# Data Transmission Reliability Detection of Hybrid Information System Based on Smart Contract

Huan-yu Wang[1](✉) and Xiao-gang Ma[2]

[1] College of Earth Environment and Science, Southwest Jiao Tong University,
Chengdu 611756, China
why1924984571@163.com

[2] Shandong Vocational College of Science and Technology, Weifang 261053, China

**Abstract.** There is a large amount of data in the information system, but the calculation process of the data transmission reliability detection method of the previous manual detection system is complex, and it is difficult to ensure the accuracy of the detection. Therefore, a data transmission reliability detection method of hybrid information system based on Intelligent contract is proposed. On the basis of designing the detection rules and design rule reuse rate compiler of the front-end input module, the system data stream used for detection is set. The machine learning algorithm is used to test the reliability of data transmission in the hybrid information system. The experimental results show that the hit rate of data transmission reliability detection based on smart contract is 96.9%, and the false alarm rate is 15.3%. Compared with mythirl tool and manual detection method, it improves the accuracy of data transmission reliability detection.

**Keyword:** Smart contract · Information system · Data transmission · Reliability monitoring

## 1 Introduction

Smart contract is the networked representation of traditional contract or protocol, which needs to be stored on the blockchain platform; At the same time, according to the contract code logic, the user input is received and the appropriate output is obtained. Traditional contracts need mutual trust agreements signed by two or more parties, so smart contracts should also meet the trust of the whole network blockchain user nodes [1]. Smart contract can have a secure and stable storage medium and operating environment, precisely because the blockchain of smart contract has the characteristics of decentralization, information transparency and difficult to tamper, which greatly expands the scope of application. However, the key feature of smart contract is that its execution does not rely on any credit endorsement, and the execution of various terms in the contract does not need to rely on an authoritative third party.

S. Wang et al. (Eds.): IoTCare 2021, LNICST 415, pp. 3–18, 2022.
https://doi.org/10.1007/978-3-030-94182-6_1

The traditional data transmission reliability detection method of hybrid information system is difficult to effectively use the contract, which leads to the poor reliability of the detection results. Therefore, this paper proposes a data transmission reliability detection method of hybrid information system based on Intelligent contract, which transforms the fault analysis problem into a logical analysis problem, rather than a physical analysis problem [2]. For the logical behavior of data transmission reliability, it is difficult to analyze its failure mode. Usually, several defects can be mapped into a fault model, or a many to one mapping. The data transmission reliability detection of hybrid information system based on smart contract is to analyze from the aspects of architecture security analysis, source code vulnerability analysis, binary vulnerability analysis and operating system vulnerability analysis, so as to find the vulnerability of data transmission reliability. This can not only effectively detect the code defects of the contract, but also ensure the high security of the hybrid information system based on smart contract, so it has a wide application prospect [3].

## 2 Data Transmission Reliability Detection Method of Hybrid Information System Based on Smart Contract

With the rapid development of integrated circuit technology, the traditional bus or point-to-point interconnection structure has become increasingly serious in scalability, communication efficiency, power consumption and other aspects, and data transmission has become a prominent performance bottleneck. Therefore, the data transmission of the hybrid information system describes the failure effect through the changes derived from the signals in the circuit or system [4]. For the reliability detection of data transmission in the hybrid information system of smart contract, the fault model is used in the circuit detection instead of the failure mode.

### 2.1 Front End Input Module

The front end of hybrid information system based on smart contract is mainly responsible for analyzing and inputting the types of smart contract, and selecting the detection rules of different data transmission according to the development language or bytecode type [5]. The front-end input module of the hybrid information system is mainly to receive the smart contract provided by the user, analyze the specific types of the contract content, and select the appropriate data transmission detection rules. At present, data transmission reliability detection of hybrid information system based on smart contract supports Ethereum, EOS, ont and other blockchain platforms. The types and suffixes of smart contracts corresponding to these platforms are shown in Table 1.

Because Ethereum bytecode is a series of bytes array generated directly, it is not saved in specific file, so it can not be judged directly by suffix [6]. Therefore, the user can select the correct data transmission reliability detection rules by specifying the contract type parameters. After selecting the type of intelligent contract, the front-end input module of hybrid information system needs to judge the current version according to the declaration information in the intelligent contract, so as to ensure that the subsequent modules can be correctly executed.

**Table 1.** Smart contract information supported by front end input module

| Blockchain platform | Smart contract | Source code | Bytecode |
|---|---|---|---|
| Ethernet | Solidity | .sol | / |
| | Vyper | .vy | / |
| EOS | C++ | .cpp | .wasm |
| ONT | Python | .py | .avm |

The use of rigorous mathematical reasoning and logical proof is the key to test the attribute security and function correctness of intelligent contract. The hybrid information system based on Intelligent contract can completely cover the behavior during code execution, thus eliminating all possible input defects in traditional testing methods. At the same time, it ensures the absolute correctness of intelligent contract in a certain range, and provides some assistance for formal verification of intelligent contract through the semantic representation of virtual machine.

In the front-end design of hybrid information system of intelligent contract, CORBA is a specified document, which is mainly used to describe the transmission data. To some extent, CORBA can provide a good technical standard for hybrid information system distributed in abnormal environment. CORBA specifies that documents can interact effectively with data in different programming languages or operating systems. In addition, CORBA provides that simultaneous interpreting of different transmission data can be considered as an object in the front end design of mixed information system, whether it runs on the client side or server side.

Each CORBA specification document will publish an interface within the hybrid information system, which lists its methods and the data types it supports. At the same time, CORBA is an image of server application in hybrid information system, and it is not related to its language program. Java, as well as c+ language, are the main programming languages in the system, and each server needs to follow the interface definition principles.

Based on the specification of CORBA, DCOM can effectively solve the limitation of the front end of hybrid information system. DCOM can make the data transfer location transparent, and in general, the way that the customer connects the component and invokes the component is the same.

In addition, in DCOM hybrid information system, its location is obviously independent, which can effectively simplify the detection process in the process of data transmission. The location independence flow of DCOM in the system is shown in Fig. 1.

In the design of the front-end module of hybrid information system, DCOM detects the reliability of data transmission by keeping an index count for each component. But in the process of data transmission, hybrid information system based on Intelligent contract can not only transmit to one customer, but also can be shared by multiple customers.

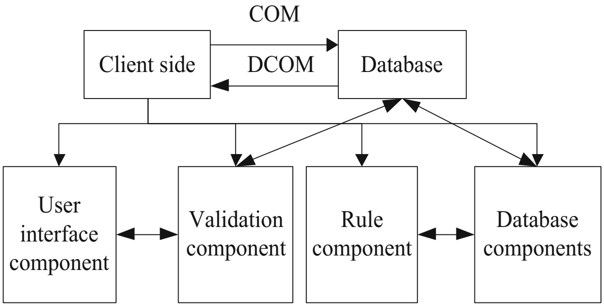

**Fig. 1.** Location independence

Due to the independence of DCOM in the system, it is necessary to transfer the distributed components of the front end of the system to other servers. Meanwhile, DCOM, which has no state or need not share with other components, can run on different servers and even generate multiple copies of data transmission detection in hybrid information system. When DCOM is used in the front end of the system, it is very easy to change the process of data transmission, but the same data transmission channel does not need to change the transmission path or recompile it.

In the front-end design of the hybrid information system of intelligent contract, the whole system shares a database and adopts the distributed application server. During data transmission, the application server is set up, and each system program server needs to be configured with two network connections. One connects to the database server through its internal network, while the other connects to the LAN to serve the client. The network structure of hybrid information system is shown in Fig. 2.

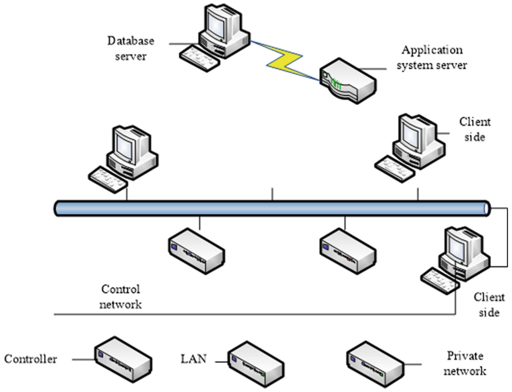

**Fig. 2.** Network structure of hybrid information system

In the front-end design of the hybrid information system of smart contract, a three-tier distributed architecture is adopted. The C/S part is developed by Delphi 7, while the B/S part is developed by Delphi 7 ASP.NET development. In the whole mixed information system, there are both C/S programs and B/S mixed mode in some interfaces, that is, browser is embedded to access B/S pages on the server side. To a certain extent, the system structure based on CS/BS mixed mode can greatly improve the superiority of DCOM through the operation effect of HTTP mode.

### 2.2 Compiler Module

The data transmission of hybrid information system based on smart contract first needs to collect a large number of verified smart contract transmission data, and label them manually and by tool scanning. Before compiling the transmission data in the hybrid information system, we need to abstract the source code, bytecode and operation code, and pave the way for the subsequent feature extraction.

In the compiler module of hybrid information system based on smart contract, it mainly includes: lexical analysis, semantic analysis, intermediate code generation, code optimization, code generation and other steps [7]. Among them, lexical analysis and syntax analysis reorganize the input smart contract into an abstract syntax tree, and the code generation part outputs the bytecode of the contract, which can be used for the analysis of data transmission reliability detection.

Through the one vs. rest strategy based on the smart contract hybrid information system to transmit data for multi label classification. At the same time, in order to keep the balance of the number of samples between training sets, we need to balance the vulnerability of dependence on data transmission order, the vulnerability of not checking return value in the process of data transmission, the vulnerability of dependence on data transmission timestamp, and the vulnerability of code reentry in the process of data transmission by smote and smotetomek. The flow chart is shown in Fig. 3.

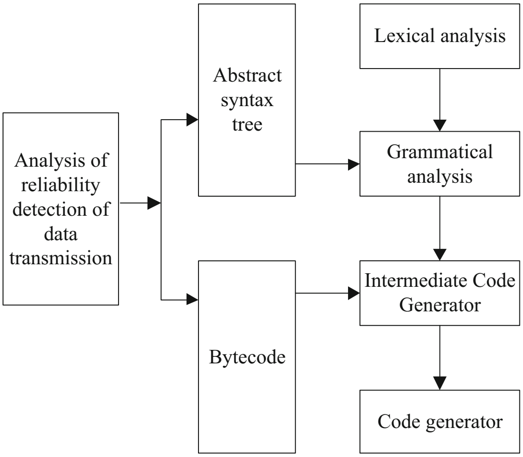
Analysis of reliability detection of data transmission
Abstract syntax tree
Bytecode
Lexical analysis
Grammatical analysis
Intermediate Code Generator
Code generator

**Fig. 3.** Compiler module flow of data transmission reliability monitoring system

In the hybrid information system based on smart contract, the compiler module is designed mainly around the development language of smart contract. In the data transmission detection and analysis of the system, the smart contract source code of the front-end input module can be divided into four types: C++, python, solidness and Vyper [8]. By using llvm and other compiler framework systems, different development languages are converted into the same set of intermediate code to generate the same bytecode. At this time, the data transmission reliability analysis module only needs to design rules for different types of smart contracts at the level of abstract syntax tree, and can share a set of rules at the level of intermediate code and bytecode to improve the reuse rate of rules.

However, most of the hybrid information systems based on smart contracts have official compilers, and the data transmission reliability test results of different contracts are often different. Using a common compilation framework will inevitably lead to problems such as difficult development and long-term maintenance. In addition, the data transmission detection of the hybrid information system also needs to consider the case that the input is the on chain bytecode of the smart contract [9]. Therefore, in the hybrid information system based on smart contract, the design scheme of compiler module for data transmission reliability detection and analysis is to integrate the official compiler module of each smart contract. At the same time, the implementation interface is provided for the new compiler to facilitate the subsequent expansion. The structure of the compiler module in the data transmission detection system is shown in Fig. 4.

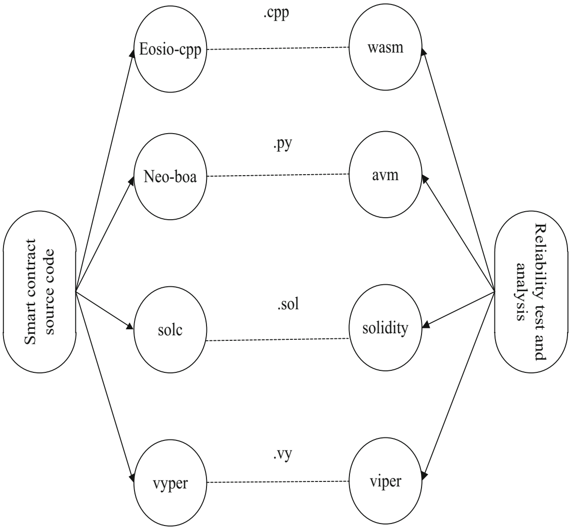

**Fig. 4.** Compiler module structure of data transmission reliability testing system

According to the hybrid information system of smart contract, the official compiler tools of smart contract are eosin CPP, Neo boa, Solc and Vyper. Eosin CPP is a tool chain of eosin. CDT, which can compile EOS smart contract into wasm bytecode and generate corresponding ABI file. Neo boa compiler module supports Python language subset. The purpose is to compile Python smart contract on ont platform into. AVM format and run it on Neo virtual machine. Both Solc and Vyper are compiler tools for

Ethereum smart contract. The former is for solidness smart contract, and the latter is Viper smart contract. Both of them provide the output interface of abstract syntax tree.

## 2.3 Data Parameter Setting of Mixed Information System

As a program analysis technology, the hybrid information system based on smart contract provides powerful and accurate formal verification. In the mixed information system, the execution data symbol is a function that uses the symbolic value instead of the input data to transform the program input into the symbolic input. In addition, in the hybrid information system, it can not only run directly on the virtual machine bytecode, but also provide the function of compiling solid source code.

In this paper, we analyze and deal with some specific vulnerabilities of smart contract, such as exception of error handling, transaction order dependence, timestamp dependence, and reentry. In view of the arrival execution path and the output of reliability parameters in the hybrid information system, different smart contracts are used to detect vulnerabilities.

The data flow analysis is a technology used to collect the information of computer programs at different points, which is widely used in the process of program compilation and optimization. Because some characteristics or properties of program data flow are closely related to the reliability of data transmission [10–13]. Therefore, data flow analysis can also be used as an important data transmission reliability detection and analysis technology.

In the data transmission reliability detection and analysis of hybrid information system based on smart contract, data flow analysis technology can be directly applied to the analysis of system software, and analyze the loopholes or defects of various data transmission reliability detection. In addition, data flow analysis is also a supporting technology of data transmission reliability detection vulnerability analysis, which can provide important data support for other vulnerability analysis methods.

In the vulnerability analysis of data transmission reliability detection, data flow analysis can be divided into flow insensitive analysis, flow sensitive analysis and path sensitive analysis according to the analysis accuracy of program path. One form of data flow analysis is to establish a data flow equation for a node in the control flow graph, and then solve it repeatedly through iterative calculation until it reaches a fixed point. The function of data flow analysis is relatively powerful, and it is generally combined with control flow information to solve the active variables with simple operation.

When setting the reliability detection parameters of data transmission based on Intelligent contract, the basic idea is an automatic vulnerability detection technology based on defect injection. It mainly uses the input of a large amount of abnormal data to the target program and monitors the running state of the target program, and uses whether there is any abnormality in the program as a sign to determine whether there is a potential vulnerability. Among them, the abnormal data detected is also called semi effective data. Without changing the parameter type, it will directly lead to the crash of hybrid information system or error triggered related loopholes in the process of data transmission.

In practical application, the hybrid information system based on Intelligent contract is deployed on the public chain. Its deployment and execution contract need to be verified by the generation of new area blocks. Therefore, on the basis of building private chain, the contract to be tested is deployed to the private chain for testing. Under the premise of deploying public chain, we need to have private chain account when the mixed information system is set up initially, so as to reduce the waiting for data transmission detection on the public chain. Therefore, the specific flow of data transmission reliability detection of intelligent contract is shown in Fig. 5:

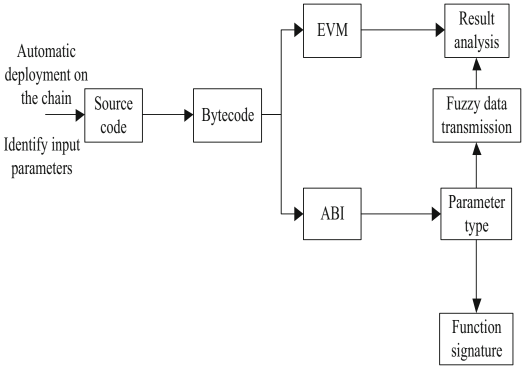

**Fig. 5.** Data transmission reliability detection process based on smart contract

To sum up, the deployment and execution of data transmission on the blockchain are realized through shell programming. Therefore, an automatic deployment tool based on smart contract is designed, including compiler call, smart contract deployment with geth, and contract code conversion. In the process of analyzing the data transmission reliability of hybrid information system, it is necessary to extract the data type of each ABI function parameter and the signature of the function used in each ABI function. For the fixed length input parameter type in the hybrid information system, it can realize the effective input generated randomly in the system. For the input parameter type with non fixed length, a positive number should be randomly generated as the length, and then selected randomly from the input field.

The data transmission reliability test of hybrid information system based on smart contract is carried out through Etherscan website etherscan.io/contractsVerified. You can view a contract list page on the web page. The list of data transmission reliability detection and analysis based on smart contract in hybrid information system shows the contract address, contract name, contract compiler version, encrypted data transmission capacity owned by the contract, and contract verification time and other important information of each smart contract. Click each contract link in the list to get to the details page of the corresponding smart contract.

In order to obtain a large number of required source code data of smart contract, it is necessary to use web crawler technology to automatically capture a large number of program scripts of Internet information according to preset rules. Web crawler starts from one or more seed URLs and gradually extends to the whole web page of the target website. Generally, crawling strategies can be divided into depth first strategy and breadth first strategy. This time, the depth first strategy is adopted for crawling, and the specific process is shown in Fig. 6.

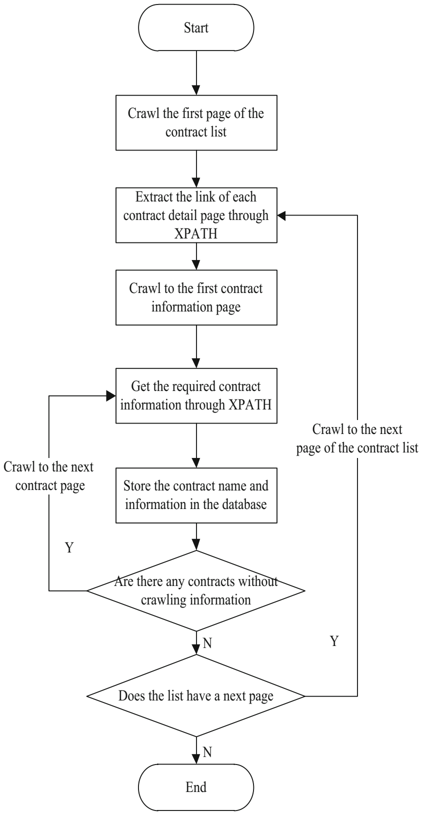
Start
Crawl the first page of the contract list
Extract the link of each contract detail page through XPATH
Crawl to the first contract information page
Get the required contract information through XPATH
Store the contract name and information in the database
Are there any contracts without crawling information
Crawl to the next contract page
Y
N
Crawl to the next page of the contract list
Y
Does the list have a next page
N
End

**Fig. 6.** Smart contract crawling process

XPath is a language used to determine the location of elements in XML or HTML markup language. Web crawlers usually use XPath to find the target elements in HTML. In addition, in order to speed up the crawling process, we need to optimize the crawling process with multiple threads.

In order to make different parallel threads cooperate with each other better, and prevent the crawling efficiency from decreasing due to the repeated data crawling, it is necessary to add crawling status fields in the database, with 0, 1 and 2 representing the three states of not crawling, crawling and crawling respectively. At the same time, the data transmission reliability detection of hybrid information system based on smart contract needs to lock the token table every time the crawling state is changed, so as to prevent multiple threads from crawling the same token repeatedly and affect the crawling rate.

## 2.4 Application of Machine Learning Algorithm to Realize Detection

The reliability detection of data transmission in hybrid information system based on Intelligent contract needs to compile the source code into bytecode through the Solc compiler after climbing to the source code of the intelligent contract solidity. However, solidity language is a young language, and its version updates are very frequent. In the crawled intelligent contract data, different versions of solidity source code will be successfully compiled into hexadecimal byte code. At the same time, according to the corresponding relationship between byte code and operation code specified in intelligent contract, the corresponding relationship is mapped into data dictionary, and then byte code is analyzed into the operation code data stream according to data dictionary. According to statistics, after data preprocessing, the average length of each contract operating code is 4364.

At the same time, in the process of data transmission reliability detection of intelligent contract hybrid information system, it will appear on the basis of existing legal test input, and can generate reliable data transmission channel through random mutation strategy, boundary value variation strategy and phase variation strategy. However, it is blind to generate completely random data transmission in hybrid information system. To some extent, not only the efficiency of reliability detection is greatly reduced, but also the coverage of transmission data code can not be effectively improved.

Based on the analysis of the stain in the intelligent contract, the input data is screened and classified, and the genetic algorithm provides guidance for the reliability detection of the transmission data in the system. By simulating the optimal solution algorithm of data transmission reliability in hybrid information system, the recombining, mutation and selection of the algorithm are introduced into the solution calculation of the optimal solution.

While retaining the optimal individual locally, the better individuals are obtained through cross, mutation and selection, and the optimal detection results of data transmission reliability are obtained through iteration. The specific data transmission reliability detection flow is shown in Fig. 7:

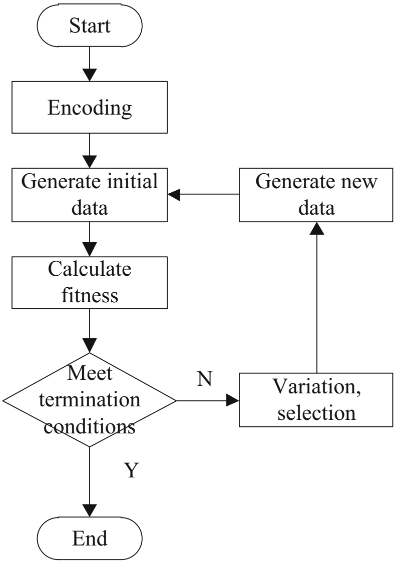

**Fig. 7.** Detection algorithm flow

If we use n-gram algorithm to extract features directly for all opcodes, because there are many kinds of opcodes and a large number of different operands, it will lead to too many features and cause dimension disaster. Through the analysis of the characteristics of solidness opcodes, it is found that many opcodes have similar functions, and some opcodes have similar vulnerability effects on data transmission reliability detection. The abstract rules of opcode are shown in Table 2.

**Table 2.** Opcode abstraction rules

| Abstract opcode | Original opcode |
|---|---|
| ARITHMETIC_OP | ADD, MUL, SUB, DIV, SDIV, SMOD, MOD, EXP |
| CONSTANT1 | BLOCKHASH, TIMESTAMP, NUMBER, DIFFICULTY, GASLIMIT |
| CONSTANT2 | ADDRESS, ORIGIN, CALLER |
| COMPARISON | LT, GT, SLT, SGT |
| LOGIC_OP | AND, OR, XOR, NOT |
| DUP | DUP1-DUP16 |
| SWAP | SWAP1-SWAP16 |
| PUSH | PUSH5-PUSH32 |
| LOG | LOG1-LOG4 |

In the data transmission reliability detection of hybrid information system based on smart contract, each PUSH instruction is followed by an operand. The number of operands varies from 1 byte to 32 bytes. These operands have little connection with the data transmission reliability detection and can be deleted.In addition, BLOCKHASH, TIMESTAMP, NUMBER, DIFFICULTY, GASLIMIT and COINBASE in class block information represent the information of the block, so they are classified into one category. After opcode abstraction, more than 140 opcodes are abstracted into more than 50, which greatly reduces the difficulty of feature dimension and machine learning model training in the subsequent feature extraction process.

By constructing the characteristic matrix $FS$, each smart contract has a corresponding characteristic vector in the matrix. The specific expression is as follows:

$$FS = \begin{bmatrix} f_{1,1}\, f_{1,2} \cdots f_{1,1619} \\ f_{2,1}\, f_{2,2} \cdots f_{2,1619} \\ \cdots \\ f_{i,1}\, f_{i,2} \cdots f_{i,1619} \\ \cdots \end{bmatrix} \tag{1}$$

where $FS = \left[f_{i,1}\, f_{i,2} \cdots f_{i,1619}\right]$ is the eigenvector of the $i$ th contract. The eigenvalue of the eigenvector of a contract is $f_{i,j}$, which is calculated according to the ratio of the number of occurrences of each bigram in the contract to the total number of bigrams in the contract. Furthermore, it can be expressed by formula 2:

$$f_{i,j} = \frac{n_{j,ci}}{n_{all,ci}} \tag{2}$$

where $f_{i,j}$ represents the characteristic frequency of the $j$ bigram in the $i$ contract, and is a decimal number between 0 and 1. In addition, $n_{j,ci}$ represents the number of $j$ bigrams in the $i$ contract; $n_{all,ci}$ represents the total number of all bigrams in the $i$ contract. If the $j$ bigram feature is not present in the $i$ contract, the corresponding $f_{i,j}$ value is 0.

By analyzing the virtual machine operation principle of opcode rules, the abstract rules of opcode are proposed, so that the number of bigram features extracted from the abstracted opcode data stream based on n-gram algorithm is greatly reduced. In the process of data transmission reliability detection of hybrid information system based on smart contract, it is necessary to explore all executable paths in the contract. In addition, the loop body in the smart contract sometimes needs a lot of iterations and consumes a lot of detection time. Therefore, the proposed data transmission detection method based on machine learning algorithm is more suitable for fast and automatic detection of a large number of smart contract vulnerabilities.

# 3 Experiment

## 3.1 Experimental Preparation

The test of data transmission reliability of hybrid information system based on Intelligent contract. Because the development language of hybrid information system is python, the test computer needs to install Python 3.6 and configure the environment. Developers can get the reliability test and analysis results of intelligent contract data transmission by executing Python script.

The development of hybrid information system based on smart contract is based on B/S architecture, the server provides services, the core code of the system is placed on the server, the client uses the browser to access, and there is no need to install a special client program. In addition, the front page of the experimental system is built with open source DWZ framework, the background program is written with java code, and based on s2sh framework, the data storage uses MySQL database, and its server program runs in Linux environment. The specific experimental running environment is shown in Table 3.

In the experiment, when users choose to upload the source code of the smart contract solidness, they need the system background to compile the source code to generate bytecode, which is completed by the solidness compilation module. In the background of the system, the solid compiler module integrates the solcj extended class library to compile the solid source code. The solcj extended class library is the Java implementation of the solid compiler Solc.

**Table 3.** System operation environment

| Project | Model or version |
|---|---|
| Server model | ThinkServer RD640 |
| CPU | Xecn E5-2660 |
| Memory | 320 GB |
| Operating system | Ubuntu 18.04 |
| MYSQL | 5.7.26 |
| Solc | V0.4.25 |
| JDK | 1.8.0_161-b12 |

### 3.2 Experimental Process

In the experimental process of data transmission reliability detection of smart contract hybrid information system, the data transmission reliability of smart contract uploaded by users can be detected. The system requires the user to upload the source code or bytecode of the smart contract in the user interface. If the user chooses to upload the source code of the smart contract, the system background will automatically compile the source code into bytecode.

In addition, the bytecode is preprocessed in the hybrid information system, including bytecode analysis, opcode abstraction and other steps, and then the n-gram algorithm is used to extract the features of the data to obtain the feature vector of the target smart contract. Then the system loads the machine learning model trained by the existing data set in the background to detect and analyze the data transmission reliability of the smart contract, The test results can be saved in the database. The specific process is shown in Fig. 8.

In the information output module, according to the results of data transmission reliability analysis and line number mapping library, the vulnerability information of data transmission reliability detection is packaged again and output according to a certain format. Among them, in the hybrid information system, the output text format of vulnerability information of data transmission reliability detection is: contract, description, title, type, etc., while line represents the line number of data transmission reliability detection code. In addition, in order to facilitate ordinary users to use the security detection system, the front-end web page is designed to display and use the function of data transmission reliability detection and analysis of hybrid information system based on Intelligent contract, so as to improve the interactivity.

The data transmission reliability detection module is the core module of the hybrid information system. In order to get the best model for reliability detection, xgboost multi label classification model is used to detect the data transmission reliability of the target smart contract code; Then the feature vector data generated by the data preprocessing module is input into the multi label classification model loaded by the data transmission reliability detection module for reliability detection, and the prediction results are output.

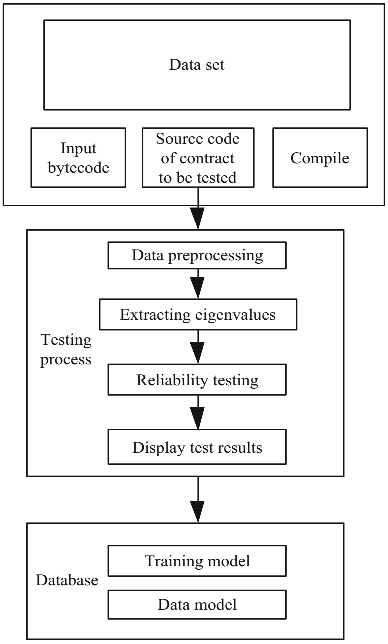

**Fig. 8.** Smart contract vulnerability detection process

### 3.3 Experimental Result

Data transmission reliability detection of hybrid information system based on smart contract refers to the number of data transmission reliability vulnerabilities that can be detected by the analysis tool of smart contract hybrid information system, and then reflects the perfection of vulnerability Library of hybrid information system. In order to detect the accuracy of data transmission reliability detection of hybrid information system based on smart contract, the two dimensions of hit rate and false alarm rate are tested and analyzed by calculating the deviation degree between the actual output and the expected result. In the case of detecting the same number of data transmission reliability test cases, the output results of the traditional monitoring method and the monitoring system based on smart contract are compared. The specific experimental comparison results are shown in Table 4.

According to the calculation results, the hit rate of data transmission reliability detection based on smart contract is 96.9%; The hit rate of mythirl tool is 36.3%; The hit rate of manual detection is only 26.7%. In addition, the false alarm rate of data transmission reliability detection of hybrid information system based on smart contract is 15.3%, which is far lower than that of mythirl tool and manual detection. Therefore, the experimental results show that the detection ability of data transmission reliability detection of hybrid information system based on smart contract is strong, and the accuracy of data transmission reliability detection is improved.

**Table 4.** Comparison of detection accuracy of various methods

| / | Detection system based on smart contract | Mythirl | Manual detection |
|---|---|---|---|
| Number of test cases | 184 | 184 | 184 |
| Total number of questions | 655 | 655 | 655 |
| Number of hits | 635 | 240 | 175 |
| Number of false positives | 115 | 226 | 167 |
| Hit rate | 96.9% | 36.6% | 26.7% |
| False positive rate | 15.3% | 48.5% | 48.8% |

## 4 Conclusion

The data transmission reliability test of a mixed information system based on smart contracts is a tool that provides symbolic abstraction methods through various security attributes in smart contracts, which can effectively detect the reliability of data transmission. This tool symbolically studies the dependency graph between the contract bytecodes, abstracts accurate semantic paradigms from it, and matches the three semantically prescribed patterns.

Compared with other methods of detecting the reliability of data transmission in the system, it greatly reduces the amount of manual tasks, and explores all contract paths by using a custom compliance model. To a certain extent, the false negatives caused by symbolic execution tools are effectively filtered, thereby improving the reliability of all possible path execution.

## References

1. Huang, Y., Li, T., Luo, C., Fujita, H., Horng, S.-J., Wang, Bin.: Dynamic maintenance of rough approximations in multi-source hybrid information systems. Information Sciences 530 (2020)
2. Li, Z., Zhang, P., Xie, N., Zhang, G., Wen, C.-F.: A novel three-way decision method in a hybrid information system with images and its application in medical diagnosis. Engineering Applications of Artificial Intelligence 92 (2020)
3. Liu, S., Liu, G., Zhou, H.: A robust parallel object tracking method for illumination variations. Mob. Netw. Appl. **24**(1), 5–17 (2018). https://doi.org/10.1007/s11036-018-1134-8
4. Zeng, J., Li, Z., Zhang, P., Wang P.: Information structures and uncertainty measures in a hybrid information system: gaussian kernel method. Int. J. Fuzzy Sys. **22**(1), 212–231 (2020)
5. Xiong, W., Xiong, L.: Data resource protection based on smart contract. Computers & Security 98 (2020)
6. Yu, G.: Information structures and uncertainty measures in a hybrid information system with images. Soft Computing **23**(24), 12961–12979 (2019)
7. Liu, S., Fu, W., He, L., Zhou, J., Ma, M.: Distribution of primary additional errors in fractal encoding method. Multimedia Tools and Applications **76**(4), 5787–5802 (2014). https://doi.org/10.1007/s11042-014-2408-1

8. Technology - Technology Research: Studies from international business machines corporation yield new data on technology research (Automatic smart contract generation using controlled natural language and template). Comp. Netw. Comm. (2019)
9. Wang, P., Zhang, P., Li, Z.: A three-way decision method based on gaussian kernel in a hybrid information system with images: an application in medical diagnosis. Appli. Soft Compu. J. **77**, 734–749 (2019)
10. Hun, K.Y.: A study on smart contract for personal information protection. J. Digi. Converg. **17**(3), 215–220 (2019)
11. Xuan, S., et al.: An incentive mechanism for data sharing based on blockchain with smart contracts. Comp. Elec. Eng. **83**, 106587 (2020)
12. ZhongAn Information Technology Service Co. Ltd.: Patent Application Titled "Smart Contract Upgrade Method And System Based On Alliance Chain" Published Online (USPTO 20190278767). Computer Technology Journal (2019)
13. Liu, S., Pan, Z., Cheng, X.: A novel fast fractal image compression method based on distance clustering in high dimensional sphere surface. Fractals **25**(4), 1740004 (2017)