**Cloud Computing**

### Student name: **姜子玥**

### Student number：71117201

#### School of computer science & engineering

#### of software engineering of artificial intelligence Southeast University

26th April 2020

**1 Introduction**

**1.1 Background**

The concept of "cloud computing" was introduced by IBM in October 2007. Then cloud computing has undergone great development from concept to practice, from technology reorganization to model innovation, all kinds of cloud computing applications have sprung up. The cloud computing trend led by Google, IBM, Amazon, Microsoft and other IT giants, have released cloud computing products and services, such as Amazon's cloud computing service AWS (Amazon Web Services), Google's Google App Engine, IBM's Blue Cloud (Blue Cloud) computing platform, Microsoft's cloud computing platform Azure.

Recent years, due to dynamic deployment, on-demand use and elastic growth, cloud computing has rapidly become a new Internet service model after distributed computing, parallel computing and grid computing, which has received extensive attention from the industry and government..

**1.2 Definition**

The detailed conceptual definition of cloud computing can be summarized by combining the definitions from the relevant literature as follows:

The term "cloud computing" generally refers to cloud computing services, cloud computing platforms that support the operation of cloud computing services and cloud computing-related technologies.First of all, cloud computing service (or "cloud computing business") is a service that provides IT resources (including computing, storage, network, software, etc.) to users on an on-demand basis through the Internet. The provider of such a service is called a cloud computing service provider. Then, cloud computing platform refers to the infrastructure supporting cloud computing services (including data center, hardware, software, operation and maintenance support, etc.), which aggregates large-scale servers, storage devices, network bandwidth and even software resources to form a shared resource pool, and provides network users with "elastic" IT service capabilities through advanced virtualization technology and resource allocation and scheduling on demand. "Elasticity" means that users can quickly access the IT resources they need based on the scale of the business, while "elasticity" also means that the cloud computing platform can act as a powerful computing system to enable tasks such as massive data storage and processing.At last, cloud computing technology refers to the core technology to ensure the efficient operation of the cloud computing platform, involving architecture, operation and maintenance, hardware and software, and other aspects. [1]

**2 Service Models**

Cloud hosting providers offer their "services" according to different models, of which the three standard models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models offer increasing abstraction; they are thus often portrayed as layers in a stack: infrastructure-as-a-service, platform-as-a-service and software-as-a-service, but these need not be related. For example, one can provide SaaS implemented on physical machines (bare metal), without using underlying PaaS or IaaS layers, and conversely one can run a program on IaaS and access it directly, without wrapping it as SaaS.

**2.1 Infrastructure as a service**

IaaS refers to online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc.

**2.2 Platform as a Service**

PaaS vendors offer a development environment to application developers.In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming-language, database, and web server. Application developers develop and run their software on a cloud platform instead of directly buying and managing the underlying hardware and software layers. With some PaaS, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually.

**2.3 Software as a Service**

SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications differ from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand. Load balancers distribute the work over the set of virtual machines.

**3 The security of cloud computing**

**3.1 Security problems**

Users can get full access to a standalone cloud host by paying a cloud hosting provider. While the service is more convenient and faster and the user has easier access to hosting resources, there are certain problems in the process, which can be concluded into three aspects.[2]

First, the data and applications of users of cloud computing services. User data and application hosting in cloud computing platforms face both security and privacy risks, including unauthorized access from cloud computing service providers and other users in multi-tenant environments, data access control, privacy protection, content security management, user authentication and identity management issues.

Second, the cloud computing service platform itself. As the business scale of cloud computing services grows and users increase, the cloud computing platform itself becomes an easy target for hackers to attack. The technical architecture of virtualized computing and storage makes the security of the cloud platform itself particularly prominent, but there is no cloud computing security risk assessment system or third-party cloud platform security assessment mechanism.

Finally, the misuse of services provided by cloud computing platforms. The resilient and scalable resources provided by cloud computing have the potential to be used as a tool for malicious cyberattacks or as a conduit for the dissemination of spam and bad information, but there is currently no monitoring mechanism for the level and legitimacy of cloud computing services.

**3.2 Existing means of protection**

**3.2.1 Cloud Computing Security Alliance**

The Cloud Computing Security Alliance identified 15 focus areas for cloud computing security, made specific recommendations for each area, and selected a number of the more important areas for the development of standards, consulting extensively with IT staff for feedback and recommendations on the statement of requirements during the development process. The 15 cloud security focus areas identified by the Cloud Computing Security Alliance are: Information lifecycle management, government and enterprise risk management, regulation and auditing, general legislation, eDiscovery, encryption and key management, authentication and access management, virtualization, application security, portability and interoperability, data centers, operations management incident response, notification and remediation, legacy security impacts (business continuity, disaster recovery, physical security), and architecture. [3]

**3.2.2 Cloud Computing companies**

Sun Corporation has released open-source cloud security tools to secure Amazon's EC2, S3 and virtual private cloud platforms. The tools include OpenSolaris VPC gateway software, which helps customers quickly and easily create multiple secure communication channels to Amazon's virtual private cloud; security-enhanced VMIs for Amazon EC2, including non-executable stacks, encrypted exchanges and auditing enabled by default; and a cloud safety box, which uses an Amazon S3-like interface to automatically compress, encrypt and disassemble content, simplifying the management of encrypted content in the cloud. Microsoft has prepared a security plan for the cloud computing platform Azure, codenamed Sydney, to help enterprise users exchange data between the server and Azure cloud to address the security of virtualized, multi-tenant environments.EMC, Intel, Vmware and other companies jointly announced a "trusted cloud architecture" cooperation project, and proposed a proof of concept system. The project uses Intel's trusted execution technology, Vmware's virtual isolation technology and RSA's enVision security information and event management platform to build a trusted multi-tenant server cluster from the bottom up. Open source cloud computing platform Hadoop has also introduced a secure version that introduces kerberos security authentication technology to authenticate and control access to users who share commercially sensitive data, preventing unauthorized access to Hadoop clusters by illegal users.

**4 Summary**

In this report, I explained the definition of cloud computing and introduced three cloud computing service models and focused on security in cloud computing. The security is not just a technical issue, it also involves standardization, regulatory model, laws and regulations and many other aspects. I hope that in the future there will be better laws and regulations and more mature technologies to ensure the security of cloud computing in all aspects.

Reference：

[1] Cloud computing. [2020-04-26]. [https://en.wikipedia.org/wiki/Cloud\_computing](https://en.wikipedia.org/wiki/Cloud_computing" \l "Service_models)

[2]刘玮,王丽宏.云计算应用及其安全问题研究[J].计算机研究与发展,2012,49(S2):186-191.

[3]冯登国,张敏,张妍,徐震.云计算安全研究[J].软件学报,2011,22(01):71-83.