Bachelor's thesis

Degree programme in Information Technology

Internet Technology

2015

Yang Ou

THE CONCEPT OF CLOUD COMPUTING AND THE MAIN SECURITY ISSUES IN IT

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information Technology | Internet Technology

June 2015 | 53

Instructor: Ossi Väänänen

Yang Ou

THE CONCEPT OF CLOUD COMPUTING AND THE MAIN SECURITY ISSUES IN IT

This thesis focuses on studying and analyzing the Cloud Computing technology in concept and its security, which is still a developing technology with great convenience and portability for exchanging information over the Internet via different platforms. Cloud Computing provides virtualized and scalable resources dynamically based on the network built with a great number of distributed computers instead of local computer or remote server. Meanwhile, the utilization and application of Cloud Computing is growing dramatically, which boosts a great number of new IT industries by integrating traditional computing technologies.

Thus, this thesis also discusses and explores the practical utility and business value of Cloud Computing. In addition, due to the feature of cloud computing that is highly dependent on worldwide Internet, Cloud Computing is becoming the main target of Internet threats, such as malware or virus, technical vulnerability and negligent behaviors. Thereby, the thesis also addresses the main security and privacy issues in Cloud Computing. Finally, the thesis proposes possible solutions and improvement in technical issues and reflects further development in the future.

KEYWORDS:

Cloud Computing, Cloud Security, Utilization of Cloud Computing, Cloud Computing Service, Cloud Service Provider.

CONTENTS

PICTURES

LIST OF ABBREVIATIONS (OR) SYMBOLS

NIST	National Institute of Standards and Technology (U.S.)
NAS	Network Attached Storage
SAN	Storage Area Network
FC	Fiber Channel
Amazon EC2	Amazon Elastic Compute Cloud
CPU	Central Processing Unit
CEO	Chief Executive Officer
NASA	National Aeronautics and Space Administration (U.S.)
PDA	Personal Digital Assistant
SLA	Service Level Agreement
VAS	Value Added Service
HTML	Hypertext Markup Language
CSS	Cascading Style Sheets
RIA	Rich Internet Applications
REST	Representational State Transfer
ESX	Elastic Sky X
SQL	Structured Query Language
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
EC	Electronic Commerce

TB	Tera Byte
GPU	Graphics Processing Unit
ESB	Enterprise Service Bus
BPM	Business Process Management
AM	Active Messenger
API	Application Programming Interface
ASP	Application Service Provider
RFID	Radio Frequency Identification Devices
GPS	Global Positioning System
SOAP	Simple Object Access Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
I/O	Input/ Output
GFS	Google File System
GB	Giga Byte
RSS	Really Simple Syndication
CLR	Common Language Runtime
WAN	Wide Area Network
SCSI	Small Computer System Interface
iSCSI	Internet Small Computer System Interface
SAS	Serial Attached SCSI
DAS	Direct Attached Storage
IPTV	Internet Protocol Television

VOD	Video on Demand
STB	Set Top Box
FPS	Frames per Second
CDN	Content Distribution Network
MS-SQL	Microsoft Structured Query Language
TPM	Trusted Platform Module
PEKS	Public key Encryption with Keyword Search
XML	Extensible Markup Language
DoS	Denial of Service
RSA	One of the first practical public-key cryptosystems created by Ron Rivest, Adi Shamir, and Leonard Adleman
SSLAP	Secure Sockets Layer Authentication Protocol
IBE	Identity-Based Encryption
IBS	Identity-Based Signature
ABE	Attribute-Based Encryption
PRE	Proxy Re-Encryption
LRE	Lazy Re-Encryption
VMC	Virtual Machine Contract
OVF	Open Virtualization Format
CSA	Cloud Security Alliance

1 INTRODUCTION

Nowadays, the word “Cloud” is becoming increasingly popular in IT. It is very common to hear about Cloud Drive, Cloud Database, Cloud Server, Cloud Security and Cloud Ecosystem. Apparently, the “Cloud” here does not refer to a natural phenomenon. The meaning is short for “Cloud Computing” which is a new aggregated computing technology that is spreading rapidly from small area researching to large-scale developing and utilizing. Obviously, the popularization of “Cloud” is not a coincidence but a demand from Internet market. In addition, it is going to be the foundation of Internet in the next generation and initiate the new pattern of Internet services.

Thus, in order to catch the step of evolving “Cloud”, it is necessary to have basic understanding in the concept of Cloud Computing. Nevertheless, the idea of Cloud Computing is still quite elusive and blurry for non-IT specialists. So, what exactly the Cloud Computing is? What are the key points to build a successful Cloud? What are the benefits and usage in our life and work? Are there any security issues with it and how can we solve them? Gradually, the mysteries of Cloud Computing will be uncovered in the thesis and presented in a methodic structure.

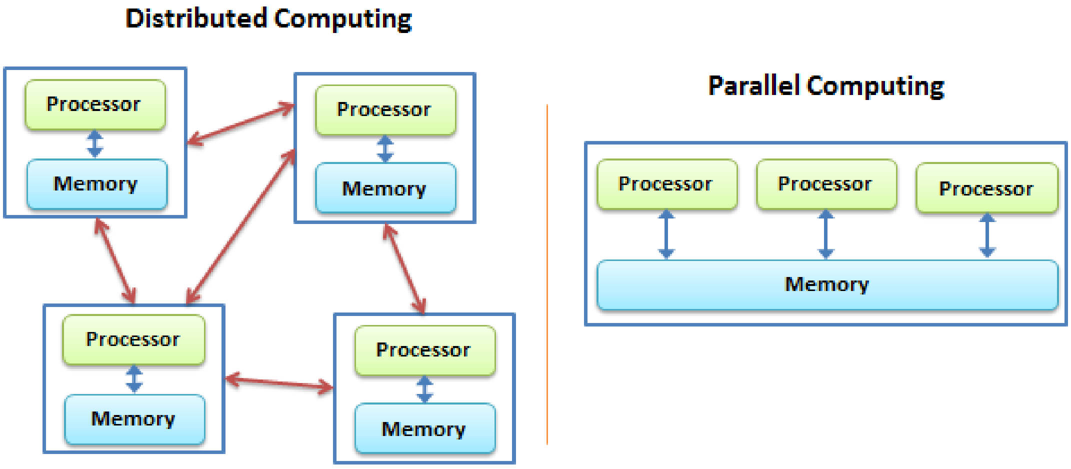
The following chapters will focus on analyzing the essence of Cloud Computing, explaining the implementation of cloud, introducing the typical utilization of it, finally illustrating the primary security issues and certain methods or schemes to solve them.

2 STRUCTURE AND DEPLOYMENT OF CLOUD COMPUTING

2.1 Brief review

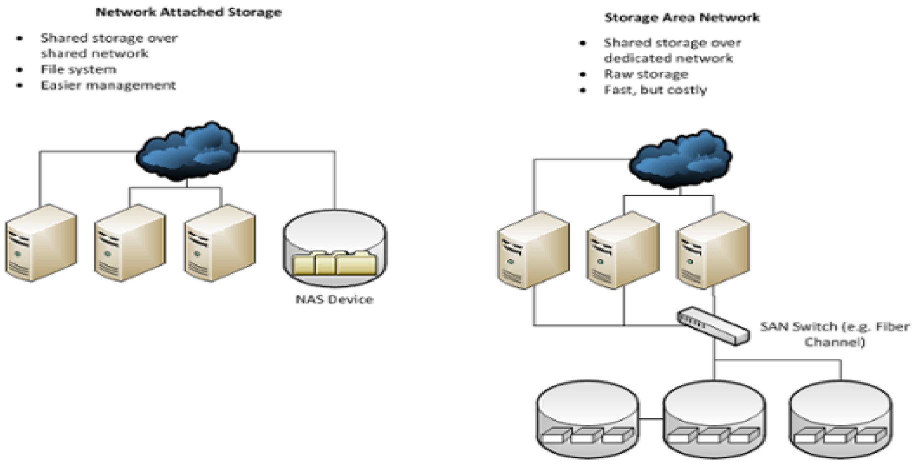
“Cloud” is a shared resource that is extremely effective because it is not only shared by a large number of users, but also can be dynamically accessed depending on the demands (Wikipedia, 2015). It is called “Cloud” due to the dynamic change of scale, abstract boundary, and ambiguous location like a real cloud in the nature, however, it does exist in the actual world. Cloud is not sets of hardware, software or services. It is the combination and integration of massive information technologies. In addition, the size of Cloud is growing since new developing technologies keep joining the group. Besides, the National Institute of Standards and Technology of U.S. Department of Commerce defined that “*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models”*. (U.S. Department of Commerce, 2011).

Generally, Cloud Computing is the combination of traditional computing methods and networking Technologies such as Distributed Computing, Parallel Computing, Utility Computing, Network Storage Technologies, Virtualization, Load Balance, High Available etc. (U.S. Department of Commerce, 2011). For instance, Distributed Computing is targeting a dividing a large computation into small segments and assigning multiple computers to calculate, then collecting all of the results and assembling them together (Equn.com, 2015). Meanwhile Parallel Computing aggregates a large number of computational resources to process a particular task, which is a highly efficient solution for parallel problems (Tu *et al*., 2010). Picture 1 shows the comparison between Distributed Computing and Parallel Computing (Kong, 2012).



Picture 1. Distributed Computing and Parallel Computing

Moreover, Network Attached Storage (NAS) Technologies connect storage devices with a group of computers via standard network topology. NAS fulfills the need for rapidly increasing storage volumes, providing sufficient storage space for the connected hosts. Meanwhile, another Network Storage Technology is Storage Area Network (SAN), which utilizes Fiber Channel (FC) connects to a group of computers without standard topology, usually used in high volume storage environment. Pictures 2 shows the different topology of NAS and SAN (Kline, 2011).



Picture 2. NAS and SAN

However, the above mentioned technologies are only part Cloud Computing, indirectly indicating the enormous scale of Cloud Computing. Thus, Cloud Computing is another giant transformation since the 80s in information technology, from mainframe computer to client-server mode. Until now, many famous IT companies have utilized and deployed the research and development of Cloud Computing due to its potential of commercial value and revolutionary technology.

2.2 History and evolutions

To understand Cloud Computing, its history and evolutions must be mentioned. The term “Cloud” dates back to 1950s; during that time, the mainframe computer was taking priority in the computation field, considered as the future of computing, becoming quite fashionable in academia and corporations. However, due to the lack of internal processing capacities and access by client computers, a proposal was made to allow multiple users to share physical access to computer and CPU time from multiple terminals. It has been known in industry as time-sharing (Strachey, 1959). Thus the rudiment of “Cloud” was formed.

In 1983, the Sun Microsystems came up with the idea that “the network is the Computer”, jumping out of the traditional boundary defined for the computer. In March 2006, Amazon published its Elastic Computer Cloud service, providing resizable computing capacity in the cloud which makes the web-scale cloud computing easier for developers. Besides, the computing resources are completely controllable and have scalable capacity with the change of computing requirements (Amazon, 2007). In the same year, on 9th of August, the CEO of Google, Eric Schmidt, firstly presented the concept of “Cloud Computing” based on the Project “Google 101” by engineer Christophe Bisciglia. In October 2007, Google and IBM stared promoting Cloud Computing in American universities, including Carnegie Mellon University, Massachusetts Institute of Technology, Stanford University, University of California Berkeley, and Maryland University. The project, aiming at reducing the cost of distributed computing in academic research, also provided support in hardware, software and technique. On January 30, 2008, Google announced initiating “The Cloud Computing Project” in Taiwan, cooperating with National Taiwan University and National Chiao Tung University to popularize this technology in campus. On February 1, 2008, IBM announced the building of the first Cloud Computing center in Wuxi, China. In the same year, on July 29, Yahoo, HP, and Intel published an associated research program in U.S.A, Germany and Singapore, targeting on building 6 datacenters as research platform, every data center configured with 1400 to 4000 processors. On August 3, 2008, Dell was applying the trademark right aiming at reinforcing the control power for this term may remodel technical architecture (Gu, 2014). In the same year, Microsoft created Microsoft Azure which is a Cloud Computing platform and infrastructure, offering applications and services establishment, implementation and management via Microsoft datacenter (Microsoft Azure, 2008). In July 2010, NASA, Rackspace, AMD, Intel and Dell proclaimed an open source project, “OpenStack”, which controls large pool of computer, storage, and networking resources throughout a data center, used as creating private and public clouds (OpenStack, 2010). Soon, IBM and Oracle announced their cloud “IBM Smart Cloud” and “Oracle Cloud” in 2011 and 2012 (Wikipedia, 2015). Through the above history and evolution of cloud, it is quite obvious that cloud technology made extremely rapid progress after 2000 and is becoming more and more mature and widespread.

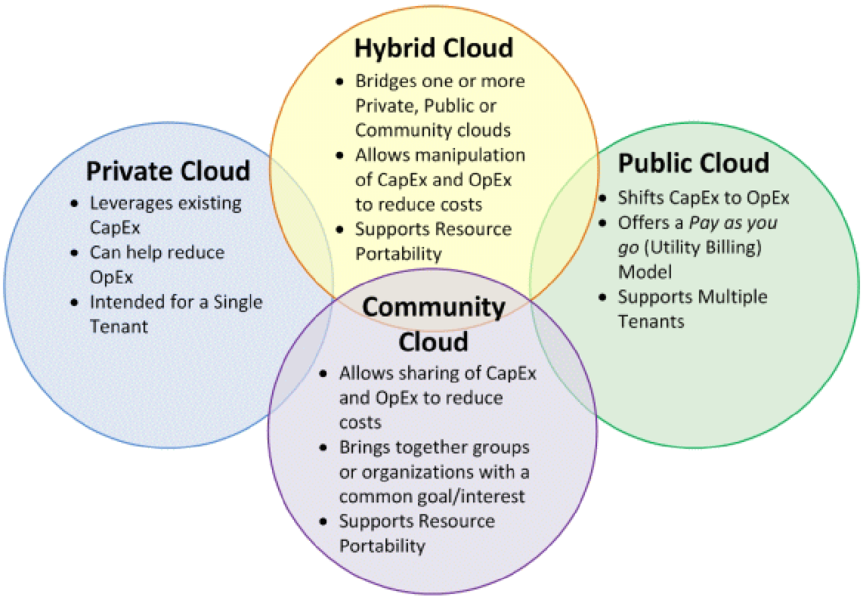
2.3 Features

It is crucial to excavate the essence of success of Cloud Computing. Why it is becoming popular and widely accepted by various IT companies and customers, what is the attractiveness of Cloud Computing, how could it rise up in a limited time?

Therefore, we have to discuss the features of it. First of all, the large-scale deployment draws the attention, in terms of statistic, worldwide IT companies such as like Amazon, Apple, Cisco, Google, HP, Lenovo, Microsoft, IBM, etc. have implemented a large number of severs for Cloud Computing. Among them, Google has over 1 million servers; Amazon, IBM, Microsoft and Yahoo has hundreds of thousands of servers, which ensures the unpredictable computation capability for the users around the world. Secondly, the benefit of virtualization is significant. It supports users access from anywhere on any terminal. All the requested resources come from the “Cloud” instead of tangible entities. The application is running somewhere inside the “Cloud”, however, there is no need for users to know the exact running place. It only requires a laptop, PDA, or smartphone to acquire the experience of a variety of services with super strong capabilities. Thirdly, the “Cloud” is a highly reliable resource. Many duplicates have been created to provide fault-tolerant, and exchangeable computing nodes to guarantee the reliability of services. It is more credible to use the “Cloud” than local computers. Meanwhile, the “Cloud” is versatile, because it does not focus on certain application. With the support of the “Cloud”, applications could be daedal. The same “Cloud” is able to sustain different running applications simultaneously. Moreover, the dimension of the “Cloud” is extensible to satisfy the needs of a growing number of applications and users. Service on demand is another critical feature of the “Cloud”. It is a huge pool of resources which users can purchase based on their requirements. The charges are the same as tap water, electricity and gas. In addition, due to the special fault-tolerance method consisting of cheap nodes in the “Cloud”, the automatic control of the “Cloud” lowers the cost of data center management dramatically; The universality and commonality of it increase the availability of resources substantially; The facility of the “Cloud” usually locates in the area where it is full of electrical resources, which leads to the decreasing of energy cost. Therefore, the cost performance is incredibly high. So, users can completely enjoy the perfect services of the “Cloud” regardless of high level of consumption and long period of computing (Liu, 2014).

2.4 Main types of cloud

In order to fully understand the work mechanism of the cloud, it is necessary to introduce the types of deployment. Here are the following common ways to utilize the cloud. Picture 3 shows the cloud deployment models (Jesús, 2012).


Hybrid Cloud
Bridges one or more Private, Public or Community clouds
Allows manipulation of CapEx and OpEx to reduce costs
Supports Resource Portability
Private Cloud
Leverages existing CapEx
Can help reduce OpEx
Intended for a Single Tenant
Public Cloud
Shifts CapEx to OpEx
Offers a Pay as you go (Utility Billing) Model
Supports Multiple Tenants
Community Cloud
Allows sharing of CapEx and OpEx to reduce costs
Brings together groups or organizations with a common goal/interest
Supports Resource Portability

Picture 3. Cloud deployment models

2.4.1 Private cloud

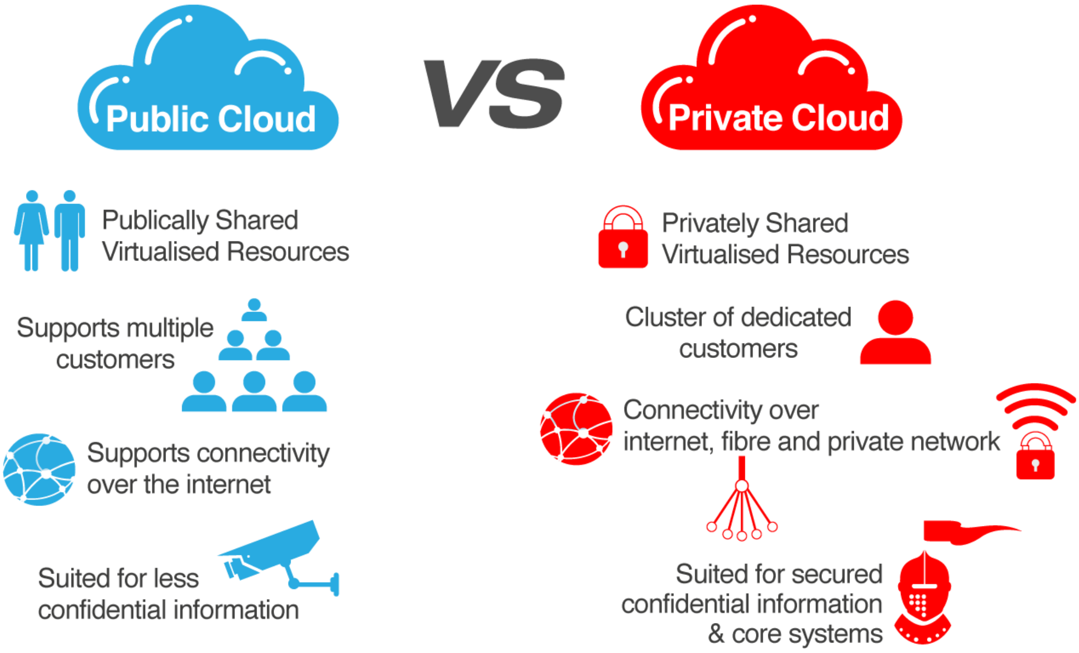
A private cloud is built for a single client or organization, which can effectively control data, security and quality of service. The company has infrastructure and manipulates the deployment of applications through it. The core value of private cloud is private resources.

Private cloud can be established by a company or a cloud service provider. Based on this hosted management, cloud service providers such as Sun and IBM are supposed to install, configure and maintain the infrastructure to support the private cloud holding the business datacenter owned by a certain company. In this way, the usage of cloud resources are strongly controlled by the company, at the same time, the professional knowledge of building and running this environment can be acquired.

The advantages of private cloud are obvious. First, the data is relatively more secure than other deployment methods. Although many public cloud providers announced that their service is extremely secure in all aspects, especially the management of data, however, to many large corporations, the data which concerns to business is their vital part, and cannot be damaged by any threat. Thus, it is impossible for them to deploy applications on public cloud, while a private cloud is usually built behind the firewall, so it is more secure than a public cloud. Then, it also benefits from SLA. When the company staff access to the applications based on a private cloud, the SLA is highly reliable regardless of the influence from unstable Internet connection because the cloud is behind a firewall instead of a remote datacenter somewhere. In addition, some private clouds are able to utilize existing hardware to build cloud and are more compatible to legacy applications than a public cloud, which reduces the cost and enhances the availability at the same time. Further, a private cloud has the advantages of maintaining data management and safety regulations without affecting the management process, while a public cloud will impact it dramatically (Microsoft, 2013).

2.4.2 Public cloud

Public cloud usually refers to the cloud offered by third-party cloud service providers achieved by accessing Internet. The cost is relatively low or free. In such way, a company provides its service external users access to their own infrastructure directly, and external users access the service through Internet without possessing cloud computing resources. There are also some merits to the public cloud. It provides a reliable and secure data storage center compare to other storage methods. In the past, many people thought the data can only be secured in their own computers; apparently this is not true. The local computers may be physically damaged, attacked by virus or hackers, even malicious action from someone who can access the computer. On the contrary, if files are stored in public cloud storage, the data will be kept in the servers permanently and authorized access will be required. In the meantime, a public cloud can support different hardware comprehensively. Besides, due to the large number of users in public cloud, it is quite convenient to share files or storage with others as well as access giant number of public resources. It integrates upstream like advertisements and VAS with downstream end users, creating a new value chain and ecosystem (Microsoft, 2013). Picture 4 illustrates the main differences between public cloud and private cloud (Skali Group, 2011).


Public Cloud
VS
Private Cloud
Publically Shared Virtualised Resources
Supports multiple customers
Supports connectivity over the internet
Suited for less confidential information
Privately Shared Virtualised Resources
Cluster of dedicated customers
Connectivity over internet, fibre and private network
Suited for secured confidential information & core systems

Picture 4. Public cloud vs Private cloud

2.4.3 Community cloud

A community cloud allows multiple independent entities to acquire cost benefits in a shared non-public cloud. It is a component in public cloud, deployed on certain range of area and formed as a community. This model has enormous potential for companies or organizations that are subject to identical regulatory, compliance, or legal restriction (Winkler, 2011). Community clouds are usually built in the place where users have similar requirements, offering unified services. For example, in university towns, the users are teachers, students, and staff from all kinds of universities, research facilities, and service agencies. The services include cloud hosts, cloud servers, cloud storage, and a cloud datacenter.

2.4.4 Hybrid cloud

A hybrid cloud is a composition of multiple clouds which remain different entities but also bound together. The benefits come from multiple deployment models (U.S. Department of Commerce, 2011). As mentioned before, a private cloud is more secure than a public cloud, but a public cloud possesses a tremendous number of public resources. Hence, a combination of a public cloud and a private cloud gives to perfect solution to this contradictory situation: hybrid cloud. It has the security features of private cloud that preserves internal important data in the local datacenter and can also utilize the computing resources from the public cloud to complete work efficiently and effectively. Besides, it breaks the hardware limitation of a private cloud by taking advantage of extensibility of the public cloud to gain higher computation capacity. Furthermore, the cost would be lower because it can switch between public cloud and private cloud based on the users' requirement that assigns application and data on the most appropriate platform.

2.5 Cloud architecture

As a part of the extension of virtualization, the influence of cloud computing is becoming more and more significant. However, the current cloud computing is not able to support a complicated enterprise environment. Therefore, the details of cloud architecture need to be developed further before cloud computing becoming mature enough. Based on the analysis of existing cloud products, the cloud architecture can be divided in four layers.

- Presentation layer

Plenty of cloud computing datacenters use this layer to display the contents that users required and the experience of services in a friendly users interface. In the meantime, the services provided by the intermediate layer, which will be introduced later, are implemented, mainly including five technologies:

HTML: a standard web pages technology, HTML4 takes the primary position, but the upcoming HTML5 will push the development of web pages in concern of video and local storage.

JavaScript: a dynamic programming language used in web pages, dramatically enriching the content of website, so users can interact with it throughout.

CSS: used to embellish the appearance of web pages, also separates the contents and manifestation elegantly.

Flash: frequently applied RIA technology, is capable to provide web-based RIA that HTML cannot offer, acquiring excellent reputation in user experience.

Silverlight: this RIA technology is from IT giant Microsoft. Although the market share is less than Flash, the programming language is friendly to developers due to the high efficiency of C#.

- Intermediate layer

This layer is a connecting links between the preceding and the following. It provides multiple services in the downstream infrastructure layer that owns resources, such as cache service and REST service, which can supply both presentation layer and is called by using, primarily five technologies:

REST: Representational State Transfer (REST) is a software architecture style (Fielding and Taylor, 2000) for creating scalable web services (Richardson and Ruby, 2007) generally runs over HTTP. By using this technology, a caller can easily obtain part of services supported by the intermediate layer with convenience and elegance.

Multiple lessees: it is achieved by assigning one single application sample to multiple organizations, while offering great isolation and security, also reduces the cost of application purchasing and maintenance.

Parallel processing: in order to process large number of data, the enormous X86 cluster is required to accomplish a huge scale of parallel processing. The Map Reduce from Google is a reprehensive of this technology.

Application server: this is an optimized server based on cloud computing. For instance, the Jetty application server is used in Google App Engine.

Distributed cache: not only can it release the pressure of backstage server due to high flow transmission, but also accelerate the responding speed. The most famous model is “Memcached”.

- Infrastructure layer

It is used to preserve computing and storage resources for upstream Intermediate layer or users. Four technologies are frequently applied:

Virtualization: in other words, it is the “Multiple lessees” in the infrastructure layer. It can achieve the goal of running multiple virtual machines on a single physical server, completely isolated with each other. The cost of server purchasing has been decreased as well as the running and maintaining fee. VMware, ESX and open source Xen are full-fledged X86 virtual machine technologies.

Distributed storage: the distributed storage can take care of abundant data and ensure the manageability of those data.

Relational database: an optimized original relational database to meet the requirements of extensibility and management, it is more compatible in cloud computing.

NoSQL: it is used to dispose certain targets that cannot be handled by relational database, such as supporting massive data and databases not based on the relational model.

- Management layer

The services on this layer are vertical and supply multiple management or maintenance technologies for the above-mentioned three layers, in following the six aspects:

Account management: the favorable account management technology provides a secure and convenient environment for users as well as management for administrators.

SLA surveillance: when applying surveillance on the services and applications of virtual machines in different layers, it is important to ensure they can run in terms of the pre-configured SLA environment.

Accounting management: it means running statistic calculation on resources that every user consumed to charge service fees.

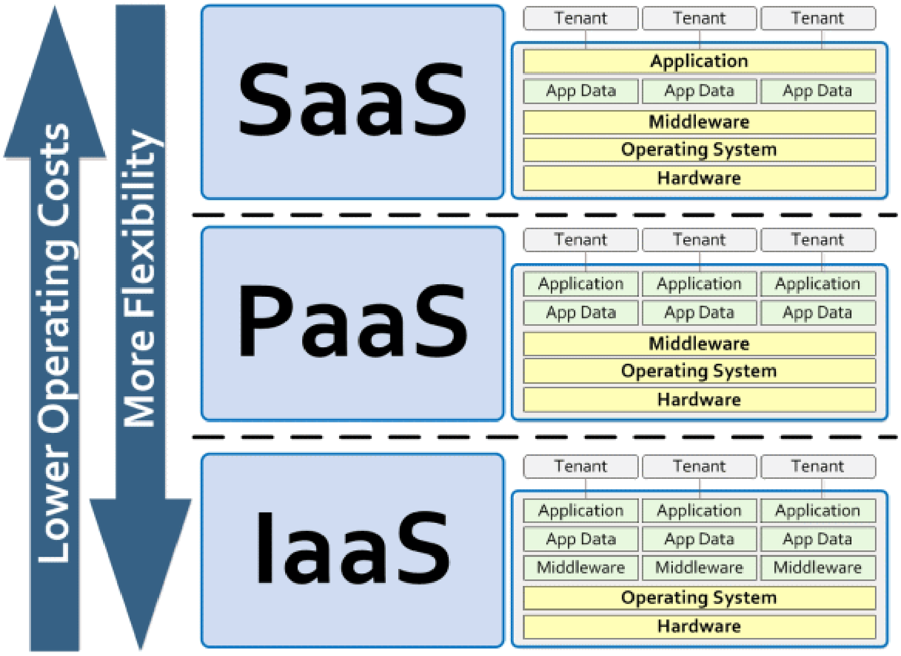
Security management: it secures data, application, account and other IT resources, preventing them from being attacked by hackers and malwares.

Load balance: it is a countermeasure that distributes traffic to instances of one application or service to deal with emergency.

Operation and maintenance management: this technology focuses on implementing specialization and atomization to the operating and maintaining process to reduce cost (Wu, 2010).

2.6 Service models

The cloud computing provides services according to the following levels: Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS) which is defied by NIST but is widely accepted around the world. Picture 5 shows the cloud service delivery models. In the stacks in each level, the yellow highlighted blocks are the components that shared by tenants (Jesús, 2012).



Picture 5. Cloud service delivery models

From Picture 5, we can clearly find out the relationship among three models vertically as well as the pattern they present. In the horizontal positon, we are also able to observe the relationship in components from each models (Jesús, 2012).

2.6.1 Infrastructure as a service (IaaS)

IaaS provides the service focusing on the utilization of all computing infrastructure, including CPU, memory, storage, network and other basic computing resources that can be deployed and run by users such as operating system and applications. Consumers are not asked to manage or control any cloud computing infrastructures, but they can control the selection of operating system, storage space and deployed application as well as acquire the right of control of restricted network components like router, firewall, and load balance controller (U.S. Department of Commerce, 2011).

Consumers can receive perfect services from computer infrastructure, which are called infrastructure as a service. The service based on Internet is part of IaaS such as storage and database. The best example to describe IaaS is there are hundreds to thousands Amazon EC2 virtual machines that process TB level documents in 36 hours in The New York Times. Without EC2, it will take days to months for New York Time to process those data.

Usually, there are three ways to apply IaaS: public cloud, private cloud and hybrid cloud that have been mentioned before. Amazon EC2 utilizes public server pools in infrastructure. More private services will use a set of public or private server pools in a company's datacenter. If the datacenter environment of the company is used to make software development, in this way, the public, private and hybrid cloud are all available. Besides, the cost of EC2 used as temporary extensive resources is quite low and shortens the development or testing cycle. However, there are vulnerabilities in IaaS. For example, if a service provider offers a shared infrastructure, that is to say, some components or function like CPU cache and GPU, are not completely isolated to system users, this will lead to a consequence that when an attacker succeeds to breach in the system, all of the servers are exposed to him or her, even with hypervisor, some of the client operation systems can gain access to infrastructure that are not controllable. Therefore, a power partition and defense strategy has to be assigned. The IaaS service provider must monitor the environment to prevent unauthorized modification and activities (Wikipedia, 2015).

Until now, plenty of manufacturers have participated in building cloud computing infrastructures such as VMware, Microsoft, IBM and HP. However, creating a private cloud through them is extremely expensive. Hence, the users have to think twice before making any risky movement.

2.6.2 Platform as a service (PaaS)

In this model, cloud service providers offer a computing platform, mainly containing an operating system, a programming language execution environment, a web server and a database (Wikipedia, 2015). The idea is to use server platform as a business model that delivers services. The service which provides programs through the Internet is called SaaS (Software as a Service), thus the server platform or developing environment are the carrier of it. Theoretically, PaaS is one of SaaS applications. PaaS is also the application infrastructure service in the cloud computing environment, called middleware as a service. PaaS is located in the middle of the service models, under SaaS and above IaaS. Based the on traditional On-premise deployment, there are plenty of different middleware, such as application server, database, ESBs, BPM, portal and AM. PaaS is usually divided into two types; one targets on application deployment and running APaaS (Application Platform as a Service). The other one is called IPaaS (Integration as a Service). Basically, PaaS refers to APaaS, like Force and Google App Engine.

PaaS is able to integrate all kinds of current business, typically as application server, business capability access, business engine, and business open platform. To downwards, it calculates infrastructure capability according to business requirement, and calls hardware resources based on the API provided by IaaS.

To upwards, it delivers business dispatch service, monitoring every kind of resources in real time and passing those resources to SaaS end users via API.

The greatest different between the PaaS service with others is that it provides the whole infrastructure platform instead of a certain application. In traditional notion, the platform is the fundamental service station for exteriors. In addition, it should be built and guarded by application service providers but PaaS has overturned this idea. The platform service providers are responsible for establishing and maintaining this platform and deliver it to the application system providers via services.

Besides, PaaS providers also support technical services such as application system development and optimization. Technical support team from Paas providers also facilitate the process of research and development in new application system to assist with stable and long-term operation.

The substance of PaaS is to transform Internet resources services into a programmable interface, supporting third-party developers with business valuable resources and platform. With the help of PaaS, developers can acquire massive programmable elements that have specific business logic to support development. This not only increases efficiency, but also saves the cost. Web applications could be developed in a more agile way and respond to users faster, which will bring solid benefits to the end users in return.

Some examples will be given for a better understanding of PaaS. The Internet giant Amazon is famous for providing the EC site to individuals. It rents out the system platform which originally built for themselves. Users can choose the operating system and middleware freely through this service that offers hardware and software platform. From 2006, Amazon EC pushed this service into market use. The renowned IT magnate Google has built a large number of datacenter around the world and is famous for its search engine as well as new types of advertisement. Google purchased cheap computers and powerful middleware plus their own technologies equipped the most powerful datacenter worldwide and high performance parallel computing cluster. In April 2008, they launched their PaaS Google App Engine that is running many Google applications such Gmail, Google Search, and Google Map making great success in integrating scattered applications or services. PaaS plays an important role in business value development (Teng, 2014).

2.6.3 Software as a service (SaaS)

With the development of Internet technology and the maturation of applied software, there is a new software application model rising in the 21th century. It has a similar idea to On-demand software, ASP, and Hosted software. The model provides software through the Internet, where manufactures place software on their own servers and clients can subscribe to applied software services via the Internet on their demand. The service fees depend on the number of services and the time of usage. Users do not need to purchase software anymore, instead, they acquire web-based software through providers by lease to manage company operations without local software maintenance that will be fully managed and controlled by providers. Software manufacturers not only offer the Internet application but also support offline operations and local data storage, which is beneficial to users because they can utilize it anytime in anywhere. For many small companies, SaaS is the best way to apply high technologies because it eliminates the barrier of purchase, establishment and infrastructure maintenance for companies.

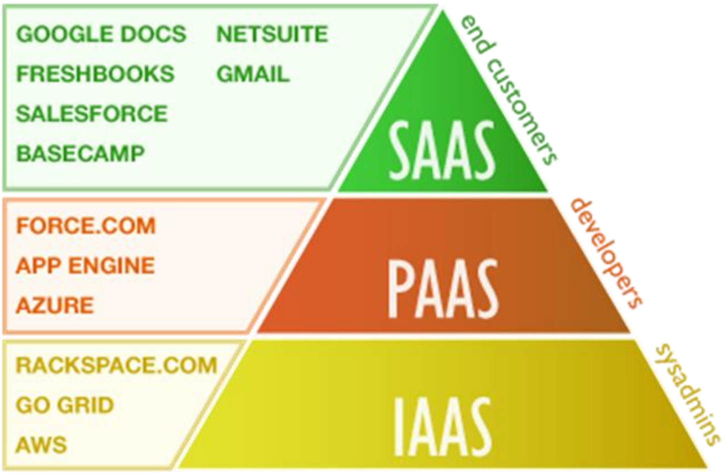
The cost of SaaS software is usually in a full package, including usual software license fee, maintenance fee as well as technical support fee that have been integrated as monthly rental fees. However, the range of SaaS is quite wide, covering from small or middle companies to large corporations. The charging method is also flexible. On the one hand, companies can add or subtract account on their needs. On the other hand, the cost from the actual account and time helps with reducing service fees and that is cheaper than the traditional charging method.

What makes SaaS so particular? Actually, when the cloud was not popular, we already made contact with some of the SaaS applications; we can use Google and the Bing search engine via web browsers; E-mail is accessible in our computers without installing a search system or email system. In contrast, when we are using old version of Microsoft Office, like Word, Excel and PowerPoint, it requires installation. However, when it comes to Google Docs and Microsoft Office Online website, no installation is required, it is enough to just open the browsers, and register an account, then all the documents are read, and modification and save are available. Users do not even bother to update and maintain software. In addition, technical measures are applied to guarantee safety and confidentiality.

The technical requirement for SaaS is crucial. Until now, SaaS has evolved from 1.0 version to 2.0 version. It has transformed from all applications and functions that offer resource in a single mode delivered by service provider to the level that service providers deliver core SaaS application. They are also supposed to cooperate with development and business partners to build a set of highly customized and fast response platforms which assist those partners to rapidly configure SaaS application, aiming at particular field or business as well as integrate with applications made by the service providers tightly. Hence, it will create a compact service ecosystem in promotion, sales, and distribution etc., finally reaching to a win-win situation by sharing profits.

The SaaS 2.0 mode asks for flexible customization, instant deployment, rapid integrated SaaS application platform that provides web-based application customize, development and deployment tools to ensure stability and reliability. With the guarantee of publishing new modules and increasing number of clients, service providers should make sure that the development and business partners can generally utilize all application configuration tools, management application including data, interface, process, logic, algorithm, statistic, and report forms. Moreover, SaaS 2.0 requires service providers to deliver a channel with rich content and shared information so that end users, development teams, distribution, partners can communicate with each other through this channel.

Problems appear with the popularization of SaaS, mainly data security and service level. Thus, it is significant to know how the providers deliver their services and how they secure information. Usually, manufacturers store and backup data in multiple storage pools. Multiple encryption algorithms have been applied during data transmission, users access etc. SLA is the tool to justify users' satisfaction, and it has been widely used by 99% of users. SLA defends the right in both sides, users and manufacturers, the terms of which are protected by laws and regulations to prevent violation (Zhou, 2011). The specification of those issues will be discussed in the following chapters. Picture 6 illustrates cloud service types and offers examples in a pyramidal model, which helps with better understanding of it (Moosa, 2014).



Picture 6. Cloud service types and example

3 TYPICAL UTILIZATION OF CLOUD COMPUTING

3.1 Internet of Things

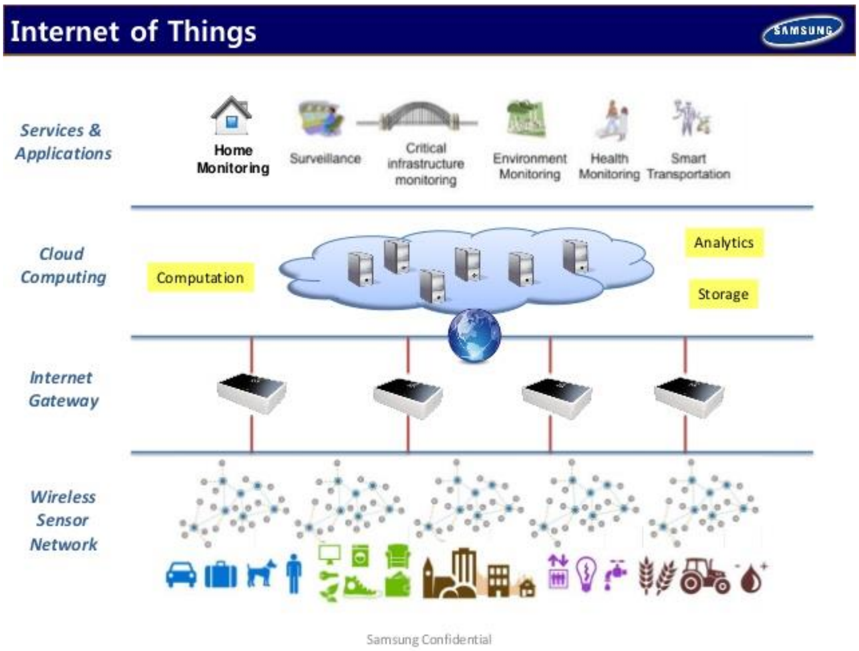
The Internet of Things is a significant part of a new generation of information technology, and a crucial phase of informatization. Internet of Things means things are connected through the Internet which has two meanings. First, the core value of the Internet of Things is still an Internet technology that extends and expands its network. Second, the definition of users enlarges to things, exchanging information and communicating. By using RFID, Infrared sensors, GPS, laser scanners and so on, according to agreed arrangements, the Internet of Things has been widely applied in aggregated networks that achieve the goal of intelligent recognition, positioning, tracing, monitoring and management on things, which is called The Third Wave in information industry after computing and Internet. It is a great technological innovation that makes everything existing in the world have a unique identifier. Through tiny but powerful RFID, Two-dimension Code Recognition, information of things will be collected and transformed into information flow then integrated with the Internet. This establishes a new type of communication between human and things, and things and things. Eventually, this way of communication will change the lifestyle and behavior patterns.

However, cloud computing technology is the core of implementing the Internet of Things and enhances the coalescence of the Internet of Things and Internet technology. The deployment of the Internet of Things can be simplified as following steps:

Step1: it identifies the property of things, including static and dynamic property while static property can be saved in labels directly but dynamic property has to be detected by sensors real-timely;

Step2: after gathering the properties of things, devices transform information into data format that is capable of network transmission;

Step3: this information is transmitted to information processing center including distributed and centralized facilities. The information processing center will process related computing to information from things. Picture 7 shows the typical model of the Internet of Things along with cloud computing (Samsung, 2014).



Picture 7. Internet of things service model

In the application field, cloud computing is always combined with the Internet of Things to create an inter-connected, massive data provided and integrated in the service platform. For example, a public smart surveillance system in a large city has combined security precaution technology, applied computer technology, network communication technology, video transmission technology, video analyzing technology, access control technology, sensor technology, wireless technology, database technology, cloud storage, and cloud computing to a giant system that is capable of automatic analyzing, switching, judging, alarming on marked video data, building a service mode and system on a cloud platform (Yang and Zhou, 2011).

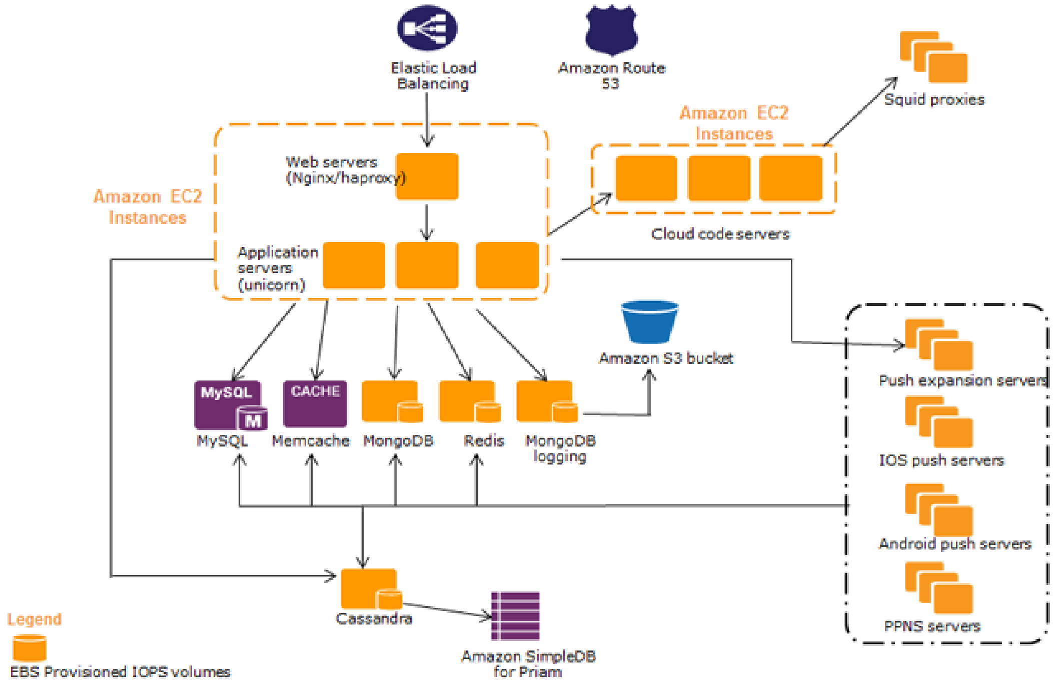
3.2 Cloud computing platform

The cloud computing platform is a new type of platform to provide cloud services. It has plenty of advantages by applying cloud computing technology and replacing the place of traditional platform. The features of cloud computing are dramatic: cloud data, cloud software, omnipresent computing, powerful computing, simple to use, advanced functions, diverse users, and shared resources. Until now, some of the IT companies have provided their cloud computing platform, like Microsoft Azure, Google App Engine and Amazon EC2. In addition, users can build their own cloud beyond that. Many open source software are available on the market, some of them for web servers, some of them for application servers, some of them for datacenters etc. So, it is possible to create a cloud computing platform based on open source software, instead of purchasing any commercial software and utilizing a private API on business platform. The company which runs this platform can charge service fees from users to cover their cost and even gain a profit. In order to understand better the cloud computing platform, it is essential to introduce some cloud computing platform service providers.

- Amazon EC2

According to the three layers model (hardware platform, cloud platform and cloud service) of the cloud computing platform, Amazon EC2 is approaching to the hardware platform, which provides hardware virtual machine to clients. Clients will feel more like using a hardware and they have rights to control the entire software layer. The exterior API of EC2 is also mainly used to request and configure those virtual devices, known as hosted cloud computing platform due to the access of remote control interface by users. From the aspect of architecture, Amazon EC2 is built based on the large-scale of cluster computing platform inside the company, while users are able to use the network interface to manipulate multiple instances on platform, and payment depends on the amount of usage. Actually, in 2006, Amazon launched its Simple Storage Service, which charges monthly for services, and at the same time, users have to pay for the network data traffic.

The Amazon network service uses REST, SOAP and other standard interfaces that allow users to access corresponding storage services. After that, Amazon developed EC2 system based on it. Users on EC2 interact with interior instances through the SOAP on HTTPS which secured the remote connection and prevented leakage of data in transmission. Picture 8 shows the complete Amazon EC2 architecture (Amazon, 2012).



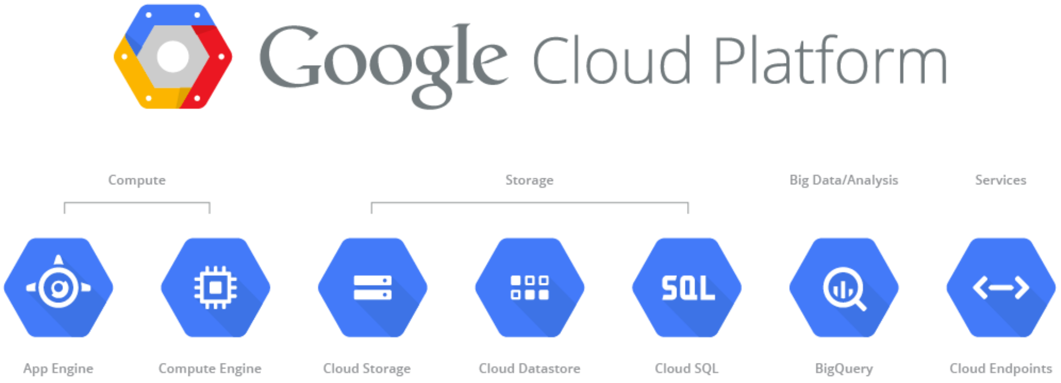
Picture 8. Amazon EC2 architecture

However, instances in EC2 are real running virtual machine servers while every instance represents a running virtual machine. When a virtual machine is assigned to a user, he or she always has full access right, including administrative user privilege. Because it is always for users to utilize more than one instance to deploy network application, there is an intranet among instances inside EC2 to implement communication of application in different instance that each of them has an internal IP address and external address which provides service for exterior. According to Amazon EC2, the hardware platform usually apply virtual technology that shares CPU and memory, but being slightly inferior on I/O sharing which could be fixed by flash memory.

- Google App Engine

The Google search engine was built on the basis of over 200 locations and over 1 million servers, in the meantime, the number is still increasing. Google Map, Gmail, Google Docs etc. are also created on this infrastructure. By using those

Apps, user data will be stored in somewhere on the Internet and always be accessible. App Engine provides a platform for traditional network applications as well as a Python application server cluster. Therefore, clients can develop and publish their own network application system. Google cloud computing platform typically consists by following components: “Google File System (GFS)” built on cluster, “Map/Reduce” programming module and large-scale distribute database “BigTable”.



Picture 9. Google Cloud Platform

Picture 9 illustrates the basic structure of Google cloud platform (Bechtolsheim, 2013). GFS has the same benefits as a traditional distributed file system, such as performance, extensibility, reliability and availability. Besides, it owns some special features. It is a normal to have node failure in cluster instead of abnormal. Due to the large number of nodes in calculating and processing as well as working simultaneously, the node failure happens quite often, which requires monitoring the dynamic running status of system by applying software application module and surveillance system to detect errors, and also integrates fault-tolerant and automatic recovery in the system. The size of file in GFS is usually measured by GB. In addition, the purpose of the file in the file system is different with ordinary file, because a big file could contain lots of small files. The read and write mode in GFS is also different from the traditional file system. The modification of file is not overwriting original file, instead, adding new data in the end of the file. There is no random write on the file. Moreover, some operations in GFS are not transparent anymore, requiring the assistance of application. The cooperation between application and the system API enhances the flexibility of entire system. Overall, GFS is designed for Google applications.

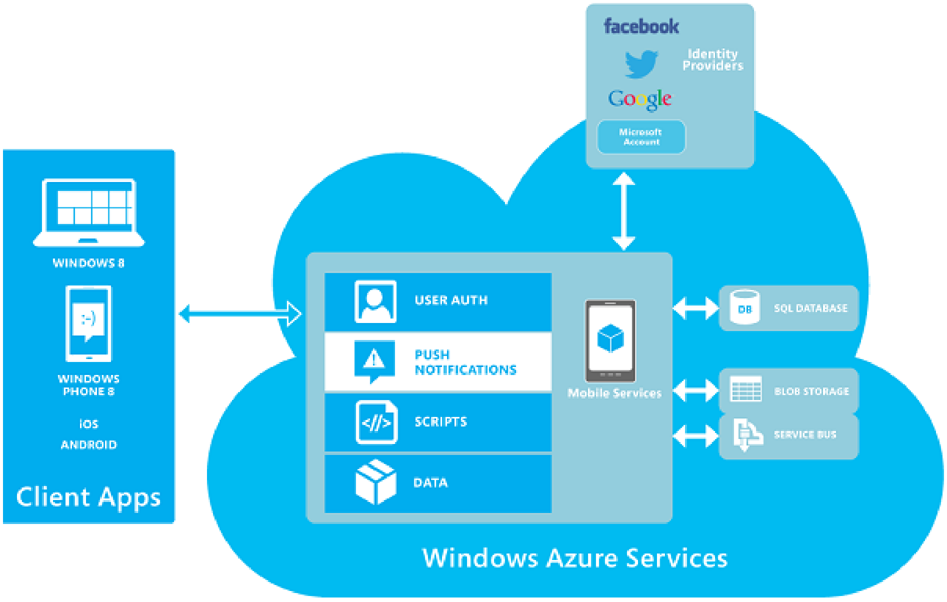
In order to build applications on the large-scale cluster, Google has designed and achieved a set of large-scale data processing programming standard called Map/Reduce system. It helps programmers to focus on application itself meanwhile the platform will handle the processing of cluster. Usually, users only need to provide their Map and Reduce function to implement large-scale distribute data processing on cluster.

Google extends their database system to distributed platform BigTable. In order to deal with massive formatted or half-formatted data, Google established large-scale database system BigTable which holds many applications like Search History, Maps and RSS reader. The content in BigTable are sorted by rows, and multiple rows form a Tablet.

Those are three main parts of the Google interior cloud computing platform.

- Microsoft Azure

The Azure platform for Microsoft is between above mentioned platforms, mainly consisting of two parts, Windows Azure and Microsoft SQL Azure. The former is an operating system, while the latter is a relational database software. Clients use .NET to write program, then the program will be compiled as CLR that is a running environment and has no relationship with the programming language. Windows Azure provides a virtual computing environment and storage based on Windows. That is to say, we can treat Windows Azure as a cloud operating system whose bottom is large number of 64-bit Windows server. Windows Azure can organize those servers effectively by using the Fabric Controller in the bottom to make sure the computation and storage capability for front-stage application as well as enhance reliability (Yang and Zhou, 2011). Picture 10 shows the architecture of Microsoft Azure (Microsoft, 2012).



Picture 10. Microsoft Azure architecture

3.3 Cloud storage

Cloud storage is a new concept as the extension of cloud computing, also a new born network storage technology. It means using cluster application, network technology or distributed file system to aggregate massive and various storage devices in the network while implementing cooperative work that provides data storage and business access. When dealing with large amount of data storage and management, the cloud computing system requires huge number of storage devices, therefore, the cloud computing system will turn into a cloud storage system. Hence, the core value of cloud storage is data storage and management. This new storage solution allows access from anytime at any place via Internet.

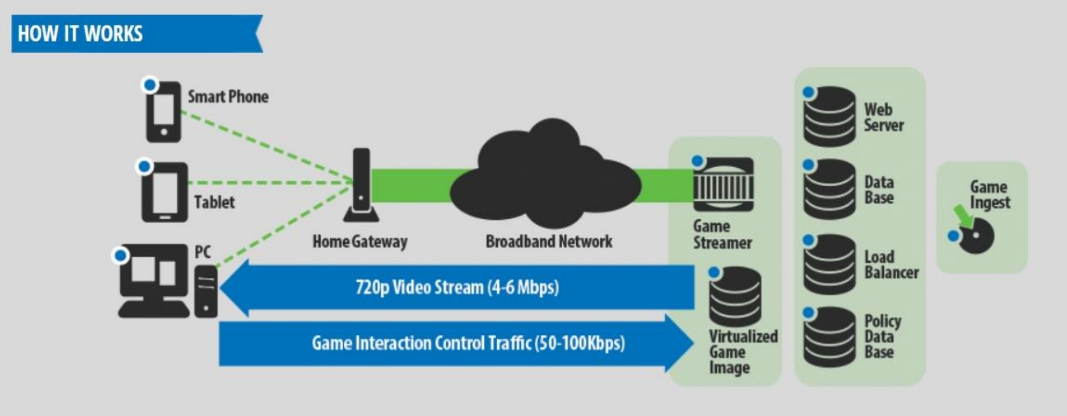
Like ubiquitous WAN and Internet, cloud storage is not a specific device, instead, it is a cluster made by enormous number of storage devices and servers. Users do not use one storage device but the data access service is provided by a cloud storage system. The combination of application and storage devices make cloud storage work and turn it from storage devices to storage service.

Generally, the cloud storage system contains four layers: storage layer, basic management layer, application interface layer and access layer. The storage layer is the fundamental of cloud storage. The storage device could be FC storage device, NAS, iSCSI and IP storage devices, also SCSI, SAS, or DAS devices. Those devices in cloud storage usually store large amounts of data and are located in different areas, connecting each other by WAN, Internet or FC network. The basic management layer is the core of cloud storage and is difficult to implement. By applying cluster, distributed file system and grid computing, the cooperative work can be achieved to supply same service and enhance larger, stronger and better data access performance. The application interface layer is the most flexible part in cloud storage. Different cloud storage units can develop various application service interfaces according to actual business types to provide diverse services such as video surveillance application platform, IPTV, VOD, network drive platform and remote data backup platform. The access layer is responsible for logging in the cloud storage system authorized users through a standard public application interface. The access type and method differs in different cloud storage operators. The cloud storage typically means saving master data or back-upping data to unknown storage pools outside of company instead of local datacenter or private remote site. Data backup, archive and disaster recovery are the main uses of cloud storage (Bao and Liu, 2010).

Typically, cloud storage can be sorted into three types: public cloud storage, internal cloud storage and hybrid cloud storage. The public cloud storage can provide a huge amount of file saving with low cost, like the Simple Storage Service from Amazon and storage provided by Nutanix. Service providers are capable of guaranteeing the independency and privacy for every client’s storage. One good example is Dropbox, which has outstanding performance in cloud storage. Internal cloud storage is similar to private cloud storage, however, the former is located inside the firewall of company. Eucalyptus, 3A Cloud, and Lenovo network drive are famous for provider private cloud storage. Meanwhile, hybrid cloud storage combines public and private cloud to configure the volume temporarily based on clients’ requirements. Certain space acquired from public cloud storage to build private or internal cloud storage can help a company with rapidly increasing load fluctuation or peak time. Even so, hybrid cloud storage brings the complexity over public and private cloud distribution (Bao and Liu, 2010).

3.4 Cloud gaming

Cloud gaming is a gaming based on cloud computing. With the cloud gaming mode, all the games are running in the server end, and sending the comprised game graphics that has already been rendered to users through a network transmission. Client do not need to purchase high-end CPU and graphic card as gaming equipment, they only require basic video decompression capability. However, until now, cloud gaming has not become popular in home and handheld gaming console platforms. If it is achieved, the console manufacturers will transform into network providers. In addition, there is no need to fund the development of new consoles constantly, instead, upgrading their server with a small amount of those money will be enough and the results are almost the same. When it comes to users, they can save a large amount of money to buy consoles but acquire top game graphics that require powerful video output hardware. It is not hard to imagine the same quality of graphics on a handheld gaming console and a home gaming console. Besides, they can even replace the position of STB in next generation for watching TV. The work mode of cloud gaming is similar to VOD and charges based on the network speed and the usage of resources. Picture 11 shows the working mode of cloud gaming (Murariu, 2012).



Picture 11. How cloud gaming works

Recently, the famous GPU manufacture NVIDIA has announced that upgrades of the GRID cloud gaming service which can provide more than 35 games supporting 1080P in 60FPS. It is the first device in the world to support this standard cloud platform which requires the SHIELD gaming device and powerful network performance. It can be considered as a great achievement in cloud gaming that is still a developing technology (Le, 2015).

3.5 Security as a service

Right after the existing of cloud computing and cloud storage, security as a service arose that is a concept that came up with Chinese enterprises and draw great attention in International cloud computing area. It is a new vision in the age of Internet information security and aggregates parallel processing, grid computing, unknown virus behavior judgement and other new technologies or concepts. By monitoring anomalies of software on the Internet through a large number of reticular clients, it acquires the latest information about Trojan, malware, then delivers to server for further analysis and processing, and eventually, sends the solution to every client.

Security as a service has been widely used in anti-virus software and gained excellent outcome. The Trend Micro presented the idea of security as a service in 2008 but also received plenty of criticism at that time, however, it has been accepted broadly now in the world (Fang, 2009). In the future, anti-virus software cannot handle the increasing number of malwares. The threats from Internet are changing from computer viruses to malwares and Trojan. In such circumstance, the virus features database cannot fulfill the defense of new types of Internet threat. With security as a service technology applied, it does not only rely on virus features database in the local hard drive, instead, the powerful network service is able to collect, analyze and process samples. The entire Internet is acting like a gigantic “anti-software”. The more users participated, the safer their devices will be, and the Internet will be more secured. In the earlier time, security as a service was considered as pseudo-proposition, but facts speak louder than words. The development of security as a service is like wind, and companies like Trend Micro, Kaspersky, McAfee, Symantec, Panda and etc. all promote security as a service solutions. Among them, Trend Micro has established five datacenters and tens of thousands online servers worldwide. According to statistic statement, security as a service can support 5.5 billion queries and 200 million sample per day in average, the hit rate of database reached to 99% the first time. By applying security as a service, Trend Micro is capable of stopping infection of virus 10 million time a day in maximum (Fang, 2009).

In order to build security as a service system, there are four main issues to be highlighted: the large number of clients, professional anti-virus technology and experience, massive funding for development and an open source system that requires plenty of partners. The large number of clients are needed to increase the sensibility of virus, Trojan, and malicious websites. It will detect and response in the first time when client gets infected. The experience of anti-virus are gathered with time and technologies such as virtual machine, smart active defense, large-scale parallel computing and so on. In this way, the information can be reported to security as a service system at the first time, then the results of processing can be sent to every member in the system. The cost of hardware in security as a service system is dramatic like server and bandwidth, not mention to the fund to development team for researching, which cannot be accomplished by non-professional manufactures. In addition, the open source system is prepared for the participation of partners and being compatible with other software, which benefits to expand the range of security as a service.

Specific examples should be given so it is easier to understand how security as a service works. The famous anti-software and Internet security company, Trend Micro, published their security as a service technology few years ago called SecureCloud that has six trump cards. This first one is Web Reputation Services. Trend Micro owns one of the biggest domain reputation library around the world. The web reputation services made reputation points to websites by applying malware behavior analysis, which analyzes the scanned webpages, the historical location changes and signs of suspicious activities. In this way, it traces the credibility of websites and prevents users from accessing infected websites. In order to increase the accuracy and reduce rate of false alarm, Trend Micro web reputation services assigned reputation points for certain pages or links on the website instead of entire website because usually only part of pages on legal website will be attacked; however, the reputation points varies with the change of time. After comparing the reputation points of different pages, the risk level of website can be evaluated. When users access website with potential risks, this will trigger notifications or block the access to help users with acknowledging the security of target website. By applying web reputation services, the source of malwares will be on guard due to the precaution mechanism based on credibility instead of actual contents. Hence, the initial download of malware can be stopped, and it works before users actually accessing Internet.

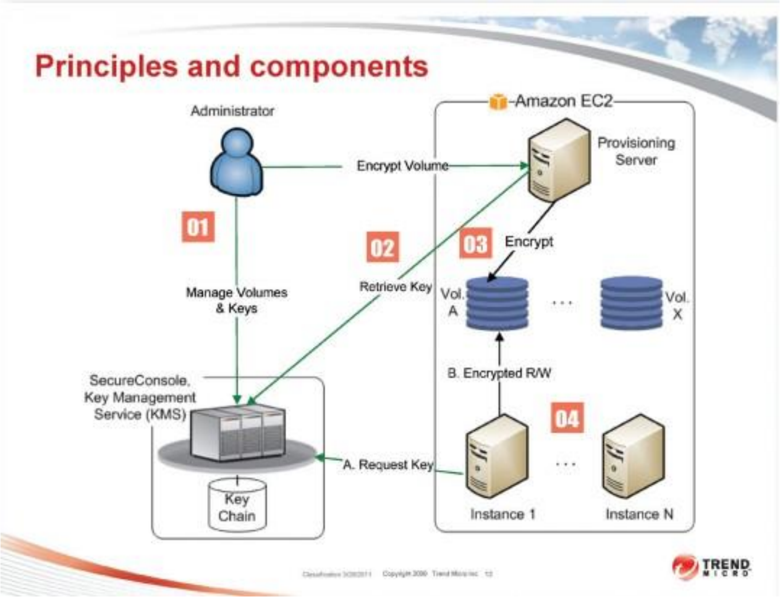
Email reputation services is the second card; Trend Micro inspects IP addresses by checking the reputation database of known spam meanwhile verifying IP address by evaluating the real time dynamic reputation services of email sender. The reputation points are becoming more specific due to the constant analysis of IP address behavior, range of motion and history. The malicious email will be incepted in the process of transmission based on the IP address of the sender to prevent the network and user computer from a Botnet attack.

Moreover, the file reputation service technology of Trend Micro is able to check the file reputation in terms of nodes, server and gateway. According to the manifests of benignant and malignant files, namely, anti-virus signature. In this process, the high performance CDN and the local buffer server will make sure the delay time remains to the minimum during the checking procedure. Due to the records of malicious messages saving in the cloud, all the users can receive them immediately. Besides, comparing to the download of traditional anti-virus signature that is endpoint space consuming it decreased the consumption of endpoint memory and system resources.

Further, security as a service of Trend Micro utilizes relevant technology of behavioral analysis to associate potential threatening activities and verify if they belong to malicious activities. The single web activity seems harmless sometimes, however, if multiple activities are running together, then probably lead to malicious result. Therefore, it is crucial to apply the heuristic method to justify the existence of threat and check the relationship of potential threatening components, which makes an outstanding advantage in protecting email and web from threats.

The other key feature of Trend Micro is the automatic feedback mechanism that communicates among Trend Micro threat products, the threat research center of the company and the technologies with full duplex update streams. By checking the reputation of route in single client to prevent new types of threat, this widely used mechanism performs like neighborhood watch by multiple communities to implement real-time supervision and protection, which benefit from setting up new threat records. The new type of threat detected by single client will be sent to all of the threat databases of Trend Micro around the world.

Researchers from the Philippines, Japan, France, Germany and China are supposed to replenish feedback and submissions for Trend Micro. In TrendLabs that is responsible for anti-virus development and technical support for Trend Micro, employs staff who can give different language support and will provide real-time respond in 24/7 to defense any kinds of attack and detect or eliminate any potential threat (Trend Micro, 2014). Picture 12 illustrates the working mechanism of the Trend Micro SecureCloud (Wong, 2011).



Principles and components

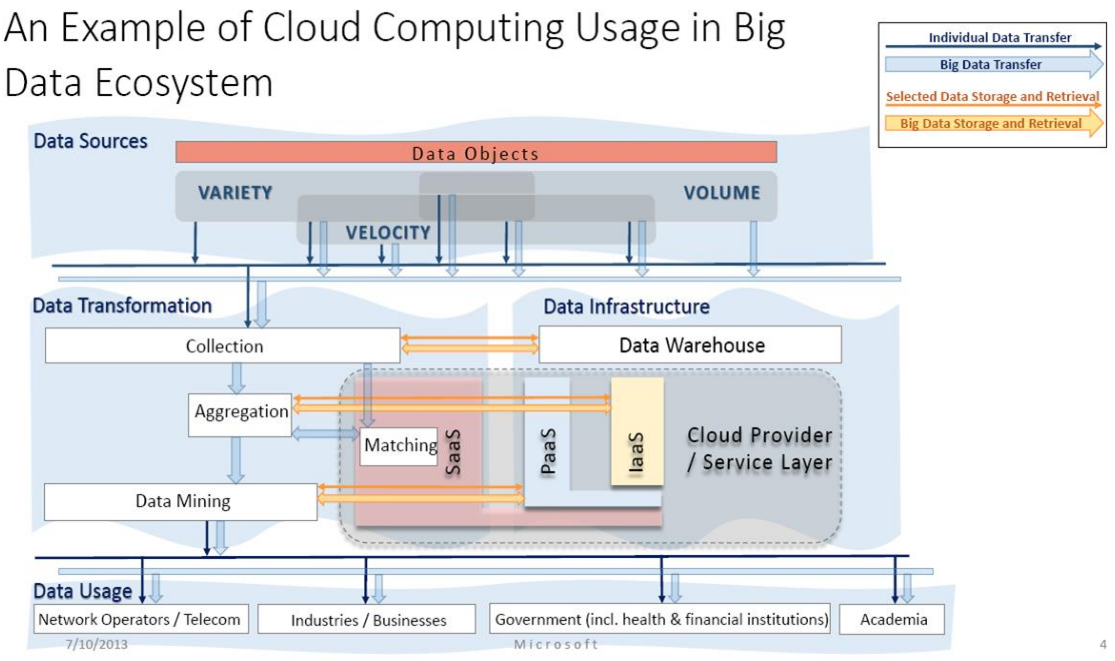
Picture 12. Trend Micro SecureCloud

3.6 Big data

Big data is an industry that uncovers the value of massive data and refines them to achieve the goal of appreciation. In the current information society, due to the rising amount of data, companies exploit big data technology to gain extra profits. Nevertheless, if the cost of discovering, processing and utilizing data is higher than the value of data itself, there is no point in making this move, but the cloud computing in public cloud, private cloud and hybrid cloud solved this problem perfectly because it is the extraordinary filter for gibberish. Usually, the 90% of the first collected data is useless information for companies, so it is critical to acquire valuable information that is able to benefit companies. There are two types of gibberish that should be considered as priority. The first one is the huge amount of temporary information that the company has no need to focus on and the second is network data from outside the firewall to the inside which is worthless. When it comes to cloud computing, it is quite efficient to filtrate those two types of information and analyze valuable information effectively.

From a technical point of view, the relationship between cloud computing and big data is like the two sides of a coin that are tightly connected. Big data cannot be performed with a single computing but applied with distributed computing architecture. It is built for excavating huge amounts of data, however, highly depending on distributed processing, distributed database, cloud storage and virtualization of cloud computing.

The big data management is proceeded by distributed file system such as Hadoop and Map Reduce data partitioning or access enforcement, which are supported by SQL interface like Hive+Hadoop to build next generation database by utilizing cloud computing on the basis of big data. Cloud computing is also used as the platform of big data processing. Despite the multiple parallel computing CPUs in the company, there is no superpower CPU that has the ability to process large-scale amount of data. Therefore, various units in a giant cloud are required to manage instantaneous massive data requests from clients. In E-commerce, this issue becomes dramatically significant. A Chinese E-commerce company called JingDong used to structure their platform with small-scale computers and servers. However, with the increasing speed of business and drastically growing data, it was not possible to handle the situation and extensive server downtime happened that resulted in heavy business damage. So, they abandoned the traditional Oracle or MS-SQL architecture and pursued a large-scale cloud computing based on MySQL+X86 distributed architecture. Thus, big data technology is highly relying on cloud computing regarding business applications. In contrast, big data reinforces the worth of cloud computing on the market (Guo, 2015). Picture 13 provides an example of cloud computing used in big data ecosystem (Levin, 2013).



An Example of Cloud Computing Usage in Big Data Ecosystem

Individual Data Transfer
Big Data Transfer
Selected Data Storage and Retrieval
Big Data Storage and Retrieval

Data Sources
Data Objects
VARIETY
VELOCITY
VOLUME

Data Transformation
Collection
Aggregation
Matching
Data Mining

Data Infrastructure
Data Warehouse
SaaS
PaaS
IaaS
Cloud Provider / Service Layer

Data Usage
Network Operators / Telecom
Industries / Businesses
Government (incl. health & financial institutions)
Academia

7/10/2013
Microsoft
4

Picture 13. Cloud computing used in big data ecosystem

4 MAIN SECURITY ISSUES IN CLOUD COMPUTING

Security is becoming more and more challenging cloud computing due to its popularization nowadays. When we enjoy the convenience that cloud computing brought to us, meanwhile, the risks are also approaching with it. Thus, it is necessary to analyze the main risks thoroughly to guarantee the protection to our information. In the recent two years, massive security issues happened frequently with cloud computing providers. On February 15th, 2008, Amazon experienced network server downtime that affected thousands of websites which applied Amazon EC2 cloud computing and S3 cloud storage, including Twitter, SmugMug, 37Sigals and AdaptiveBlue. In 2009, Google Gmail had a global malfunction and services were suspended longer than four hours because one of the datacenter in Europe was under maintenance while the other one was overloaded and this caused chain effect to other datacenters. In the same year, a large number of user files leaked in Google. On 15 March 2009, Microsoft Azure was suspended about 22 hours, however the detail of cause has not been given by Microsoft. On 11 June 2009, Amazon EC2 service was interrupted for several hours due to the broken electrical equipment that supplied datacenter damaged by lightning stoke (Wu *et al*., 2011).

4.1 Privacy management

One of the feature of cloud computing is the participation of huge number of users, and it is inevitable to have privacy problems. Many users worry that their private data will be collected by cloud technology. Therefore, plenty of service providers promised to avoid collecting user's privacy information and keep them confidential if they acquired that information. Nevertheless, users still cannot be satisfied with the guarantee is credible, while their concerns make sense.

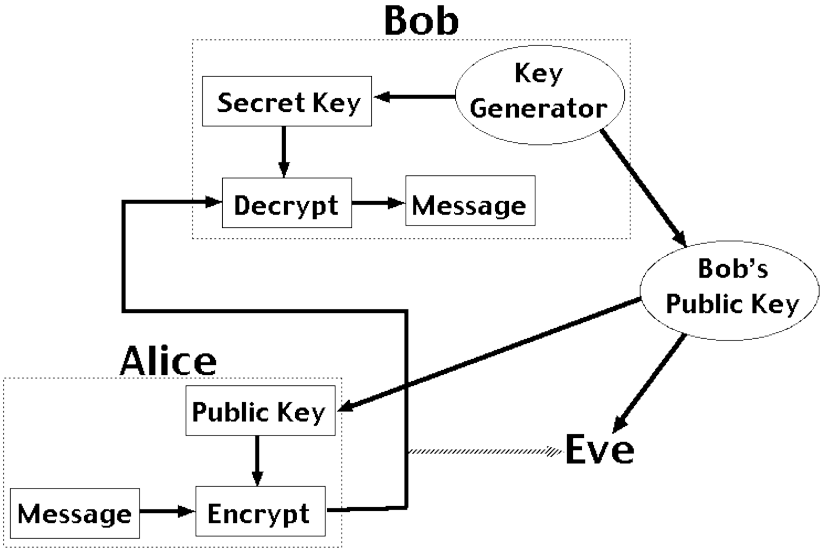
In cloud computing environment, one of the most important is that user data is not stored in local device, instead, it is stored in the cloud, in which some sensitive data will result in privacy leakage. Despite numerous cloud guidelines about not uploading sensitive data to cloud, it is not a perfect solution and probably neutralize certain benefits brought by cloud. In addition, it hinders the development of cloud computing. Besides, the on demand service provided by cloud calculates service fees by accessing user data on the cloud, and some local laws or commercial operation have particular requests concerning the storage and utilization of data. In this situation, an effective mechanism is required to monitor and audit data without leaking sensitive content.

Most of privacy management in cloud computing emphasizes the use of cloud server by applying management component in the cloud. However, there is a new type of privacy manager based on users providing a trust model in terms of users. With the assistance of service provider, users are able to control their own sensitive information. By using obfuscation, even without the help of service provider or malicious action of service provider, users still can secure their privacy data. Another privacy manager offers encryption to privacy data and transfers it to the cloud through privacy manager. This mechanism is based on a shared key by user and a privacy manager that proceed obfuscation and de-obfuscation to conceal the real content in cloud but display authentic result in client side. Moreover, the privacy manager completely utilizes TPM to protect obfuscation key, strengthening privacy protection feature.

The above mentioned privacy managers are all used obfuscation technology. Generally, obfuscation means that user creates a function f(x) in terms of x which indicates privacy data and upload f(x) to server. In the meantime, the service provider calculates f’(x) with acquired f(x) but without knowing of x in a certain cloud service. Then, the service provider will send f’(x) as the result of service to the user for further processing. Though obfuscation is an excellent method, there are still some mistakes in calculation due to unware of input data. In addition, it will increase the calculation obstacle on user’s information processing with frequent computation.

For cloud stored data, on the one hand, users wish for a service provider that can give correct result according to their inquiries, on the other hand, they do not want service provider to know the actual content, namely, implementing encrypted data query. Therefore, a keyword search with protected privacy feature that uses

PEKS has been created. In the scenario where B sends email to A, by utilizing the trapdoor provided by A, the third-party tests if certain word exits in the email without aware of the content. This scheme allows for a service provider partially participating in content decryption and search but is not able to read whole plain text, which helps with releasing pressure on user information processing with protected privacy (Yang *et al*., 2012). Picture 14 shows the process of public key encryption (Prabhu, 2014).



Picture 14. Public key encryption

4.2 Data security and confidentiality

In cloud computing, users cannot have full controllability of their data when they upload them to cloud, so it is crucial that a cloud service provider offers effective safety guarantee, maintaining the integrity and availability of data. Compared to traditional computing, it brings new challenges.

In terms of cloud computing model, IaaS usually provided by the interface of web service which means accessed by web browser. PaaS is achieved by applying the combination of above mentioned technologies, while XML is the carrier of protocols belongs to network application layer in data transmission and parameters and there is evidence indicating that certain security problems related to web service and bowser have a connection with it such as attack to XML signature. In addition, the security problem of browser not only should be solved by transmission layer security technology, but also enforces XML encryption in the core code of browser. Due to the security issue with browser, the identification based on it is also vulnerable. Besides, the feature on integrity and virtual machine applied to cloud, there are existing malwares, metadata fraud and DoS attacks to server. Thus, in the view of application, it is supposed to focus on web browser and web service framework to enhance security.

According to the web 2.0 application, a system file framework aiming at securing file storage service was published. By utilizing the result of secured client cross-domain scheme, an independent file system service was created for web service that users regain the control of data. Another mechanism was given, which separates the content and format of document meanwhile it encrypts them before transmission going to outside. It lowers the risk of content leakage also containing an optimized document authorization access method.

Until now, it is quite popular to combine the Merkle hash tree and encrypted block cipher for implementing confidentiality and integrity of document on an encrypted network system on the basis of random access. Data storage exits in cloud in the form of distributed file system. It is significant to verify the validity of document and locate false data in terms of dynamic operating data block. A possible solution that applied the result of erasure codes may help it out of the dilemma. The user has to calculate the authentication token beforehand, after the server receives the authentication challenge from the user, according to the generated particular block signature and sends it back to the user. Then, the user can identify validity by comparing those signature and pre-calculated token. This method perfectly achieves the goal of validity and false data locating features, also supports secure and efficient dynamic data operating simultaneously including data updating, adding, and removing (Yang *et al*., 2012).

4.3 Data audit

The user data in cloud is not possessed by users, therefore it is significant to make sure their data having been stored and processed properly, namely, conducting integrity verification. In addition, from the point of data security, legal issues and network supervision, a scheme is required to proceed audit remotely and publicly.

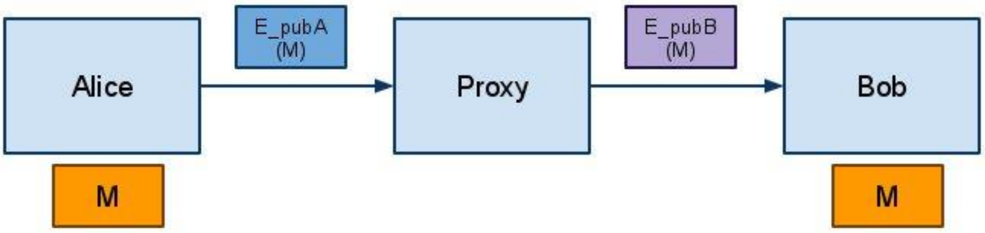
Certain methods have appeared to verify data remotely. For example, implementing provable data possession by utilizing a RSA-based homomorphic tag. With the foundation of it, by applying the classical Merkle hash tree, the model of proof of retrievability was improved. Finally, it achieved the goal of data integrity verification with privacy protected through third party audit that user's participation is unnecessary and avoids privacy leakage. As for high efficient audit, the method with homomorphic authenticator equipped with random masking to protect privacy studied bilinear aggregate signature technology and expanded to multi-users environment. When it comes to integrity, an extensive framework RunTest was established to guarantee integrity of the result of data stream processing running on cloud infrastructure, and locates malicious service provide when the results do not match (Yang *et al*., 2012).

4.4 Authentication and access control policy

When a client is using cloud storage and a computing service, the authentication must be applied by the cloud service provider and utilize certain access control policy to manage the access of data and service. In addition, different service providers should be able to verify each other.

SSLAP was used in cloud computing authentication, but this protocol is quite sophisticated and overloads communication. In cloud computing, each user has own digital ID, thus one of the possible solution is to use ID as the fundamental of authentication. On the basis of IBE and IBS, a protocol that has encryption and signature was used in cloud computing and cloud service, which is also based on identity authentication has been proposed. Compared to SSLAP, it does not ask for authentication certificate, and perfectly satisfies the requirements of cloud computing. By testing on a simulation platform Grid-Sim, it shows more advantages than SSLAP in a lower load.

Access control policy should be defined in terms of data attribute. There is a policy that was created on the basis of ABE, PRE and LRE in which ABE is a one-to-many public key scheme by utilizing bilinear mapping and discrete logarithm. This allows security data distribution between single data owner and multiple data owners. While PRE is an encryption mechanism, whose semi-trusted proxy is able to transfer cipher that uses public key of person A to another cipher, without knowing original plain text, it can be decrypted by person B’s private key. Picture 15 illustrates this process (Yoosuf, 2011).



Picture 15. Proxy re-encryption

LRE allows a cloud server to accumulate tasks from multiple operating systems and conduct batch computing. The complexity of cloud server computation is in direct proportion to the number of system attributes but unrelated to the number of users in the cloud. Thereby, extensibility can be achieved as well as preventing the user privacy from leaking in the cloud (Yang *et al*., 2012).

4.5 Virtual machine security and automated management

Virtualization and virtual machine technology are one of the fundamentals in building the cloud computing concept. In SaaS, the application is created on the visualized platform, and users share physical computing resources with others in a transparent way. In IaaS and PaaS mode, the application is served as a virtual machine or virtualized platform. Except for the traditional network, system and software, different virtual machines should be isolated when sharing physical computing resources and storage resources. In addition, the virtual machine surveillance program is supposed to be trustable and not refer to user privacy information.

In many situations, a cloud service provider does not offer a virtual machine image. Hence, it is necessary to have a better way to manage it. VMware Virtual Appliance Market Place and Amazon EC2 came up with idea of image library. However it has only the basic save and extraction function. Therefore, an image management system Mirage was created to control the access of image and trace the source of image, which provides an effective image filter and scan for cloud users and administrators to detect and fix image leaks. According to the configuration requirements of virtual machine, monitor and physical resources, a new concept VMC was brought forward. It is achieved by extending the OVF to express VMC and manage them in a unified way. OVF is an industrial standard supported by VMware and other large manufactures. It contains the OVF descriptor in XML format to refer to the metadata configuration of virtual devices as well as a virtual disk file set. VMC demonstrates a path of automated control and management for virtual machine in large datacenter and cloud computing environment. Besides, it assists in implementing virtual machine detection, virtual network access control and disaster recovery (Yang *et al*., 2012).

5 CONCLUSION

The rising of cloud computing marks the beginning of the new era of information technology that steps in the aggregated computing model. Meanwhile, this leads to the transform of application from local to cloud environment which dramatically benefits our life and work. Moreover, cloud computing popularized mysterious and elusive professional concepts such as distributed computing, parallel computing, virtualization, and so on. Nevertheless, comparing to other terms, the name “Cloud” seems to be abstract and illusory, and it is hard to imagine the connection between “Cloud” and IT. On the other hand, it will be more acceptable and understandable for the public to describe the technology in a visual way. Further, this vigorous developing industry will have an influences on other domains in the future. For example, cloud computing will strongly boost the development of Internet industry since it is the foundation of implementing cloud computing, meanwhile its intense impact on hardware industry can be predicted because cloud computing has processed sophisticated computation and delivered results to clients.

Due to the continuous expansion of cloud computing, more and more utilization will be introduced. In the meantime, the challenge from security issues is unprecedented, which requires the constant exploration of researchers from IT and information security fields. Hence, famous organizations such as CSA that supports the security of cloud computing, were established to facilitate the best utilization of cloud computing and provide solid protection to it (Feng *et al*, 2011). However, it is not only related to technical problems, but also to the aspects connected with standardization, supervision model, law and regulations. Thereby, it is not enough to solve cloud computing security from a technical view, it also demands the assistance from academia in information security, industries and departments of government.

Overall, cloud computing is a new pattern based on the expansion, utilization and interaction of Internet. The thesis has elaborated the on concept, structure, deployment, typical utilization and main security issues of cloud computing thoroughly. Therefore, intelligible answers have been given to the questions in the introduction chapter. The purpose of this thesis was to study and investigate the principle of cloud computing and current main security issues as well as expound them in plain words instead of sophisticated technical terms. The future of cloud computing is unlimited and the evolution is unimaginable in E-commerce and services as well as the way of life and the basic understanding of cloud computing will build the path to reach the summit of cloud technology.

REFERENCES

Amazon (2007/2015) Amazon web services. Available at: http://aws.amazon.com/ec2/?nc1=f_ls (accessed 26 April 2015).

Amazon (2012) *AWS Case Study: Parse*. Available at: http://aws.amazon.com/solutions/case-studies/parse/ (accessed 1 May 2015).

Bao, L. and Liu, W. (2010) *Application of Cloud Storage in Digital Library Resources Storage*. PhD thesis. Shandong University of Technology.

Bechtolsheim, B. (2011/2015) ‘An ode to Sharkon’, *Google Cloud Platform Blog*, 6 December. Available at: http://googlecloudplatform.blogspot.fi/2013/12/an-ode-to-sharkon.html (accessed 1 May 2015).

Equn.com (2015). *What Is Distributed Computing?* Available at: http://www.equn.com/wiki/%E6%96%B0%E6%89%8B%E6%8C%87%E5%8D%97:%E4%BB%80%E4%B9%88%E6%98%AF%E5%88%86%E5%B8%83%E5%BC%8F%E8%AE%A1%E7%AE%97 (Accessed 29 May 2015).

Fang, J. (2009) *Introduction to Cloud Security*. Bachelor thesis. Langfang Teachers University.

Feng, D., Zhang, M., Zhang, Y. and Xu, Z. (2011) ‘Study on Cloud Computing Security’, *Journal of Software*, 22 (1): 71-83.

Fielding, R. and Taylor, R. (2000) *Principled Design of the Modern Web Architecture*. New York: ACM.

Gu, X. (2014) *Basic review of Cloud Computing*. Available at: http://www.51testing.com/html/41/n-867441.html (accessed 25 April 2015).

Guo, Y. (2015) *Big Data Storage: Practical Guide to MongoDB*. Beijing: Posts & Telecom Press.

Jesús. J.D. (2012) ‘Navigating the IBM Cloud, Part 1: A primer on Cloud Technologies’, IBM Developer Work, [Internet]. Available from: http://www.ibm.com/developerworks/websphere/techjournal/1206_dejesus/1206_dejesus.html [accessed 27 April 2015].

Kline, S. (2011) *Difference between NAS and SAN - 3 Considerations*. Available at: http://www.turbotekcomputer.com/resources/small-business-it-blog/bid/58074/Difference-Between-NAS-and-SAN-3-Considerations (accessed 26 April 2015).

Kong, W. (2012) *Parallel vs Distributed Computing*. Available at: https://kongwenbin.wordpress.com/2012/07/30/parallel-vs-distributed-computing/ (accessed 26 April 2015).

Le, L. (2015) *New Development in NVIDIA Cloud Game Service*. Available at: http://www.ali213.net/news/html/2015-5/156039.html (accessed 3 May 2015).

Levin, O. (2013) *Big Data Ecosystem Reference Architecture*. Available at: http://semanticommunity.info/Big_Data_at_NIST (accessed 7 May 2015).

Liu, P. (2014) ‘The Concept and Connotation of Cloud Computing’, China Cloud, [Internet]. Available from: http://www.chinacloud.cn/show.aspx?id=14668&cid=17 [accessed 26 April 2015].

Microsoft (2012/2015) ‘Mobile Services’, *Microsoft Developer Network*, 9 May. Available at: https://msdn.microsoft.com/en-us/library/azure/jj554228.aspx (accessed 1 May 2015).

Microsoft (2013) *Understanding of Cloud Computing*. Available at: https://wacnstorage.blob.core.chinacloudapi.cn/marketing-resource/documents/1%20%E8%AE%A4%E8%AF%86%E4%BA%91%E8%AE%A1%E7%AE%97.pdf (accessed 27 April 2015).

Microsoft Azure (2008/2015). *Microsoft Azure*. Available at: http://azure.microsoft.com/en-us/ (accessed 26 April 2015).

Moosa, F. (2014) ‘Types of Cloud Computing’, Cloud Drive Consulting, [Internet]. Available from: http://clouddriveconsulting.restoreup.com/2014/01/types-of-cloud-computing.html [accessed 28 April 2015].

Murariu, C. (2012) ‘AMD Invests in a Cloud Gaming Company’, SOFTPEDIA, [Internet]. Available from: http://news.softpedia.com/news/AMD-Invests-in-a-Cloud-Gaming-Company-291523.shtml [accessed 3 May 2015].

OpenStack (2010/2015). *OpenStack*. Available at: https://www.openstack.org/ (accessed 26 April 2015).

Prabhu, M. (2011/2014) ‘Encryption, Cryptanalysis and Hash Functions’, *Blog Spot*, 6 July. Available at: http://techilistic.blogspot.fi/ (accessed 7 May 2015).

Richardson, L. and Ruby, S. (2007) *RESTful Web Services*. Sebastopol: O’Reilly Media.

Samsung (2014) *Internet of things service model*. Available at: http://www.slideshare.net/zinnov/internet-of-things-by-samsung (accessed 30 April 2015).

Skali Group (2011) *Public Cloud vs Private Cloud*. Available at: http://skali.net/public-cloud-vs-private-cloud (accessed 27 April 2015).

Strachey, C. (1959). ‘Time Sharing in Large Fast Computers’, Proceedings of the International Conference on Information processing, UNESCO, B.2.19: 336–341.

Teng, X. (2014) ‘The Future and Application of PaaS’, Tech Target Cloud Computing, [Internet]. Available from: http://www.searchcloudcomputing.com.cn/showcontent_84737.htm [accessed 29 April 2015].

Trend Micro (2014) *Trend Micro SecureCloud: Securing and Controlling Sensitive Data in the Cloud*. Available at: http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_securecloud.pdf (accessed 6 May 2015).

Tu, H., Zou, H. and Lin, R. (2010) *Design and Implementation of Enhanced Parallel Computing Framework System*. PhD thesis. Beijing University of Posts and Telecommunications.

U.S. Department of Commerce (2011) ‘*The NIST Definition of Cloud*’. Gaithersburg: National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed 25 April 2015).

Wikipedia (2015) *Cloud computing*. Available at: http://en.wikipedia.org/wiki/Cloud_computing (accessed 25 April 2015).

Winkler, V. (2011) *Securing the Cloud*. Waltham: Elsevier.

Wong, A. (2011) *How to Secure Cloud Files With Trend Micro SecureCloud*. Available at:

http://www.bqjournal.com/%E4%BF%9D%E8%AD%B7%E9%9B%B2%E7%AB%AF%E8%B3%87%E6%96%99%E5%AE%89%E5%85%A8-trend-micro-securecloud (accessed 4 May 2015).

Wu, J., Shen, Q., Zhang, J., Shen Z. and Ping, L. (2011) *Cloud Computing: Cloud Security to Trusted Cloud*. PhD thesis. Hangzhou Normal University and Zhejiang University.

Wu, Z. (2010) *Analysis of Cloud Architecture in Technical View*. Available at: http://www.infoq.com/cn/articles/analyze-cloud-architecture/ (accessed 27 April 2015).

Yang, J., Wang, H., Wang, J. and Yu, D. (2012) ‘Survey on Security Issues of Cloud Computing’, *Journal of Chinese Computer Systems*, 33 (3): 473-479.

Yang, Z. and Zhou, F. (2011) *Cloud Computing and the Internet of Things*. Beijing: Tsinghua University press.

Yoosuf, N. (2011/2015) ‘Proxy Re-Encryption’, *Blog Spot*, 2 March. Available at: http://mohamednabeel.blogspot.fi/2011/03/proxy-re-encryption.html (accessed 9 May 2015).

Zhou, H. (2011) *Cloud Computing: ICT's Tower of Babel*. Beijing: Publishing House of Electronics Industry.