# GTI Computing Force Network Service Security White Paper

| | |
|---|---|
| **Version:** | V1.0.0 |
| **Deliverable Type** | □ **Procedural Document**<br>☑ **Working Document** |
| **Confidential Level** | □ **Open to GTI Operator Members**<br>□ **Open to GTI Partners**<br>☑ **Open to Public** |
| **Working Group** | **Terminal WG** |
| **Task** | **PM3-PJ9-task5: Computing force Network Service Security White Paper** |
| **Source members** | CMCC |
| **Support members** | |
| **Editor** | Yiran Zhang(CMCC), Huizheng Geng(CMCC), Li Su(CMCC), Li Lu(CMCC)、Tingting Yang(CMCC)、Yue Wang(CMCC) |
| **Last Edit Date** | （08-25-2022） |
| **Approval Date** | |

# Document History

| Date | Meeting # | Version # | Revision Contents |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# 1 Computing Force Network Overview

## 1.1 Introduction

In order to realize ubiquitous computing capability, the computing force network has the potential demand to introduce multi-source computing force nodes such as cloud computing and edge computing. The integration of multi-source computing force and network opens the original closed network and system, then the network, applications and data have been more exposed. Therefore, the security problems commonly existing in cloud computing and edge computing will be more severe in the computing force network. In addition, due to the characteristics of wide distribution and large number of computing force nodes, it will bring some unique security and privacy protection problems. The computing force network introduces idle computing force and pan terminal equipment of third-party society such as personal terminals to perform computing tasks, while the service operators may not have full control over the nodes and cannot ensure the security and credibility of the computing nodes. Moreover, the degree of security provided by computing nodes in computing power networks also varies greatly, which greatly improves the breadth and difficulty of security protection.

## 1.2 Service Operation Mechanism

According to Figure 1-1, the service operation mechanism of the computing force network is mainly composed of four steps:

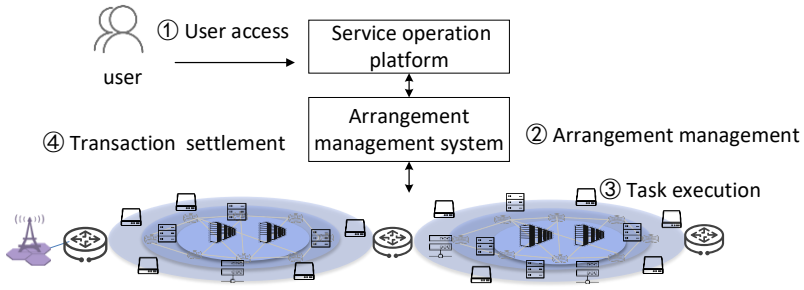


**Figure 1-1 service operation mechanism of computing force network**

1. User access: the user accesses the computing force network.
2. Arrangement management: the user uploads data to the computing force network, and the arrangement management system carries out global optimal deployment and scheduling base on the requirements of user.
3. Task execution: task execution can be carried out after the task is scheduled to the infrastructure layer of computing force network.
4. Transaction settlement: the network returns the result of task execution to the user and complete the transaction.

# 2 Security Threats

## 2.1 Threats to User Access Security

The users in computing force are computing force consumers. The complexity and diversity of computing force consumers make attackers have more opportunities to fake legitimate users to access the service or conduct unauthorized operations after legitimate users access the service, which has an impact on service stability and data security.

## 2.2 Threats to Arrangement Management Security

Since there is not a one-to-one match between the security capability of computing resources and the security requirements of computing tasks, the analysis of security capability and security requirements will affect the deployment of computing tasks on computing resources, so that the arrangement management without considering security is not suitable for computing force networks. How to introduce security policies into the existing computing force network scheduling and realize the collaborative scheduling of security, computing force and networks is the key problem.

## 2.3 Threats to Task Execution Security

The computing force network will access various forms of computing force nodes such as third-party computing force and personal terminal computing force. The security levels of these nodes are uneven, and the computing force operators do not have complete control over these computing force resources. In addition, the ubiquitous computing force nodes also make the flow of data more complex, which increases the risk of data leakage.

## 2.4 Threats to Transaction Settlement Security

The security challenges in the transaction settlement include the credibility problem of calculation results and the credibility problem of computing force transactions.

Credibility problem of calculation results: the computing force resources of the computing force network can complete the calculation, but the reliability and integrity of the calculation results cannot be guaranteed, and there is the possibility of tampering and leaking data. Firstly, the computing resource may forge data to participate in the calculation; secondly, the computing resource may not use the agreed computing force application to perform the task; finally, the computing resource may directly return the wrong calculation results inconsistent with the actual situation.

Credibility problem of computing force transaction: computing force network provides computing force transaction services, which may lead to malicious billing, evasion of billing and other repudiation behaviors.

# 3 Security Policy

## 3.1 Security of User Access

User access security is divided into the secure access of computing force consumers and the secure access of computing force providers.

The secure access of computing force consumers is to verify the identity information of each user accessing the computing force network, restrict the operations that users can perform, and protect user information by using mechanisms such as secure storage, access control, account management and operation audit, so as to prevent attackers from accessing services for network attacks or stealing sensitive information.

The secure access of computing force providers refers to the security assessment, monitoring and management of computing force nodes in the whole process. Before the computing force nodes are incorporated into the computing force network for unified arrangement and given the qualification to provide computing services, the security assessment of nodes and the provision of security access methods are carried out. After the computing force node is connected to the network, the security status of the nodes is dynamically monitored by deploying security monitoring agents on the nodes.

## 3.2 Security of Arrangement Management

This research report proposes an implementation scheme of computing force network arrangement management system, as shown in Figure 3-1. (1) Users put forward service requirements. (2) Demand analysis module analyzes user demand, and converts it into security demand, computing force demand, network demand, etc. (3) According to the result of the demand analysis module, the security arrangement module evaluate the security of computing resources, selects the data security processing method and the security calculation method. (4) According to the results of demand analysis module and security arrangement module, the computing force scheduling module and network scheduling module flexibly allocate corresponding computing, storage and network resources for users. (5) The network scheduling module and the computing force scheduling module cooperate to deploy the service gateway and route the computing task to the processing node. (6) User services are deployed.

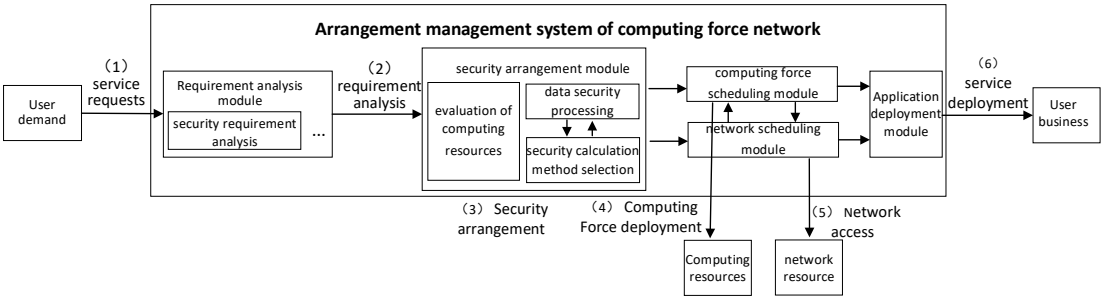


**Figure 3-1 arrangement management system of computing force network**

The security strategy of computing force network arrangement management system mainly includes the security requirement analysis in the requirement analysis module,

evaluation of computing resources, data security processing, security calculation method selection in the security arrangement module.

1. security requirement analysis

Analyze the security requirements of the service, use the security identification to classify and grade the security requirements of the computing tasks. The security requirements of computing tasks reflect the security requirements of computing tasks on the confidentiality of computing data and the accuracy of computing results, which are determined by user security requirements, computing task type, computing task data type and other computing task attributes.

2. evaluation of computing resources

The security of computing resources is classified according to the security capability, security configuration, evaluation results, supplier reputation endorsement and other dimensions of computing resources.

3. data security processing

According to the results of the security requirements analysis module and considering the cost of data security processing, the optimal data security processing methods are selected, including data desensitization, digital watermarking, and other data processing methods.

4. security calculation method selection

According to the results of the security requirements analysis module, the selection of data security processing methods is integrated, and the calculation complexity, traffic, security and precision loss of the security calculation method are considered to select the optimal security calculation method, including confidential calculation, secure multi-party calculation, federated learning and other technologies.

## 3.3 Security of Task Execution

The computing force resources of the computing force network are composed of trusted nodes and untrusted nodes. The execution modes of user computing tasks can be divided into three types: " fully-trusted mode (fully-1 model)" in which all computing tasks are completed by trusted nodes; The "untrusted mode (fully-0 model)" in which the computing task is executed in the third-party computing force node; “Mixed mode (Mixed 0-1 Mode)” in which the user performs some computing tasks on trusted nodes and some tasks on third-party computing nodes.

1. fully trusted mode

In fully trusted mode, computing force network provides users with trusted nodes, which are completely controlled and trusted nodes of computing force network. In practical applications, the nodes with the trusted computing environment are generally considered to be trusted nodes, as shown in Figure 3-2.

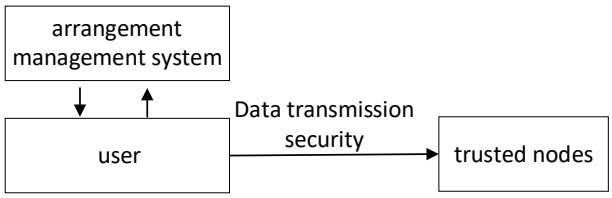


**Figure 3-2 Fully trusted mode of computing force network**

In this mode, the computing force network arrangement management system schedules the computing tasks to the trusted node to complete the calculation. The confidentiality, integrity and availability of data in the process of data calculation can be guaranteed, and only the security of data in the process of network transmission needs to be considered. Transmission security mainly ensures the security of data in the transmission process through secure transmission protocols, such as TLS, IPSec, etc.

2. untrusted mode

In the untrusted mode, the computing force network provides users with untrusted nodes, which are the third-party nodes accessing the computing force network, as shown in Figure 3-3.

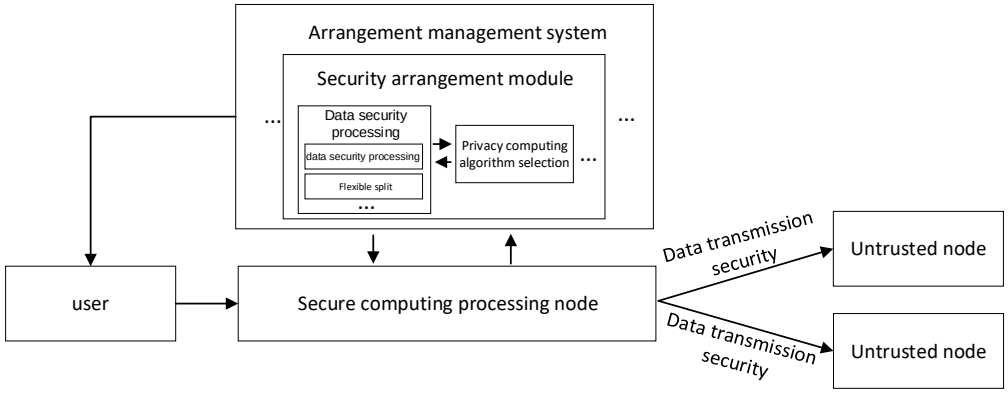


**Figure 3-3 Untrusted mode of computing force network**

In this mode, the arrangement management system schedules the computing tasks to the third-party computing force node and completes the calculation tasks. In addition to the problem of transmission security, the computing process occurs in untrusted nodes, so appropriate secure computing methods are needed to complete the computing task while ensuring the data security. Specifically, the security calculation method selection module of the arrangement management system selects the appropriate calculation method, and the data security processing module specifies the corresponding processing algorithm to safely process the user data. Additional secure computing methods and data processing algorithms will increase the amount of computing and communication. Compared with the fully trusted mode, the efficiency of computing tasks in untrusted nodes may be reduced.

3. Mixed mode

In the Mixed mode, the computing force network provides users with both trusted nodes and untrusted nodes to perform computing tasks. Computing tasks can be flexibly scheduled

among nodes with different credibility according to the characteristics of business scenarios to meet different security requirements, as shown in Figure 3-4.

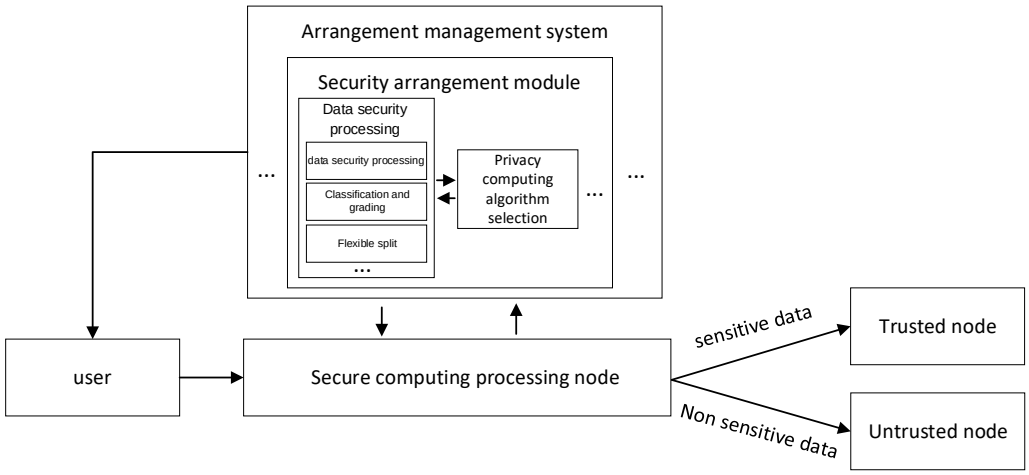


**Figure 3-4 Mixed mode of computing force network**

In this mode, the computing task is first sent to the secure computing processing node, which processes the data according to the security arrangement policy, forwards them to the trusted node and the untrusted node that cooperates to complete the computing task. The data security processing module of the arrangement management system can formulate the strategies of classification and classification, data splitting, decomposition and scheduling, split the data according to the security level, and schedule the data to the computing force nodes with different credibility respectively. Then the collaborative calculation between nodes is realized using multi-party computing technology to obtain the final calculation results.

## 3.4 Security of Transaction Settlement

The trusted mechanism of the computing force network based on blockchain is considered to solve the reliability problem of calculation results and computing force trading in the transaction settlement stage, as shown in Figure 3-5. In the operation of network services, the data to be stored on the chain includes (1) in user access stage: the computing power demand initiated by computing power consumers to computing power network; (2) in arrangement management stage: the scheduling results; (3) in task execution stage: the digital signature of user data and final calculation results; (4) in transaction settlement stage: the complete transaction information. This section introduces the security of Transaction settlement in detail from the perspective of credible result and credible transaction.

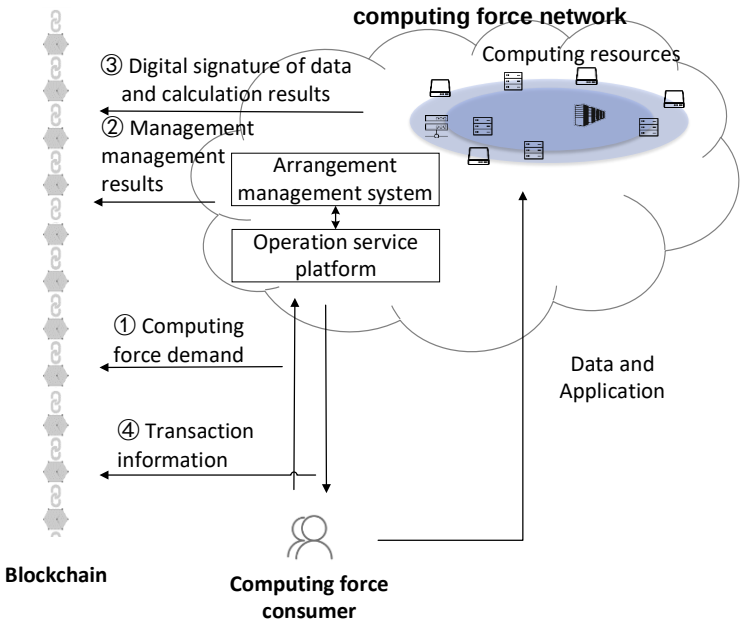


**Figure 3-5 Trusted transaction settlement method based on block chain in computing force network**

1. credible result

In order to ensure the authenticity and reliability of the calculation results, a result trusted verification method based on blockchain and digital signature in the computing force network is constructed, as shown in Figure 3-6. In the preprocessing stage, the computing force application generates a pair of application public and private keys, the private key k is built in the computing force application, and the public key $p$ is mastered by the user for signature verification.

After the computing force application receives the data, it first signs the data and the computing resource identification information ($sig_1 = Sign_k(data||ID)$, where $k$ is the private key, $data$ is the user data, and $ID$ is the computing resource identification) and uploads them to the blockchain. After the calculation of computing force application is completed, it performs the above similar steps ($sig_2 = Sign_k(res||ID)$), where $res$ is the calculation result), then $sig_1, sig_2$ are sent to the user and uploads them to the blockchain. On the one hand, the user can verify the signature successfully only if the specified computing force application performs the calculation and generates the digital signature using the built-in application private key, so as to verify the source of the calculation result and ensure that the calculation result is generated by the legal computing force node using the given data, thus proving the credibility of the calculation result. On the other hand, the digital signature chain of the calculation results makes the calculation results open and verifiable, which increases the cost of forgery, denial, data tampering and dishonest calculation, and improves the reliability of the computing network.

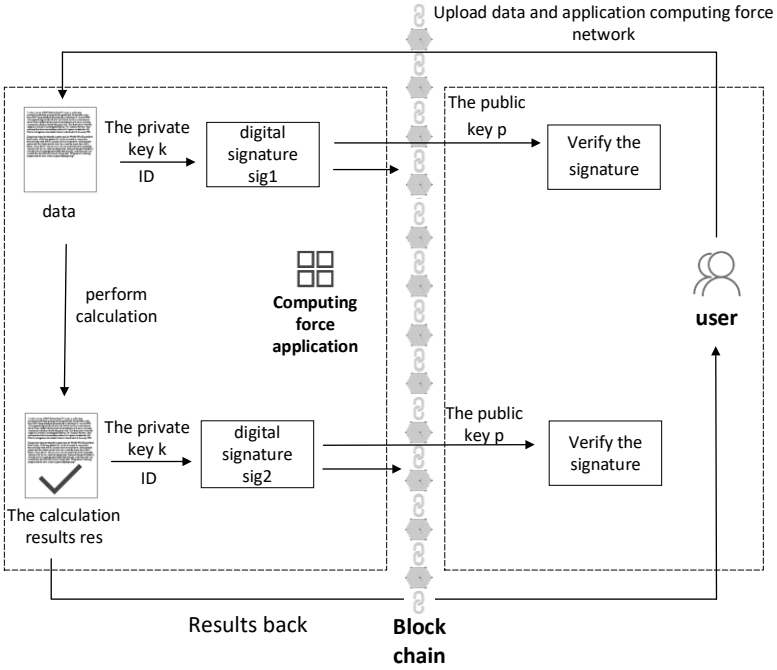


**Figure 3-6 The result trusted verification method based on blockchain and digital signature in the computing force network**

2. credible transaction

In view of the transaction reliability problem of computing force network, with the help of blockchain technology, transaction information (service object, computing force demand, computing force consumption, service time, billing information, payment information, etc.) is recorded and stored on the chain to ensure that billing can be audited and traced. In addition, the computing service requests (security requirements, computing requirements, network requirements, algorithm requirements, etc.) and the arrangement management results (computing nodes, data security processing methods, secure computing methods, etc.) related to computing transactions need to be stored in the chain to ensure mutual trust between computing force consumers and computing force networks.

# 4 Outlook

The computing force network interconnects distributed computing nodes, coordinates scheduling, and provides users with the best resource allocation and network connection scheme through the improvement of network architecture and protocols, so as to achieve the optimal use of network resources. With the development of computing force network, we will carry out overall construction on the basis of the current network security to ensure a secure computing force network service operation environment.