ParaVul: A Parallel Large Language Model and Retrieval-Augmented Framework for Smart Contract Vulnerability Detection

Tenghui Huang, Jinbo Wen, Jiawen Kang, Senior Member, IEEE, Siyong Chen, Zhengtao Li, Tao Zhang, Dongning Liu, Senior Member, IEEE, Jiacheng Wang, Chengjun Cai, Yinqiu Liu, and Dusit Niyato, Fellow, IEEE

Abstract—Smart contracts play a significant role in automating blockchain services. Nevertheless, vulnerabilities in smart contracts pose serious threats to blockchain security. Currently, traditional detection methods primarily rely on static analysis and formal verification, which can result in high false-positive rates and poor scalability. Large Language Models (LLMs) have recently made significant progress in smart contract vulnerability detection. However, they still face challenges such as high inference costs and substantial computational overhead. In this paper, we propose ParaVul, a parallel LLM and retrieval-augmented framework to improve the reliability and accuracy of smart contract vulnerability detection. Specifically, we first develop Sparse Low-Rank Adaptation (SLoRA) for LLM fine-tuning. SLoRA introduces sparsification by incorporating a sparse matrix into quantized LoRA-based LLMs, thereby reducing computational overhead and resource requirements while enhancing their ability to understand vulnerability-related issues. We then construct a vulnerability contract dataset and develop a hybrid Retrieval-Augmented Generation (RAG) system that integrates dense retrieval with Best Matching 25 (BM25), assisting in verifying the results generated by the LLM. Furthermore, we propose a meta-learning model to fuse the outputs of the RAG system and the LLM, thereby generating the final detection results. After completing vulnerability detection, we design chain-of-thought prompts to guide LLMs to generate comprehensive vulnerability detection reports. Simulation results demonstrate the superiority of ParaVul, especially in terms of F1 scores, achieving 0.9398 for single-label detection and 0.9330 for multi-label detection.

Index Terms—Smart contract, vulnerability detection, LLMs, SLoRA, hybrid RAG, BM25, meta-learning models.

I. Introduction

- T. Huang, J. Kang, S. Chen, and Z. Li are with the School of Automation, Guangdong University of Technology, Guangzhou 510006, China (e-mails: 3123000938@mail2.gdut.edu.cn, kavinkang@gdut.edu.cn, 3122000875@mail2.gdut.edu.cn, 3123000988@mail2.gdut.edu.cn).
- J. Wen is with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: jinbo1608@nuaa.edu.cn).
- T. Zhang is with the School of Cyberspace Science and Technology, Beijing Jiaotong University, Beijing 100044, China (e-mail: taozh@bjtu.edu.cn).
- D. Liu is with the School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China (e-mail: li-udn@gdut.edu.cn).
- J. Wang, Y. Liu, and D. Niyato are with the College of Computing and Data Science, Nanyang Technological University, Singapore (e-mails: jiacheng.wang@ntu.edu.sg, yinqiu001@ntu.edu.sg, dniyato@ntu.edu.sg).
- C. Cai is with the Department of Computer Science, City University of Hong Kong, Hong Kong (e-mail: chengjun.cai@cityu-dg.edu.cn).

Corresponding author: Jiawen Kang.

which the advancement of distributed ledger technologies such as blockchain [1], [2] and Web 3.0 [3], [4], smart contracts have become an indispensable foundation for decentralized finance ecosystems [5]. They can automatically execute and verify transactions based on predefined conditions, significantly enhancing transaction efficiency. However, once deployed on blockchains, the immutable nature of smart contracts can expose potential vulnerabilities to malicious exploitation, leading to significant security risks and economic losses [6]. Notably, high-profile security incidents, such as the decentralized autonomous organization attack [7], underscore the severe consequences of these vulnerabilities, which have attracted attention from academia and industry [8]. Therefore, smart contract vulnerability detection is crucial for the security of the blockchain ecosystem [9].

Traditional methods for smart contract vulnerability detection typically depend on static analysis, dynamic detection, and formal verification [8], [9]. Although these methods are capable of detecting certain contract security issues, they still face several critical limitations, including low efficiency, inability to meet real-time analysis demands for large-scale contracts, limited generalization and adaptability to emerging vulnerability types, and insufficient understanding of complex contract logic [8], [10]. These limitations can result in high false-positive rates [9]. As smart contract applications become more complicated, the limitations of traditional methods in addressing new vulnerabilities become more obvious [9].

Recent advances in Large Language Models (LLMs) [11], [12] and Retrieval-Augmented Generation (RAG) technologies in natural language processing offer new approaches for smart contract vulnerability detection [12]-[14]. On the one hand, LLMs are capable of directly understanding and analyzing smart contracts to identify semantic security vulnerabilities. The prominent advantages of LLMs in smart contract vulnerability detection lie in their ability to understand complex contract logic, adapt to new types of vulnerabilities, and generate explanations and repair suggestions, significantly enhancing both the intelligence and practicality of detection. On the other hand, RAG retrieves similar cases from the vulnerability knowledge base to enhance the identification capability of LLMs. The applications of LLMs in smart contract vulnerability detection have attracted increasing attention. For instance, the authors in [15] combined LLMs with controlflow graph analysis to enhance detection accuracy. Similarly, RAG technology has also been applied to smart contract vulnerability detection. For instance, the authors in [14] integrated a vector database of vulnerable contracts with LLMs to enhance detection. However, existing studies still suffer from several limitations, including high computational cost, reliance on high-quality datasets, and considerable false-positive rates. Moreover, directly applying these technologies to smart contract vulnerability detection remains challenging due to insufficient code semantic understanding, high resource consumption, and poor generalization.

To this end, in this paper, we propose ParaVul, a parallel LLM and retrieval-augmented framework for smart contract vulnerability detection. In this framework, we first develop Sparse Low-Rank Adaptation (SLoRA) to reduce the computational overhead of LLM fine-tuning, thereby enhancing the performance of the LLM in vulnerability detection. We then propose a hybrid RAG system to verify the detection results generated by the LLM. Unlike single RAG systems, the hybrid RAG system filters results through multiple retrieval strategies. Furthermore, we feed the filtered results, together with the outputs of the LLM, into a meta-learning model [16], which performs weighted processing to generate the final detection results. Finally, we utilize Chain-of-Thought (CoT) prompt techniques to guide the LLM to create detailed and accurate vulnerability reports. These reports provide an indepth analysis of the detected vulnerabilities, assisting auditors in understanding their specific characteristics. The main contributions of this paper are summarized as follows:

- We propose ParaVul, a novel smart contract vulnerability detection framework that integrates an LLM with RAG to analyze smart contracts and identify potential vulnerabilities efficiently. ParaVul employs parallel processing to synchronize LLM-based detection with RAG-based detection, effectively enhancing detection accuracy. Moreover, we design a vulnerability detection report template to help users clearly understand identified vulnerabilities and corresponding remediation suggestions.
- We develop SLoRA based on Quantized LoRA (QLoRA)
 to reduce the computational overhead of LLM fine-tuning
 while enhancing detection performance. Specifically, we
 dynamically remove non-critical connections and freeze
 the backbone parameters of the LLM, training only the
 adapter layers. Through this design, SLoRA is capable of
 improving LLM performance in smart contract vulnerability detection while reducing computational cost.
- To mitigate hallucinations in LLM-based vulnerability detection, we construct a vulnerability contract dataset and develop a hybrid RAG system that integrates dense retrieval with Best Matching 25 (BM25). By retrieving relevant vulnerability samples from the database through these complementary strategies, the RAG system provides auxiliary validation for the detection results of the LLM, thereby improving detection reliability.
- We propose a verification module that leverages a metalearning model to refine the final results of smart contract vulnerability detection. By aggregating the outputs of LLM and RAG detection, the meta-learning model

TABLE I: Key Mathematical Notations of this Paper

Notations	Definition					
В	Batch size					
C	Contracts in dataset					
\mathcal{D}	Vulnerable smart contract dataset					
$f_{ m ID}$	Inverse document frequency					
f_T	Term frequency					
\overline{k}	Number of nonzero entries to retain in $oldsymbol{S}$					
l	Document length					
\bar{l}	Average document length					
L	Vulnerability labels on smart contract					
M	Binary mask matrix, $oldsymbol{M}_{ij} \in \{0,1\}$					
\overline{n}	Number of terms in the query					
$oldsymbol{q}$	Query of smart contract codes					
\overline{r}	LoRA rank					
\boldsymbol{S}	Trainable sparse matrix					
T	Number of epochs					
au	Threshold value, the k -th largest entry of $ oldsymbol{S} $					
α	Sparsity level					
η	Learning rate of adapters					

constructs a fusion feature vector and trains a Multi-Layer Perceptron (MLP) as the meta-learner, enabling accurate vulnerability identification. This verification module can adaptively integrate the advantages of LLMs and RAG, thereby improving overall detection performance. In terms of F1-scores, the verification module achieves at least a 4% improvement over LLMs and a 12% improvement over RAG.

The remainder of this paper is structured as follows: Section III reviews the related work. In Section III, we propose ParaVul. Sections IV, V, and VI present the designs of SLoRA, the hybrid RAG system, and the verification module, respectively. Section VII evaluates the performance of ParaVul. Section VIII concludes the paper. Key mathematical notations of this paper are illustrated in Table I.

II. RELATED WORK

In this section, we review the related work across three domains: traditional smart contract vulnerability detection, LLM-based vulnerability detection, and sparse optimization of adapter fine-tuning. The comparison of the current literature and this paper is summarized in Table II.

A. Traditional Smart Contract Vulnerability Detection

Conventional approaches to smart contract vulnerability detection primarily consist of static analysis, dynamic analysis, and formal verification [8]. Static analysis discovers potential vulnerabilities by checking the source code or bytecode of smart contracts. For example, the authors in [10] proposed a static analysis framework designed to efficiently provide detailed information about Ethereum smart contracts. Dynamic analysis identifies vulnerabilities by executing smart

Literature [10] [17] [18] [15] [19] [14] [20] [21] [22] [23] [24] **Our Paper Detection Performance Optimization** Computational Resource **Objectives** Latency Traditional **Solutions** LLM-based RAG-based

TABLE II: Comparison Between the Current Literature and This Paper

contracts and observing their runtime behaviors. In [17], the authors proposed a practical open-source fuzzer, which statically analyzes smart contract bytecodes to predict effective transaction sequences. The proposed fuzzer also identifies constraints that each transaction must satisfy. Dynamic analysis can also discover potential vulnerabilities related to runtime performance [25]. Meanwhile, formal verification leverages mathematical methods to rigorously prove the security of smart contracts [26]. For instance, the authors in [18] proposed a formal modeling approach to verify smart contract behaviors within the execution environment. However, these traditional approaches face inherent limitations when addressing complex vulnerabilities and emerging attack vectors.

B. LLM-based Vulnerability Detection

With the development of LLMs, their applications in smart contract vulnerability detection have emerged as a research hotspot. For example, the authors in [15] proposed a method that integrates LLMs with program analysis to detect logic vulnerabilities. In [11], the authors conducted a systematic assessment of the capabilities and limitations of LLMs in vulnerability detection. The authors in [19] proposed a method that combines LLMs with control-flow graph context fusion analysis, leveraging dual-modal features to improve both accuracy and localization precision. However, the applications of LLMs in vulnerability detection still face challenges, such as the need for high-quality datasets, the interpretability of models, and the consumption of computational resources.

The applications of RAG in the field of smart contract vulnerability detection are also an emerging topic. The authors in [14] created a vector database involving 830 known vulnerability contracts and combined it with GPT to build a RAG system for smart contract vulnerability detection. In [20], the authors proposed a RAG-enhanced LLM framework by utilizing QLoRA to fine-tune LLMs. Moreover, the authors combined the proposed framework with a standard library knowledge base to perform contextual inference and vulnerability detection. The authors in [21] proposed a method that merges a three-stage decompose-retrieve-generate pipeline with multi-agent collaboration. However, these works still suffer from high false-positive rates.

C. Sparse Optimization of Adapter Fine Tuning

To mitigate the high computational demands of LLMs, sparsification techniques have been explored on top of LoRA [22]– [24]. In [22], the authors proposed sparse LoRA, which combines LoRA with a sparse gating mechanism. In [23], the authors proposed a LoRA-based method for sparse LLMs, which combines sparse structure preservation with LoRA injection to achieve effective sparsification. Similarly, in [24], the authors proposed a low-rank unified modeling method that balances compression and acceleration through trainable sparse structures, thereby enabling efficient sparsification of LLMs. Although these adapter-based sparsification approaches achieve computational compression in large-scale model training environments, their complexity results in extremely low transferability. To this end, we propose SLoRA, which integrates a sparse matrix into QLoRA-based LLMs to reduce computational overhead, while ensuring both architectural simplicity and high transferability.

III. FRAMEWORK DESIGN

In this section, we introduce ParaVul, a framework consisting of four stages: data preprocessing, parallel detection using LLMs and the hybrid RAG system, detection result verification, and report generation. These stages are tightly integrated to ensure both the efficiency of the detection process and the accuracy of the detection results. The architecture of ParaVul is shown in Fig. 1.

A. Data Preprocessing

At this stage, we preprocess the original smart contract code to ensure that the input data used for subsequent detection is both high-quality and semantically complete. Specifically, we standardize the smart contract code and convert it into a unified JSON format. Each smart contract is then represented by a binary vector [27], where each element (0 or 1) indicates the absence or presence of a specific vulnerability type. This binary vector serves as the label representation for the corresponding contract in our dataset. At the same time, we perform noise elimination, remove redundant information and non-critical comments, and retain the complete semantic context, thereby ensuring that LLMs and the hybrid RAG system can comprehensively capture code security information.

B. LLM and RAG Parallel Detection

LLMs leverage robust code semantic understanding and contextual reasoning capabilities to automatically identify potential logical flaws and unsafe implementations [28]. Meanwhile, RAG integrates external security knowledge bases and

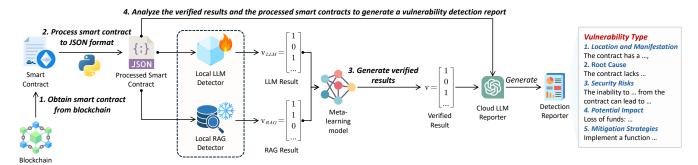


Fig. 1: The architecture of ParaVul, which is an intelligent framework for smart contract vulnerability detection that leverages parallel LLMs and RAG. In ParaVul, smart contracts are directly sourced from the blockchain. To ensure detection efficiency, we locally deploy an LLM, the hybrid RAG system, as well as the verification module. Finally, we use API calls to access a cloud-based LLM to generate comprehensive vulnerability detection reports.

specifications, ensuring that detection results are both accurate and traceable [29]. In the following, we present ParaVul, which leverages these two detection paths in parallel to fully exploit their respective advantages and achieve comprehensive identification of smart contract vulnerabilities.

- LLM Detector: We locally deploy an LLM and finetune it using SLoRA. The model takes structured smart contracts as input and outputs vector representations corresponding to the detected vulnerability types.
- RAG Detector: We locally deploy the proposed hybrid RAG system, which consists of two components: a dense retrieval and a BM25 retrieval. These two retrieval strategies employ distinct data preprocessing pipelines and voting mechanisms.

The processed smart contract code is simultaneously analyzed by both LLM and RAG detectors. Their detection outputs are subsequently vectorized [30], enabling structured comparison and comprehensive quantitative analysis [31]. The vector representations ensure consistency across the two detectors and facilitate efficient integration of results into the overall framework [32], while parallel detection significantly reduces the overall processing time.

C. Detection Result Verification

To ensure the reliability of detection results, we design a verification module based on a meta-learning model, which refines the final results of smart contract vulnerability detection. This module uses the detection results from both the LLM and RAG detectors as input. By leveraging a meta-learning model [16], it can rapidly adapt to new tasks while learning the importance weights of different features. Through this verification module, the outputs of the two detectors are weighted and aggregated to produce the final detection results. By jointly considering the strengths of both LLM and RAG detectors, the verified results achieve higher accuracy and robustness in vulnerability detection.

D. Report Generation

The verified detection results then enter the report generation stage, which aims to provide users with intuitive, comprehensive, and practically instructive vulnerability detection reports. To this end, we design a CoT-based report template tailored for smart contract vulnerability detection. Unlike ordinary reports that merely list vulnerability types [33], [34], our detection report offers a structured overview of the detected vulnerabilities, comprising the following five elements:

- 1) Location and manifestation: A detailed description of the specific location and manifestation of vulnerabilities within the smart contract. For example, a fallback function may permit token deposits but lack a withdrawal mechanism [35]. This vulnerability can cause tokens to become permanently locked within the smart contract.
- 2) Root causes: The report provides an in-depth analysis of the root causes of vulnerabilities. For instance, it may highlight that the smart contract lacks functionality for withdrawing or transferring Ether, which is the native cryptocurrency of the Ethereum blockchain [36]. Furthermore, it may indicate scenarios where Ether becomes irretrievable from the smart contract under certain conditions.
- 3) Security risks: The report explicitly outlines the potential security risks associated with vulnerabilities. For instance, it can emphasize the risk of permanent fund loss if Ether is inadvertently sent to the smart contract address or if the transfer operation of the owner fails.
- 4) Potential impact: The report specifies the potential impact of the vulnerability, noting that blockchain tokens sent to the smart contract address may become unrecoverable, potentially resulting in financial loss.
- 5) Mitigation strategies: The report outlines concrete mitigation strategies. For instance, it can recommend the implementation of a withdrawal function that allows the smart contract owner to retrieve blockchain tokens, thereby ensuring that any tokens sent to the contract remain recoverable.

IV. SPARSE LOW-RANK ADAPTATION

In this section, we introduce the developed SLoRA. The inputs to SLoRA include a pre-trained LLM, a smart contract dataset, and a set of hyperparameters, including batch size B, learning rate η , number of training epochs T, low-rank dimension, early stopping patience, and the sparsity ratio [37]. The objective of SLoRA is to produce a fine-tuned and sparsified model. Similar to LoRA, SLoRA freezes all layers except

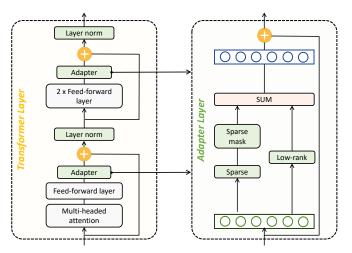


Fig. 2: The architecture of SLoRA, which incorporates two adapter modules into each transformer layer: one placed after the projection layer following multi-head attention, and the other after the two fully connected layers. Each adapter consists of a sparse layer and a LoRA layer. The sparse layer masks a subset of nodes, while the LoRA layer applies a low-rank matrix transformation to the data.

the adapter layer, and during fine-tuning, only the parameters of the adapter layer are updated, significantly reducing the computational requirements for LLM fine-tuning.

As shown in Fig. 2, SLoRA enhances the quantized base model with two additional modules: a low-rank adapter and a sparse adapter. This design improves the expressive power of LLMs while minimizing the number of trainable parameters, thereby optimizing both performance and efficiency.

A. Low-Rank Adapter

Given an input feature matrix $x \in \mathbb{R}^{n \times d}$, where n is the number of samples and d is the feature dimension of each sample [38], we introduce a rank-r decomposition of the weight increment as

$$\Delta W_{\text{low}} = UV, \tag{1}$$

where $U \in \mathbb{R}^{d \times r}$ and $V \in \mathbb{R}^{r \times d}$. The corresponding low-rank output increment is given by

$$O_{\text{low}} = \boldsymbol{x} (\boldsymbol{U} \boldsymbol{V}). \tag{2}$$

This decomposition leverages the low-rank structure to capture the essential features of the data in a lower-dimensional space, thereby reducing the number of parameters required for training and enhancing computational efficiency [38].

B. Sparse Adapter

We first define a trainable sparse matrix $S \in \mathbb{R}^{d \times d}$ with a sparsity level $\alpha \in [0,1]$. The number of entries to retain is determined by

$$k = \left[(1 - \alpha) d^2 \right]. \tag{3}$$

Algorithm 1: SLoRA for Smart Contract Vulnerability Detection by LLMs

```
1 Initialize frozen quantized weights W_q.
2 Initialize low-rank parameters U \in \mathbb{R}^{d \times r}, V \in \mathbb{R}^{r \times d}.
3 Initialize sparse matrix S \in \mathbb{R}^{d \times d}
4 Initialize binary mask M \in \mathbb{R}^{d \times d}.
   for each training iteration do
        ### Low-Rank Adapter ###
 6
        Compute the low-rank increment: \Delta W_{\text{low}} = UV.
7
        Obtain the low-rank output: O_{low} = x(UV).
 8
        ### Sparse Adapter ###
 9
        Calculate active entries: k = \lfloor (1 - \alpha)d^2 \rfloor.
10
11
        Select the top-k elements of S.
        Construct the binary mask M.
12
        Obtain the sparse output: O_{\text{spr}} = x (S \odot M).
13
14
        ### Combined Outputs ###
15
        Compute the base output: O_{\text{base}} = \boldsymbol{x} W_q.
16
        Compute the final output:
          O = O_{\text{base}} + O_{\text{low}} + O_{\text{spr}}.
        ### Frozen Base Parameters ###
17
        Keep base parameters fixed: \frac{\partial \mathcal{L}}{\partial W_a} = 0.
18
        Update only U, V, S.
19
        ### Loss Function ###
20
        Optimize with multi-label BCE loss:
21
        \hat{\mathcal{L}} = -\frac{1}{L} \sum_{i=1}^{L} [y_i \log \hat{y}_i + (1 - y_i) \log(1 - \hat{y}_i)].
22
23 end
```

We then construct the binary mask $oldsymbol{M} \in \mathbb{R}^{d imes d}$ as

24 **return** the adapter parameters U, V, S.

$$\mathbf{M}_{ij} = \begin{cases} 1 & \text{if } |\mathbf{S}_{ij}| \ge \tau, \\ 0 & \text{otherwise,} \end{cases}$$
 (4)

where τ represents the k-th largest element of |S|. This mask retains only the top-k elements of S in terms of the absolute value, enforcing sparsity in the adapter layer while ignoring less significant connections. Hence, similar to (2), the sparse output increment is given by

$$O_{\rm spr} = \boldsymbol{x} (\boldsymbol{S} \odot \boldsymbol{M}), \tag{5}$$

where \odot denotes the Hadamard product between matrices.

This sparse adapter introduces sparsity into the transformer layer, reducing the number of trainable parameters and enhancing its capacity to focus on the most relevant features.

C. Combined Output

The final output of the adapter layer is obtained by summing the quantized base output with the incremental outputs from the low-rank and sparse adapters, as expressed by

$$O = O_{\text{base}} + O_{\text{low}} + O_{\text{spr}},\tag{6}$$

where $O_{\mathrm{base}} = xW_q$ denotes the output of the quantized base model. This combined formulation allows the transformer layer to capture both low-rank and sparse structures, improving representation capacity while keeping the number of trainable parameters minimal.

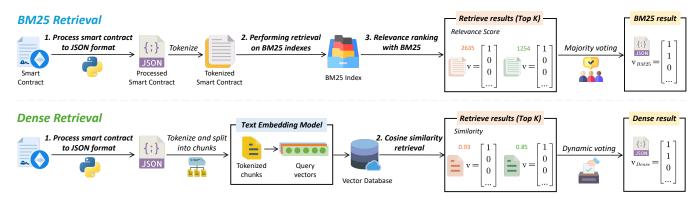


Fig. 3: The architecture of the hybrid RAG system, which presents the vulnerability detection process corresponding to the BM25 retrieval strategy and the dense retrieval strategy, respectively.

D. Frozen Base Model Parameters

Considering the need to handle multiple labels simultaneously, we use the multi-label Binary Cross-Entropy (BCE) loss and define the training objective of SLoRA as

$$\mathcal{L} = -\frac{1}{L} \sum_{i=1}^{L} \left[y_i \log \hat{y}_i + (1 - y_i) \log(1 - \hat{y}_i) \right], \quad (7)$$

where L is the number of labels, $y_i \in \{0, 1\}$ represents the binary label i, and \hat{y}_i is the predicted probability for label i. Based on (7), we freeze the weight matrix W_q of the quantized transformer model during fine-tuning, which is given by

$$\frac{\partial \mathcal{L}}{\partial W_a} = 0. {8}$$

Note that parameter updates are confined to U, V, and S. This strategy preserves the knowledge embedded in the quantized transformer model while allowing the adapters to learn task-specific refinements that enhance overall performance.

E. Computational Complexity Analysis

For the low-rank adapter, the computational complexity is $\mathcal{O}(ndr) + \mathcal{O}(nrd) = \mathcal{O}(ndr)$, which is significantly lower than the cost of a full-rank update $\mathcal{O}(nd^2)$ [38]. For the sparse adapter, the computational complexity is O(nk), which is significantly lower than the dense case, particularly when the sparsity level α is close to 1. Therefore, the overall computational complexity of SLoRA is expressed as

$$\mathcal{O}(n(dr+k)) \ll \mathcal{O}(nd^2).$$
 (9)

In conclusion, SLoRA provides a principled approach for enhancing model expressivity while maintaining a minimal parameter footprint. By jointly leveraging low-rank and sparse adapters, SLoRA achieves a balanced trade-off between performance and computational efficiency, making it particularly suitable for resource-constrained applications. The procedural implementation of SLoRA is outlined in Algorithm 1.

V. HYBRID RAG SYSTEM WITH DENSE AND BM25 RETRIEVAL STRATEGIES

In this section, we present the proposed hybrid RAG system, which integrates BM25 with dense retrieval to identify vulnerabilities in smart contracts. The architecture of the hybrid RAG system is illustrated in Fig. 3.

A. BM25 Retrieval

- 1) Knowledge base construction: The source code of each contract undergoes systematic preprocessing, including code cleaning, extraction of key components, tokenization with lowercase normalization, identification of security-related keywords, pattern-based feature extraction, and intelligent deduplication. This process yields an optimized token list for each contract. We then construct a BM25 model based on the tokenized text, with term statistics initialized and computed [39]. To ensure accurate mapping between BM25 indices and the original contracts, the order of preprocessed documents is strictly aligned with the training metadata.
- 2) BM25 retrieval strategy: Each query contract in the test set is first processed through word segmentation, and the resulting tokens are then fed into the constructed BM25 model. The BM25 model computes the relevance scores between the query and all smart contracts in the knowledge base, using the following formulation [39]:

$$BM25(\boldsymbol{q}, \boldsymbol{d}) = \frac{\sum_{i=1}^{n} f_{ID}(\boldsymbol{q}_i) (k_1 + 1) f_T(\boldsymbol{q}_i, \boldsymbol{d})}{k_1 (1 - b + \frac{l_D b}{T}) + f_T(\boldsymbol{q}_i, \boldsymbol{d})}, \quad (10)$$

where n denotes the number of terms in the query \mathbf{q} , $f_T(\mathbf{q}_i, \mathbf{d})$ represents the frequency of the term \mathbf{q}_i in the document \mathbf{d} , k_1 is a free parameter that adjusts the term frequency scaling, and b is another free parameter that controls the strength of length normalization. Moreover, l_D denotes the length of the document \mathbf{d} , and \bar{l} is the average document length in the collection. Finally, $f_{\rm ID}(\mathbf{q}_i)$ represents the inverse document frequency of the term \mathbf{q}_i , which is calculated as

$$f_{\rm ID}(\mathbf{q}_i) = \log\left(\frac{N - n_{\mathbf{q}_i} + 0.5}{n_{\mathbf{q}_i} + 0.5} + 1\right),$$
 (11)

where N represents the total number of contracts in the dataset, and n_{q_i} represents the number of contracts that contain

the term q_i . After computing the relevance scores, the BM25 model ranks all contracts in descending order and selects the most relevant ones. To ensure the objectivity and validity of the retrieval results, any document corresponding to the query contract itself is excluded during this process.

B. Dense Retrieval

1) Knowledge base construction: Since the source code of smart contracts often exceeds the maximum input sequence length, we adopt an advanced sliding window segmentation mechanism [40] to address this issue. This mechanism is designed to mitigate the loss of critical information due to truncation. Following recent studies on long-context modeling as LongEmbed [41], the segmentation parameters are empirically determined to achieve a balance between contextual completeness and computational efficiency. Specifically, we set the window size to 1500 characters to provide sufficient contextual coverage without exceeding the input capacity of the dense model, and the overlap is set to 300 characters, corresponding to about 20% of the window size, to maintain semantic continuity. The fragments, which are shorter than 100 characters, are removed to avoid semantically insignificant segments. Each valid segment is then converted into a highdimensional embedding vector using the semantic model, assigned a unique identifier and metadata, and subsequently batch-uploaded to the vector database.

2) Dense retrieval strategy: After generating the query vector, the RAG system retrieves relevant contextual information from the knowledge base through dense retrieval. The query vector is submitted to a vector database specifically designed for high-dimensional similarity searches, where cosine similarity is used to compare the query vector against all stored vectors in the knowledge base. The number of relevant vectors $N_{\rm ret}$ retrieved in each search depends on the length of the query contract and the number of its segmented blocks. Specifically, given the length of a query contract L_q , a window size s, and an overlap o, the number of retrieved vectors $N_{\rm ret}$ can be expressed as

$$N_{\rm ret} = \chi \left[\frac{L_q - o}{s - o} \right], \tag{12}$$

where χ denotes the number of top-ranked vectors returned for each segment. The retrieved fragments inherit the vulnerability labels from the original contracts, and the final vulnerability prediction is obtained through a label aggregation mechanism. The dense retrieval score is computed based on the cosine similarity [42], which is given by

Score
$$(q, d) = \frac{q \cdot d}{\|q\| \cdot \|d\|}$$
. (13)

To ensure the independence of aggregation, fragments originating from the query contract are excluded from the retrieval results. The vulnerability labels of the remaining fragments are aggregated through a dynamic voting mechanism, where label frequency reflects its relative evidence across retrieved fragments. Unlike fixed-threshold aggregation, we adopt an adaptive thresholding strategy that dynamically adjusts based on the total number of retrieved fragments. This approach

effectively reduces noise from semantically similar but non-vulnerable code segments, thereby enhancing the robustness of multi-label vulnerability detection in smart contracts. Specifically, the dynamic voting threshold τ^* is defined as the greater of 40% of the retrieved fragments or a minimum threshold of 1, which is given by

$$\tau^* = \max(N^* \times 0.4, 1), \tag{14}$$

where N^* represents the total number of retrieval results.

This adaptive approach systematically accounts for variations in contract complexity and length, ensuring that both simple contracts, which generate relatively few fragments, and complex contracts, which produce numerous fragments, are subject to appropriately calibrated thresholding. The votes corresponding to each vulnerability label are then aggregated across all retrieved fragments, and only the labels whose vote counts exceed the dynamic voting threshold are retained in the final prediction. Specifically, during aggregation, each retrieved fragment casts one vote for its associated vulnerability labels. The dynamic threshold τ^* specifies the minimum number of supporting votes required for a label to be retained. A higher threshold enforces stronger consensus and reduces false positives, whereas a lower threshold increases sensitivity but may introduce spurious labels. The adaptive design of τ^* balances these trade-offs according to the retrieval volume.

C. Result Outputs

The hybrid RAG system ultimately outputs all vulnerability types detected for the current smart contract. These results are then comprehensively evaluated alongside the outputs of the LLM during the subsequent verification module, thereby enhancing the overall reliability and coverage of vulnerability detection. When executed in parallel, the two detection pathways complement each other through distinct retrieval mechanisms. The dense retrieval pathway captures deep semantic and contextual vulnerability patterns, such as logical inconsistencies and hidden contract dependencies [42], while the BM25-based pathway focuses on lexical matching to identify explicit code-level vulnerabilities [39]. This integration provides a unified representation that combines semantic and logical perspectives, thereby enhancing both detection coverage and interpretability of the hybrid RAG system.

VI. META-LEARNING GATED VERIFICATION MODULE

In this section, we propose a meta-learning gated verification module to enhance the reliability of vulnerability detection results. This module takes as input the detection outputs from both the LLM and the hybrid RAG system. By leveraging meta-learning techniques [16], the module can rapidly adapt to new tasks and effectively learn the importance weights of different features, thereby improving the robustness and generalization of the final verification process.

A. Dynamic Feature Weighting

The meta-learning model comprises two key components: a meta-learner and a base learner. The meta-learner guides the optimization of the base learner, enabling rapid adaptation to new tasks even with limited labeled data. Through this hierarchical learning structure, the input features are dynamically reweighted based on their learned importance. Specifically, we denote w as the feature-weight vector of the meta-learner and \tilde{w}_t as the task-specific weight vector for detection task t [16]. The adaptation process can be formulated as [16]

$$\tilde{w}_t = \operatorname*{argmin}_{\tilde{w}} \mathcal{L}_t(\tilde{w}) + \frac{\lambda}{2} \|\tilde{w} - w\|_2^2, \tag{15}$$

which constrains the parameters of the base learner to remain close to the initialization of the meta-learner while allowing task-specific adjustments. The regularization coefficient λ controls the balance between stability and adaptability, namely a larger λ enforces stronger adherence to the prior knowledge of the meta-learner, whereas a smaller λ promotes faster adaptation to new task-specific distributions. By leveraging knowledge from historical tasks, the meta-learning model automatically adjusts feature weights, enabling it to swiftly identify and emphasize the most relevant features when encountering new tasks.

B. Model Training

The meta-learning model is capable of extracting representative feature weights by learning from multiple related tasks [43]. These learned weights are then applied to process features in the current task, thereby enhancing detection accuracy. Furthermore, the model adaptively adjusts these weights according to the feature distributions of different tasks [44]. This dynamic feature-weight adjustment mechanism enhances the adaptability of the meta-learning model across diverse detection scenarios, effectively reducing the risks of false positives and negatives, and ultimately enhancing the overall performance of smart contract vulnerability detection.

To train the model, we first define the training dataset as

$$\mathcal{D} = \{ (\tilde{x}_i, y_i) \}_{i=1}^N, \tag{16}$$

where $\tilde{x}_i \in \mathbb{R}^d$ denotes the *d*-dimensional original feature vector of the *i*-th sample. The goal of the meta-learning model is to learn a mapping, which is given by

$$\mathcal{F}_{\boldsymbol{\theta}}: \mathbb{R}^d \to [0, 1], \tag{17}$$

where θ is the parameters of the meta-learner. This mapping predicts the probability of a vulnerability for each input sample, while enabling rapid adaptation to new tasks with limited labeled data.

C. Feature Construction

For each sample, the prediction results from $\boldsymbol{\Psi}$ base models are aggregated into

$$\hat{\mathbf{y}}_i = \left[\hat{y}_i^{(1)}, \hat{y}_i^{(2)}, \dots, \hat{y}_i^{(\Psi)} \right]^{\top} \in \mathbb{R}^{\Psi}.$$
 (18)

In this study, we set $\Psi=3$, where the three base models correspond to the dense retrieval model, the BM25 model, and the SLoRA model, respectively. The input to the metalearner is subsequently formed as a weighted combination

of the prediction outputs from these base models, which is expressed as [16]

$$\mathbf{x}_i = \mathbf{w} \odot \hat{\mathbf{y}}_i, \tag{19}$$

where $\mathbf{w} = [w_1, w_2, w_3]^{\top}$ denotes the learnable weight vector, and \odot represents element-wise multiplication, which quantifies the relative contribution of each base model to the final metafeature representation.

D. Meta-Learner Architecture

The meta-learner is implemented as an MLP consisting of two hidden layers and the final layer:

$$\mathbf{h}^{(1)} = \sigma \left(\mathbf{W}^{(1)} \boldsymbol{x}_i + \mathbf{b}^{(1)} \right), \tag{20}$$

$$\mathbf{h}^{(2)} = \sigma \left(\mathbf{W}^{(2)} \mathbf{h}^{(1)} + \mathbf{b}^{(2)} \right), \tag{21}$$

$$\hat{y}_i = \operatorname{sigmoid}\left(\mathbf{W}^{(3)}\mathbf{h}^{(2)} + \mathbf{b}^{(3)}\right),$$
 (22)

where $\sigma(\cdot)$ denotes the ReLU activation function, $\hat{y}_i \in [0, 1]$ represents the predicted probability, and $\mathbf{W}^{(l)}$ and $\mathbf{b}^{(l)}$ denote the learnable weights and biases of the l-th layer, respectively. This architecture facilitates non-linear integration of the base model predictions, enabling the meta-learner to capture complex feature interactions and thereby enhance the overall accuracy of vulnerability detection.

E. Objective Function

Similar to the training objective of SLoRA, we optimize the meta-learner by minimizing the BCE loss, defined as

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^{N} \left[y_i \log \hat{y}_i + (1 - y_i) \log(1 - \hat{y}_i) \right]. \tag{23}$$

The learnable parameters $\theta = \{\mathbf{W}^{(l)}, \mathbf{b}^{(l)}\}$ are optimized as

$$\boldsymbol{\theta}^* = \operatorname*{argmin}_{\boldsymbol{\theta}} \mathcal{L}(\boldsymbol{\theta}). \tag{24}$$

Based on the above formulation, we design a meta-learning model that integrates the prediction results of multiple base models through a trainable meta-learner, enabling adaptive fusion of features and improved classification accuracy.

F. Computational Complexity Analysis

The computational complexity of the proposed metalearning model mainly arises from the forward and backward propagation of the meta-learner during training, and the inference process that aggregates the outputs of the base models.

1) Training computational complexity: Considering that each input feature vector $x_i \in \mathbb{R}^{\Psi}$ is processed by a two-layer MLP with hidden dimensions h_1 and h_2 , the forward propagation of the meta-learner requires $\mathcal{O}(\Psi h_1 + h_1 h_2 + h_2)$ operations per sample, and the backward propagation introduces the same order of computation. Therefore, for N samples in the training dataset, the total training computational complexity is $\mathcal{O}(N(\Psi h_1 + h_1 h_2 + h_2))$, which scales linearly with both the dataset size N and the number of base models Ψ . Since both Ψ and the hidden layer dimensions are small, the additional training overhead of the meta-learner is negligible relative to that of the base models.

2) Inference computational complexity: During inference, each base model independently produces its prediction, with a total computational cost of $\sum_{\phi=1}^{\Psi} \mathcal{O}(\mathcal{C}_{\phi})$, where \mathcal{C}_{ϕ} denotes the inference complexity of the ϕ -th base model. The metalearner then performs a lightweight fusion operation, requiring $\mathcal{O}(\Psi h_1 + h_1 h_2 + h_2)$ operations per prediction. Hence, the overall inference complexity can be expressed as

$$\mathcal{O}\left(\sum_{\phi=1}^{\Psi} C_{\phi} + \Psi h_1 + h_1 h_2 + h_2\right). \tag{25}$$

Given the compact structure of the MLP, the additional cost of meta-level fusion remains minimal, allowing efficient realtime integration of base model outputs in smart contract vulnerability detection.

VII. SIMULATION RESULTS

In this section, we first provide the experimental setup and security analysis of ParaVul. We then evaluate the effectiveness of SLoRA in enhancing LLM-based smart contract vulnerability detection, followed by a detailed evaluation of the hybrid RAG system under both single-label and multilabel scenarios. Finally, we validate the superiority of the proposed verification module, demonstrating its robustness and reliability in achieving accurate vulnerability detection.

A. Experimental Settings

We implement ParaVul on a server equipped with an Intel Xeon(R) Gold 6133 CPU and an NVIDIA RTX A6000 GPU, using Python 3.10.14 with CUDA 12.1. The main parameter settings of ParaVul are detailed in Table III.

To evaluate the performance of ParaVul in detecting both single-vulnerability and multi-vulnerability smart contracts, we utilize the SC_UEE¹ and ScrawlD [45] datasets, which encompass various types of vulnerability collected from real-world blockchain platforms and open-source repositories. To ensure seamless integration and enhance processing efficiency, we standardize the SC_UEE and ScrawlD datasets into a unified JSON format containing the contract code and corresponding vulnerability labels.

B. Security Analysis

ParaVul ensures both security and reliability through its decentralized architecture and adaptive learning design.

- 1) Decentralization: ParaVul removes dependence on any single trusted authority. Specifically, the LLM detector and the RAG detector operate independently, while the metalearning gated verification module fuses their outputs in a decentralized manner, thereby eliminating single points of failure and improving system resilience.
- 2) Integrity and traceability: All analyzed contract fragments and detection results are securely stored with unique identifiers in a tamper-resistant vector database, ensuring traceable and reproducible vulnerability analysis.

TABLE III: Main Parameter Settings of ParaVul

Notations	Definition			
Learning rate of adapters η [46]	5×10^{-5}			
Batch size B [46]	8			
Number of epoch T [46]	5			
LoRA rank r [38]	8			
Top-K selection of the BM25 model [39]	7			
Top- K selection of the dense model [42]	5			
Voting threshold of the BM25 model [39]	4			
Parameter k_1 of the BM25 model [39]	1.5			
Parameter b of the BM25 model [39]	0.9			

3) Robustness and privacy: In ParaVul, the adaptive fusion mechanism mitigates the influence of biased or adversarial detectors, while sensitive contract data are locally processed or encrypted to prevent information leakage.

Overall, ParaVul provides a secure, interpretable, and trust-worthy approach for smart contract vulnerability detection.

C. Performance Evaluation of SLoRA

As shown in Table IV, we summarize the performance of multiple LLMs with different fine-tuning techniques on both single-label and multi-label vulnerability detection tasks. The evaluation metrics include accuracy, recall, precision, and F1-score, which comprehensively reflect model effectiveness in smart contract vulnerability detection. From Table IV, we observe that LLaMA13b with SLoRA achieves state-of-the-art performance across all evaluation metrics, significantly outperforming QLoRA [47] and Quantization-Aware LoRA (QALoRA) [48]. Furthermore, LLaMA13b with SLoRA surpasses both pre-trained GPT-40 and LLaMA7b across all metrics. In particular, it achieves an F1-score of 0.9021, compared with 0.2485 for GPT-40 in single-label tasks.

In single-label detection, LLaMA13b with SLoRA achieves an accuracy of 0.8611, a recall of 0.8759, a precision of 0.9300, and an F1-score of 0.9021. This performance exceeds that of LLaMA13b with QLoRA, which attains an F1-score of 0.8778, by a margin of 2.8%, and surpasses LLaMA13b with QALoRA by 1.9%. Although these margins may appear numerically modest, they represent substantial improvements in the context of smart contract analysis, where each percentage point of F1-score corresponds to a considerable reduction in undetected or misclassified vulnerabilities. In multilabel detection, SLoRA further demonstrates its effectiveness, achieving an accuracy of 0.8637, a recall of 0.9294, a precision of 0.9500, and an F1-score of 0.9396, outperforming QLoRA. In addition, SLoRA achieves a faster detection time of 0.7789 seconds, compared with 0.7855 seconds for QLoRA. Furthermore, it surpasses QALoRA with a 0.9% higher F1-score and a shorter inference time. The consistent improvement can be attributed to the architecture design of SLoRA, which integrates low-rank adaptation with sparse structure modeling. This design enables more expressive gradient updates and better parameter utilization under limited fine-tuning budgets,

¹SC_UEE is available at https://github.com/1052445594/SC_UEE

Single Labeled Multi Labeled Models Accuracy[†] Recall[†] Precision ↑ F1-score↑ Time (s)↓ Accuracy[↑] Recall[↑] Precision ↑ F1-score↑ Time (s)↓ GPT-40 0.0139 0.6852 0.1518 0.2485 4.0833 0.0058 0.5685 0.4006 0.4700 2.9049 LLaMA7b 0.0008 0.3873 0.0890 0.1448 0.7912 0.0028 0.4206 0.2440 0.3088 0.7886 0.4000 LLaMA7b + QLoRA 0.8125 0.9043 0.8559 0.9199 0.9287 0.9243 0.7731 0.41730.8173 LLaMA7b + OALoRA 0.7129 0.7480 0.8616 0.8008 0.4190 0.7420 0.8846 0.9068 0.8956 0.4108 LLaMA7b + SLoRA 0.8055 0.8228 0.8931 0.8565 0.3998 0.7913 0.9237 0.9262 0.9249 0.4140 LLaMA13b 0.0010 0.5275 0.0890 0.1972 0.4301 0.0115 0.4287 0.2894 0.3455 0.8393 LLaMA13b + QLoRA 0.8240 0.8346 0.9257 0.8778 0.7662 0.8318 0.9225 0.9365 0.9295 0.7855 LLaMA13b + QALoRA 0.8240 0.8492 0.9224 0.8842 0.7891 0.8202 0.9213 0.9404 0.9307 0.7745 0.8611 0.8759 0.9300 0.9021 0.7960 0.8637 0.9294 0.9500 0.9396 0.7789 LLaMA13b + SLoRA

TABLE IV: Performance of LLMs in Smart Contract Vulnerability Detection

TABLE V: GPU Memory Usage Comparison for Fine-Tuning Techniques

Models	GPU Memory Usage (MiB)				
	Single Labeled	Multi Labeled			
LLaMA7b	16464	16452			
LLaMA7b + QLoRA	8910	8910			
LLaMA7b + QALoRA	8976	8976			
LLaMA7b + SLoRA	8992	9012			
LLaMA13b	24966	24966			
LLaMA13b + QLoRA	14548	14586			
LLaMA13b + QALoRA	14476	14474			
LLaMA13b + SLoRA	14676	14674			

effectively enhancing both accuracy and computational efficiency. In summary, the above results demonstrate that SLoRA effectively enhances both the accuracy and efficiency of LLMs in smart contract vulnerability detection.

As shown in Table V, we compare the GPU memory consumption across different fine-tuning techniques. Compared with the pre-trained LLMs, SLoRA reduces GPU memory usage by more than 41% during fine-tuning. Furthermore, relative to QLoRA and QALoRA [48], the increase in GPU memory usage with SLoRA is limited to within 1.1%. These results demonstrate that SLoRA not only enhances the performance of LLMs in smart contract vulnerability detection but also maintains high computational efficiency and memory economy during fine-tuning.

D. Performance Evaluation of the Hybrid RAG System

Table VI presents the performance evaluation of the hybrid RAG system on both single-label and multi-label tasks. Specifically, we observe that in single-label tasks, the dense retrieval approach achieves an F1-score of 0.6851, higher than the 0.6253 achieved by BM25, and demonstrates greater accuracy, recall, and precision, indicating superior detection capability. However, BM25 records a much shorter processing time of 0.1190 seconds compared with 6.1852 seconds for

dense retrieval, reflecting higher time efficiency. For multilabel detection, the dense retrieval method again surpasses BM25, achieving an F1-score of 0.8666 compared with 0.8327 for BM25, while also maintaining better accuracy, recall, and precision. Nevertheless, BM25 shows an advantage in efficiency, with a processing time of 0.1180 seconds compared with 6.3855 seconds for dense retrieval. Overall, dense retrieval provides stronger performance in both single-label and multi-label vulnerability detection, particularly in identifying multiple vulnerability types, while BM25 offers significantly better time efficiency. Combining these two retrieval strategies enables complementary strengths and provides more reliable auxiliary verification for LLM-based detection.

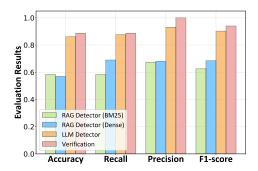
E. Performance Evaluation of the Verification Module

We evaluate the proposed verification module against three baselines: the LLM detector, the RAG detector with BM25 retrieval, and the RAG detector with dense retrieval. As shown in Fig. 4(a) and Fig. 4(b), the module consistently outperforms all baselines in accuracy, precision, recall, and F1-score across both single-label and multi-label tasks. In particular, it achieves substantial gains in precision and recall, demonstrating enhanced robustness and reliability in vulnerability detection. The superior performance of the verification module can be attributed to its meta-learning-based adaptive fusion capability, which effectively integrates the complementary strengths of multiple detectors to achieve more accurate vulnerability predictions. These results confirm that the proposed approach effectively addresses the shortcomings of previous methods and offers a more dependable solution for smart contract security.

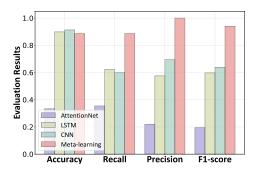
As shown in Fig. 4(c) and Fig. 4(d), we evaluate the performance of the proposed meta-learning method against traditional machine learning approaches, including Attention-Net [49], Long Short-Term Memory (LSTM), and Convolutional Neural Network (CNN). All baseline models are carefully optimized through grid search on validation data to ensure fair comparison, with hyperparameters such as learning rate, batch size, and hidden dimensions tuned to achieve their best performance. In single-label detection, the meta-learning method achieves an F1-score over 380% higher than

TABLE VI: Performance of the Hybrid RAG System in Smart Contract Vulnerability Detection

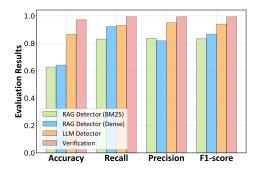
Retrieval Strategies	Single Labeled				Multi Labeled					
	Accuracy↑	Recall↑	Precision [↑]	F1-score↑	Time (s)↓	Accuracy [†]	Recall†	Precision [†]	F1-score↑	Time (s)↓
Dense	0.5694	0.6898	0.6804	0.6851	6.1852	0.6406	0.9213	0.8181	0.8666	6.3855
BM25	0.5833	0.5833	0.6738	0.6253	0.1190	0.6261	0.8304	0.8349	0.8327	0.1180



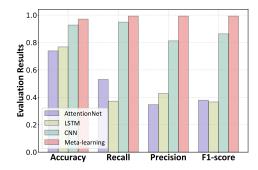
(a) Performance of the verification module in single-label smart contract vulnerability detection.



(c) Performance of the meta-learning method in single-label smart contract vulnerability detection.



(b) Performance of the verification module in multi-label smart contract vulnerability detection.



(d) Performance of the meta-learning method in multi-label smart contract vulnerability detection.

Fig. 4: Performance evaluation of the verification module in smart contract vulnerability detection. Note that the LLM and RAG detectors take raw smart contracts as input, whereas the verification module operates on the intermediate detection outputs generated by these detectors.

AttentionNet, approximately 57% higher than LSTM, and around 47% higher than CNN, with recall also significantly improved. Although CNN attains slightly higher accuracy, the substantial advantages of the meta-learning method in recall and F1-score demonstrate its superior overall effectiveness. In multi-label detection, the meta-learning method achieves an F1-score about 162% higher than AttentionNet, 171% higher than LSTM, and approximately 15% higher than CNN, while maintaining precision and recall near perfect levels. Its accuracy also shows consistent improvement compared with all baseline models. These results confirm the robustness and overall superiority of the meta-learning method, particularly in handling complex multi-label classification tasks.

F. Smart Contract Vulnerability Detection Reports

As shown in Fig. 5, we present a smart contract vulnerability detection report. The generated report provides a comprehensive overview of the detected vulnerabilities. It begins with detailed analyses of individual vulnerabilities, including

their location, root cause, associated risks, potential impacts, and recommended mitigation strategies. The findings are then consolidated into a structured summary that highlights vulnerability types, affected code locations, potential consequences, and corresponding mitigation measures. In addition, the report offers general recommendations to enhance the overall security and reliability of the smart contract.

VIII. CONCLUSION

In this paper, we have proposed ParaVul, a parallel LLM and retrieval-augmented framework for accurate and reliable smart contract vulnerability detection. Specifically, based on QLoRA, we have developed SLoRA to fine-tune LLMs, which effectively improves their detection performance. To enhance the reliability of LLM outputs, we have designed a hybrid RAG system that integrates dense retrieval with BM25. To further improve the detection accuracy of ParaVul, we have introduced a meta-learning gated verification module that performs weighted fusion of LLM and hybrid RAG results.

1) Smart Contract Vulnerability Detection Report

```
**Horaction:**

The fallback function:

**Olatiful public payable (
recert();

**Menifestation:**

The fallback function is marked as 'payable' but immediately reverts any incoming Ether. This means that Ether sent to the contract (either accidentally or maliciously) will be rejected, and the transaction will fail. However, if Ether is sent to the contract using address(this):

**Menifestation:**

The failback function is marked as 'payable' but immediately reverts any incoming Ether. This means that Ether sent to the contract (either accidentally or maliciously) will be rejected, and the transaction will fail. However, if Ether is sent to the contract using address(this):

**Recontract does not implement a mechanism to handle Ether sent via 'selfdestruct', and the fallback function explicitly reverts any direct Ether transfers.

**Security Risks:**

If Ether is sent to the contract via 'selfdestruct', it will be permanently locked, as there is no function to withdraw it. This could lead to loss of funds if the contract is expected to handle Ether in the future.

**Plottential impact:**

Locked funds in the contract, leading to a loss of usability and potential financial loss for users or the owner.

**Plottential impact:**

Locked funds in the contract, leading to a loss of usability and potential financial loss for users or the owner.

**Plottential impact:**

Locked funds in the contract, leading to a loss of usability and potential financial loss for users or the owner.

**Plottential information**

Locked funds in the contract, leading to a loss of usability and potential financial loss for users or the owner.

**Plottential fundamental function for the owner to recover any Ether accidentally sent to the contract:

**Security Risks:**

Locked funds in the contract, leading to a loss of usability and potential financial loss for users or the owner.

**Plottential fundamental fundamental function for the owner to recover any Ether accidentally sent to the contract:

**Contract to the contract (with the funda
```

Summary of Smart Contract Vulnerability Detection

Fig. 5: The generated vulnerability detection report comprises two parts: a detailed analysis of each smart contract vulnerability, describing its location, root cause, associated risks, potential impacts, and recommended mitigation strategies; and a structured summary that consolidates all identified vulnerabilities along with their corresponding solution.

Additionally, we have employed CoT prompt techniques to guide LLMs in generating detailed vulnerability detection reports. Simulation results demonstrate the effectiveness and robustness of ParaVul. For future work, we aim to further optimize SLoRA and develop more advanced verification modules to better handle complex smart contracts, thereby enhancing the overall performance of ParaVul.

REFERENCES

- W. Li, X. Li, Y. Mao, and Y. Zhang, "Interaction-aware vulnerability detection in smart contract bytecodes," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–18, 2025.
- [2] J. Kang, J. Wen, D. Ye, B. Lai, T. Wu, Z. Xiong, J. Nie, D. Niyato, Y. Zhang, and S. Xie, "Blockchain-empowered federated learning for healthcare metaverses: User-centric incentive mechanism with optimal data freshness," *IEEE Transactions on Cognitive Communications and Networking*, vol. 10, no. 1, pp. 348–362, 2024.
- [3] J. Wen, J. Kang, Z. Xiong, H. Du, Z. Yang, D. Niyato, M. Shen, Y. Jiao, and Y. Zhang, "Optimal AoI-based block propagation and incentive mechanism for blockchain networks in Web 3.0," *IEEE Transactions on Cognitive Communications and Networking*, vol. 11, no. 4, pp. 2568–2583, 2025.
- [4] J. Liao, J. Wen, J. Kang, C. Yi, Y. Zhang, Y. Jiao, D. Niyato, D. I. Kim, and S. Xie, "Graph attention network-based block propagation with optimal AoB and reputation in Web 3.0," *IEEE Transactions on Cognitive Communications and Networking*, vol. 10, no. 6, pp. 2427–2441, 2024.
- [5] Z. Liu and X. Li, "SoK: Security analysis of blockchain-based cryptocurrency," arXiv preprint arXiv:2503.22156, 2025.

- [6] J. Chen, L. Wang, and H. Zhu, "SmartGuard: Making prediction verifiable through transaction sequences for smart contract vulnerability detection," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 6117–6132, 2025.
- [7] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack," *Journal of Cases on Information Technology (JCIT)*, vol. 21, no. 1, pp. 19–32, 2019.
- [8] D. Liu, J. Zhang, Y. Wang, H. Shen, Z. Zhang, and T. Ye, "Blockchain smart contract security: Threats and mitigation strategies in a lifecycle perspective," ACM Comput. Surv., Sep. 2025.
- [9] B. Wang, Y. Tong, S. Ji, H. Dong, X. Luo, and P. Zhang, "A review of learning-based smart contract vulnerability detection: A perspective on code representation," ACM Trans. Softw. Eng. Methodol., Jul. 2025.
- [10] J. Feist, G. Grieco, and A. Groce, "Slither: A static analysis framework for smart contracts," in 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2019, pp. 8–15.
- [11] C. Chen, J. Su, J. Chen, Y. Wang, T. Bi, J. Yu, Y. Wang, X. Lin, T. Chen, and Z. Zheng, "When ChatGPT meets smart contract vulnerability detection: How far are we?" ACM Transactions on Software Engineering and Methodology, vol. 34, no. 4, pp. 1–30, 2025.
- [12] Y. Liu, Y. Xue, D. Wu, Y. Sun, Y. Li, M. Shi, and Y. Liu, "PropertyGPT: LLM-driven formal verification of smart contracts through retrievalaugmented property generation," arXiv preprint arXiv:2405.02580, 2024.
- [13] B. Boi, C. Esposito, and S. Lee, "Smart contract vulnerability detection: The role of Large Language Model (LLM)," ACM SIGAPP Applied Computing Review, vol. 24, no. 2, pp. 19–29, 2024.
- [14] J. Yu, "Retrieval augmented generation integrated large language models in smart contract vulnerability detection," arXiv preprint arXiv:2407.14838, 2024.

- [15] Y. Sun, D. Wu, Y. Xue, H. Liu, H. Wang, Z. Xu, X. Xie, and Y. Liu, "GPTScan: Detecting logic vulnerabilities in smart contracts by combining GPT with program analysis," in *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, ser. ICSE '24. Association for Computing Machinery, 2024.
- [16] S. Lin, L. Yang, Z. He, D. Fan, and J. Zhang, "MetaGater: Fast learning of conditional channel gated networks via federated meta-learning," in 2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, 2021, pp. 164–172.
- [17] J. Choi, D. Kim, S. Kim, G. Grieco, A. Groce, and S. K. Cha, "SMAR-TIAN: Enhancing smart contract fuzzing with static and dynamic data-flow analyses," in 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE, 2021, pp. 227–239.
- Automated Software Engineering (ASE). IEEE, 2021, pp. 227–239.
 T. Abdellatif and K.-L. Brousmiche, "Formal verification of smart contracts based on users and blockchain behaviors models," in 2018 9th IFIP international conference on new technologies, mobility and security (NTMS). IEEE, 2018, pp. 1–5.
- [19] R.-Y. Choi, Y. Song, M. Jang, T. Kim, J. Ahn, and D.-H. Im, "Smart contract vulnerability detection using large language models and graph structural analysis." *Computers, Materials & Continua*, vol. 83, no. 1, 2025.
- [20] J. Kevin and P. Yugopuspito, "SmartLLM: Smart contract auditing using custom generative AI," in 2025 International Conference on Computer Sciences, Engineering, and Technology Innovation (ICoCSETI). IEEE, 2025, pp. 260–265.
- [21] Y. Jin, C. Li, P. Fan, P. Liu, X. Li, C. Liu, and W. Qiu, "LLM-BSCVM: An LLM-based blockchain smart contract vulnerability management framework," arXiv preprint arXiv:2505.17416, 2025.
- [22] N. Ding, X. Lv, Q. Wang, Y. Chen, B. Zhou, Z. Liu, and M. Sun, "Sparse low-rank adaptation of pre-trained language models," arXiv preprint arXiv:2311.11696, 2023.
- [23] Y. Hu, J. Zhang, X. Chen, Z. Zhao, C. Li, and H. Chen, "LoRS: Efficient low-rank adaptation for sparse large language model," arXiv preprint arXiv:2501.08582, 2025.
- [24] A. Han, J. Li, W. Huang, M. Hong, A. Takeda, P. K. Jawanpuria, and B. Mishra, "SLTrain: a sparse plus low rank approach for parameter and memory efficient pretraining," *Advances in Neural Information Processing Systems*, vol. 37, pp. 118 267–118 295, 2024.
- [25] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Ethereum smart contract analysis tools: A systematic review," *Ieee Access*, vol. 10, pp. 57 037–57 062, 2022.
- [26] M. Almakhour, L. Sliman, A. E. Samhat, and A. Mellouk, "A formal verification approach for composite smart contracts security using FSM," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 70–86, 2023.
- [27] J. Huang, K. Zhou, A. Xiong, and D. Li, "Smart contract vulnerability detection model based on multi-task learning," *Sensors*, vol. 22, no. 5, p. 1829, 2022.
- [28] C. Wang, W. Zhang, Z. Su, X. Xu, and X. Zhang, "Sanitizing large language models in bug detection with data-flow," in *Findings of the Association for Computational Linguistics: EMNLP 2024*, 2024, pp. 3790–3805.
- [29] G. Yu, L. Liu, H. Jiang, S. Shi, and X. Ao, "Retrieval-augmented few-shot text classification," in *Findings of the Association for Computational Linguistics: EMNLP 2023*, 2023, pp. 6721–6735.
- [30] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "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, volume 1 (long and short papers), 2019, pp. 4171–4186.
- [31] S. Kornblith, M. Norouzi, H. Lee, and G. Hinton, "Similarity of neural network representations revisited," in *International conference* on machine learning. PMIR, 2019, pp. 3519–3529.
- [32] C. Liu, C. Lou, R. Wang, A. Y. Xi, L. Shen, and J. Yan, "Deep neural network fusion via graph matching with applications to model ensem-

- ble and federated learning," in *International Conference on Machine Learning*. PMLR, 2022, pp. 13 857–13 869.
- [33] C. Sendner, H. Chen, H. Fereidooni, L. Petzi, J. König, J. Stang, A. Dmitrienko, A.-R. Sadeghi, and F. Koushanfar, "Smarter contracts: Detecting vulnerabilities in smart contracts with deep transfer learning." in NDSS, 2023.
- [34] M. Rossini, M. Zichichi, and S. Ferretti, "Smart contracts vulnerability classification through deep learning," in *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '22. New York, NY, USA: Association for Computing Machinery, 2023, p. 1229–1230.
- [35] T. Jiao, Z. Xu, M. Qi, S. Wen, Y. Xiang, and G. Nan, "A survey of Ethereum smart contract security: Attacks and detection," *Distributed Ledger Technologies: Research and Practice*, vol. 3, no. 3, pp. 1–28, 2024.
- [36] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 2018, pp. 67–82.
- [37] T. Dettmers, R. Svirschevski, V. Egiazarian, D. Kuznedelev, E. Frantar, S. Ashkboos, A. Borzunov, T. Hoefler, and D. Alistarh, "SpQR: A sparse-quantized representation for near-lossless LLM weight compression," arXiv preprint arXiv:2306.03078, 2023.
- [38] E. J. Hu, Y. Shen, P. Wallis, Z. Allen-Zhu, Y. Li, S. Wang, L. Wang, W. Chen et al., "LoRA: Low-rank adaptation of large language models." ICLR, vol. 1, no. 2, p. 3, 2022.
- [39] S. Robertson, "BM25 and all that-a look back," in Proceedings of the 48th International ACM SIGIR Conference on Research and Development in Information Retrieval, 2025, pp. 5–8.
- [40] M. Hirzel, S. Schneider, and K. Tangwongsan, "Sliding-window aggregation algorithms: Tutorial," in *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems*, 2017, pp. 11–14.
- [41] D. Zhu, L. Wang, N. Yang, Y. Song, W. Wu, F. Wei, and S. Li, "LongEmbed: Extending embedding models for long context retrieval," in *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing*. Miami, Florida, USA: Association for Computational Linguistics, Nov. 2024, pp. 802–816.
- [42] W. X. Zhao, J. Liu, R. Ren, and J.-R. Wen, "Dense text retrieval based on pretrained language models: A survey," ACM Transactions on Information Systems, vol. 42, no. 4, pp. 1–60, 2024.
- [43] Y. Mao, Z. Wang, W. Liu, X. Lin, and P. Xie, "Metaweighting: Learning to weight tasks in multi-task learning," in *Findings of the Association* for Computational Linguistics: ACL 2022, 2022, pp. 3436–3448.
- [44] T. Iwata, A. Kumagai, and Y. Ida, "Meta-learning task-specific regularization weights for few-shot linear regression," in *The 28th International Conference on Artificial Intelligence and Statistics*, 2025.
- [45] C. S. Yashavant, S. Kumar, and A. Karkare, "ScrawlD: A dataset of real world Ethereum smart contracts labelled with vulnerabilities," arXiv preprint arXiv:2202.11409, 2022.
- [46] C. Wang, X. Liu, and A. H. Awadallah, "Cost-effective hyperparameter optimization for large language model generation inference," in *Inter*national Conference on Automated Machine Learning. PMLR, 2023, pp. 21–1.
- [47] T. Dettmers, A. Pagnoni, A. Holtzman, and L. Zettlemoyer, "QLoRA: Efficient finetuning of quantized LLMs," *Advances in neural information processing systems*, vol. 36, pp. 10088–10115, 2023.
- [48] Y. Xu, L. Xie, X. Gu, X. Chen, H. Chang, H. Zhang, Z. Chen, X. Zhang, and Q. Tian, "QA-LoRA: Quantization-aware low-rank adaptation of large language models," arXiv preprint arXiv:2309.14717, 2023.
- [49] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," Advances in neural information processing systems, vol. 30, 2017.