Journal of Computer and Communications, 2016, 4, 7-14
Published Online May 2016 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2016.47002

Education Technology Cloud Platform Framework Establishment and Security

Guoqiang Hu, Yanrong Yang*, Li Li

Network and Education Technology Center, Northwest A&F University, Yangling, China
Email: *yyr0718@nwsuaf.edu.cn

Received 1 April 2016; accepted 16 May 2016; published 19 May 2016

Abstract

With more educational business absorbed into information management system at universities, traditional information management platform seems unable to provide efficient service for teaching and research. Some universities then resort to cloud computing platform. In view of the problems existing in the traditional information platform, this study presented an information management framework designed with cloud technology, and introduced the security techniques for its protection.

Keywords

Cloud Platform, Framework, Security

1. Introduction

As the digital campus construction of Northwest Agriculture & Forestry University keeps advancing, great achievements have been made in network construction, information services and educational technology. Through years of relentless exploration, the university's digital campus has built up a traditional information platform integrating the network construction, information services and educational technology. However, a number of problems have been discovered during the actual application of the traditional information platform in recent years, so how to solve these problems has become a top priority for the construction of the digital campus.

2. Problems in the Traditional Information Platform

2.1. Huge Quantity and Great Variety of Equipment Make Equipment Management Harder and Harder

At present, the wireless internet covers 80% of our campus with over 1200 network devices and more than

*Corresponding author.

How to cite this paper: Hu, G.Q., Yang, Y.R. and Li, L. (2016) Education Technology Cloud Platform Framework Establishment and Security. *Journal of Computer and Communications*, **4**, 7-14. http://dx.doi.org/10.4236/jcc.2016.47002

50,000 points of access information. Private networks for finance, campus cards, libraries, video surveillance and control system, and medical treatment have been set up, but it is difficult for the existing network platform to incorporate more network devices.

2.2. Equipment Installation and Maintenance Are Mainly Carried Out by Stand-Alone Operation, Which Is Troublesome and Onerous

Public network services that have been built up and in operation in our university includes: The domain name service (http://nwsuaf.edu.cn/, the platform for public resources (the network for educational resources, FTP, PT, etc.), the website groups (including about 100 websites such as the university's homepage, the secondary website and the websites for special topics), e-mail system (with over 33,000 users), the mobile portal, VOD, VPN, IPTV, the recording and broadcasting system, and the system for releasing campus information. Every service is installed on an independent server, the software installation and debugging of which are mainly carried out by stand-alone operation. Therefore, it takes a large amount of time-consuming maintenance in the event of a failure. In addition, the application of the virtual technology is confined to a single physical host with little use of resource pooling, leading to a low utilization.

2.3. The Storage Resource Is Insufficient and Is Greatly Wasted When Allocated

There are mainly two storage devices in the university, respectively IBM DS4800 (24TB) and IBM DS5100 (130TB). With the data of the digital campus increasing, the storage resource of 154TB is severely insufficient with low utilization.

2.4. It Is Difficult to Satisfy Teachers and Students' Personalized Needs and the Support for (Long-Distance) Mobile Working Is Far from Enough

There are many problems in the traditional platform, which considerably restrain the growth of the Data Center and the development of the university's educational informatization. The expansion speed of the Network and Educational Data Center being faster than the growth of the traditional infrastructure has become a major bottleneck for the current development of the Center. And a new educational information platform is needed for the expansion of businesses and the diverse development of educational technologies in the future.

Cloud computing as a new model for resource utilization and delivery is bringing a profound and extensive revolution for electronic information technology. Virtualization-based cloud computing boasts the technical advantages of high reliability, on-demand service, and high scalability. In consideration of them, this paper designs a cloud computing platform to solve the problems existing in traditional platforms. The new platform built with cloud computing not only can solve the problems in the traditional platform, but have an improved data protection system.

3. In the Building of Could Platform, the Work That I Had Done Includes: Cloud Platform Framework Design Objectives

3.1. More Convenience for Providing Educational Resources

Different physical and virtual resources can be classified and released dynamically according to the needs of teachers and students, and resources can be provided quickly and flexibly by adding available resources to match the newly added demands; if the users no longer use this part of resources they will be released. Cloud computing conveniently provides users with computing resources, realizing the expandability of educational resource utilization.

3.2. Customizable Self-Services

Cloud computing provides users with self-help resource services so that users are able to obtain self-help computing resources without needing to be face-to-face with the providers. Meanwhile, the cloud system provides certain application server directories for the users to choose service items and content to meet their needs on their own.

3.3. More Convenience for Teachers and Students

The components and overall structure of cloud computing are integrated by SDN and provide services for teachers and students through network. Campus users can visit educational and book resources they are interested in with different end devices through 3G/4G or wireless network at any places inside the campus while users outside campus can visit educational resources through VPN. In this way, cloud services for education are ubiquitous.

3.4. Quantifiable Services

When providing cloud services for users inside and outside campus, the resources are monitored and controlled in real-time to automatically control and optimize their allocation for different types of services provided for users, and thus to ensure that every user's requirements are met timely.

3.5. Resource Pooling and Transparency

For the teachers at Network and Educational Data Center, computing resources, storage resources, network resources and educational resources can be collectively managed and coordinated, becoming a "resource pool" to provide services for teachers and students; for other teachers and students, they only need to be concerned about whether their needs are met, rather than knowing about the resources and the internal operation process by themselves [1].

3.6. Framework Building of Cloud Platform

Generally, cloud computing provides services according to the usage amount of users. This kind of service model provides a configurable shared pool of computing resources (including networks, servers, storage and application software) for the users in time by offering available, convenient and on-demand network accesses. With a little of management and few interactions with service providers, users can get the service resources they need. The cloud computing platform is composed of a series of resources that can be shared, upgraded dynamically and virtualized, and users can simply use the resources on the cloud computing platform according to their own requirements without needing to master technologies related to cloud computing. Based on the levels of the services, the cloud computing is divided into three categories, *i.e.* SaaS, PaaS and IaaS [2]. IaaS, Infrastructure-as-a-Service, includes resources such as computing resources (physical and virtual machines), storage resources, network resources, load balancing and firewalls. PaaS, Platform-as-a-Service, includes operating systems, operating environment for programming languages, database, Web Server and WebSphere Application Server. SaaS, Software-as-a-Service, provides software services (for WEB, WAP, Android/IOS/WP) through the Internet. The cloud platform in our university consists of 3 sub-platforms, respectively the application cloud platform, the application-based cloud platform and the campus-based cloud platform according to their services models. By combining this with practical application services, the framework for campus cloud platform is proposed in this paper.

3.7. Layer of Infrastructure

This layer is corresponded to the IaaS in the cloud computing service model, which mainly integrates and uniformly allocates hardware resources through virtualization technology with infrastructure resources of digital campus as its core. With a series of unified management services such as optimal management, storage management and security management, all heterogeneous and loose nodes are integrated into a tight "virtual super computers" with a single image [3]. Users can deploy and operate the operating systems and software applications on the cloud platform composed of all the hardware resources. When doing this, rather than being concerned about the deployment and management of the infrastructure layer, users only need to obtain their service resources through the service interface provided for them. In this paper, the infrastructure layer is sorted into four layers, *i.e.*, layer of resource pools, layer of virtualization, layer of management support and layer of service. The detailed design is as shown in **Figure 1**.

1) Layer for resource pools

This layer is mainly composed of computing resources (service cluster related to cloud computers), network

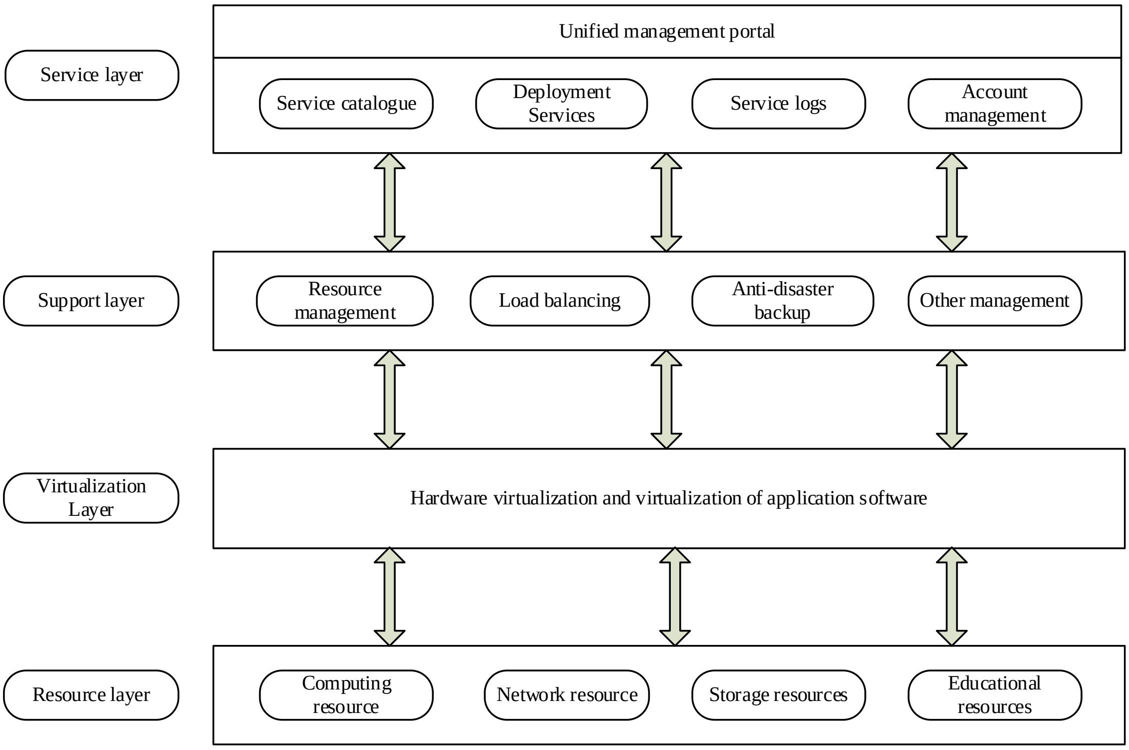

Figure 1. The framework for infrastructure layer.

resources (a large network consisting of NPE, NCE, gateways, routers and switches) and storage resources (disk arrays). It is to provide hardware and software support for the cloud platform.

2) The layer of virtualization

The technology of virtualization is used to integrate various kinds of heterogeneous resources that are originally irrelevant to form the unified and controllable resource pools. Teachers and students with authentication and authorization can therefore use the resources in the resource pool dynamically.

3) Layer of management support

This layer is designed for achieving the dynamic and security management of virtualized resources optimizing resources scheduling management, the purposes of which are to effectively lower resource costs, improve resource utilization, and ensure the availability, safety and liability of resource services by means of backup and disaster recovery and security isolation.

4) Layer of service portal

Users are provided with a unified interface for applying for and using the computing, storage and network services, and for safety, a unified authentication management portal is adopted by the Center. The users need to log onto the platform before applying for services.

3.8. The Layer of Basic Services for Digital Campus Cloud Platform

This layer is corresponded to the PaaS in the cloud computing service model. Different kinds of application services are effectively managed in this layer to ensure the stable operation of the campus cloud platform. With the support of other relevant services, the interactions and service sharing between application systems can be realized in this layer. It is subdivided into platform resource services layer, platform data management layer, platform security management layer and user management. The detailed design is as shown in **Figure 2**.

1) Layer of platform resource services

It includes database management, virtual machine management, and the technologies of middleware processing and parallel processing, which provides technical support for the normal operation of the services.

2) Layer of platform database management

Data generated by each sub-system are processed and analyzed in this layer. With data scheduling, data caching,

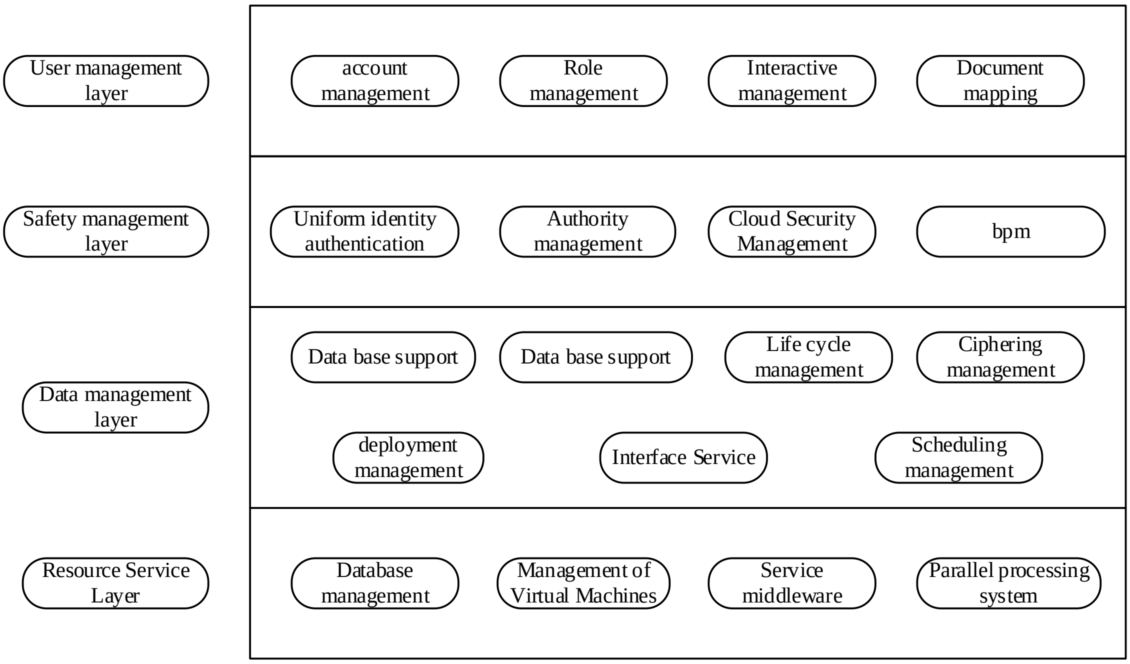

Figure 2. The structure for basic services layer.

data sharing and data security, the liability and stability of data storage are guaranteed.

3) Layer of platform safety management

It is mainly composed of services related to the platform security. The authentication system and permission administration allow the teachers and students to visit the resources and customize the services in a secured way.

4) Layer of platform user management

It mainly manages user accounts and user permissions. Self-services are provided for the teachers and students so that they can modify their passwords, pay their fees, and check the record application resources on the cloud platform.

3.9. Layer of Application Services on the Digital Campus Cloud Platform

This layer is to provide software applications for the users, and all the application software needs the support of the application-based cloud platform and the campus-based cloud platform. Uses are able to choose specific applications based on their permissions. The cloud platform of the university is mainly designed to provide various kinds of software services for teachers and students who can also customize different applications to meet their demands in their work and scientific researches.

4. Security Issues in the Using of the Cloud Platform

Whine providing users and companies with storage resources, software resources and computing resources at a low cost with extremely great convenience, safety issues may pose one of the biggest challenges for cloud computing. By the multi-layered and multidimensional real-time monitoring and off-line analyses of the traditional platform, it is found that the campus cloud platform is faced with security threats in terms of business, information and operation and maintenance, which have basically covered all the safety issues in Internet applications. Only by effectively prevent the cloud platform from these three kinds of safety threats can it provide liable security protection for different applications for the teachers and students. To solve security issues, the following measures are adopted.

4.1. To Set up an Operation and Maintenance Platform to Safeguard Daily Safety

As to Hosting applications, the teachers and students are generally concerned more about whether it is safe or not to deploy the code on the campus servers. To protect the applications of them, the cloud computing platform should be given security and protection strategies from different levels like system, network, data and passwords [4].

1) Resource isolation

Isolation of hardware resources can be divided into CPU isolation, network isolation and disk I/O isolation. The strategy for CPU isolation: To bind all the virtual CPUs and the Domain-0 to physical CPUs.

The strategy for network isolation: iptables+tc is used for network isolation, with strategy limits on the incoming traffic implemented and HTB traffic control for bridge devices conducted. Network isolation providing security for data transfer has become a mechanism applied extensively in financial areas such as e-banking and e-payment. The other ways to ensure network security and isolation includes VLAN technology, VPN technology and HTTP/SSL technology [5].

Disk I/O isolation: dm-ioband is used with a principle of setting only the proportion yet no absolute cap.

The strategy of access quarantine is used between different businesses to prevent safety issues caused by internal malicious access between applications.

2) Security reinforcement

The reinforcement of operating systems and software: the configuration of the operating systems and the server software is consolidated to prevent security holes at the operating system level, and the developers will be informed in time to deal with them accordingly. All the servers attached to the platform should receive timely software upgrades so as to patch the software that has vulnerabilities and to even change the secondary websites or the software that has powerful vulnerabilities.

Database reinforcement: to install operating systems and data files in the database programs onto different NTFS partitions; to install database programs and files onto non-system volumes; to install the components necessary for the businesses instead of those unnecessary ones such as upgrade tools, development tools, code samples and online books; to restrict the client computers to link to the scope of the protocols that can be used by the database servers and ensure the safety of these protocols, like limiting using TCP/IP only; to restrict the client computers to link to the specific ports that are used by the data servers without using default ports.

3) Network security

The powerful defense system of the Network Education Center is made full use of to help the applications resist network attacks and intrusions. The Center will clear abnormal traffic and monitor botnets at a regular interval, will hide the surveillance and financial intranets and isolate the security domains, and will set up firewalls respectively at the exits of each intranet. An IPS is deployed on the cloud platform, which can interrupt, adjust and isolate some abnormal internet transfer immediately. The anti-virus server is deployed on the cloud computing system to manage anti-virus software; the safety patch server is deployed on the management node on the cloud computing platform to automatically install patches, test and roll back, which helps the teachers and students to install patches with automatic tools.

4) Data security

The most advanced technology of virtualized mass storage has been adopted to store and manage data resources so as to back up timely and extensively and store various kinds of core data resources reliably for a long time. Corresponding safety mechanism includes data encryption, data isolation, data verification, data backup and disaster recovery. The data between different applications are isolated because teachers and students with development demands are only able to access the data under their corresponding accounts after they apply for the virtual machines. Through the end-to-end VLAN isolation, the data isolation in terms of management level, business level and storage level is realized, and thus to avoid the impact that the mutual effects between each aspect have on the data security. In addition, with regard to the data upload and download between the Internet and the intranet, the campus cloud computing platform should provide special passage for the upload and download on FTP and run a security scan for the applications so as to prevent the test code or code that has safety holes from being published to the Internet.

5) Password safety

The unified identity authentication platform based on LDAP can manage the campus users and permissions in a unified and centralized way, so the users only need to log onto the campus information portal to visit all the systems inside the campus. When campus users log onto the servers directly, multifactor authentication is used to guarantee the safety of passwords effectively and carry out multi-level fine authorization.

6) Daily scanning of security vulnerabilities

The applications are scanned for security holes so as to discover them in time and give an alert. With regard to hosting applications, the security server daemon will run a safety scan for the applications deployed on the server and regularly send audit reports to the email boxes of the teachers and students who apply for servers. The secondary portal sites will be regularly scanned for safety holes which will be delivered in time to the website maintainers.

4.2. Business Safety

The cloud platform should provide a one-stop security platform to check, manage and operate the security information. The business security platform includes two modules:

1) Open API audit information check module

The security server daemon will automatically analyze the data that the applications call from the Open API, and will identify applications with abnormal accesses based on dimensions of active users, user visits, frequency and abnormal IP to give an alert.

2) Anti-addiction module

The "anti-addiction system" is a system launched by the government in 2005 to prevent juveniles from addicting to online games by limiting their times online playing games with technical means so as to protect their mental and physical health [6]. More and more students have lost themselves in the Internet when they no longer receive the strict regulation from parents and society. Moreover, "anti-addiction" is not limited to juveniles. An "anti-addiction system" should be developed specially to restrict college students from surfing online.

4.3. Information Security

The cloud platform should introduce information filtering and detecting mechanism. The technology of Internet spam detection and filtration can identify and filter malicious information on the dimensions of character recognition, user behavior analysis and credit system, ensuring the coverage while effectively reducing misjudge rate. The information security can be divided into three parts:

1) To improve information classification and management and strictly control users' access rights to information.

Combining the setting of permission, universities can strictly control user's access rights by classifying the information and users according to a certain sequence and based on information security level and category of the information needed by users. Besides, the identity authentication system should be linked so that only the users who are permitted by the authentication system can visit the educational resources on the cloud. For the cloud computing is environmentally dynamic, cross-organizational, and diverse in services, the technologies of the unified identity authentication platform and access control are used to strictly control the teachers and students or visitors' access to the information, and thus the information security is effectively ensured.

2) To protect the integrity of information during transmission by using encryption technologies

In order to make sure that the information on the "educational cloud" won't be illegally intercepted, tampered or maliciously damaged during storage and transmission, the cloud platform should combine the technologies of encryption, digital signature and information hiding to protect the confidentiality and integrity of data so as to create a safe cloud platform for teachers and students.

3) To take proactive actions to ensure information security

The provider of the cloud platform should adopt the technology of proactive defense by publishing the newest methods to prevent Trojan viruses on the one hand and warning users when they are visiting malicious webpages or virus programs on the other hand.

5. Conclusion

This paper has designed the framework of for the cloud platform of educational technology, which mainly includes layer of infrastructure, layer of basic services and layer of application services. The cloud platform designed based on the framework has completely solved the problems in the traditional information platforms. Besides, prevention strategies are proposed to address the security issues in the using of new platform, thus making sure that users can use the cloud platform of educational technology safely.

Acknowledgements

The authors wish to thank the helpful comments and suggestions from my leaders in Network and Education Technology center. This work is supported by Research project of teaching reform of higher education in Shaanxi (No.13BY13).

References

[1] Miller, T.D. and Crawford, I.L. (2010) System and Method for Allocating Computing Resources for a Grid Virtual System. US, US7765552.

[2] Celesti, A., Tusa, F., Villari, M. and Puliafito, A. (2011) An Approach to Enable Cloud Service Providers to Arrange IaaS, PaaS, and Saas Using External Virtualization Infrastructures. 2011 *IEEE World Congress on Services* (*SERVICES*), Washington DC, 4-9 July 2011, 607-611. http://dx.doi.org/10.1109/SERVICES.2011.92

[3] Knoch, T.A. (2011) DNA Sequence Patterns—A Successful Example of Grid Computing in Genome Research and Building Virtual Super-Computers for the Research Commons of e-Societies. 8*th International Desktop Grid Foundation* (*IDGF*) *Workshop*, Max Planck Institute for Gravitational Physics, Hannover, 17 August 2011.

[4] Godhankar, P.B. and Gupta, D. (2014) Review of Cloud Storage Security and Cloud Computing Challenges. *International Journal of Computer Science & Information Technology*, **5**, 528-533.

[5] Jiang, Y. (2014) To Explore the Application of Vlan Technology in Network Security and Access Control and Practice. *Network Security Technology & Application*, **7**, 18-19.

[6] Van Melderen, L. and De Bast, M.S. (2009) Bacterial Toxin-Antitoxin Systems: More than Selfish Entities? *PLoS Genet*, **5**, Article ID: e1000437. http://dx.doi.org/10.1371/journal.pgen.1000437