Scheme Construction of VR Cloud Integration Intelligent System Based on Internet of Things

Jianlan Ren¹, Xiong Wenxin²

¹Jiangxi Vocational and Technical College of Communication Jiangxi-Nanchang 330013, China
²National Defense Science & Technology Information and Satellite Application Center of Jiangxi, China Jiangxi-Nanchang 330012, China

Abstract. With the rapid development of mobile Internet and intelligent terminals, the privacy data generated by mobile applications is increasing. Because of the limited computing and storage capacity of mobile intelligent terminals, the security measures designed for traditional network terminal devices are not suitable for mobile intelligent terminals. This paper analyses the current application situation of virtual reality technology and Internet of Things technology and the bottleneck of engineering application and popularization, and probes into relevant problems. On this basis, a new model of intelligent system based on virtual reality and Internet of Things is proposed. The extended Spice protocol provides efficient support for front-end separation of displays and calculations. The encryption master key is generated by splicing the keys generated by the authentication cloud and the mobile intelligent terminal, and the master key is used to effectively prevent the mobile intelligent terminal and the cloud storage server from leaking the privacy data of the mobile user. Realize the unified management, flexible deployment, flexible delivery and automatic operation and maintenance of basic resources, and promote the transformation of application deployment from applying for equipment to applying for service.

1. Introduction
In the era of mobile Internet, users use mobile intelligent terminals to access the Internet for mobile office, mobile payment, mobile medical treatment, mobile entertainment and other services. Through mobile intelligent terminals to understand various information, it can be said that mobile users can not live without mobile intelligent terminals [1]. The concept of Internet of Things (IOT) has been applied to various industries, giving more "intelligent" elements to the economy and society, and realizing the mutual exchange and cooperation of data. Supported by various application modes, such as virtual tourism, games, industrial design, etc. It has rapidly become the hot response mode of the current market, and rapidly promotes social development and progress with the support of various virtual reality engines [2]. Users can access their consistent virtual office environment by accessing their applications, desktops, and data services subscribed to in the cloud center from any networked terminal. Under the current rapid development of mobile Internet and cloud computing technologies, traditional B/S architecture GIS applications can no longer meet the increasingly diverse application requirements [3]. In the era of the Internet of Things, natural cloud network integration, whether it is virtual reality or smart home, data will play a big role, so the change of interaction mode will change all aspects of human life, including changes in business models.
In the mobile cloud storage system, the mobile intelligent terminal is only used as the access end, the data storage is implemented in the cloud and transparent to the mobile intelligent terminal, and the mobile intelligent terminal does not need to know the specific location where the data is stored in the storage cloud [4]. Each module communicates through message queues and builds a unified database cluster to store configuration and management data. This architecture design not only facilitates the flexible expansion of the platform, but also enhances the stability of the system [5]. The realization of virtual reality and Internet of Things technology greatly makes up for the blank of visual control in special environment such as underground where traditional video surveillance cannot be installed and reached. Therefore, it is necessary to deeply study the security protection technology of mobile cloud storage technology [6]. The purpose of this paper is to design and implement a user-controlled cloud-based integrated security system to ensure the integrity, confidentiality, security and availability of mobile user privacy data generated by mobile intelligent terminals. The rise of cloud computing has brought new opportunities for the development of integrated intelligent system. The introduction of cloud computing technology will further promote the development of integrated intelligent system technology.

2. Methodology

Cloud computing is the delivery and usage model of IT resources, that is, users get the IT resources they need through the network in an on-demand and scalable manner, typically including hardware, platform and software resources. Cloud computing is divided into three categories according to service model differences, namely SaaS, PaaS and IaaS. Mobile cloud storage systems should enhance access control to users. At the same time, because the mobile user's private data is stored, the mobile cloud storage system should provide confidentiality protection for the user's private data while ensuring data availability. With the development of the times, the need for efficient processing of work transactions puts forward higher requirements for the traditional operating environment. The security protection and flexible access of users' private data is also an important part of cloud computing. The process is no longer terminated in the output of processing and analysis results, but can distribute and share the results among multi-users and multi-devices, and can be further used and edited by other users. According to the components of mobile cloud storage, the information security of mobile cloud storage will be threatened by two security threats: security threats faced by mobile intelligent terminals and security threats faced by cloud storage terminals. These security threats will eventually lead to the leakage of users' privacy data and bring huge losses to mobile users. In order to solve the problem of system delay in the case of multi-input, it is necessary to establish the corresponding setting method of user input priority, and to apply the fuzzy comprehensive evaluation method to the setting of user response priority.

Compared with the traditional operating system, which only drives local hardware resources and runs single-machine applications, cloud operating system drives the whole data center resources downward and runs applications distributed across clusters. In the data acquisition stage, the existing Internet of Things technology can be used. After data acquisition, the database should be used for analysis, and the artificial intelligence should be used to meet the customers' professional requirements for the industry [7]. In order to meet the system administrator's monitoring and management system status, service providers publish and manage applications and provide virtual storage, virtual computing, virtual desktop and virtual application services. Ordinary users need to access virtual applications and desktops, while ensuring the system's scalability and flexibility. It is required to have intelligent clustering capability; due to the spatial data correlation and massive characteristics, it is required to support distributed storage and distributed cut graph capabilities. Users use software that runs on a cloud computing platform. These provided software can access the browser or client from a variety of sources. Users do not need to actively control the underlying cloud computing architecture such as network, server, operating system and storage. At the same time, the containerized application is split into small isolated task units, and the basic resources are dynamically allocated according to the demand fine granularity. Just as the operating system allocates and releases resources for different processes, the concept of the cloud operating system comes from this.
Figure 1 below shows the cloud shared data model. In the data integrity verification process, users, third-party audits, and cloud service providers often involve privacy breaches and user identity tracking issues.

In this article, by introducing a privilege distribution center (as shown in Figure 2), users will be reasonably grouped and RDC will record data operations performed by users. RDC first performs initialization operations to set the global parameters of the system.

The current Internet of Things system emphasizes the acquisition of information. In the aspect of data transmission, the main way is the single channel. Users can not control and integrate the equipment in the control platform. Its basic function is to provide the functions of virtual instance allocation, operation, closure, preservation and recovery. In order to alleviate the pressure of intensive computing, such as network analysis, buffer analysis, submergence analysis, filling and excavation analysis, which are generated by massive data, it is required to have the ability of distributed computing and parallel computing [8]. Users use a variety of commonly used development tools deployed on cloud computing platforms or the environment configuration needed to support programming language development. Responsible for deploying applications on cloud computing platforms without requiring user management or control of the underlying cloud computing architecture. Compared with the traditional operating system, the technical architecture of the cloud operating system is mainly designed as a four-tier architecture: the hardware abstraction layer connects to the underlying hardware through distributed unified storage, and the resource abstraction component, and provides upwards including computing, storage, network, block storage, and object storage, mirroring, container, and resource orchestration interface [9]. Through the Internet of Things technology, all physical devices are connected to the data network to realize the full networking of physical resources and provide interfaces for subsequent resource management and control. Allocate a network for virtual instances and provide for the creation, connection, and separation management of persistent storage volumes.

Data are classified according to their sensitivity to the organization. The conclusion is that the data in Class I is highly sensitive and requires additional security. Therefore, data in Category I can be further divided into different partitions based on its criticality. In addition to classification, data segmentation
further reduces sensitivity. To stick to this, the data owner must identify important breakpoints and must split the data into normal and critical segments. For data segmented into normal segments and critical segments, different security algorithms are required. The data classification of the organization information system with normal and critical data segments is shown in Figure 3.

Fig.3 Classification and segmentation of organizational information systems

The traditional management method of document data requires specific editing. The software depends on the operating system type, the operating system depends on the hardware device, the data needs multiple copies, and the user faces the problem that the storage of the single device is not easy to expand. The virtual system only stays in the 3D modeling and virtual demonstration stage, unable to effectively read various pipeline data, and can not operate and control the key joints of each pipe network. The system management layer interacts with the container management module, the resource coordination module, and the hardware abstraction module through the application management, the cluster management module, the continuous integration module, the infrastructure resource management module, the log management module, and the monitoring component. Visual operation interface is provided to users, so users can perform various operations through human-computer interaction. The user's operations are combined with authentication cloud and storage cloud, and they can accomplish the willingness of mobile users together (such as setting local key, searching data files according to key, registering, authenticating cloud and storing cloud, uploading and downloading data files, etc.). Distributed parallel cutting technology can make full use of the hardware resources in the organization, make comprehensive use of multiple nodes parallel cutting, and store it through tile distributed storage. Monitoring the resource usage status of computing nodes (including memory, CPU, storage, node configuration, etc.) is an important reference information for system scheduling.

The cloud storage service provides data owners with data storage capabilities so that clients do not need to back up locally when using it, reducing the pressure on local storage. When a cloud service provider receives TPA challenges, it generates evidence indicating data integrity and sends it to TPA based on stored files. According to the proposed scheme, on the one hand, cloud service providers process data sent by users and obtain raw data through processing (see Figure 3 below).
Cloud storage mainly completes the mobile user data storage function. On the one hand, it can expand the limited storage space of mobile intelligent terminals; on the other hand, it provides support for mobile user data backup and recovery. It also provides a call interface for upper-level cluster management. The container management layer will invoke the resource layer interface to support the deployment of cluster containerized applications [10]. The three-dimensional visual simulation embodying the real environment must not only reflect the equipment at any angle and position, but also reflect the relationship between related equipment. The Access Protocol Agent provides proxy services for specific remote access protocols, allowing users to access the virtual instance's console through a unified proxy IP without exposing compute nodes. Off-line mode is more important when data needs to be kept secret, network conditions are not good or even without network. Because of the local encryption upload in mobile intelligent terminal, that is, the data in cloud storage server is in cipher text state, cloud storage administrators do not know the key and the specific encryption and decryption algorithm. The basic functions of the system do not need to be coded twice, only need to be customized according to the requirements. The data obtained from the physical layer, as well as the control and status of the controllable devices by the big data service layer, should be instantly reflected. We should break through the limitation of time and space and reproduce the past or future environmental state at any time.

3. Result Analysis and Discussion
To avoid the proxy server becoming the bottleneck of the system, when the number of computing nodes is large, the computing nodes are divided into several sets, each set is scheduled by a proxy server, each proxy server shares the account management database, and has its own load balancing database. Therefore, besides direct links, cloud terminals may also adopt multi-level and hybrid links across intranet and intranet, and face different degrees of complex problems. In order to meet the diverse needs of mobile users, cloud integrated security system provides local storage and cloud storage. Users can store the data locally and generate the encrypted master key by key splicing technology. It mainly performs standardization encapsulation by calling the mainstream physical host, and registers with the resource service list of the cloud operating system to realize resource scheduling for the physical machine. Develop various application algorithms for industry requirements, and use artificial intelligence technology to provide early warning and processing of high-risk data. At this point, the newly created virtual machine is actually cloned through a parent. And this kind of cloning is done dynamically. If a piece of information already exists, it is read directly. The cloud collaboration technology is used to solve the problems of low utilization rate of multi-service source resources and low service access efficiency under large data volume, and realizes multi-user and multi-terminal optimization coordination and efficient links between cloudy and multi-end.

Typically, cloud servers run large amounts of storage and computing resources. Cloud servers attempt to minimize bandwidth and optimize storage usage through client-side cross-user redundancy. The client uploads data and accesses outsourced data at any time. The management server distributes the message-derived keys and manages the challenge index. Specifically, as shown in Figure 4 below.
Cloud storage server mainly completes mobile user data storage functions, including data backup center and recovery center. According to the preferences of mobile users, cloud storage service providers can be selected, that is, users can connect different cloud storage servers. Large data platforms need to be redeployed in cloud operating systems, and data from large data platforms need to be migrated to new clusters through data replication. The developed management system should provide the interface of PC terminal, mobile terminal and professional equipment terminal, provide UI interface and humanized management method, and support various virtual gloves and glasses driver provided by virtual reality. If a file system is constructed, it can be dynamically cloned for users and according to the data parent. This file system will have a distributed file system feature that can be accessed globally, regardless of whether the master or copy is managed by it. Open standards are used to provide common services, such as OGC standard services and REST standard interfaces, so that services can be accessed and used more efficiently by more terminals. It ensures that data security stored in the cloud is still guaranteed when the cloud storage is not completely trusted. As an infrastructure component, the cloud operating system completes the underlying resource layer support for a full-service unified data center, including relational data services and unstructured data services. Thereby, the response of the input and output device can be independent, the user interaction behavior is grouped by level, and important response events can be executed according to the priority to ensure that the system can operate normally under the condition of multiple input by the user.

When mobile users use cloud-based integrated security system, they need to register user identity information with authentication cloud. After binding the identity information, users can login with their own identity information. With distributed scheduling technology as the core, all kinds of resources in data center are integrated and dispatched, so that the mixed resources such as physical resources, virtual resources and containers can be displayed logically as a single machine. In addition to the construction of three-dimensional models, the existing virtual reality systems emphasize more on the various functions of the three-dimensional engine, emphasizing human senses and human visual control of the environment. Similar to authentication systems, service providers may have their own customized billing systems that they want to design to provide integrated interfaces. The mobile user can store the data in the cloud, generate an encrypted master key through the key splicing technology, and use the master key to encrypt the data to be backed up selected by the mobile user and upload it to the cloud storage server. After the cloud operating system is deployed, you only need to provide basic hardware information and IPMI configuration information of the physical server, and you can control the physical server as a bare metal node with one click. Using a variety of integrated methods to measure underground pipelines, confirm the correctness of the data information, establish a standard and standardized data management system, and leave an interface for the expansion of the underground
A private cloud environment was deployed in our organization, including three systems, Server 1, Server 2, and Server 3, and a client system to interact with the deployed cloud server. Server 1 runs all components of Nova, Glance, Swift, Keystone, and Horizon. Server 2 and server 3 only run Nova computer components. One or more client systems can interact with deployed open stack components, as shown in Figure 5.

Fig. 6. Open Stack private cloud settings

After assigning a virtual machine to each user, you also need to consider the issue of user-specific data access. I hope to assign a private data area to each user. Through server-side aggregation and client-side aggregation, it is convenient for clients to link information from multiple sources and make full use of this data. Among them, on the mobile terminal side, data loss is a major security threat, mainly caused by the loss of the mobile intelligent terminal, failure or user misoperation. During the implementation process, you need to consider the specific implementation of the storage solution. You can select the local disk of the physical host or the object storage provided by the cloud operating system. Under the artificial management mode, the system can view the data of each joint point of underground pipeline network at any time, and also can open and close the joint point quantitatively at any time. Each file will be processed in blocks. When accessing a data block of a shadow file each time, if the data block has never been written, it can be directly redirected to the corresponding data block of the original file for reading. The process is no longer terminated in the output of processing and analysis results, but can distribute and share the results among multi-users and multi-devices, and can be further used and edited by other users. Mobile users can choose cloud storage services according to their preferences, complete their own identity registration, and then prepare for the identity authentication of mobile users by cloud storage.

4. Conclusion
This paper analyses the security threats faced by existing mobile cloud storage services, and proposes a user-controlled cloud integrated security solution. In the application mode of data processing as an example, the main role is no longer confined to the desktop, but more user terminals are playing their role in all parts of the data process. At the same time, considering the limited capacity of mobile intelligent terminals, a hierarchical privacy protection scheme is proposed, which uses different security intensity cryptographic algorithms to encrypt. A fully virtualized solution business has a clear business application scenario. The business application dynamically creates a big data computing service cluster through the cloud operating system to realize the dynamic response of big data computing. Free users from dependence on operating system platforms, hardware device dependencies, application installation management, data synchronization management, and access time and access location restrictions. The
security module APP can implement key splicing and encrypt the backup data to the storage cloud and download data from the storage cloud and decrypt it locally. However, the research on VR cloud integrated intelligent system is still in its infancy, and many problems need to be solved step by step. As an available cloud intelligent system model, cloud integrated intelligent system system needs further improvement in the future.

Acknowledgments
2018 Jiangxi Provincial Department of Education Science and Technology Project, project number: GJJ181549, project name: VR cloud integrated intelligent teaching system based on Internet of Things

References
[1] Ibanez J G, Zeadally S, Contrerascastillo J. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies[J]. IEEE Wireless Communications, 2015, vol. 22, No. 6, pp. 122-128.
[2] Wang X V, Wang L. A cloud-based production system for information and service integration: an internet of things case study on waste electronics[J]. Enterprise Information Systems, 2017, vol. 11, No. 7, pp. 952-968.
[3] Chen M, Ma Y, Li Y, et al. Wearable 2.0: Enabling Human-Cloud Integration in Next Generation Healthcare Systems[J]. IEEE Communications Magazine, 2017, vol. 55, No. 1, pp. 54-61.
[4] Chandra S R, Yafeng W. Cloud Things Construction - The integration of Internet of things and cloud computing[J]. Future Generation Computer Systems, 2016, vol. 56, pp. 684-700.
[5] Xiong G, Timo R N R, Dong X, et al. Intelligent Technologies and Systems of Material Management[J]. Intelligent Systems Reference Library, 2015, vol. 87, pp. 295-330.
[6] Computing Systems[J]. International Journal of Distributed Sensor Networks, 2016, vol. 12, No. 7, pp. 9764287-9764287.
[7] Longo F, Bruno D, Distefano S, et al. Stack4Things: a sensing-and-actuation-as-a-service framework for IoT and cloud integration[J]. Annals of Telecommunications, 2017, vol. 72, No. 1-2, pp. 53-70.
[8] Pang Z, Zheng L, Tian J, et al. Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things[J]. Enterprise Information Systems, 2015, vol. 9, No. 1, pp. 86-116.
[9] Kumarage H, Khalil I, Alabdulatif A, et al. Secure Data Analytics for Cloud-Integrated Internet of Things Applications[J]. IEEE Cloud Computing, 2016, vol. 3, No. 2, pp. 46-56.
[10] Villari M, Fazio M, Dustdar S, et al. Osmotic Computing: A New Paradigm for Edge/Cloud Integration[J]. IEEE Cloud Computing, 2016, vol. 3, No. 6, pp. 76-83.