# AN END-TO-END TRUSTWORTHY SCHEME FOR GREEN COMMUNICATIONS

*Qin Qiu[1]; Tianni Xu[1]; Gaoshan Zhang[2]; Hua Zhu[2]; Ben Zhou[2]*

[1]China Mobile Communications Group Co., Ltd

[2]Organization: China Mobile Group Design Institute Co., Ltd.

## ABSTRACT

*Energy conservation has become a worldwide consensus in recent years. The Chinese government has proposed the east-data-west-computing project to develop large-scale cross-regional green communications and computing. In the process of balancing computing and energy resource demands between the eastern and western regions, the security concern of cross-regional data circulation rises. This paper presents a trustworthy scheme to address the problem of untrusted computing nodes, immature computing security capabilities, and unsecured data transmission within cross-regional data circulation. The solution focuses on building a secure and trustworthy environment to protect the device and data, ensuring the confidentiality, integrity, and availability of data usage. Practical deployment and testing have demonstrated that our solution can effectively safeguard data privacy and security in the carrier's networks, enhancing the encryption performance of security services by more than 20 times, providing a new security paradigm for the efficient and green development of the communications industry.*

**Keywords** – Green Communications, the East-data-west-computing Project, Data Security, Trustworthy Scheme

## 1. INTRODUCTION

To adhere to a path of green, environmentally friendly, and sustainable development, China has promoted the construction of the east-data-west-computing project. With the goal of green communications, the project encourages the migration of data centers to the western regions. Leveraging the abundant renewable energy resources in the west regions, it supports the storage and computing of data from the east regions, effectively reducing carbon emissions in the telecommunications industry.

CNC (Coordination of Networking and Computing) [1] is the core technical concept to achieve the east-data-west-computing project, which is implemented through a resource scheduling system by integrating distributed computing and networking resources, achieving efficient resource allocation through real-time perception and scheduling. However, as the project progresses, new security issues have arisen with the cross-regional data transmission. Particularly, challenges related to data and device security have become key obstacles to further development. During the collection, transmission, and computing of data, there are three main security concerns, including untrusted computing noes, immature computing security capabilities, and unsecured data transmission.

**1) Untrusted computing nodes:** The ubiquitous connection of various computing nodes in the computing network, such as clouds, edges, and terminals, leads to complex and diverse security exposure surfaces. However, the authentication mechanism of ubiquitous computing nodes is not yet established. In addition, the security capability between computing nodes is different, and the credibility evaluation and security authentication mechanism of computing nodes are not yet mature.

**2) Immature computing security capabilities:** The computing power of ubiquitous computing nodes varies and has differences in security capabilities. Trusted computing and security capabilities such as TEE (Trusted Execution Environment) are not commonly deployed on computing devices. Security risks exist in the computing environment during sensitive data processing.

**3) Unsecured data transmission:** The security and reliability of data transmission between computing nodes is the basic requirement of computing network security. In east-data-west-computing project, data is transmitted across nodes and levels, resulting in risks such as theft and tampering.

To address these security problems, this paper proposes a solution and has conducted practical verification. The results show that our solution can effectively secure the data transmission process, and speeds up the encryption performance by more than 20 times compared with off-the-shelf encryption algorithms.

## 2. END-TO-END TRUSTWORTHY SCHEME DESIGN

To solve the problems of untrusted computing nodes, immature computing security capabilities, and unsecured

data transmission, this paper proposes a solution including confidential computing, blockchain, and high-speed encryption. The solution covers the life cycle of data transmission from the east region to the west region, starting from the certification of scaled computing devices, establishing a trustworthy environment for heterogeneous computing nodes, securing data transmission under dynamic conditions, and ensuring the fidelity of cross-domain data content. This aims to safeguard the entire security and trustworthiness of computing nodes and network transmission. .

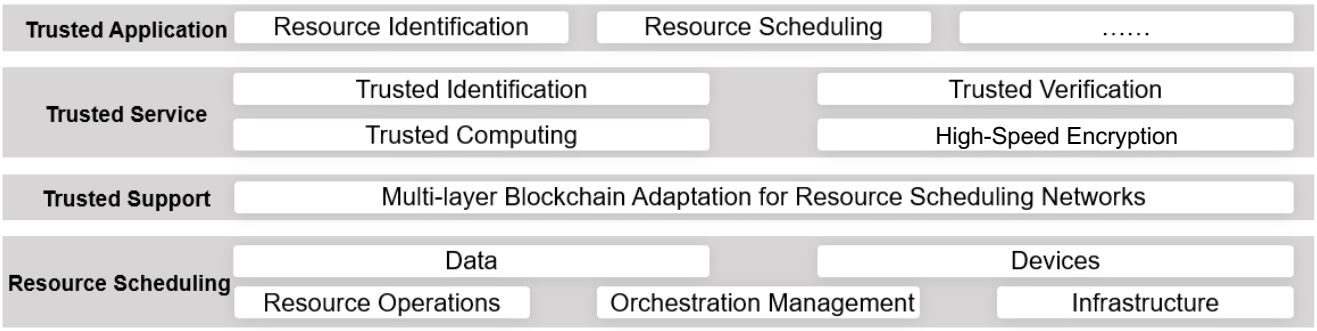


**Figure 1 - End-to-end Trustworthy Scheme Architecture**

The scheme mainly consists of the Trusted Collaboration Layer, Trusted Support Layer, Trusted Service Layer, and Trusted Application Layer. The architecture of the scheme is shown in Figure 1. The overall design of the scheme is as follows:

**Resource Scheduling Layer:** This layer performs resource operations and orchestration management, to manage the CNC infrastructure. The infrastructure management aims at two key asset elements of CNC, which are data and devices, ensuring the security of data circulation and device trustworthy.

**Trusted Support Layer:** This layer fits the infrastructure for the corresponding blockchain functionality. The blockchain records the allocation information of computing tasks and resources. The consensus algorithms verify devices, data content, and status. The smart contracts automate the scheduling of computing tasks and resource allocation.

**Trusted Service Layer:** This layer is the core capability layer of the scheme, consisting of Trusted Identification, Trusted Computing, Trusted Verification, and High-Speed Encryption.

- **Trusted Identification:** Measuring the computing devices under the node as the basic unit, issuing DID identity to each computing device to form an asset trusted management system for computing devices.

- **Trusted Computing:** Utilizing TEE [2] to achieve trusted isolation, constructing a secure network defense network, and ensuring the trustworthiness of the node computing environment.

- **Trusted Verification:** Leveraging blockchain signature technology to achieve trusted marking of data, providing data verification function, and completing the security audit of the data circulation path.

- **High-Speed Encryption:** To mitigate the data transfer efficiency and the encryption performance, our scheme proposes a hardware-accelerated high-speed encryption algorithm for large files, which reduces the overall system latency.

**Trusted Application Layer:** This layer includes applications such as resource identification and resource scheduling, which calls for the capabilities on the Trusted Service Layer.

## 3. INTEGRATED SECURITY CAPABILITIES

The key security capabilities of the scheme are implemented by the Trusted Service Layer, modularly encapsulating the Trusted Identification, Trusted Computing, Trusted Verification, and High-Speed Encryption into four components. These components form a security service resource pool, which can be flexibly selected according to different resource scheduling business scenarios, providing a one-stop security service.

### 3.1 Trusted Identification

The computing devices are usually located in different data centers. The security authentication and effective integration of these large-scale, distributed, heterogeneous computing devices are the prerequisites of computing power allocation. The security foundation of the device access, environmental perception, data tracking, and permission management processes relies on the uniqueness, consistency, and anti-counterfeiting of device identities.

Asset-trusted identification technology utilizes blockchain's tamper-proof distributed ledger technology to provide

trusted asset identity management. Through smart contracts, it manages the computing resources data throughout its entire lifecycle, establishing a complete and trustworthy asset management system.

The specific implementation involves combining the blockchain's trusted identity management approach with the existing W3C-standard decentralized identity (DID) [3] system as shown in Figure 2.

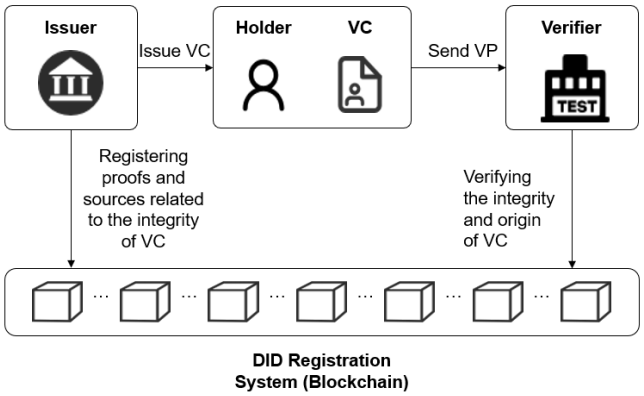


**Figure 2 - Schematic Diagram of DID Trusted Asset Identification**

Within the resource scheduling system, admission certification access points are established as professional security identity audit and issuance institutions. The issuer issues a verifiable statement of DID identity and Verifiable Claims to the connected device nodes and users. Accessing devices, nodes, etc., through a unique, unified trusted identity verification, encodes and marks information for each data circulation, operation, and flow, building a unified and cross-system data identity marker. This facilitates the initial screening of data sources and permission management of nodes.

Compared to traditional identity management systems, trusted identification possesses the decentralized characteristics of blockchain. The identity of each user is not controlled by a trusted third party but by its owner, allowing individuals to manage their own identities autonomously. By using Verifiable Credentials (VC) and Verifiable Poofs (VP), the authentication process does not depend on the application provider offering the identity, avoiding the concentration of identity data in a single centralized authoritative institution and preventing identity data leakage and attack risks.

### 3.2 Trusted Computing

The implementation of the resource scheduling system relies on the computing within nodes and the transmission between nodes. The trusted computing of nodes is the source of data security. Attackers infiltrating nodes to steal data being computed, stored, or transited on devices, or gaining control of devices to masquerade as secure nodes and wait for opportunities to damage the system, pose significant challenges to internal security.

The capability for secure computing within the Trusted Service Layer is realized by the node's TEE key management system function.

The TEE key management system employs the hardware-supported TEE technology to provide hardware security isolation. Combining with encryption algorithms, the system offers a reliable key management method, and ensures the reliability and integrity of keys. This establishes an effective node identity authentication and authorization mechanism, including permission control, audit tracking, and other functions, to prevent unauthorized access and use, ensuring the security of the internal operating environment of nodes.

**1) Trusted Execution Environment (TEE)**

The Trusted Execution Environment (TEE) serves as a crucial component deployed in various nodes of the resource scheduling system, including computing, storage, and network nodes. TEE ensures the secure isolation of the storage and the use of keys, by allocating independent computing and storage spaces in CPU and memory. It also provides API interfaces for applications to call, achieving secure system communication, data transfer, and transaction protection.

**2) Key Management Module**

The key management module provides centralized control and key management for nodes. This module is deployed within TEE section, execute key functions such as key generation, distribution, storage, accessing, updating, and revocation. The management working flow is as shown in Figure 3. Through secure key management systems on various nodes, it performs operations like identity verification and encrypted communication, building an intrusion protection network to ensure the security and reliability of the entire system.

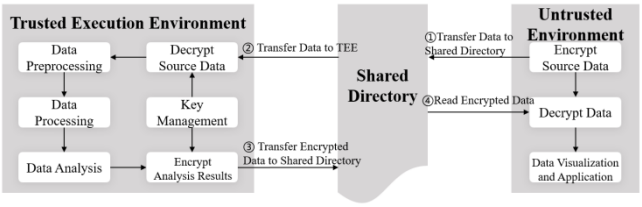


**Figure 3 - Key Management Based on TEE**

### 3.3 Trusted Verification

The diversification of data cross-domain flow paths leads to a significant increase in risk exposure, with the transmission process facing threats of tampering and distortion. The authenticity of content requires secure and trustworthy means of protection. This scheme utilizes blockchain technology to encode and mark important files and data information, building cross-system and cross-node data circulation marking capabilities and authentication capabilities, achieving controllable and perceivable data management.

Employing blockchain technology for encoding and marking data with trustworthy techniques, this approach generates distributed data credentials based on blockchain, serving as the basis for data verification, authentication, and tracking, ensuring the security and trustworthiness of signed data. Commercial cryptographic algorithm and hash algorithms are used to ensure the authenticity, integrity, privacy, and security of data on the blockchain. The structure of one block and the chain is shown in Figure 4.

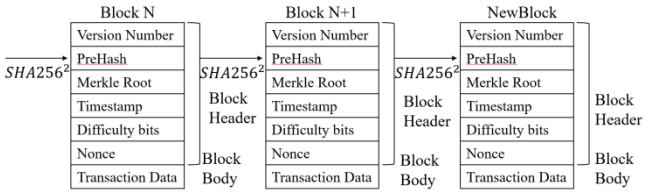


**Figure 4 - Blockchain chain structure**

Data marking technology adopts secure computing hash algorithms, utilizing the decentralized and tamper-proof technical features of blockchain to safeguard the integrity and credibility of data throughout its lifecycle. At the transmission's start, the sender computes a hash value of the data through a HASH operation, resulting in a fixed-length hash value. Smart contracts deployed on the blockchain will automatically record the hash value, storing data signatures in the distributed database as a unique identity mark for the data. Upon the data's arrival at the destination, the recipient computes the hash value of the data again and compares it with the value stored on the blockchain to verify whether the data has been tampered with or lost during transmission. Throughout the data transmission process, the nodes and operations that data passes through will be recorded on the blockchain, providing users with a transparent and traceable data circulation pathway.

### 3.4 High-speed encryption

In the processes of data transmission and storage, to prevent data from being stolen by attackers, encryption algorithms play a crucial role in ensuring data security. However, the cryptographic computation increases the overhead of the system, which contradicts the high throughput and low latency requirements of the resource scheduling system. Traditional encryption technologies can no longer meet the demands of high-speed data transfer.

GPU acceleration technology is a solution for hardware-acceleration of the cryptographic algorithms based on CPU+GPU heterogeneous computing architecture [4], aimed at achieving low-latency encryption and decryption of data in nodes. This solution shifts traditional serial cryptographic computation into parallel processing, the parallel principle is as shown in Figure 5. Utilizing hardware-accelerated commercial cryptographic algorithms enables fast and secure processing of large files in the resource scheduling system using the commercial cryptographic algorithms such as SM2, SM3, SM4, etc. This method increases the encryption speed and enhances the efficiency of the algorithms, providing strong security for data transfer.

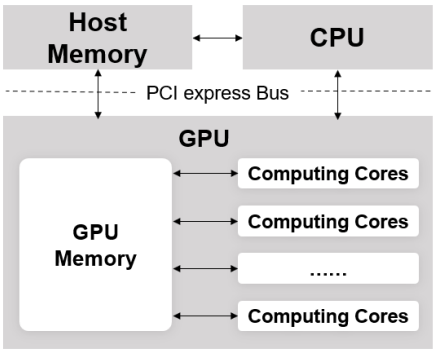


**Figure 5 - CPU+GPU Heterogeneous Collaboration**

The specific implementation methods are as follows:

**1) Hardware Acceleration**

Using GPU-based hardware acceleration technology, the parallel processing of the cryptographic computing for encryption and decryption are transferred to the GPU. Leveraging the GPU's vector processing units and high-speed memory bandwidth, this technology rapidly processes the encryption and decryption computation for large-scale data, increasing the encryption algorithm's speed.

**2) Heterogeneous Computing Architecture**

Our solution adopts a heterogeneous architecture based on CPU+GPU, the computing capabilities of both CPU and GPU are used in tandem. The cryptographic computation process is divided into two parts. CPU is responsible for the control and scheduling of computing tasks. Meanwhile, GPU handles the parallel computing of the commercial cryptographic algorithms. This specialized division of labor enhances the encryption efficiency.

**3) Parallel Processing**

Parallel processing adaptations are carried out for the commercial cryptographic algorithms such as SM2, SM3, SM4, etc., by loading the message expansion, key expansion, and block encryption operations in the algorithms into the GPU, and dividing the assignment or logic operation tasks with low data correlation into each parallel computing unit. Therefore, the large batch of input data can be simplified into small-scale data blocks Each block is assigned to different computing units for parallel processing, fully utilizing the computing resources.

## 4. IMPLEMENTATION RESULTS

In this section, we take our practice in Guizhou Province as a case study. Guizhou locates in the western of China, and has abundant green hydropower and sufficient land scale. It has already established numerous datacenters, serving as a western hub node in the east-data-west-computing project. Our study selects the DPI log data migration scenario as a "test field", which generates 350TB of data every day, to fully leverage the real-world environment in Guizhou and

verify the secure and trustworthy protection capabilities proposed in this paper.

Our solution can reduce the overall energy consumption by storing warm and cold data in the western region instead of in the eastern region. For example, taking storing 1000 TB of data as an example, the energy consumption for storage is about 22.68 kW for one day, and 143.64 kW for computing. Typical economically active eastern regions such as Zhejiang Province have an electricity bill of about 1.0 yuan. But for Guizhou Province in the western region has an electricity bill of about 0.5 yuan. Intuitively, the off-site storage of data can save 50% on electricity bills. In addition, Guizhou has abundant water resources and low average temperatures. The use of clean energy can reduce carbon emissions, and the suitable temperature can also reduce the cooling energy consumption of operating datacenters.

In the deployment and testing, the capabilities of trusted identification, trusted computing, trusted verification, and high-speed cryptography mentioned in this paper all functioned normally and achieved the anticipated goals. Trusted identification uniformly issues trusted identities to the eastern node and western node, implementing device access management. Trusted computing builds secure storage spaces within different nodes, strengthening key management of devices. Trusted verification uses the blockchain to certify DPI log information, ensuring the integrity of data content. High-speed encryption builds a secure channel between nodes, completing data encryption and decryption. Particularly, the GPU heterogeneous cryptographic acceleration technology increases the encryption performance of SM2, SM3, and SM4 by 20-55 times compared with encryption without hardware acceleration, as shown in Figure 6.

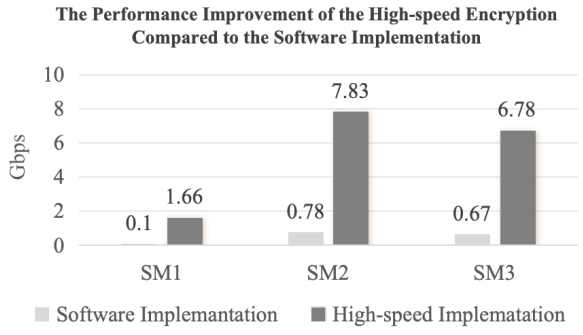


**Figure 6 - High-Speed Encryption Performance Improvement**

In real-world deployments, CPU chips that support TEE are not yet widely used, and GPUs are still a scarce resource in datacenters. Therefore, our solution provides a partially deployed version. For example, we can only configure the blockchain capability to verify the east-west data transmission, sacrificing some performance without using GPUs. We can also use pluggable TEE hardware devices for more flexible deployment.

This case in Guizhou demonstrates that the scheme proposed in this paper can provide a reliable asset access method in real environments, effectively reduce the operational costs of security services, protect the privacy and security of CNC, and offer technical support and practical evidence for a communication concept that emphasizes both "green" and "security".

## 5. CONCLUSION

This paper proposes a comprehensive technical solution aimed at optimizing the use of computing resources, reducing energy consumption, and addressing security issues introduced by cross-regional data flow. The implementation of this solution in the context of the east-data-west-computing project has the following advantages over existing technologies:

**1) Green Communications Practice:** The solution presented in this paper is based on the concept of green communications. It explores the practical issues arising in the east-data-west-computing project and provides a complete solution, thereby facilitating the practical implementation of the east-data-west-computing project and pushing the communications industry towards a path of green, low-carbon, and sustainable development.

**2) Enhanced Security Assurance:** Combining technologies such as confidential computing, blockchain, and high-speed encryption, the solution offers a solid technical foundation for the secure and trustworthy protection of CNC. Through actual deployment and testing, the solution has been proven to effectively protect data privacy and device security in real environments, ensuring the safety of cross-domain data flow.

**3) Innovative Data Management:** The solution conducts in-depth research and innovative applications in areas such as the certification of computing devices, the establishment of a trustworthy environment for heterogeneous computing nodes, and the secure transmission of data in dynamic environments. Through these measures, it effectively achieves secure data circulation and trustworthy management, enhancing the credibility and security of data throughout its lifecycle in the resource scheduling process.

## REFERENCES

[1] ITU, "Use cases for supporting the coordination of computing and networking for Developing Countries": https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19170

[2] Rabimba Karanjai, Rowan Collier, Zhimin Gao, Lin Chen, Xinxin Fan, et al." Decentralized Translator of Trust: Supporting Heterogeneous TEE for Critical Infrastructure Protection.," Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '23). ACM, New York, pp.249-264.2023.

[3] Clemens Brunner, Ulrich Gallersdörfer, Fabian Knirsch, Dominik Engel, and Florian Matthes,

"DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust," Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications (ICBTA '20). Association for Computing Machinery, New York, pp. 61–66, 12.2021.

[4] Sparsh Mittal, Jeffrey S. Vetter, "A Survey of CPU-GPU Heterogeneous Computing Techniques," ACM Computing Surveys, the Association for Computing Machinery, New York, pp. 1–35, 07.2015.