



# Pre-training by Predicting Program Dependencies for Vulnerability Analysis Tasks

Zhongxin Liu  
The State Key Laboratory of  
Blockchain and Data Security,  
Zhejiang University  
China  
liu\_zx@zju.edu.cn

Zhijie Tang  
Zhejiang University  
China  
tangzhijie@zju.edu.cn

Junwei Zhang  
Zhejiang University  
China  
jw.zhang@zju.edu.cn

Xin Xia\*  
Huawei  
China  
xin.xia@acm.org

Xiaohu Yang  
The State Key Laboratory of  
Blockchain and Data Security,  
Zhejiang University  
China  
yangxh@zju.edu.cn

## ABSTRACT

Vulnerability analysis is crucial for software security. Inspired by the success of pre-trained models on software engineering tasks, this work focuses on using pre-training techniques to enhance the understanding of vulnerable code and boost vulnerability analysis. The code understanding ability of a pre-trained model is highly related to its pre-training objectives. The semantic structure, e.g., control and data dependencies, of code is important for vulnerability analysis. However, existing pre-training objectives either ignore such structure or focus on learning to use it. The feasibility and benefits of learning the knowledge of analyzing semantic structure have not been investigated. To this end, this work proposes two novel pre-training objectives, namely Control Dependency Prediction (CDP) and Data Dependency Prediction (DDP), which aim to predict the statement-level control dependencies and token-level data dependencies, respectively, in a code snippet only based on its source code. During pre-training, CDP and DDP can guide the model to learn the knowledge required for analyzing fine-grained dependencies in code. After pre-training, the pre-trained model can boost the understanding of vulnerable code during fine-tuning and can directly be used to perform dependence analysis for both partial and complete functions. To demonstrate the benefits of our pre-training objectives, we pre-train a Transformer model named PDBERT with CDP and DDP, fine-tune it on three vulnerability analysis tasks, i.e., vulnerability detection, vulnerability classification, and vulnerability assessment, and also evaluate it on program

dependence analysis. Experimental results show that PDBERT benefits from CDP and DDP, leading to state-of-the-art performance on the three downstream tasks. Also, PDBERT achieves F1-scores of over 99% and 94% for predicting control and data dependencies, respectively, in partial and complete functions.

## CCS CONCEPTS

• **Software and its engineering** → *Language features*; • **Security and privacy** → **Vulnerability management**; • **Computing methodologies** → *Knowledge representation and reasoning*.

## KEYWORDS

Source Code Pre-training, Program Dependence Analysis, Vulnerability Detection, Vulnerability Classification, Vulnerability Assessment

## ACM Reference Format:

Zhongxin Liu, Zhijie Tang, Junwei Zhang, Xin Xia, and Xiaohu Yang. 2024. Pre-training by Predicting Program Dependencies for Vulnerability Analysis Tasks. In *2024 IEEE/ACM 46th International Conference on Software Engineering (ICSE '24)*, April 14–20, 2024, Lisbon, Portugal. ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/3597503.3639142>

## 1 INTRODUCTION

Software vulnerabilities are flaws or weaknesses that could be exploited to violate security policies [54]. It is crucial to detect, categorize and assess vulnerabilities. Due to the rapid increase in the number of software vulnerabilities and the success of deep learning techniques, researchers have proposed diverse deep-learning-based approaches to automate vulnerability analysis, such as vulnerability detection [14, 68], classification [8, 70], patch identification [66, 69] and assessment [37, 38], and achieved promising results.

Recently, inspired by the impressive effectiveness of pre-training large models in the natural language processing (NLP) field [10, 17, 50], researchers proposed to pre-train large models on large-scale code-related corpora for capturing the common knowledge of programming languages. We refer to such models as *pre-trained*

\*Corresponding author.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](https://permissions.acm.org).

ICSE '24, April 14–20, 2024, Lisbon, Portugal

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 979-8-4007-0217-4/24/04...\$15.00

<https://doi.org/10.1145/3597503.3639142>

*code models*. Pre-trained code models have shown consistent performance improvements over the neural models without being pre-trained (for short, *non-pre-trained models*) on various software engineering (SE) tasks, e.g., code search [20], code clone detection [26], and code completion [57]. Motivated by these studies, this work aims to boost vulnerability analysis using pre-training, with a focus on helping neural models better understand vulnerable code through pre-training techniques.

The code understanding ability of a pre-trained code model largely hinges on its pre-training objectives. Effective objectives can guide the model to learn the prior knowledge that is helpful for downstream tasks. Early pre-trained code models [20, 33] directly use the pre-training objectives designed for natural languages (NL), e.g., Masked Language Model (MLM) [17], ignoring the syntactic and semantic structure of code. Recently, some researchers [18, 62] specifically design several pre-training tasks, e.g., predicting Abstract Syntax Tree (AST) node types, to capture the syntactic structure of code.

The semantic structure of code, e.g., control and data dependencies [21], plays an important role in vulnerability analysis [12, 14, 68]. For example, to detect a use-after-free vulnerability, a model needs to identify whether the argument of a memory-releasing function call is used (which relies on data dependencies) in a statement that may be executed after this call (which is related to control dependencies). To the best of our knowledge, only two pre-trained code models, i.e., CODE-MVP and GraphCodeBERT, consider the semantic structure of code. CODE-MVP takes control flow graph (CFG) as input during pre-training. GraphCodeBERT takes as input data flow edges during pre-training and inference. On the other hand, prior studies have proposed some non-pre-trained models that consider semantic structure for vulnerability analysis [14, 44, 68]. These approaches first extract control and data dependencies, i.e., program dependencies, using static analysis tools, e.g., Joern [64], and then train a neural model to learn from the extracted dependencies. These pre-trained and non-pre-trained models have two main limitations. First, they require the input code to be correctly parsed to extract its semantic structure, and cannot handle partial code (e.g., incomplete functions). However, the ability to analyze partial code is useful and valuable for some real-world scenarios, e.g., detecting vulnerable code snippets shared on Stack Overflow [60]. Second, they target learning representation **from** the extracted semantic structure, or learning to use such structure. Considering that different downstream tasks can utilize the semantic structure in various ways, the generality of such representation can be limited.

To this end, this work introduces the idea of pre-training code models to incorporate the knowledge required for end-to-end program dependence analysis (i.e., from source code to program dependencies), and proposes two novel pre-training objectives, i.e., Control Dependency Prediction (CDP) and Data Dependency Prediction (DDP), to instantiate this idea. Specifically, CDP and DDP ask the model to predict all statement-level control dependencies and token-level data dependencies in a program relying solely on source code. Different from existing pre-training objectives, CDP and DDP target guiding the model to learn the representation that **encodes** the semantic structure of code **only based on source code**. However, it is not easy to train DDP. Because the number of token-level data dependencies is much lower than all possible

token pairs in code, i.e., DDP suffers from severe data imbalance. To address this problem, we leverage a masking strategy to filter impossible token pairs and enable DDP to function effectively.

To demonstrate the effectiveness of CDP and DDP, we pre-trained a Transformer model named PDBERT (**P**rogram **D**ependence **B**ERT) on 1.9M C/C++ functions using CDP and DDP as well as MLM. CDP and DDP bring several benefits to PDBERT: First, PDBERT only requires source code as input and is capable of handling the code snippets that cannot be correctly parsed, e.g., partial code. Second, PDBERT incorporates the knowledge of end-to-end program dependence analysis, which is more general than the knowledge of using program dependencies, and can better boost diverse downstream tasks. Third, PDBERT can be directly used to perform program dependence analysis for partial and complete code. Please note that existing static analysis tools, e.g., Joern [64], cannot correctly derive program dependencies in partial code without manual intervention. Thus, although program dependence analysis is only one of PDBERT's usage scenarios, PDBERT complements static analysis tools with the ability to analyze partial code.

We evaluate PDBERT in both intrinsic and extrinsic ways. For intrinsic evaluation, we directly apply PDBERT to analyze control and data dependencies for both partial and complete functions based only on their source code. Experimental results show that the F1-scores of PDBERT for identifying statement-level control dependencies and token-level data dependencies are over 99% and 95%, respectively, for partial functions, and over 99% and 94% for complete functions. These results indicate that PDBERT successfully learns the knowledge of program dependence and can effectively analyze both partial and complete functions. Moreover, the throughput of PDBERT is **23 times** higher than the state-of-the-art program dependence analysis tool Joern, indicating that PDBERT is more suitable for the use cases where some low levels of imprecision are tolerant and the throughput matters more. For extrinsic evaluation, we fine-tune and evaluate PDBERT on three vulnerability analysis tasks, i.e., vulnerability detection, vulnerability classification, and vulnerability assessment. PDBERT benefits from CDP and DDP and outperforms the best-performing baselines by 5.9%-9.0% on the three tasks.

In summary, the contributions of this work are as follows:

- We introduce the idea of pre-training code models to incorporate the knowledge required for end-to-end program dependence analysis, and propose two novel pre-training objectives, i.e., CDP and DDP, to instantiate this idea.
- We have built a pre-trained model named PDBERT with CDP, DDP and MLM, which to the best of our knowledge, is the first neural model that can analyze statement-level control dependencies and token-level data dependencies.
- We conduct both intrinsic and extrinsic evaluations, which show that PDBERT can accurately and efficiently identify program dependencies in both partial and complete functions, and can facilitate diverse vulnerability analysis tasks.

Our replication package is available at [2, 3].

## 2 PRELIMINARY

This section introduces Program Dependence Graph (PDG) and describes why handling partial code is useful.

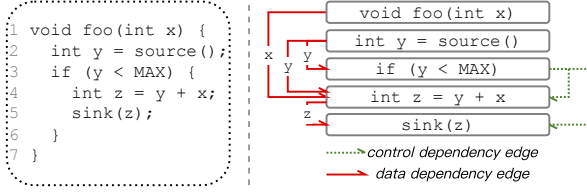


Figure 1: A sample function and its PDG.

## 2.1 Program Dependence Graph

Program dependencies, including control and data dependencies, reflect the semantic structure of code. Program dependence graph (PDG) [21] explicitly represents control and data dependencies with different types of edges and is frequently adopted by previous studies for vulnerability analysis [12, 14, 68]. Figure 1 represents a sample function and its PDG. In a PDG, each node denotes a statement or a predicate, and there are two types of edges: control dependency edges and data dependency edges. Control dependency edges (dotted green lines in Figure 1) present the control flow relationships between predicates and statements, and can be used to infer the control conditions on which a statement depends. Data dependency edges (solid red lines in Figure 1) present the def-use relationships, and each of them is labeled with a variable that is defined in the source node and used in the target node. By predicting control and data dependencies in programs, the model can learn to strengthen the connections between computationally related parts of a program and better capture the semantic structure of code.

## 2.2 Usage Scenario of Handling Partial Code

Compared to prior work, one advantage of PDBERT is that it can handle partial code, including performing program dependence analysis and downstream tasks on partial code. One usage scenario of this feature is analyzing the code snippets on Stack Overflow. Prior work [5, 6] has shown that novices and even more senior developers copy code snippets from Stack Overflow into production software. If the copied snippets are vulnerable, their production software will be prone to attacks. Specifically, Fischer et al. [22] observed that insecure code snippets from StackOverflow are copied into popular Android applications installed by millions of users. From 72K C++ code snippets used in at least one GitHub repository, Verdi et al. [60] found 99 vulnerable code snippets of 31 types, and these snippets had affected 2,859 GitHub projects. Considering these facts, it is essential and valuable to analyze the code snippets on Stack Overflow before they are scattered to other places. We argue that PDBERT can be used as a fundamental tool/model in this scenario.

## 3 APPROACH

This section first describes how PDBERT represents the input (§3.1) and how to construct ground truth for CDP and DDP (§3.2 and §3.3). Then, we elaborate on the three pre-training tasks used by PDBERT (§3.4) and the usages of PDBERT (§3.5).

### 3.1 Input Representation

PDBERT only requires source code as input. Given the source code  $C$  of a program, PDBERT first uses a subword-based tokenizer, e.g., a Byte-Pair Encoding (BPE) tokenizer [53], to tokenize it into a sequence of tokens and prepends this sequence with a special token [CLS]. The resulting token sequence, denoted as  $T = [t_{cls}, t_1, \dots, t_n]$ , is then fed into a multi-layer Transformer model to obtain the contextual embedding of each token. We denote these contextual embeddings as  $H^t = [h_{cls}^t, h_1^t, \dots, h_n^t]$ . For each token  $t_i$ , its char span is represented as  $S_{t_i} = [I_{t_i}^l, I_{t_i}^r]$  and recorded, where  $I_{t_i}^l$  and  $I_{t_i}^r$  denote the start and end character indices of  $t_i$  in the source code.

### 3.2 Program Dependency Extraction

To construct ground truth for CDP and DDP, we need to extract control and data dependencies in programs. Given a program, we first leverage a static analysis tool named Joern [64] to construct its PDG and AST based on its source code, and combine them into a joint graph. Then, we extract control and data dependencies from this graph.

**3.2.1 Control Dependency Extraction.** As described in Section 2.1, the control dependency edges in the PDG represent control dependencies. We encode them at the statement level into a matrix  $G^c \in \mathcal{R}^{m^c \times m^c}$ , where  $m^c$  denotes the maximum number of nodes in the PDG and is set to 50 by default.  $G_{i,j}^c \in \{1, 0\}$  denotes whether the  $j$ -th PDG node (statement) is control-dependent on the  $i$ -th PDG node (predicate).

**3.2.2 Data Dependency Extraction.** Similar to control dependencies, statement-level data dependencies can be extracted based on the data dependency edges in the PDG and encoded as a matrix. However, data dependencies are naturally defined on variables. Such matrix is coarse-grained, ignoring the information of variables. Therefore, we extract and encode data dependencies at a finer level to consider variable information and capture finer-grained code structure. Recall that each data dependency is represented by a data dependency edge associated with a variable  $var$  in the PDG. For the  $i$ -th data dependency edge  $D_i$ , we first identify the two AST nodes that correspond to the  $var$  defined in  $D_i$ 's source PDG node and the  $var$  used in  $D_i$ 's target PDG node from the joint graph. We refer to them as the *start node*  $s_i$  and the *end node*  $e_i$  of  $D_i$ , respectively. Then, we represent  $D_i$  as the combination of  $s_i$  and  $e_i$ , i.e.,  $D_i = [s_i, e_i]$ . Consequently, the data dependencies in the program are represented as  $\hat{G}^d = [D_1, D_2, \dots]$ .

### 3.3 Token-Level Data Dependency Construction

DDP aims to produce token-level data dependencies in the input program. In Section 3.2, data dependencies have been encoded as a set of AST node pairs  $\hat{G}^d$ . Each AST node corresponds to a code element. But each code element may be mapped into multiple tokens in  $T$  due to the subword-based tokenizer. Therefore, we need to refine  $\hat{G}^d$  to represent token-level data dependencies. As illustrated by Figure 2, we achieve this by converting  $\hat{G}^d$  into a matrix  $G^d$ , where  $G_{i,j}^d \in \{0, 1\}$  denotes whether the  $j$ -th token is data-dependent on the  $i$ -th token in  $T$ , as follows:

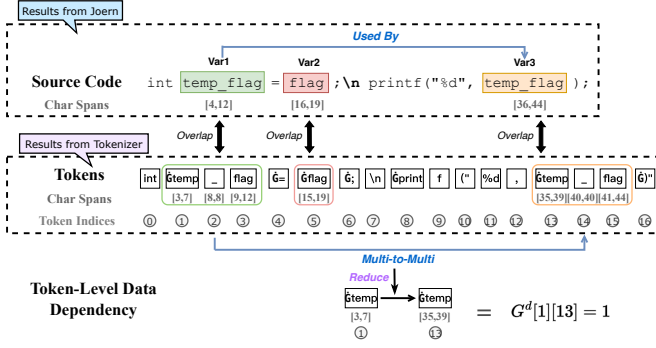


Figure 2: Constructing the ground truth  $G^d$  of DDG.

**Mapping AST nodes to tokens.** We retrieve the code element that corresponds to each AST node  $a_i$  in  $\hat{G}^d$ , and map the code element into its char span  $S_{a_i} = [I_{a_i}^l, I_{a_i}^r]$ , where  $I_{a_i}^l$  and  $I_{a_i}^r$  denote the indices of  $a_i$ 's start and end characters in the source code, respectively. For example, in Figure 2, the char span of the first `temp_flag` is [4,12]. Based on the char spans of  $a_i$  and the tokens in  $T$ , we map  $a_i$  into a subsequence of  $T$ , namely  $T_{a_i}$ . Specifically, we find the tokens in  $T$  of which the char spans are overlapped with  $a_i$ 's char span, and gather these tokens in order to construct  $T_{a_i} = [t_1^{a_i}, t_2^{a_i}, \dots]$ . For example, in Figure 2, each `temp_flag` is mapped to `[temp, _, flag]`, where `_` is used by the tokenizer to denote the space before a word. After this mapping, each data dependency edge  $D_i$  is represented as a pair of token sequences  $T_{s_i}$  and  $T_{e_i}$ , where  $s_i$  and  $e_i$  are the start and end nodes of  $D_i$ .

**Generating token edges.** Based on the new representations of data dependency edges, each token-level data dependency can be represented by the edges between the tokens in  $T_{s_i}$  and the tokens in  $T_{e_i}$ . Intuitively, we can connect the tokens in  $T_{s_i}$  to the tokens in  $T_{e_i}$  using the Cartesian production. However, this will produce plenty of edges and most of them are unnecessary. Therefore, for each data dependency edge  $D_i$ , we choose to connect only the first tokens in  $T_{s_i}$  and  $T_{e_i}$ , which effectively represents this data dependency and produces only one token-level edge, i.e.,  $t_1^{s_i} \rightarrow t_1^{e_i}$ . For example, in Figure 2, the first tokens of the two `temp_flag` are connected. After this step, each data dependency edge  $D_i$  is represented as a pair of tokens, e.g.,  $D_i = [t_1^{s_i}, t_1^{e_i}]$ .

**Constructing  $G^d$ .** We initialize  $G^d \in \mathcal{R}^{m^d \times m^d}$  as a matrix filled with zeros, where  $m^d$  is the max sequence length of the model. Each element in  $G^d$  represents the data dependency between two tokens in the code. For each data dependency edge  $D_i = [t_1^{s_i}, t_1^{e_i}]$ , we retrieve the token indices of  $t_1^{s_i}$  and  $t_1^{e_i}$  in  $T$ , assuming that they are  $x$  and  $y$ , and set  $G_{x,y}^d$  to 1. For the data dependency edge presented in Figure 2,  $x = 1, y = 13$ , so  $G_{1,13}^d$  is set to 1.  $G^d$  will be used as the ground truth of DDP.

### 3.4 Pre-training Tasks

PDBERT is pre-trained using three tasks: Masked Language Model (MLM), statement-level Control Dependency Prediction (CDP) and token-level Data Dependency Prediction (DDP), as shown in Figure 3. MLM is widely used by existing pre-trained models [20, 26,

46]. When used for programming languages (PL), it can guide the model to capture the naturalness and to some extent the syntactic structure of code [61]. CDP and DDP can help the model learn the knowledge about the semantic structure of code, strengthening the attention between computationally related code elements. The three tasks complement each other.

**3.4.1 Masked Language Model (MLM).** MLM requires the model to reconstruct randomly masked tokens from the corrupted input sequence. Before being encoded by the Transformer model, a certain proportion of tokens in  $T$  are sampled and replaced with a special token [MASK]. Based on the contextual embeddings  $H^t$  produced by the Transformer model, we use a two-layer MLP (Multi-Layer Perceptions) with the Softmax function to predict the original token of each [MASK], and calculate the loss of MLM, as follows:

$$P(t_i|h_i^t) = \text{Softmax}_{t_i \in V}(\text{MLP}(h_i^t)) \quad (1)$$

$$\mathcal{L}^{mlm} = \frac{1}{|M^t|} \sum_{i \in M^t} -\log P(t_i|h_i^t) \quad (2)$$

where  $V$  is the vocabulary of the model,  $\text{Softmax}_{t_i \in V}$  denotes the probability of producing  $t_i$ , and  $M^t$  are the indices of the sampled tokens. Following prior work [20, 26, 46], we sample 15% of tokens to mask. We also replace 10% of them with random tokens and unmask another 10% of them to alleviate the inconsistency between pre-training and fine-tuning.

**3.4.2 Statement-Level Control Dependency Prediction (CDP).** CDP aims to predict all the statement-level control dependencies in a program based on its source code. As described in Section 3.2.1, we encode the ground truth of CDP as a matrix  $G^c$ . To predict  $G^c$ , we encode each PDG node into a feature vector based on the contextual embeddings  $H^t$ , and predict whether there is a control dependency between each pair of PDG nodes based on their feature vectors. In detail, first, for each PDG node  $q_k$  we identify the tokens in  $T$  that belong to  $q_k$  and average the contextual embeddings of these tokens to obtain a vector  $\hat{h}_k^q$ . Next, we input  $\hat{h}_k^q$  into a one-layer MLP activated by the ReLU function for dimension reduction and obtain a vector  $h_k^q$ , as follows:

$$\hat{h}_k^q = \frac{1}{|q_k|} \sum_{t_i \in q_k} h_i^t \quad (3)$$

$$h_k^q = \text{ReLU}(\text{MLP}(\hat{h}_k^q)) \quad (4)$$

where  $|q_k|$  is the number of tokens belonging to  $q_k$ .  $h_k^q$  is regarded as the feature vector of  $q_k$ . Then, we use a bilinear layer, a commonly used module for relation predictions [55], to predict the probability  $P_{i,j}^c$  that a PDG node  $q_j$  is control-dependent on another PDG node  $q_i$ , as follows:

$$P_{i,j}^c = \sigma(h_i^{q_i \top} W_c h_j^q + b_c) \quad (5)$$

where  $W_c$  and  $b_c$  are trainable parameters and  $\sigma$  is the Sigmoid function. Because the inputs of the bilinear layer are not commutative, the predicted control dependencies between two PDG nodes are asymmetric, i.e.,  $P_{i,j}^c$  is not necessarily equal to  $P_{j,i}^c$ . This is in accord with the fact that control dependencies are directional. Finally, we calculate the cross entropy as the loss of CDP based on



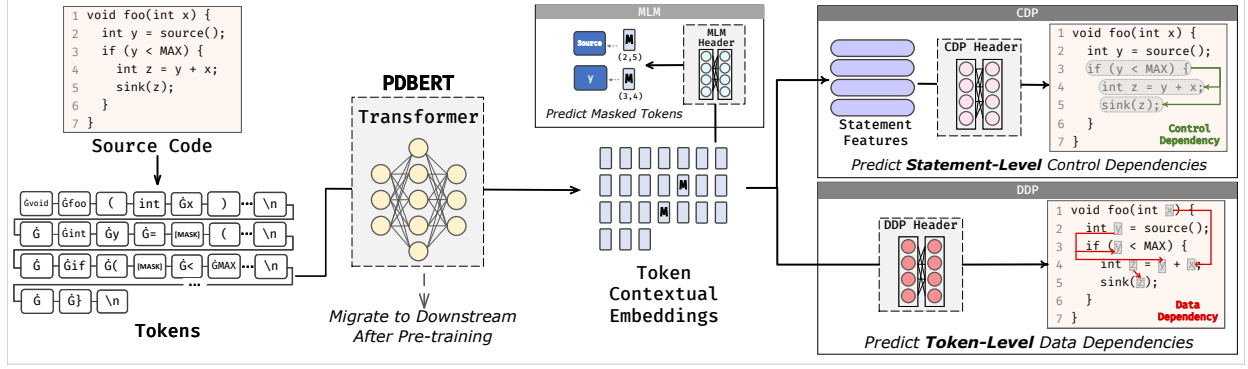


Figure 3: The pre-training tasks of PDBERT.

the predicted probabilities and the ground truth  $G^c$  of size  $|G^c|$ :

$$\mathcal{L}^{cdp} = \frac{1}{|G^c|} \sum_{i,j} -G_{i,j}^c \log P_{i,j}^c - (1 - G_{i,j}^c) \log (1 - P_{i,j}^c) \quad (6)$$

**3.4.3 Token-Level Data Dependency Prediction (DDP).** DDP targets predicting all the token-level data dependencies in a program only based on its source code. As described in Section 3.3, the ground truth of DDP is encoded as a matrix  $G^d$ . The contextual embeddings  $H^t$  are naturally the feature vectors of the tokens in  $T$ . To predict  $G^d$ , DDP also uses a one-layer MLP with the ReLU function for dimension reduction and a bilinear layer for prediction, as follows:

$$\hat{h}_i^t = \text{ReLU}(\text{MLP}(h_i^t)) \quad (7)$$

$$P_{i,j}^d = \sigma(\hat{h}_i^{t\top} W_d \hat{h}_j^t + b_d) \quad (8)$$

where  $W_d$  and  $b_d$  are trainable parameters. Nevertheless, compared to  $G^c$ ,  $G^d$  focuses on token-level relations and there are usually a large number of elements in  $G^d$ . For example, if the length of  $T$  is 512, the size of  $G^d$  would be over 262,144. Even worse, considering that the number of data dependencies is much lower than all possible token pairs in a program,  $G^d$  is usually highly sparse. If DDP directly predicts all elements in  $G^d$ , the model will mostly learn from the large proportion of zeros in  $G^d$  and constantly predict that there is no data dependency between two tokens.

To alleviate this problem, we propose a token-type-based masking strategy to mask the values associated with one or more non-Identifiers in  $G^d$ . Specifically, we first use a lexer to tokenize the input program  $C$  into a sequence of *code tokens*  $T' = [t'_1, t'_2, \dots, t'_{|T'|}]$  with their token types (e.g., Keyword and Identifier) labeled and char spans recorded. Note that  $T'$  is different from the token sequence  $T$  produced by the subword-based tokenizer, and each code token  $t'_i$  may be overlapped with multiple tokens in  $T$ . Next, for each code token  $t'_i$ , we identify its overlapping tokens in  $T$  based on their char spans and gather such tokens in order into a token sequence  $T_{t'_i}$ . The token type of  $t'_i$  is propagated to each token in  $T_{t'_i}$ . Then, we mask non-Identifier tokens in  $T$  and calculate the loss of DDP as follows:

$$\mathcal{L}^{ddp} = \frac{\sum_{i,j} m_i^d m_j^d [-G_{i,j}^d \log P_{i,j}^d - (1 - G_{i,j}^d) \log (1 - P_{i,j}^d)]}{(\sum_{k=1}^n m_k^d)^2} \quad (9)$$

$m_i^d \in \{0, 1\}$  indicates whether  $t_i$ 's token type is Identifier. This

formula means that the prediction loss of  $G_{i,j}^d$  will be masked if the token type of either  $t_i$  or  $t_j$  is not Identifier. It is also possible to introduce more and stronger priors to tackle this problem, e.g., only predicting data dependencies between identical identifiers. We only consider token types, which can help the model learn more knowledge related to program dependence analysis, e.g., the knowledge of recognizing identical identifiers.

Besides this masking strategy, another way to consider token types during pre-training is to explicitly provide identifier pairs to the model for prediction. However, during inference, this way requires additional tools to gather identifier pairs, while the masking strategy can be easily disabled to enable end-to-end program dependence analysis. Also, the masking strategy implicitly guides the model to focus on identifier pairs, which can help the model learn more syntactic knowledge of code.

### 3.5 The Usages of PDBERT

PDBERT takes as input only a code snippet, which can be either a partial or a complete function. Like existing pre-trained models [17, 20, 26], PDBERT outputs a sequence of contextual embeddings by itself. Such embeddings are converted to task output, such as a classification label or a token sequence, by a header (i.e., an output layer). During pre-training, different headers are connected to PDBERT for different pre-training tasks, as shown in Figure 3. After pre-training, we can simply connect PDBERT with the headers of CDP and DDP to infer the statement-level control dependencies and the token-level data dependencies in a code snippet. For a downstream task, a new header (usually an MLP) is connected to PDBERT and fine-tuned with PDBERT on a task-specific dataset. Each header is task-specific and is trained to contain the information about producing task output based on the contextual embeddings output by PDBERT. Such information is usually unhelpful for other tasks [15]. As the headers of MLM, CDP and DDP are task-specific and are not used for downstream tasks, we argue they have no side effects. Please note that PDBERT only takes as input the source code and does not require parsing the input program or constructing its PDG during fine-tuning. We hypothesize that the knowledge of program dependence has been learned and absorbed by PDBERT during pre-training, and such knowledge can boost the downstream tasks that are sensitive to program dependencies.

## 4 PRE-TRAINING SETUP

This section describes the dataset and the configurations used to pre-train our model.

### 4.1 Pre-training Dataset

In this work, we target C/C++ vulnerabilities. We use the dataset collected by Hanzi et al. [29] as our pre-training dataset. It contains over 2.28M C/C++ functions either extracted from the top 1060 C/C++ open-source projects on GitHub or gathered from the Draper dataset [52]. We shuffle these functions and partition them into the training, validation and test sets, referred to as  $PT_{train}$ ,  $PT_{val}$  and  $PT_{test}$ , respectively.  $PT_{val}$  is used for hyperparameter tuning during pre-training.  $PT_{test}$  is leveraged to evaluate PDBERT on program dependence analysis. To construct ground truth for CDP and DDP, we leverage Joern to build the AST and PDG of each function. Some functions in this dataset cannot be analyzed by Joern in a reasonable time, and are filtered by setting timeout to 30 minutes. In addition, we deduplicate  $PT_{valid}$  and  $PT_{test}$  and remove the functions in them that also appear in  $PT_{train}$ . Finally,  $PT_{train}$ ,  $PT_{val}$  and  $PT_{test}$  contain about 1.9M, 155.0K and 60.4K C/C++ functions, respectively.

### 4.2 Pre-training Model Configurations

Following CodeBERT [20], PDBERT uses a 12-layer Transformer with 768 dimensional hidden states and sets the max sequence length to 512. During pre-training and fine-tuning, we truncate the code snippets with more than 512 tokens or  $m^c$  statements to fit the model. CDP and DDP only consider the control and data dependencies within the tokens input to the model. We initialize PDBERT with the parameters of CodeBERT to accelerate the training process following GraphCodeBERT [26]. The pre-training objective of PDBERT is to jointly minimize the losses of the three pre-training tasks:

$$\mathcal{L} = a_1 \mathcal{L}^{ctrl} + a_2 \mathcal{L}^{data} + a_3 \mathcal{L}^{mlm} \quad (10)$$

where  $a_1$ ,  $a_2$  and  $a_3$  are the weights of the three losses. In our implementation, we set  $a_1 = 5$ ,  $a_2 = 20$  and  $a_3 = 1$  based on grid search on  $PT_{valid}$ . PDBERT is pre-trained on 4 Nvidia RTX 3090 GPUs for 10 epochs with batch size 128. We use the Adam optimizer [35] with an initial learning rate  $1e-4$  and apply the polynomial decay scheduler ( $p = 2$ ). It takes approximately 72 hours to finish pre-training.

## 5 EVALUATION

To demonstrate the effectiveness of PDBERT, we conduct both intrinsic and extrinsic evaluations. For intrinsic evaluation, we directly use PDBERT to perform program dependence analysis for both partial and complete functions. For extrinsic evaluation, we fine-tune and evaluate PDBERT on three function-level vulnerability analysis tasks, i.e., vulnerability detection, vulnerability classification, and vulnerability assessment. Please note that since some baselines cannot handle partial functions, the extrinsic evaluation is conducted on complete functions.

### 5.1 Intrinsic Evaluation

**5.1.1 Motivation.** To understand to what extent PDBERT has learned the knowledge of program dependence, we apply PDBERT to perform CDP and DDP without further training or fine-tuning.

**Table 1: Intrinsic evaluation results on partial code in terms of F1-score.**

Dependency	5	10	15	20	25	30
<b>Control</b>	98.99	99.29	99.30	99.25	99.23	99.21
<b>Data</b>	97.38	96.61	96.05	95.63	95.44	95.08
<b>Overall</b>	97.69	97.51	97.29	97.07	97.00	96.84

**Table 2: Intrinsic evaluation results on complete functions in terms of F1-score.**

Dependency	(0, 10]	(10, 20]	(20, 30]	(30, +∞]
<b>Control</b>	99.91	99.82	99.44	99.23
<b>Data</b>	97.59	96.35	95.28	94.31
<b>Overall</b>	98.07	97.56	96.93	96.46

\* (0, 10] denotes the subset where the LOC of each function is over 0 and no more than 10, and so forth.

**5.1.2 Experimental Setup.** We conduct the intrinsic evaluation on  $PT_{test}$ , which is **never** used during pre-training. PDBERT takes as input only a code snippet and predicts all the elements in its  $G^c$  and  $G^d$ . During evaluations, we do not assume that the types of code tokens are available and thus do not use the token-type-based masking strategy (cf. Section 3.4.3). F1-score is used as the evaluation metric, which is calculated by flattening and concatenating the predicted graphs of all test samples.

We first evaluate the feasibility of PDBERT in analyzing partial code, as this is a unique benefit of PDBERT. Specifically, we extract the first  $K$  consecutive statements of each function in  $PT_{test}$  to craft sub test sets.  $K$  is set to {5,10,15,20,25,30}. For each sub test set, a unique  $K$  is used and the functions with less than  $K$  statements are ignored. PDBERT takes as input each partial code snippet and predicts the program dependencies among its  $K$  statements. To further understand the knowledge learned by PDBERT, we also evaluate PDBERT's effectiveness in analyzing complete functions. Following CodeBERT, the max sequence length of PDBERT is set to 512. Thus we filter out the complete functions with over 512 tokens in  $PT_{test}$ , and over 83% of the functions in  $PT_{test}$  are kept. We partition the remaining functions into several non-overlapping subsets based on their Lines of Code (LOC) and apply PDBERT to them, aiming to show PDBERT's effectiveness across functions of varying lengths. Besides, to demonstrate the throughput of PDBERT, we measure the average time cost of PDBERT to perform CDP and DDP for a complete function and compare it with Joern, the state-of-the-art program dependence analysis tool. Specifically, PDBERT is deployed on one Nvidia RTX 3090 GPU to perform predictions with batch size 1. Joern is run on two Intel Xeon 6226R CPUs with 64 cores in total using the default configuration.

**5.1.3 Results.** Table 1 shows the evaluation results of PDBERT on partial code in terms of F1-score. The results presented in the "Overall" row are calculated on the combination of control and data dependencies. We can see that PDBERT performs very well on CDP, achieving F1-scores of about 99% for all  $K$ s. As for DDP, PDBERT achieves F1-scores of over 95%, which is also impressive. Note

that for each code snippet, DDP instances are highly imbalanced. Thus, DDP is more challenging than CDP. The overall F1-scores of PDBERT are over 96% for all Ks, indicating the feasibility and effectiveness of PDBERT in analyzing program dependencies for partial code. We also notice that the control, data and overall F1-scores of PDBERT slightly decrease as  $K$  increases. This trend is attributed to the increased difficulty in analyzing long code snippets compared to shorter ones. Please note that existing static analysis tools, e.g., Joern, lack the ability to automatically derive program dependencies in partial code, and thus are unsuitable for this scenario.

Table 2 presents the performance of PDBERT on complete functions, which closely aligns with that on partial code. Across all LOC ranges, PDBERT achieves control, data and overall F1-scores of over 99%, 94% and 96%, respectively, demonstrating the effectiveness and potential utility of PDBERT in performing program dependence analysis on complete functions. Similarly, there is a slight decrease in the control, data, and overall F1-scores as the LOC increases.

Regarding throughput, on average, Joern takes over 460ms to derive the PDG of a complete function, whereas PDBERT accomplishes the same task in just 19ms, making it 23 times faster than Joern. Please note that this comparison may not be entirely fair, as PDBERT is deployed on a GPU while Joern is run on two CPUs. The result only highlights the advantage of PDBERT in throughput and does not mean PDBERT can replace Joern in all use cases. Nevertheless, it implies that PDBERT is more suitable than Joern for the use cases where some low levels of imprecision are tolerant and high throughput matters more.

To conclude, PDBERT has learned the knowledge of program dependence and can accurately extract program dependencies for both partial and complete functions with high throughput.

## 5.2 Common Baselines and Variants for Extrinsic Evaluation

The extrinsic evaluation aims to investigate whether the pre-training of PDBERT is effective and can boost vulnerability analysis tasks. To this end, we compare PDBERT with the pre-trained code models using other pre-training objectives and non-pre-trained models. As a proof of concept, PDBERT is pre-trained based on an encoder-only Transformer model, because decoder-only models are sub-optimal for understanding tasks [17, 25] and encoder-decoder models require much more data and time to converge [7, 63]. For example, Ahmad et al. [7] spent 2,208 GPU hours and used 727 million functions/documents to pre-train PLBART. Following Ding et al. [18], to perform a fair comparison, we only consider encoder-only pre-trained models as baselines.

Specifically, for pre-trained code models, we use **CodeBERT** [20], **GraphCodeBERT** [26], **VulBERTa** [29] and **DISCO** [18] as baselines. CodeBERT is widely used in various software engineering tasks [30, 36, 66, 67], and PDBERT is initialized with the parameters of CodeBERT. GraphCodeBERT might be considered somewhat similar to our DDP task (cf. Section 7.1). Comparing PDBERT with GraphCodeBERT can help demonstrate the benefits of DDP and PDBERT. VulBERTa [29] is pre-trained by Hanzi et al. with their collected C/C++ functions (cf. Section 4.1) using MLM. DISCO is

**Table 3: The statistics of datasets.**

Dataset	#Func	#Vul	#Non-Vul	LOC		CC	
				Mean	Median	Mean	Median
<b>ReVeal</b>	22.6K	2.2K	20.4K	37.2	15	7.1	3
<b>Big-Vul</b>	188.6K	10.9K	177.7K	25.0	12	5.9	3
<b>Devign</b>	27.2K	12.4K	14.8K	51.8	26	11.2	5
<b>VC</b>	7.6K	7.6K	N/A	80.5	32	16.7	6
<b>VA</b>	9.9K	9.9K	N/A	79.1	32	16.3	6

\* #Func, #Vul and #Non-Vul refer to the numbers of all, vulnerable, and non-vulnerable functions. CC denotes cyclomatic complexity. VC and VA refer to the datasets used for vulnerability classification and vulnerability assessment, respectively.

the state-of-the-art encoder-only pre-trained code model, which uses MLM, node-type MLM (NT-MLM), and a contrastive learning objective for pre-training, and is also evaluated on vulnerability detection. Unfortunately, the pre-trained model of DISCO is not publicly available. Therefore, we can only compare PDBERT with DISCO on vulnerability detection based on the results reported in its paper [18]. There are also other encoder-only pre-trained code models, including CuBERT [33], ContraCode [31] and CODE-MVP [62]. But they are pre-trained only on Python or JavaScript programs and hence are not suitable for C/C++ programs. In addition, for most of them, the pre-trained models are not released.

For non-pre-trained models, we adopt a bidirectional LSTM (**Bi-LSTM**) [24] and a multi-layer **Transformer** model [59] as baselines. They are frequently used as encoders to handle sequential inputs. To eliminate the Out-of-Vocabulary (OoV) problem [34], their vocabularies and tokenizers are built using the BPE algorithm [53].

We build four variants of PDBERT, namely **MLM**, **MLM+CDP**, **MLM+DDP** and **MLM+CDP+DDP**. They are pre-trained using the same settings but with different pre-training objectives, as reflected by their names. Comparing their performance can help understand the contributions of different objectives to different tasks.

## 5.3 Vulnerability Detection

**5.3.1 Introduction.** Vulnerability detection is a fundamental problem in software security. Following prior work [14, 18], this task aims to predict whether a function is vulnerable or not, i.e., function-level vulnerability detection.

**5.3.2 Experimental Setup.** We evaluate PDBERT on three widely-used C/C++ function-level vulnerability detection datasets, i.e., ReVeal [14], Big-Vul [19] and Devign [68]. Their statistics are presented in Table 3.

**ReVeal** is released by the ReVeal paper [14], and is collected from Linux Debian Kernel and Chromium. This dataset is imbalanced and close to real-world scenarios. We randomly split 70%/10%/20% of the dataset for training, validation and testing, respectively, following prior work [14, 18]. Considering the data imbalance and following prior work [14, 18], we use F1-score as the evaluation metric.

**Big-Vul** is released by Fan et al. [19], and is collected from 348 Github projects. Considering the large scale of this dataset and following prior work [41], we randomly split it into training,

**Table 4: Evaluation results on vulnerability detection.**

Model	Dataset		
	ReVeal (F1-score)	Big-Vul (F1-score)	Devign (Accuracy)
Bi-LSTM	34.25	33.11	61.24
Transformer	40.91	34.90	60.51
VulDeePecker	29.03	13.07	45.68
Devign	26.43	13.77	52.27
SySeVR	33.73	24.80	48.87
ReVeal	32.24	23.93	54.55
CodeBERT	44.27	54.48	62.08
GraphCodeBERT	45.03	54.06	64.02
VulBERTa	44.19	36.75	62.88
DISCO <sup>†</sup>	46.4 <sup>*</sup>	-	63.8
<b>PDBERT</b>			
MLM	44.65	55.99	65.52
MLM+CDP	45.93	56.28	66.29
MLM+DDP	47.42	58.51	65.85
MLM+CDP+DDP	<b>48.38</b>	<b>59.41</b>	<b>67.61</b>

<sup>†</sup> The pre-trained model of DISCO is not publicly available. Its results are copied from the DISCO paper [18].

<sup>\*</sup> Since the ReVeal dataset does not provide official splits, the test set used by DISCO can be different from other approaches.

validation and testing sets by 80%/10%/10%. Since this dataset is highly imbalanced, we also use F1-score as the evaluation metric.

**Devign** is released by the Devign paper [68], containing 27.2K functions collected from FFmpeg and Qemu. This dataset is balanced and less realistic than ReVeal and Big-Vul. We use this dataset because it is included in the frequently used CodeXGLUE benchmark [47]. We also use the train/valid/test splits from CodeXGLUE. Following the design of CodeXGLUE and prior work [18], we use Accuracy as the evaluation metric.

For PDBERT and the common baselines introduced in Section 5.2, a new MLP is appended to each model to perform prediction. Apart from the common baselines, we also compare PDBERT with the state-of-the-art non-pre-trained models that are specially designed for vulnerability detection, including VulDeePecker [44], Devign [68], SySeVR [43], and ReVeal [14]. For Devign, its implementation is not released, so we use the implementation and settings provided by the authors of ReVeal [14]. For other baselines, we use their official implementation and settings to conduct experiments.

**5.3.3 Results.** Table 4 presents our evaluation results on this task. We can see that the pre-trained models outperform all the non-pre-trained models on the three datasets by substantial margins, confirming the effectiveness of pre-training. It is a little surprising that Bi-LSTM and Transformer perform better than the other non-pre-trained models. One possible reason is that they both use BPE tokenizers, which have been shown to be effective in modeling code by prior work [34, 58]. Ding et al. [18] also reported similar results. On the ReVeal, Big-Vul and Devign datasets, PDBERT improves the best-performing baselines, i.e., DISCO, CodeBERT, and GraphCodeBERT, by 4.3%, 9.0% and 5.6%, respectively, in F1-score or Accuracy. It is worth mentioning that among the baselines, the

best-performing baseline on one dataset usually does not perform best on another. Nevertheless, PDBERT consistently performs better than all the baselines.

For the variants of PDBERT, MLM+CDP+DDP outperforms MLM on the three datasets by substantial margins, highlighting the effectiveness of our pre-training objectives. MLM+CDP+DDP performs better than MLM+CDP and MLM+DDP, indicating that CDP and DDP are both helpful. In addition, MLM+DDP outperforms GraphCodeBERT, indicating the benefits of DDP.

In summary, PDBERT is more effective in vulnerability detection than the baselines on the three datasets. Both CDP and DDP contribute to PDBERT’s effectiveness.

## 5.4 Vulnerability Classification

**5.4.1 Introduction.** After a vulnerability is detected, it will usually be labeled with a category to help practitioners understand its root cause, impact and possible mitigation [70]. However, this labeling process requires experts to manually analyze the vulnerability. This task aims to automate this process by automatically classifying a vulnerable function based on its source code. Specifically, we focus on the Common Weakness Enumeration (CWE) categories, which are adopted by many well-known software vulnerability databases, such as NVD [1] and VulDB [4], for vulnerability classification. This task is a multi-class classification task.

**5.4.2 Experimental Setup.** We construct a dataset for this task based on the Big-Vul dataset [19]. Besides source code, the Big-Vul dataset also collects other vulnerability-related information, such as the CWE category and the Common Vulnerability Scoring System (CVSS) scores, for each vulnerable function. To construct our dataset, we remove all the non-vulnerable functions. We also filter out the vulnerable functions belonging to the CWE categories with less than 100 (about 1%) instances, to avoid the absence of some CWE categories after data splitting. The resulting dataset contains 7.6K vulnerable functions in 14 CWE categories. We randomly split 80%/10%/10% of this dataset for training/validation/testing.

Due to the long-tailed distribution of CWE categories, we use three metrics, i.e., Macro F1, Weighted F1 and the multi-class version of Matthews Correlation Coefficient (MCC) [23], for evaluation. These metrics are also used by other vulnerability-related studies [28, 38]. Macro F1 is the unweighted mean of the F1-scores of all categories, whereas Weighted F1 considers weighted mean. MCC measures the differences between actual values and predicted values. Note that MCC ranges from -1 to 1 and is not directly proportional to F1-score. A new MLP is used by PDBERT and each of the common baselines, respectively, as the classifier. To the best of our knowledge, existing approaches for CWE category prediction either are based on vulnerability descriptions or require inter-procedural analysis. Considering that this task only takes as input vulnerable functions, there is no suitable task-specific baseline.

**5.4.3 Results.** Table 5 presents the evaluation results on this task. We can see that the pre-trained models outperform all the non-pre-trained baselines, i.e., Bi-LSTM and Transformer, by large margins. For pre-trained models, VulBERTa achieves similar performance to CodeBERT. PDBERT improves CodeBERT in Macro F1, Weighted F1 and MCC by 11.7%, 9.1% and 12.2%, respectively. PDBERT also



**Table 5: Evaluation results on vulnerability classification.**

Model	Macro F1(%)	Weighted F1(%)	MCC
Bi-LSTM	26.48	39.45	0.3001
Transformer	35.35	46.34	0.3737
CodeBERT	51.91	57.37	0.5030
GraphCodeBERT	54.74	59.82	0.5331
VulBERTa	50.11	57.36	0.5035
<b>PDBERT</b>			
MLM	54.49	60.42	0.5372
MLM+CDP	56.51	59.93	0.5325
MLM+DDP	56.93	62.07	0.5614
MLM+CDP+DDP	<b>57.96</b>	<b>62.60</b>	<b>0.5644</b>

outperforms GraphCodeBERT in the three metrics by 5.9%, 4.6% and 5.9%, demonstrating its effectiveness in this task.

As for PDBERT’s variants, MLM+CDP+DDP outperforms MLM in all the metrics by substantial margins, highlighting that our pre-training objectives are effective. MLM+CDP+DDP improves MLM+CDP and MLM+DDP, which indicates that CDP and DDP are both beneficial. Also, MLM+DDP outperforms GraphCodeBERT by substantial margins, confirming the benefits of DDP.

In summary, PDBERT can boost vulnerability classification and both CDP and DDP are effective and beneficial for this task.

## 5.5 Vulnerability Assessment

**5.5.1 Introduction.** Vulnerability assessment is a process that determines various characteristics of vulnerabilities and helps practitioners prioritize the remediation of critical vulnerabilities [37, 38]. CVSS is a commonly used expert-based vulnerability assessment framework. It defines a series of metrics, i.e., CVSS metrics, to measure the severity of a vulnerability relative to other vulnerabilities. However, quantifying these metrics for a new vulnerability requires manual efforts of security experts and there is usually a delay in such manual process [38]. To this end, the vulnerability assessment task aims to automatically assess the CVSS metrics for vulnerabilities. In this work, we focus on function-level vulnerability assessment, which takes as input a vulnerable function and outputs the values of CVSS metrics for it. Specifically, this task targets four metrics that are important and could be inferred based on source code, including Availability, Confidentiality, Integrity, and Access Complexity.

**5.5.2 Experimental Setting.** We also construct a dataset for this task based on the Big-Vul dataset [19]. Specifically, we remove the vulnerable functions with invalid CVSS scores (e.g. “???”), resulting in a dataset with 9.9K vulnerable functions and their CVSS scores. We randomly split 80%/10%/10% of them for training/validation/test. We use the state-of-the-art vulnerability assessment approach named DeepCVA [38] as the task-specific baseline. DeepCVA uses Convolutional Neural Networks (CNN) to extract features from vulnerable code and predict multiple CVSS metrics in parallel through multi-task learning. To perform a fair comparison, we reuse

the official implementation of DeepCVA, and train and evaluate DeepCVA on our dataset. For each CVSS metric, we append a new MLP to PDBERT and each of the common baselines, respectively, as the classifier. Following DeepCVA, we use two evaluation metrics, i.e., Macro F1 and the multi-class version of MCC.

**5.5.3 Results.** Table 6 presents the evaluation results on the vulnerability assessment task. On average, the pre-trained models perform better or at least no worse than the best non-pre-trained model, i.e., DeepCVA, demonstrating the effectiveness of pre-training. Note that assessing CVSS metrics often requires more context and project-specific information, e.g., the system configuration required to exploit the vulnerability, than detecting or classifying vulnerabilities. Such information can hardly be found in the vulnerable function. Therefore, the performance improvements that can be achieved by improving code understanding are limited. Nevertheless, PDBERT outperforms the best-performing baseline, i.e., GraphCodeBERT, on each CVSS metric. On average, MLM+CDP+DDP improves GraphCodeBERT in Macro F1 and MCC by 2.8% and 3.3%. The performance improvements of the best-performing variant, i.e., MLM+CDP, over GraphCodeBERT in the two metrics are 3.2% and 6.0%, respectively. These results indicate that our pre-training technique is effective in assessing vulnerabilities.

For the variants of PDBERT, MLM+CDP+DDP outperforms MLM on all the CVSS metrics and on average, highlighting the contribution of our pre-training objectives. The performance of MLM+CDP and MLM+CDP+DDP is very close when assessing Availability, Integrity, and Confidentiality. However, MLM+CDP performs better than MLM+CDP+DDP on Access Complexity. One possible reason is that Access Complexity cares more about the conditions or privileges required to execute the vulnerable statements, which are highly related to control dependencies. This shows that for vulnerability assessment, DDP does not provide significant benefits. Besides, MLM+DDP still outperforms GraphCodeBERT, indicating the effectiveness of DDP.

In summary, PDBERT is effective in vulnerability assessment and CDP is more important than DDP for this task.

## 6 DISCUSSION

This section discusses the limitations of our approach and the threats to validity of this work.

### 6.1 Limitations

Due to the limitations of computation resources, following CodeBERT, we set the max sequence length of PDBERT as 512 in this work. Consequently, when used for program dependence analysis, PDBERT cannot properly analyze code snippets with over 512 tokens. However, as shown in Section 5.1.2, over 83% of C/C++ functions in the test set constructed from open-source projects adhere to this length limit. Based on our intrinsic evaluation, we argue that PDBERT is effective and efficient for analyzing most functions in practice. When applied to downstream tasks, PDBERT truncates long code snippets before processing them. Although this may negatively affect the performance, our extrinsic evaluation shows that PDBERT still effectively boosts downstream tasks. On the other hand, this limitation comes from the Transformer

**Table 6: Evaluation results on vulnerability assessment.**

Model	Access Complexity		Availability		Integrity		Confidentiality		Mean	
	Macro F1(%)	MCC	Macro F1(%)	MCC	Macro F1(%)	MCC	Macro F1(%)	MCC	Macro F1(%)	MCC
Bi-LSTM	59.20	0.4302	66.07	0.5423	72.26	0.5802	71.29	0.5589	67.21	0.5279
Transformer	47.33	0.3590	63.52	0.5115	71.33	0.5595	69.56	0.5256	62.93	0.4889
DeepCVA	73.06	0.6093	74.50	0.6579	75.64	0.6394	75.30	0.6290	74.63	0.6337
CodeBERT	69.69	0.6054	76.98	0.6908	77.59	0.6580	76.24	0.6368	75.13	0.6477
GraphCodeBERT	74.78	0.6484	77.21	0.6895	76.72	0.6490	75.94	0.6305	76.16	0.6544
VulBERTa	68.97	0.6062	75.11	0.6615	77.46	0.6621	75.36	0.6184	74.23	0.6371
<b>PDBERT</b>										
MLM	75.08	0.6639	75.64	0.6782	78.15	0.6731	77.46	0.6482	76.58	0.6658
MLM+CDP	<b>79.75</b>	<b>0.7300</b>	<b>78.31</b>	<b>0.6998</b>	78.85	0.6851	<u>77.48</u>	<b>0.6605</b>	<b>78.60</b>	<b>0.6939</b>
MLM+DDP	76.58	0.6655	77.97	<u>0.6993</u>	<u>79.37</u>	<b>0.6925</b>	77.26	0.6474	77.59	0.6724
MLM+CDP+DDP	<u>78.06</u>	<u>0.6682</u>	<u>78.15</u>	0.6965	<b>79.38</b>	<u>0.6884</u>	<b>77.52</b>	<u>0.6519</u>	<u>78.28</u>	<u>0.6763</u>

The best results are bold, and the second-best results are underlined.

architecture [59], not from our pre-training technique. It can be mitigated by simply increasing the max sequence length of PDBERT, which requires more computation resources and advanced hardware. Considering that our pre-training technique is orthogonal to the underlying model architecture, one can also adopt specialized model architectures for long code snippets, such as LongFormer [9] and LongCoder [27], to address this limitation. Since this work focuses on pre-training techniques, we choose the most widely used Transformer architecture, follow the settings of prior work [20, 26], and leave handling long code snippets as future work.

In addition, CDP focuses on statement-level control dependencies and does not handle the control flow within a single statement, e.g., ternary operators. Future work may improve CDP by considering such control flow.

## 6.2 Threats to Validity

**Generalization of PDBERT.** PDBERT is pre-trained on C/C++ programs and may not be suitable for other programming languages. However, our proposed pre-training objectives are language-agnostic. Practitioners can pre-train their models with CDP and DDP for other or even multiple programming languages.

**The limitations of using Joern.** To build ground truth for CDP and DDP, we use Joern to extract PDGs. Therefore, PDBERT is expected to predict the program dependencies analyzed by Joern, and may share the same limitations as Joern. However, Joern is the state-of-the-art source-code-based program dependence analysis tool. It is of high accuracy and has been widely used for vulnerability-related tasks [12, 14, 68]. In addition, our pre-training technique can be regarded as training the model to learn the program dependence analysis knowledge of Joern, which can still be beneficial (as shown by our extrinsic evaluation). Our intrinsic evaluation demonstrates the unique benefits of PDBERT in program dependence analysis and at least assesses how close PDBERT is to Joern in analyzing complete functions. Therefore, we argue that the limitations of Joern do not affect the conclusions of this work.

**Data Contamination.** It is possible that some functions in the pre-training dataset also appear in some fine-tuning datasets, as

they are all collected from open-source repositories. However, the pre-training dataset contains both vulnerable and benign functions, and the task-specific labels of each function are unknown during pre-training. In addition, prior work [10] has shown that data contamination may have little impact on the performance of pre-trained models. Therefore, we argue that this threat is limited.

## 7 RELATED WORK

### 7.1 Pre-Trained Code Models

Existing pre-trained code models can generally be divided into encoder-only [18, 20, 26, 31, 33, 62], decoder-only [40, 45, 57] and encoder-decoder models [7, 13, 25, 32, 42, 48, 49, 63, 65]. As a proof of concept, this work focuses on pre-training an encoder-only model for vulnerability analysis. For existing encoder-only pre-trained models, some of them [20, 33] directly adopt the pre-training tasks designed for NL. For example, CodeBERT [20] adopts MLM [17] and Replaced Token Detection (RTD) [16]. These models can capture the naturalness of code. Recently, some pre-training techniques [18, 62] are proposed to help models learn the syntactic structure of code. For example, DISCO [18] adopts a pre-training objective to predict the masked AST types in the input. Some prior work [11, 18, 31, 62] also leverages contrastive learning (CL) objectives to help models learn high-level functional similarities between programs. Different from them, our pre-trained objectives aim to help models learn to capture the semantic structure of code.

To the best of our knowledge, only two pre-trained code models, i.e., CODE-MVP [62] and GraphCodeBERT [26], consider the semantic structure of code (e.g., control- and data-flow information). CODE-MVP explicitly takes control flow graph (CFG) as input during pre-training and target learning representation **from** CFG. GraphCodeBERT is pre-trained by predicting a few masked data flow edges with other unmasked ones and a variable sequence as input. During inference, the variable sequence and all data flow edges of a program need to be extracted as input. This implies that GraphCodeBERT also targets learning representation **from** data flow, as mentioned in its paper [26]. Compared to them, first, PDBERT considers control and data dependencies simultaneously,

thus it can learn more comprehensive knowledge about program dependence. More importantly, PDBERT targets learning the representation that **encodes** the semantic structure of code and is designed to **“absorb” the knowledge required for end-to-end program dependence analysis**, which has not been investigated. As discussed in Section 1 and demonstrated in Section 5, this design brings several unique and significant benefits: (1) PDBERT only takes source code as input and can properly process “unparsable” code. (2) The knowledge learned by PDBERT is more general and can better boost downstream tasks. (3) PDBERT can directly be used to analyze statement-level control dependencies and token-level data dependencies, which to the best of our knowledge, cannot be achieved by existing neural models. Therefore, we believe PDBERT provides significant contributions compared to existing pre-trained code models.

## 7.2 Deep Learning for Vulnerability Analysis

Many deep-learning-based approaches have been proposed for vulnerability analysis [14, 38, 44, 68, 70]. For **vulnerability detection**, the state-of-the-art approaches first leverage static analysis tools, e.g., Joern, to extract PDGs, and represent programs in different forms, such as code gadgets [44], syntax-based, semantics-based, and vector representations [43], or graph-based representations [14, 41, 68], based on their PDGs. Then, they leverage different neural models, such as Bi-LSTM [44], CNN [43, 68], and GNN [14, 41, 68], to extract the feature vector of each input program for vulnerability detection. Compared to these approaches, PDBERT does not require program dependencies as input and can handle partial code, providing unique advantages. Also, these approaches are trained from scratch to learn how to use program dependencies on a specific task, while PDBERT is pre-trained to learn the knowledge of program dependence and can be easily applied to multiple vulnerability analysis tasks. For **vulnerability classification**, most existing studies focus on predicting CWE categories based on expert-curated vulnerability descriptions [8, 51].  $\mu$ VulDeePecker [70] is the only work that predicts CWE categories based on source code, but it uses inter-procedural analysis, while our work focuses on function-level vulnerabilities. For **vulnerability assessment**, most prior work predicts the CVSS metrics based on vulnerability descriptions instead of source code [39, 56]. DeepCVA [38] leverages CNN and multi-task learning for commit-level vulnerability assessment. Le et al. [36] proposed to predict the CVSS metrics based on vulnerable statements, which require significant manual efforts to identify or require vulnerability fixes to be known.

## 8 CONCLUSION AND FUTURE WORK

In this work, we propose two novel pre-training objectives, i.e., CDP and DDP, to help incorporate the knowledge of end-to-end program dependence analysis into neural models and boost vulnerability analysis. CDP and DDP aim to predict the statement-level control dependencies and the token-level data dependencies in a program only based on its source code. As a proof of concept, we build a pre-trained model named PDBERT with CDP and DDP, which achieves F1-scores of over 99% and 94% for predicting control and data dependencies, respectively, in partial and complete functions. We

also fine-tune and evaluate PDBERT on three vulnerability analysis tasks, i.e., vulnerability detection, vulnerability classification, and vulnerability assessment. Experimental results indicate PDBERT benefits from CDP and DDP and it is more effective than the state-of-the-art baselines on all these tasks.

In the future, we would like to investigate how to pre-train encoder-decoder models with CDP and DDP. We plan to investigate the effectiveness of PDBERT on more downstream tasks and pre-train PDBERT with a multilingual corpus. In addition, for the downstream tasks where static analyzers can successfully extract the program dependencies in the input code, it would be interesting to investigate whether combining our pre-training technique with explicitly provided program dependencies can further improve performance.

## ACKNOWLEDGMENTS

This research/project is supported by the National Natural Science Foundation of China (No. 62202420) and the Fundamental Research Funds for the Central Universities (No. 226-2022-00064). Zhongxin Liu gratefully acknowledges the support of Zhejiang University Education Foundation Qizhen Scholar Foundation.

## REFERENCES

- [1] 2023. National vulnerability database. <https://nvd.nist/>.
- [2] 2023. Our GitHub repository. <https://github.com/ZJU-CTAG/PDBERT>.
- [3] 2023. Our replication package. <https://doi.org/10.5281/zenodo.8196552>.
- [4] 2023. VulDB. <https://vuldb.com/?kb.sources>.
- [5] Rabe Abdalkareem, Emad Shihab, and Juergen Rilling. 2017. On code reuse from StackOverflow: An exploratory study on Android apps. *Inf. Softw. Technol.* 88 (2017), 148–158. <https://doi.org/10.1016/j.infsof.2017.04.005>
- [6] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. 2016. You Get Where You’re Looking for: The Impact of Information Sources on Code Security. In *Proceedings of the 2016 IEEE Symposium on Security and Privacy*. 289–305. <https://doi.org/10.1109/SP.2016.25>
- [7] Wasi Uddin Ahmad, Saikat Chakraborty, Baishakhi Ray, and Kai-Wei Chang. 2021. Unified Pre-training for Program Understanding and Generation. In *Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*. 2655–2668.
- [8] Masaki Aota, Hideaki Kanehara, Masaki Kubo, Noboru Murata, Bo Sun, and Takeshi Takahashi. 2020. Automation of Vulnerability Classification from Its Description Using Machine Learning. In *Proceedings of the 2020 IEEE Symposium on Computers and Communications*. 1–7.
- [9] Iz Beltagy, Matthew E. Peters, and Arman Cohan. 2020. Longformer: The Long-Document Transformer. *CoRR abs/2004.05150* (2020). arXiv:2004.05150 <https://arxiv.org/abs/2004.05150>
- [10] Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel M. Ziegler, Jeffrey Wu, Clemens Winter, Christopher Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. 2020. Language Models Are Few-Shot Learners. In *Advances in Neural Information Processing Systems 33: Annual Conference on Neural Information Processing Systems 2020, NeurIPS 2020*.
- [11] Nghi DQ Bui, Yijun Yu, and Lingxiao Jiang. 2021. Self-Supervised Contrastive Learning for Code Retrieval and Summarization via Semantic-Preserving Transformations. In *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*. 511–521.
- [12] Sicong Cao, Xiaobing Sun, Lili Bo, Rongxin Wu, Bin Li, and Chuanqi Tao. 2022. MVD: Memory-Related Vulnerability Detection Based on Flow-Sensitive Graph Neural Networks. In *Proceedings of the 44th IEEE/ACM International Conference on Software Engineering*. 1456–1468.
- [13] Saikat Chakraborty, Toufique Ahmed, Yangruibo Ding, Premkumar T. Devanbu, and Baishakhi Ray. 2022. NatGen: Generative Pre-Training by “Naturalizing” Source Code. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 18–30.
- [14] Saikat Chakraborty, Rahul Krishna, Yangruibo Ding, and Baishakhi Ray. 2022. Deep Learning Based Vulnerability Detection: Are We There Yet? *IEEE Trans. Software Eng.* 48, 9 (2022), 3280–3296.

- [15] Ting Chen, Simon Kornblith, Mohammad Norouzi, and Geoffrey Hinton. 2020. A simple framework for contrastive learning of visual representations. In *Proceedings of the 37th International Conference on Machine Learning*. PMLR, 1597–1607.
- [16] Kevin Clark, Minh-Thang Luong, Quoc V. Le, and Christopher D. Manning. 2020. ELECTRA: Pre-training Text Encoders as Discriminators Rather Than Generators. In *Proceedings of the 8th International Conference on Learning Representations*.
- [17] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*. 4171–4186.
- [18] Yangruibo Ding, Luca Buratti, Saurabh Pujar, Alessandro Morari, Baishakhi Ray, and Saikat Chakraborty. 2022. Towards Learning (Dis)-Similarity of Source Code from Program Contrasts. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. 6300–6312.
- [19] Jiahao Fan, Yi Li, Shaohua Wang, and Tien N. Nguyen. 2020. A C/C++ Code Vulnerability Dataset with Code Changes and CVE Summaries. In *Proceedings of the 17th International Conference on Mining Software Repositories*. 508–512.
- [20] Zhangyin Feng, Daya Guo, Duyu Tang, Nan Duan, Xiaocheng Feng, Ming Gong, Linjun Shou, Bing Qin, Ting Liu, Daxin Jiang, and Ming Zhou. 2020. CodeBERT: A Pre-Trained Model for Programming and Natural Languages. In *Findings of the Association for Computational Linguistics: EMNLP 2020 (Findings of ACL, Vol. EMNLP 2020)*. 1536–1547.
- [21] Jeanne Ferrante, Karl J. Ottenstein, and Joe D. Warren. 1987. The Program Dependence Graph and Its Use in Optimization. *ACM Transactions on Programming Languages and Systems* 9, 3 (1987), 319–349.
- [22] Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Colin B. Backes, and Sascha Fahl. 2017. Stack overflow considered harmful? the impact of copy&paste on android application security. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)*. 121–136.
- [23] Jan Gorodkin. 2004. Comparing Two K-category Assignments by a K-category Correlation Coefficient. *Computational biology and chemistry* 28, 5–6 (2004), 367–374.
- [24] Alex Graves, Abdel-rahman Mohamed, and Geoffrey E. Hinton. 2013. Speech recognition with deep recurrent neural networks. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*. 6645–6649.
- [25] Daya Guo, Shuai Lu, Nan Duan, Yanlin Wang, Ming Zhou, and Jian Yin. 2022. UniXcoder: Unified Cross-Modal Pre-training for Code Representation. In *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. 7212–7225.
- [26] Daya Guo, Shuo Ren, Shuai Lu, Zhangyin Feng, Duyu Tang, Shujie Liu, Long Zhou, Nan Duan, Alexey Svyatkovskiy, Shengyu Fu, Michele Tufano, Shao Kun Deng, Colin B. Clement, Dawn Drain, Neel Sundaresan, Jian Yin, Daxin Jiang, and Ming Zhou. 2021. GraphCodeBERT: Pre-training Code Representations with Data Flow. In *Proceedings of the 9th International Conference on Learning Representations*.
- [27] Daya Guo, Canwen Xu, Nan Duan, Jian Yin, and Julian J. McAuley. 2023. Long-Coder: A Long-Range Pre-trained Language Model for Code Completion. In *International Conference on Machine Learning, ICML 2023 (Proceedings of Machine Learning Research, Vol. 202)*. PMLR, 12098–12107. <https://proceedings.mlr.press/v202/guo23j.html>
- [28] Zhuobing Han, Xiaohong Li, Zhenchang Xing, Hongtao Liu, and Zhiyong Feng. 2017. Learning to Predict Severity of Software Vulnerability Using Only Vulnerability Description. In *Proceedings of the 2017 IEEE International Conference on Software Maintenance and Evolution*. 125–136.
- [29] Hazim Hanif and Sergio Maffei. 2022. VulBERTa: Simplified Source Code Pre-Training for Vulnerability Detection. In *Proceedings of the 2022 International Joint Conference on Neural Networks*. 1–8.
- [30] Qing Huang, Zhiqiang Yuan, Zhenchang Xing, Xiwei Xu, Liming Zhu, and Qinghua Lu. 2022. Prompt-tuned code language model as a neural knowledge base for type inference in statically-typed partial code. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*. 1–13.
- [31] Paras Jain, Ajay Jain, Tianjun Zhang, Pieter Abbeel, Joseph Gonzalez, and Ion Stoica. 2021. Contrastive Code Representation Learning. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*. 5954–5971.
- [32] Xue Jiang, Zhuoran Zheng, Chen Lyu, Liang Li, and Lei Lyu. 2021. Treebert: A Tree-Based Pre-Trained Model for Programming Language. In *Uncertainty in Artificial Intelligence*. 54–63.
- [33] Aditya Kanade, Petros Maniatis, Gogul Balakrishnan, and Kensen Shi. 2020. Learning and Evaluating Contextual Embedding of Source Code. In *International Conference on Machine Learning*. 5110–5121.
- [34] Rafael-Michael Karampatzis, Hlib Babii, Romain Robbes, Charles Sutton, and Andrea Janes. 2020. Big code != big vocabulary: open-vocabulary models for source code. In *Proceedings of the 42nd International Conference on Software Engineering*. 1073–1085.
- [35] Diederik P. Kingma and Jimmy Ba. 2015. Adam: A Method for Stochastic Optimization. In *Proceedings of the 3rd International Conference on Learning Representations, Yoshua Bengio and Yann LeCun (Eds.)*.
- [36] Triet Huynh Minh Le and M. Ali Babar. 2022. On the Use of Fine-Grained Vulnerable Code Statements for Software Vulnerability Assessment Models. In *Proceedings of the 19th International Conference on Mining Software Repositories*. 621–633.
- [37] Triet Huynh Minh Le, Huaming Chen, and Muhammad Ali Babar. 2023. A Survey on Data-driven Software Vulnerability Assessment and Prioritization. *ACM Comput. Surv.* 55, 5 (2023), 100:1–100:39.
- [38] Triet Huynh Minh Le, David Hin, Roland Croft, and Muhammad Ali Babar. 2021. DeepCVA: Automated Commit-level Vulnerability Assessment with Deep Multi-task Learning. In *Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering*. 717–729.
- [39] Triet Huynh Minh Le, Bushra Sabir, and Muhammad Ali Babar. 2019. Automated Software Vulnerability Assessment with Concept Drift. In *Proceedings of the 2019 IEEE/ACM 16th International Conference on Mining Software Repositories*. 371–382.
- [40] Yujia Li, David Choi, Junyoung Chung, Nate Kushman, Julian Schrittwieser, Rémi Leblond, Tom Eccles, James Keeling, Felix Gimeno, Agustin Dal Lago, et al. 2022. Competition-level code generation with alphacode. *Science* 378, 6624 (2022), 1092–1097.
- [41] Yi Li, Shaohua Wang, and Tien N. Nguyen. 2021. Vulnerability detection with fine-grained interpretations. In *Proceedings of the 29th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 292–303.
- [42] Zhiyu Li, Shuai Lu, Daya Guo, Nan Duan, Shailesh Jannu, Grant Jenks, Deep Majumder, Jared Green, Alexey Svyatkovskiy, and Shengyu Fu. 2022. Automating Code Review Activities by Large-Scale Pre-Training. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 1035–1047.
- [43] Zhen Li, Deqing Zou, Shouhuai Xu, Hai Jin, Yawei Zhu, and Zhaoxuan Chen. 2021. SySeVR: A Framework for Using Deep Learning to Detect Software Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing* 19, 4 (2021), 2244–2258.
- [44] Zhen Li, Deqing Zou, Shouhuai Xu, Xinyu Ou, Hai Jin, Sujuan Wang, Zhijun Deng, and Yuyi Zhong. 2018. VulDeePecker: A Deep Learning-Based System for Vulnerability Detection. In *Proceedings of the 25th Annual Network and Distributed System Security Symposium*.
- [45] Fang Liu, Ge Li, Yunfei Zhao, and Zhi Jin. 2020. Multi-Task Learning Based Pre-Trained Language Model for Code Completion. In *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*. 473–485.
- [46] Yinhan Liu, Mylène Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. 2019. RoBERTa: A Robustly Optimized BERT Pretraining Approach. *CoRR abs/1907.11692* (2019), arXiv:1907.11692.
- [47] Shuai Lu, Daya Guo, Shuo Ren, Junjie Huang, Alexey Svyatkovskiy, Ambrosio Blanco, Colin B. Clement, Dawn Drain, Daxin Jiang, Duyu Tang, Ge Li, Lidong Zhou, Linjun Shou, Long Zhou, Michele Tufano, Ming Gong, Ming Zhou, Nan Duan, Neel Sundaresan, Shao Kun Deng, Shengyu Fu, and Shujie Liu. 2021. CodeXGLUE: A Machine Learning Benchmark Dataset for Code Understanding and Generation. In *Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks 1, NeurIPS Datasets and Benchmarks 2021*.
- [48] Antonio Mastropaolo, Simone Scalabrino, Nathan Cooper, David Nader Palacio, Denys Poshyvanyk, Rocco Oliveto, and Gabriele Bavota. 2021. Studying the Usage of Text-to-Text Transfer Transformer to Support Code-Related Tasks. In *Proceedings of the 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*. 336–347.
- [49] Changan Niu, Chuanyu Li, Vincent Ng, Jidong Ge, Liguang Huang, and Bin Luo. 2022. SPT-Code: Sequence-to-Sequence Pre-Training for Learning Source Code Representations. In *Proceedings of the 44th IEEE/ACM 44th International Conference on Software Engineering*. 1–13.
- [50] Colin Raffel, Noam Shazeer, Adam Roberts, Katherine Lee, Sharan Narang, Michael Matena, Yanqi Zhou, Wei Li, and Peter J. Liu. 2020. Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer. *J. Mach. Learn. Res.* 21, 140 (2020), 1–67.
- [51] Jukka Ruohonen and Ville Leppänen. 2018. Toward Validation of Textual Information Retrieval Techniques for Software Weaknesses. In *Database and Expert Systems Applications - DEXA 2018 International Workshops, BDMICS, BLOKDD, and TIR (Communications in Computer and Information Science, Vol. 903)*. 265–277.
- [52] Rebecca L. Russell, Louis Y. Kim, Lei H. Hamilton, Tomo Lazovich, Jacob Harer, Onur Ozdemir, Paul M. Ellingwood, and Marc W. McConley. 2018. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. In *Proceedings of the 17th IEEE International Conference on Machine Learning and Applications*. 757–762. <https://doi.org/10.1109/ICMLA.2018.00120>
- [53] Rico Sennrich, Barry Haddow, and Alexandra Birch. 2016. Neural Machine Translation of Rare Words with Subword Units. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics Volume 1: Long Papers*.
- [54] Robert Shirey. 2000. *Internet security glossary*. Technical Report.
- [55] Richard Socher, Danqi Chen, Christopher D. Manning, and Andrew Y. Ng. 2013. Reasoning With Neural Tensor Networks for Knowledge Base Completion. In *Advances in Neural Information Processing Systems 26: 27th Annual Conference on Neural Information Processing Systems 2013*. 926–934.

- [56] Georgios Spanos and Lefteris Angelis. 2018. A Multi-Target Approach to Estimate Software Vulnerability Characteristics and Severity Scores. *Journal of Systems and Software* 146 (2018), 152–166.
- [57] Alexey Svyatkovskiy, Shao Kun Deng, Shengyu Fu, and Neel Sundaresan. 2020. Intellicode Compose: Code Generation Using Transformer. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 1433–1443.
- [58] Patanamon Thongtanunam, Chanathip Pornprasit, and Chakkrit Tantithamthavorn. 2022. AutoTransform: automated code transformation to support modern code review process. In *Proceedings of the 44th International Conference on Software Engineering*. 237–248.
- [59] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, and Illia Polosukhin. 2017. Attention is All you Need. In *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017*. 5998–6008.
- [60] Morteza Verdi, Ashkan Sami, Jafar Akhondali, Foutse Khomh, Gias Uddin, and Alireza Karami Motlagh. 2020. An empirical study of c++ vulnerabilities in crowd-sourced code examples. *IEEE Transactions on Software Engineering* 48, 5 (2020), 1497–1514.
- [61] Yao Wan, Wei Zhao, Hongyu Zhang, Yulei Sui, Guandong Xu, and Hai Jin. 2022. What do they capture? a structural analysis of pre-trained language models for source code. In *Proceedings of the 44th International Conference on Software Engineering*. 2377–2388.
- [62] Xin Wang, Yasheng Wang, Yao Wan, Jiawei Wang, Pingyi Zhou, Li Li, Hao Wu, and Jin Liu. 2022. CODE-MVP: Learning to Represent Source Code from Multiple Views with Contrastive Pre-Training. In *Findings of the Association for Computational Linguistics: NAACL 2022*. 1066–1077.
- [63] Yue Wang, Weishi Wang, Shafiq R. Joty, and Steven C. H. Hoi. 2021. CodeT5: Identifier-aware Unified Pre-trained Encoder-Decoder Models for Code Understanding and Generation. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*. 8696–8708.
- [64] Fabian Yamaguchi, Nico Golde, Daniel Arp, and Konrad Rieck. 2014. Modeling and Discovering Vulnerabilities with Code Property Graphs. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. 590–604.
- [65] Jiyang Zhang, Sheena Panthaplackel, Pengyu Nie, Junyi Jessy Li, and Milos Gligoric. 2022. Codit5: Pretraining for Source Code and Natural Language Editing. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*. 1–12.
- [66] Jiayuan Zhou, Michael Pacheco, Zhiyuan Wan, Xin Xia, David Lo, Yuan Wang, and Ahmed E. Hassan. 2021. Finding a Needle in a Haystack: Automated Mining of Silent Vulnerability Fixes. In *Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering*. 705–716.
- [67] Xin Zhou, DongGyun Han, and David Lo. 2021. Assessing generalizability of codebert. In *Proceedings of the 2021 IEEE International Conference on Software Maintenance and Evolution*. IEEE, 425–436.
- [68] Yaqin Zhou, Shangqing Liu, Jing Kai Siow, Xiaoning Du, and Yang Liu. 2019. Devign: Effective Vulnerability Identification by Learning Comprehensive Program Semantics via Graph Neural Networks. In *Advances in Neural Information Processing Systems 32: Annual Conference on Neural Information Processing Systems 2019*. 10197–10207.
- [69] Yaqin Zhou, Jing Kai Siow, Chenyu Wang, Shangqing Liu, and Yang Liu. 2021. Spi: Automated Identification of Security Patches via Commits. *ACM Transactions on Software Engineering and Methodology (TOSEM)* 31, 1 (2021), 1–27.
- [70] Deqing Zou, Sujuan Wang, Shouhuai Xu, Zhen Li, and Hai Jin. 2019.  $\mu$ VulDeePecker: A Deep Learning-Based System for Multiclass Vulnerability Detection. *IEEE Transactions on Dependable and Secure Computing* 18, 5 (2019), 2224–2236.