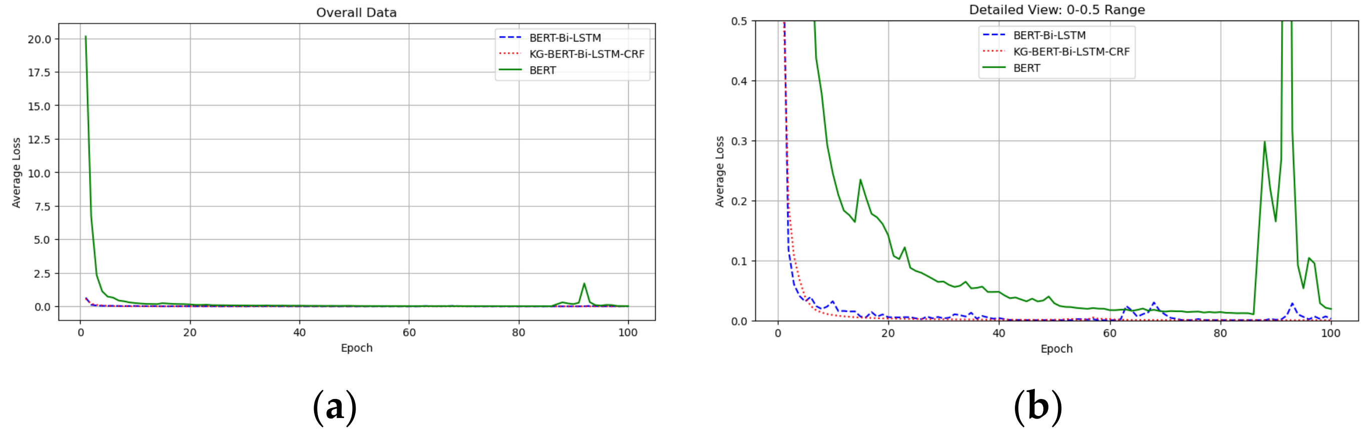


Figure 8. Model precision Recall and F1-score comparison diagram.

As depicted in Figure 9, a comparative analysis of the loss rates incurred by the three distinct models reveals several key insights. Initially, the KG-BERT-Bi-LSTM-CRF model exhibits a substantially lower initial loss rate compared to the BERT model, suggesting a more expedited convergence to a stable state. Subsequently, when stability is achieved, the KG-BERT-Bi-LSTM-CRF model exhibits a reduced variability in the loss rate compared to the BERT-Bi-LSTM model, indicating a higher degree of performance stability.



(**a**) (**b**)

Figure 9. Comparison of loss rate diagram. This figure presents the training loss progression for three different models over multiple training epochs. Panel descriptions are as follows: (**a**) this panel displays the average loss for all epochs across three models: BERT-Bi-LSTM (blue dashed line), KG-BERT-Bi-LSTM-CRF (red dotted line), and BERT (green solid line); (**b**) this panel specifically focuses on the detailed view of the average loss between 0 and 0.5, providing a zoomed-in perspective of the initial training phase.

- Experiment III: Cybersecurity Testing Command Generation

In this study, the previously employed entity recognition model is integrated with a curated database of command-line inputs for cybersecurity testing tools. Initially, a named entity recognition model is used to extract key information from the text, identifying entities such as tools ('tool'), functions ('function'), and IP addresses ('ip'). These recognized entities are then mapped to their respective entries in the command-line database. Through this mapping, the required command lines are autonomously generated based on the input text.

Table 7 displays the outcomes for a subset of the test cases employed.

Table 7. Experimental result 3.

Test Statement	Tool	Function	Command Line
I need to use OpenVas now, please enable OpenVas for me.	OpenVas (22.7.3)	enable	openvas-start
I want to use OpenVas, which has the function of creating a target with an IP address of 192.168.1.1.	OpenVas	creating a target	gvm-cli socket --xml <create_target><name>Target Name</name><hosts>192.168.1.1</hosts></create_target>
Use OpenVas to obtain a list of reports.	OpenVas	obtain a list of reports	gvm-cli socket --xml "<get_reports/>"

Experiment III results demonstrate the model's capability to accurately recognize key information in the NER task and validate its practical application when integrated with the command-line database. Through integration, the system automatically extracts keywords such as "tool", "function", and "target IP" from user instructions and maps them to command-line templates in the database, generating the corresponding command-line statements.

5. Discussion

In this study, named entity recognition (NER) technology in the cybersecurity field is significantly advanced by introducing the KG-BERT-BiLSTM-CRF model, demonstrating its outstanding performance in accurately identifying specific cybersecurity entities. The uniqueness of this model lies in its integration of knowledge graphs and its direct impact on the attention mechanisms within the graph attention network (GAT), enhancing the precision and adaptability of identifying complex cybersecurity entities. Compared to traditional NER systems that rely on textual data, this research method effectively utilizes the relational information from knowledge graphs, thereby providing significant improvements in accuracy and adaptability.

Additionally, an information entropy method is employed in this study, based on transformer for validating entity annotations. This method enhances annotation reliability by quantifying uncertainty, providing an effective way to improve data annotation quality without extensive manual effort. This approach has not been widely applied in the works of Dasgupta et al. [40] whose research, although demonstrating various deep learning-based NER algorithms on cybersecurity datasets, did not fully address the issues of annotation quality and handling dynamic changes.

Moreover, compared to the Bi-LSTM with CRF approach used by Ma et al. [41], our model shows better robustness in handling dynamic cybersecurity terms and scenarios. Furthermore, although Fang et al. [42] have made significant progress in processing Chinese cybersecurity NER by combining graph convolutional networks with hybrid embeddings, the model's adaptability and accuracy is significantly enhanced in our study by integrating broader semantic and syntactic information across multiple languages.

In summary, the KG-BERT-BiLSTM-CRF model sets a new standard in NER technology for the cybersecurity domain through its unique integration of advanced techniques, clearly outperforming existing NER systems. This model provides more intelligent and efficient technological support for cybersecurity defenses, broadening the applicability of NER systems in specialized domains.

6. Conclusions

This research employed a custom-built corpus specific to the domain of cybersecurity testing for the training process, wherein the KG-BERT-Bi-LSTM-CRF model exhibited notable enhancements in performance when contrasted with models that were solely based on BERT or the fusion of BERT and Bi-LSTM. These outcomes not only corroborate the efficacy of the composite model in intricate named entity recognition tasks, but also by leveraging the mapped relationship with the cybersecurity testing command line database, accomplish proficient and precise command line generation. This underscores the model's superior potential for application in terms of both entity recognition accuracy and command line generation efficiency.

The findings of this study have practical value for cybersecurity operations, particularly in automating the generation of testing commands for diverse cybersecurity scenarios. Integrating this model into existing cybersecurity tools could significantly reduce manual workload, improve response times, and enhance the accuracy of vulnerability detection in real-world network environments. Furthermore, this model could be adapted for use in dynamic cybersecurity defense systems, autonomously updating entity recognition and command generation processes in response to emerging threats, thereby strengthening the robustness of network security defenses.

Future research may further refine the model architecture and training process by integrating advanced self-attention mechanisms and investigating more efficacious sequence labelling strategies. Moreover, augmenting the corpus to encompass a broader spectrum of cybersecurity incidents and scenarios is crucial for enhancing the model's generalization capabilities. Furthermore, research should concentrate on the efficiency and stability of model deployment within real network environments, as well as on the effective integration of real-time data updates to counteract rapidly evolving cybersecurity threats. The approach will facilitate the development of more automated and intelligent cybersecurity defense systems, thereby exerting a profound impact on the cybersecurity domain.

Author Contributions: J.Y.: conceptualization, methodology, algorithm framework design; Y.L.: data curation, software, writing—original draft preparation; Z.J.: test data generation, validation; Z.L.: writing—reviewing and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China, grant number 2024QY1703.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: This work was supported by the National Key R&D Program of China under Grant No. 2024QY1703. The authors would like to express their sincere gratitude for the financial and technical support provided by the program, which significantly facilitated the progress of this research. Additionally, special thanks are due to Yao Yifan for his assistance in enriching the dataset content.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Holkovič, M.; Ryšavý, O.; Dudek, J. Automating Network Security Analysis at Packet-level by using Rule-based Engine. In Proceedings of the 6th Conference on the Engineering of Computer Based Systems (ECBS '19), New York, NY, USA, 2–3 September 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 1–8. [CrossRef]
2. Aota, M.; Kanehara, H.; Kubo, M.; Murata, N.; Sun, B.; Takahashi, T. Automation of Vulnerability Classification from its Description using Machine Learning. In Proceedings of the 25th IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 26–32. [CrossRef]
3. Shaalan, K. A Survey of Arabic Named Entity Recognition and Classification. *Comput. Linguist.* **2014**, *40*, 469–510. [CrossRef]
4. Xi, T.; Jiang, D.C. A Weakly Supervised Chinese Named Entity Recognition Method Combining First-Order Logic. *IEEE Access* **2024**, *12*, 59893–59900. [CrossRef]
5. Kanakogi, K.; Washizaki, H.; Fukazawa, Y.; Ogata, S.; Okubo, T.; Kato, T.; Kanuka, H.; Hazeyama, A.; Yoshioka, N. Comparative Evaluation of NLP-Based Approaches for Linking CAPEC Attack Patterns from CVE Vulnerability Information. *Appl. Sci.* **2022**, *12*, 3400. [CrossRef]
6. Bhuiyan, F.A.; Sharif, M.B.; Rahman, A. Security Bug Report Usage for Software Vulnerability Research: A Systematic Mapping Study. *IEEE Access* **2021**, *9*, 28471–28495. [CrossRef]
7. Lin, J.J.; Zhao, Y.Z.; Huang, W.Y.; Liu, C.F.; Pu, H.T. Domain knowledge graph-based research progress of knowledge representation. *Neural Comput. Appl.* **2021**, *33*, 681–690. [CrossRef]
8. Peng, C.Y.; Xia, F.; Naseriparsa, M.; Osborne, F. Knowledge Graphs: Opportunities and Challenges. *Artif. Intell. Rev.* **2023**, *56*, 13071–13102. [CrossRef]
9. Yang, Q.Y.; Jiang, J.; Feng, X.Y.; He, J.M.; Chen, B.R.; Zhang, Z.Y. Named Entity Recognition of Power Substation Knowledge Based on Transformer-BiLSTM-CRF Network. In Proceedings of the 2020 International Conference on Smart Grids and Energy Systems (SGES 2020), Perth, Australia, 23–26 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 952–956. [CrossRef]
10. Wang, S.W.; Xu, R.F.; Liu, B.; Gui, L.; Zhou, Y. Financial Named Entity Recognition Based on Conditional Random Fields and Information Entropy. In Proceedings of the 2014 International Conference on Machine Learning and Cybernetics (ICMLC), Lanzhou, China, 13–16 July 2014; IEEE: Piscataway, NJ, USA, 2014; Volume 2, pp. 838–843.
11. Xu, E.Z.; Qin, D.H.; Huang, J.; Zhang, J.B. Multi Text Classification Model Based on BRET-CNN-BiLSTM. In Proceedings of the 2022 IEEE the 5th International Conference on Big Data and Artificial Intelligence (BDAI 2022), Fuzhou, China, 8–10 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 184–189. [CrossRef]
12. Zhang, L.; Xia, P.F.; Ma, X.X.; Yang, C.W.; Ding, X. Enhanced Chinese Named Entity Recognition with Multi-Granularity BERT Adapter and Efficient Global Pointer. *Complex Intell. Syst.* **2024**, *10*, 4473–4491. [CrossRef]
13. Arslan, S. Application of Bi-LSTM-CRF model with different embeddings for product name extraction in unstructured Turkish text. *Neural Comput. Appl.* **2024**, *36*, 8371–8382. [CrossRef]
14. Wei, K.W.; Wen, B. Named Entity Recognition Method for Educational Emergency Field Based on BERT. In Proceedings of the 2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 20–22 August 2021; Li, W.Z., Ed.; IEEE: Piscataway, NJ, USA, 2021; pp. 145–149. [CrossRef]
15. Li, H.; Yu, L.; Zhang, J.; Lyu, M. Fusion Deep Learning and Machine Learning for Heterogeneous Military Entity Recognition. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1103022. [CrossRef]
16. Li, Z.W.; Zhang, X.D. Research on Named Entity Recognition Methods for Urban Underground Space Disasters Based on Text Information Extraction. In *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*; El-Sheimy, N., Abdelbary, A.A., El-Bendary, N., Mohasseb, Y., Eds.; Geospatial Week 2023 48-1; ISPRS: Bethesda, MA, USA, 2023; pp. 547–552. [CrossRef]

17. Chu, J.; Liu, Y.M.; Yue, Q.; Zheng, Z.X.; Han, X.K. Named Entity Recognition in Aerospace Based on Multi-Feature Fusion Transformer. *Sci. Rep.* **2024**, *14*, 827. [CrossRef]
18. Zhang, Y.; Xiao, G. Named Entity Recognition Datasets: A Classification Framework. *Int. J. Comput. Intell. Syst.* **2024**, *17*, 71. [CrossRef]
19. Wang, P.; Si, N.; Tong, H.P. A Named Entity Recognition Model Based on Entity Trigger Reinforcement Learning. In Proceedings of the 2022 IEEE 2nd International Conference on Computer Communication and Artificial Intelligence (CCAI 2022), Beijing, China, 6–8 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 43–48. [CrossRef]
20. Shishehgarkhaneh, M.B.; Moehler, R.C.; Fang, Y.H.; Hijazi, A.A.; Aboutorab, H. Transformer-Based Named Entity Recognition in Construction Supply Chain Risk Management in Australia. *IEEE Access* **2024**, *12*, 41829–41851. [CrossRef]
21. Jeong, H. A Transfer Learning-Based Pairwise Information Extraction Framework Using BERT and Korean-Language Modification Relationships. *Symmetry* **2024**, *16*, 136. [CrossRef]
22. Mao, T.Y.; Xu, Y.B.; Liu, W.T.; Peng, J.C.; Chen, L.L.; Zhou, M.W. A Simple but Effective Span-Level Tagging Method for Discontinuous Named Entity Recognition. *Neural Comput. Appl.* **2024**, *36*, 7187–7201. [CrossRef]
23. Wang, S.H.; Qin, B. A Novel Joint Training Model for Knowledge Base Question Answering. *IEEE ACM Trans. Audio Speech Lang. Process.* **2024**, *32*, 666–679. [CrossRef]
24. Ma, T.T.; Wu, Q.H.; Jiang, H.Q.; Lin, J.R.; Karlsson, B.F.; Zhao, T.J.; Lin, C.Y. Decomposed Meta-Learning for Few-Shot Sequence Labeling. *IEEE ACM Trans. Audio Speech Lang. Process.* **2024**, *32*, 1980–1993. [CrossRef]
25. Tian, C.; Yin, W.P.; Li, D.; Moens, M.F. Fighting Against the Repetitive Training and Sample Dependency Problem in Few-Shot Named Entity Recognition. *IEEE Access* **2024**, *12*, 37600–37614. [CrossRef]
26. He, A.X.; Abisado, M. Text Sentiment Analysis of Douban Film Short Comments Based on BERT-CNN-BiLSTM-Att Model. *IEEE Access* **2024**, *12*, 45229–45237. [CrossRef]
27. Han, Z.W.; Lin, S.F.; Huang, Z.S.; Guo, C.H. Named Entity Recognition for Long COVID Biomedical Literature by Using Bert-BiLSTM-IDCNN-ATT-CRF Approach. In Proceedings of the 2023 4th International Symposium on Artificial Intelligence for Medicine Science (ISAIMS 2023), Chengdu, China, 20–22 October 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1200–1205. [CrossRef]
28. Zheng, Y.C.; Han, Z.G.; Cai, Y.M.; Duan, X.B.; Sun, J.L.; Yang, W.; Huang, H.S. An imConvNet-based Deep Learning Model for Chinese Medical Named Entity Recognition. *BMC Med. Inform. Decis. Mak.* **2022**, *22*, 303. [CrossRef]
29. Tikhomirov, M.; Loukachevitch, N.; Sirotina, A.; Dobrov, B. Using BERT and Augmentation in Named Entity Recognition for Cybersecurity Domain. In Proceedings of the Natural Language Processing and Information Systems (NLDB 2020), Saarbrücken, Germany, 24–26 June 2020; Metais, E., Meziane, F., Horacek, H., Cimiano, P., Eds.; Lecture Notes in Computer Science. German Research Center for Artificial Intelligence: Kaiserslautern, Germany, 2020; Volume 12089, pp. 16–24. [CrossRef]
30. Ghanem, M.C.; Chen, T.M.; Nepomuceno, E.G. Hierarchical Reinforcement Learning for Efficient and Effective Automated Penetration Testing of Large Networks. *J. Intell. Inf. Syst.* **2023**, *60*, 281–303. [CrossRef]
31. Tikayat Ray, A.; Pinon Fischer, O.J.; Mavris, D.N.; White, R.T.; Cole, B.F. aeroBERT-NER: Named-Entity Recognition for Aerospace Requirements Engineering Using BERT. In Proceedings of the AIAA SCITECH 2023 Forum, National Harbor, MD, USA, 23–27 January 2023. AIAA Paper 2023-2583. [CrossRef]
32. Ye, Y.; Ji, S. Sparse Graph Attention Networks. *IEEE Trans. Knowl. Data Eng.* **2023**, *35*, 905–916. [CrossRef]
33. Chen, W.A.; He, H.Y.; Liu, J.G.; Yang, J.B.; Zhang, K.; Luo, D.S. Photovoltaic power prediction based on sliced bidirectional long short term memory and attention mechanism. *Front. Energy Res.* **2023**, *11*, 1123558. [CrossRef]
34. Yulita, I.N.; Fanany, M.I.; Arymurthy, A.M. Gesture Recognition using Latent-Dynamic based Conditional Random Fields and Scalar Features. *J. Phys. Conf. Ser.* **2017**, *812*, 012113. [CrossRef]
35. Ma, X.; Liu, Z.Z.; Zheng, M.X.; Wang, Y.Q. Application and exploration of self-attention mechanism in dynamic process monitoring. *IFAC PapersOnLine* **2022**, *55*, 139–144. [CrossRef]
36. He, J.C.; Li, L.; Xu, J.C. ReLU deep neural networks from the hierarchical basis perspective. *Comput. Math. Appl.* **2022**, *120*, 105–114. [CrossRef]
37. Hu, J.Y.; Yang, W.Q.; Yang, H.F.; Wei, S.M.; Sun, Z. Named Entity Recognition Method for Power Equipment Based on BERT-BiLSTM-CRF. In Proceedings of the 2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 12–15 September 2022; Fortino, G., Gravina, R., Guerrieri, A., Savaglio, C., Eds.; IEEE: Piscataway, NJ, USA, 2022; pp. 694–699. [CrossRef]
38. Zhong, M.S.; Liu, G.L.; Xiong, J.; Zuo, J.L. DualNER: A Trigger-Based Dual Learning Framework for Low-Resource Named Entity Recognition. *IEEE Intell. Syst.* **2022**, *37*, 79–87. [CrossRef]
39. Gim, J. A Study on the Performance Analysis of Entity Name Recognition Techniques Using Korean Patent Literature. *J. Adv. Inf. Technol. Converg.* **2020**, *10*, 139–151. [CrossRef]
40. Dasgupta, S.; Piplai, A.; Kotal, A.; Joshi, A. A Comparative Study of Deep Learning-based Named Entity Recognition Algorithms for Cybersecurity. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 2596–2604. [CrossRef]

41. Ma, P.C.; Jiang, B.; Lu, Z.G.; Li, N.; Jiang, Z.W. Cybersecurity Named Entity Recognition Using Bidirectional Long Short-Term Memory with Conditional Random Fields. *Tsinghua Sci. Technol.* **2021**, *26*, 259–265. [CrossRef]
42. Fang, Y.; Zhang, Y.; Huang, C. CyberEyes: Cybersecurity Entity Recognition Model Based on Graph Convolutional Network. *Comput. J.* **2021**, *64*, 1215–1225. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.