Recent Advances in Cloud Security

Jiyi Wu1,2
1.Key Lab of E-Business and Information Security, Hangzhou Normal University, Hangzhou, China
2.School of Computer Science and Technology, Zhejiang University, Hangzhou, China
Email: Dr_PMP@yahoo.com.cn

Qianli Shen1,3, Tong Wang1,4, Ji Zhu1,3, Jianlin Zhang1,3
3.Alibaba Business School, Hangzhou Normal University, Hangzhou, China
4.Information and Communication Engineering College, Harbin Engineering University, Harbin 150001, China;
Email: alpenadler@gmail.com, wangtong@hrbeu.edu.cn, 87704267@qq.com, zhangjohn@vip.sina.com

Abstract—Cloud computing emerges as a new computing paradigm which aims to provide reliable, customized and QoS guaranteed dynamic computing environments for end-users. Although cloud computing industry promises tremendous prospects of market growth, for users of cloud services, cloud computing has a wide range of potential risks and safety issues. This article gives a quick introduction to cloud security. It covers the key technologies of cloud computing, security challenge and problem in cloud computing, recent advances in cloud security.

Index Terms—distributed computing, cloud computing, cloud security, survey

I. INTRODUCTION

When compared to the infinitely powerful Internet cloud, PCs seem like lightweight terminals allowing users to utilize the cloud. From this perspective, cloud computing seems like a “return” to the original mainframe paradigm [1]. As Fig.1 shows, a conceptual layer—a cloud on the Internet—hides all available resources (either hardware or software) and services, but it publishes a standard interface. As long as users can connect to the Internet, they have the entire Web as their power PC. Cloud computing thus refers to the techniques that enable and facilitate this scenario [2][3].

According to IDC, the global market size of Cloud Computing is expected to be increased from 16 billion dollars in 2008 to 42 billion U.S. dollars in 2012 [4], and the proportion of total investment is expected to rise from 4.2% to 8.5%, as shown in the Fig.2. Moreover, according to forecasts, in 2012, the input of Cloud Computing will take up 25% of the annual increase of IT investment, and 30% in 2013. According to the data analysis of the most authoritative IT research and consulting firm in the world, Gartner, it is believed that the market revenue of the Cloud Computing in 2009 will rise to above 20%, exceeding to 56 billion dollars; yet, the investment institution, Merrill Lynch, believes that Cloud Computing will occupy 160 billion dollars of market shares in 2011. On the basis of different definitions and understandings of Cloud Computing in every company, the market scale and valuation of the market can be clarified. The emergence of Cloud Computing technology enables people to acquire applications and computing power through the network directly. The new mode will generate a great reform for the traditional IT industry, and Cloud Computing is progressing towards a developmental tendency.

Although Cloud Computing industry promises tremendous prospects of market growth, for users of cloud services, Cloud Computing has a wide range of potential risks and safety issues. On the basis of objective analysis of the current security challenge problem in the field of Cloud Computing, the latest research process in the field of Cloud Security is concluded, indicating the major research direction of the field. The integration studies of Cloud Computing and trusted computing technology will become an important direction of cloud security.
In the past two years, the cloud service providers have been frequently interrupted by various insecure events. On February 15, 2008, Amazon was blocked by the Web Services Downtime, affecting thousands of websites of EC2 Cloud Computing and S3 cloud storage dependent on Amazon, including Twitter, SmugMug, 37Signals and AdaptiveBlue etc. On February 24, 2009, a global failure occurred in Google Gmail, and the service was interrupted for 4 hours. As the genesis of the breakdown was due to routine maintenance of the data center in Europe, the overload of another data center in Europe was intruded, the chain effect expanding to other data centers, ultimately resulting in a global disconnection. On March 7, 2009, files of a large number of users of Google were leaked. On March 15, 2009, Azure, the Cloud Computing platform of Microsoft, was halted from operation for about 22 hours, and Microsoft did not give out any detailed failure causes. On June 11, 2009, EC2 of Amazon was interrupted for hours because the lightening stroked the power equipment of the company's data center, leading to the disconnection of some AWS client services. On July 19, 2009, the Cloud Computing Web Services of Amazon was interrupted again.

While Cloud Computing greatly facilitating users and enterprises to use low-cost storage resources, software resources and computing resources, the greatest challenge or the existing problem comes from the security.

II. WHAT’S CLOUD COMPUTING

A. Services in Cloud Computing

Cloud computing is about moving services, computation or data—for cost and business advantage—off-site to an internal or external, location-transparent, centralized facility or contractor. By making data available in the cloud, it can be more easily and ubiquitously accessed, often at much lower cost, increasing its value by enabling opportunities for enhanced collaboration, integration, and analysis on a shared common platform.

Depending on the type of provided capability, there are four scenarios where Clouds are used as showed in Fig.3.

a) Infrastructure as a Service

IPs manage a large set of computing resources, such as storing and processing capacity. Through virtualization, they are able to split, assign and dynamically resize these re-sources to build ad-hoc systems as demanded by customers, the SPs. They deploy the software stacks that run their ser-vices. This is the Infrastructure as a Service (IaaS) scenario.

b) Platform as a Service

Cloud systems can offer an additional abstraction level: instead of supplying a virtualized infrastructure, they can provide the software platform where systems run on. The sizing of the hardware resources demanded by the execution of the services is made in a transparent manner. This is denoted as Platform as a Service (PaaS). A well-known example is the Google Apps Engine.

c) Storage as a Service

Commonly known as Storage as a Service (SaaS), it facilitates cloud applications to scale beyond their limited servers. SaaS allows users to store their data at remote disks and access them anytime from any place. Cloud storage systems are expected to meet several rigorous requirements for maintaining users’ data and information, including high availability, reliability, performance, replication and data consistency; but because of the conflicting nature of these requirements, no one system implements all of them together.

d) Software as a Service

Finally, there are services of potential interest to a wide variety of users hosted in Cloud systems. This is an alter-native to locally run applications. An example of this is the online alternatives of typical office applications such as word processors. This scenario is called Software as a Service (SaaS).
B. Advantage and Challenges

a) Advantage of cloud computing

With everything, as has been said before, the devil is in the details. Certainly, there are more examples of the growing popularity of cloud computing and valid business reasons for its popularity. Here are five key benefits of using cloud computing and of applications that take advantage of storage in the cloud.

- **Ease of management:** The maintenance of the software, hardware and general infrastructure to support storage is drastically simplified by an application in the cloud. Applications that take advantage of storage in the cloud are often far easier to set up and maintain than deploying an equivalent service on premise. At the customer site, often all that is needed to manage your storage implementation is a simple web browser leaving the headaches to the service provider.

- **Cost effectiveness:** For total cost of ownership, cloud computing is a clear winner. Elimination of the costly systems and the people required to maintain them typically provides organizations with significant cost savings that more than offset the fees for cloud computing. The costs of being able to provide high levels of availability and the scalability an organization needs are also unmatched. The economies of scale achieved by data centers simply can’t be matched by all but the very largest of organizations.

- **Lower impact outages and upgrades:** Typically cloud computing provides cost effective redundancies in storage hardware. This translates into uninterrupted service during a planned or unplanned outage. This is also true for hardware upgrades which for the end user will no longer be visible.

- **Disaster preparedness:** Off site storage isn’t new. Keeping important data backed up off site has been the foundation of disaster recovery since the inception of the tape drive. Cloud computing services not only keep your data off premise, but they also make their living at ensuring that they have redundancy and systems in place for disaster recovery.

- **Simplified planning:** Cloud computing solutions free the IT manager from detailed capacity planning. Cloud-based solutions are flexible and provide storage as needed. This eliminates the need to over provision for storage that may be needed to meet

b) Challenges in the implementation

However, with every type of cloud computing, there are challenges in the implementation (i.e. the devil is in the details).

1) **Physical Security**

First, understand some things about the data center that is hosting the cloud where your data is stored:

- Is the data center physically secure?

- What about it’s ability to withstand power outages?

- For how long?

- Are there multiple, independent (on different grids) electrical power paths?

- How are communications facilities enabled and where does the fiber enter the facility?

- How many communications providers have a POP (point of presence) at the facility?

- How is the data center certified (SAS 70 Type II)?

World class data centers are expensive, and they are also well understood. What is the tier rating of the data center? (Tier IV is best). Make sure you do business with a cloud computing service provider who makes use of such facilities.

2) **Data encryption**

Encryption is a key technology for data security. Understand data in motion and data at rest encryption. Remember, security can range from simple (easy to manage, low cost and quite frankly, not very secure) all the way to highly secure (very complex, expensive to manage, and quite limiting in terms of access). You and the provider of your Cloud computing solution have many decisions and options to consider. For example, do the Web services APIs that you use to access the cloud, either programatically, or with clients written to those APIs, provide SSL encryption for access, this is generally considered to be a standard. Once the object arrives at the cloud, it is decrypted, and stored. Is there an option to encrypt it prior to storing? Do you want to worry about encryption before you upload the file for cloud computing or do you prefer that the cloud computing service automatically do it for you? These are options, understand your cloud computing solution and make your decisions based on desired levels of security.

3) **Access Controls**

Authentication and identity management is more important than ever. And, it is not really all that different. What level of enforcement of password strength and change frequency does the service provider invoke? What is the recovery methodology for password and account name? How are passwords delivered to users upon a change? What about logs and the ability to audit access? This is not all that different from how you secure your internal systems and data, and it works the same way, if you use strong passwords, changed frequently, with typical IT security processes, you will protect that element of access.

4) **Service Level Agreements (SLA)**

What kind of service commitment is your provider willing to offer you? Are they going to be up 99.9% of the time or 99.99% of the time? And how does that difference impact your ability to conduct your business? What is the backup strategy that your cloud provider uses, and does it include alternative site replication? Do they use one at all, or is backup something you have to provide for? Is there any SLA associated with backup, archive, or preservation of data. If your account becomes inactive (say you don't pay your bill), do they keep your
data? For how long? Once again, realize that there are different services, with different features, at different costs, and you get what you pay for.

5) Trusted Service Provider

The trusted service provider is a critical link. Unlike your in-house IT department, you are now putting your trust in a 3rd party. You must feel confident that they will do what they say they will do. Can they demonstrate that the safeguards they claim are indeed delivered? What is their record? Do you have a successful business relationship with them already, and if not, do you know of others who do? Remember, are they in business to serve business, or is it simply another service that they offer, focused first on cost per gigabyte, versus service and support. This is where many IT service providers have made their living, providing world class service and support, along with effective, efficient, low cost infrastructure.

As shown in Fig. 4, the problem include security, control, performance, support, vendor lock-in, are concerned by users with cloud services.

![Figure 4. Survey on concerns with cloud computing services.](image)

These challenges include:

- Security (always an issue and not necessarily a cloud computing specific issue)
- Data integrity (making sure the stored data is “correct”)
- Power (since you have copies you will have extra storage which adds power)
- Replication time and costs (how fast can you replicate data since this can be important to data resiliency)
- Cost (how much extra money do you have to pay to buy the extra storage for copies)
- Reliability

III. RECENT ADVANCES IN CLOUD SECURITY

In the literature [5] conclusion, ten opportunities and ten problems of Cloud Computing are illustrated in Table 1. Among them, Availability of Service, Data Lock-In, Data Confidentiality and Auditability, Data Transfer Bottlenecks, Performance Unpredictability, Bugs in Large-Scale Distributed Systems, Reputation Fate Sharing and so on are correlated with confidentiality and reliability. The literature [2] also proposes that Cloud Computing should tackle with security, Data and Application Interoperability, Data and Application Portability, Governance and Management, Metering and Monitoring properly. Otherwise, its realization promise will be affected. According to the 2009 White Paper on China Cloud Computing Development [6] released by “CCW Research”, it is indicated that “how the security, stability and reliability of Cloud Computing technology is” will be one of the major considerations of Cloud Computing among domestic users. Cloud Computing experts, Patrick Goldsack et al of HP believe that: infrastructure services of Cloud Computing must be equipped with the privacy and security, service quality and performance assurance, flexibility, upward and downward scalability and fault resilience and other specific attributes so as to satisfy the enterprise-level demands.

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability of Service</td>
<td>Use Multiple Cloud Providers; Use Elasticity to Prevent DDoS</td>
</tr>
<tr>
<td>Data Lock-In</td>
<td>Standardize APIs, Compliant SW to enable Surable Computing</td>
</tr>
<tr>
<td>Data Confidentiality and Auditability</td>
<td>Deploy Encryption, VLANs, Firewalls, Geographical Data Storage</td>
</tr>
<tr>
<td>Data Transfer Bottlenecks</td>
<td>FileEditing Dirks; Data Backup/Audited, Higher BW Switches</td>
</tr>
<tr>
<td>Performance Unpredictability</td>
<td>Improved VM Support; Pool Memory; Gang Schedule VMs</td>
</tr>
<tr>
<td>Scalable Storage</td>
<td>Invest Scalable Store</td>
</tr>
<tr>
<td>Bugs in Large-Scale Distributed Systems</td>
<td>Invest Debugging tools on Distributed VMs</td>
</tr>
<tr>
<td>Scaling Quickly</td>
<td>Invest Auto-Scaler that relies on ML, Snapshots for Conservation</td>
</tr>
<tr>
<td>Reputation For Sharing</td>
<td>Offer reputation guarding services like those for email</td>
</tr>
<tr>
<td>Software Licensing</td>
<td>Pay-for-use licenses; Billing service</td>
</tr>
</tbody>
</table>

As studies of the field of Cloud Computing just began, there are few studies on Cloud Security with blurred fundamental concepts or definitions of the latest studies of Cloud Security. New findings in the field of Cloud Computing by RSA [7], Gartner [8], CSA [9], SUN [10], IBM [11] and other organizations have positive significances of the development of management and technology of Cloud Security. In its White Paper on Cloud Computing Security, RSA listed security metrics on aspects like supplier management, technical standards, data mobility, data confidentiality and privacy, visiting control, compliance, and security services, with the conclusion of three major categories of Cloud Computing security elements, and summarized Infrastructure,
Identity, Information, three principles for securing the cloud. Kevin D.Bowers [7] et al in RSA laboratory also puts up with HAIL, the Cloud Storage model of high reliability and completeness with experiments of safety and efficiency.

In July 2008, the international research institute, Gartner, issued a report named “Teleworking in the Cloud: Security Risks and Remedies [8] “, also listed seven major threats in Cloud Computing, namely, the access for VIP users, review, data location, data isolation, data recovery, investigation support, and long-term survival. The report believes that Cloud Computing needs security risk assessment in fields like data integrity, data recovery and privacy. In addition, legal assessment on electronic retrieval, review and audition should be conducted.

According to the White Paper on “Emerging Security Technologies Prospects” [12] by IBM in October 2008, it is estimated that during the next 2 to 5 years, 9 important tendencies and technologies will affect the security environment, among which, the tendency ranking the top should be to “protect the security of virtualized environments”. Specifically, the solution of three aspects of problems in Cloud Computing environment is in demand:

1. (1) Organizations (cloud service providers) should prepare the intensified individual management capabilities and separate the exclusive application, data and infrastructure for a user from other users through the separation strategies among several virtualization platforms;

2. (2) Just like the protection of physical environment, the integrity of virtual environments should be carefully managed and controlled. Traditional security features such as network monitoring and intrusion prevention should be applied to virtual environment;

3. (3) As virtualized resource serves as data image storage, possible contamination could emerge. Organizations should create image management functions so as to protect and maintain the resource definitions of powerful changes and processing batch management procedures.


Cloud Security is a comprehensive concept and issue, probing into the security problems at all levels such as Environment, Process, Technique, Management, Service involved in the process of Cloud Computing. If the definition is given from a single perspective, such as the technical point of view, it will be undoubtedly one-sided, and undoubtedly incompetent to fundamentally reveal the nature of the problem. The goal of Cloud Security is to achieve Secure Cloud or Secure Cloud Computing, although in fact it is a direction without a terminal.

At present, the cloud service providers are constrained in information security. Generally, stored data are encrypted with SSL and SSH and other security protocols to ensure data transmission security and user security access. Yet, when the user data is processed in the back-end server RAM, the processing only can be implemented in plain text form, which provides possibility of attacking RAM data from leaks of the operation system. How to protect and separate the data in memory will be one of the important security needs for Cloud Computing.

As shown in the Fig. 5, the literature [13] proposed the Secured Cloud, in which the user data of the public cloud are separated and stored from other organizations. Through the adoption of Secured & Isolated Cloud Area, the virtual machine resources are provided to ensure the intensive isolation. More importantly, the data is processed through the encrypting from the design and test of experts. Through the encrypted VPN channel, the communication between the Cloud service providers and the organizations is consistent with the log management and resource security management policies organized by users for security strategy design. In addition, it is also in conformity with demands in aspects like the Portability, Administrative Access, Testing, Transparency, and Compliance and so on.

Digital Identity Management Services is an important measure of service access control of Cloud Computing platform in accordance with Identity Properties and Interaction Histories. The literature [14] has proposed a solution based on identity, AgZKPK encryption protocol and the semantic matching technology.

In the literature, Mao Wen-Bo [15] et al of EMC have proposed the latest studies on Cloud Computing Security, which is expanded and decomposed from the front end (client-side, user-side) to the back-end (server-side, data centre), layer by layer, providing significant reference value.

The design of Nuno Santos [16] et al puts up with the Trusted Cloud Computing Platform (TCCP), including a series of confidence-building nodes (N), trust coordinator (TC), non-trust cloud manager (CM) and external trust

![Figure 5. Secured Cloud.](image-url)
entities (ETE), etc., as shown in Fig.6. TC is maintained by specific external trust entities (ETE). Through a black box environment, TCCP ensures the safety of the guest virtual machine, while allowing users to test and verify the security.

In China, Chen Hai-Bo, Zang Bin-Yu et al [17] studied from the aspects of the security, maintainability, availability, reliability and so on of the Cloud Computing platform, namely, the research on “Cloud Computing Platform Credibility Enhancement Technology” with the “groundbreaking” significance to a great extent. The concept is close to the view of Professor Jin Hai [18] of Huazhong University of Science and Technology in his masterpiece, a “safe and creditable virtual computing system”.

The literature [19] analyzes how virtual technologies improve the system security, and it is indicated that the virtualization has incalculable impact on the security enhancement on at least three aspects:

1) it can easily isolate and shield unstable applications or those with security risks;

2) support powerful sound crime analysis and highly effective disaster recovery solutions;

3) virtualization also provides intrusion detection tools of lower costs.

Fudan University, Wuhan University, Huazhong University of Science and Technology, Tsinghua University and EMC jointly launched the “Daoli” study project [20], specifically devoting in the global study coordination on the credibility and reliance under Cloud Computing environment with the integration of trusted computing technology and hardware virtualization security to achieve the verifiable security application isolation and acting codes for users. Thus, the protection of digital property of users in Cloud Computing and cloud storage services can be enhanced. Through the enhanced safety of systematical structure, trusted computing technology can improve the security of the computing platform. With the analysis of the development of the studies in this field, the integration of Cloud Computing and trusted computing technology for better solutions of the security problem in cloud services is becoming a feasible and important tendency. Fig.7 depicts the architecture.

IV. CONCLUSION

Cloud Computing declares a termination of device-centric computing era, which is then replaced by the internet-centric computing model rather than winning praises by flubdb [21]. Cloud Computing enables users to outsource a part or all the computing processing task, and the information department will need no more professionals specifically for the maintenance and configuration of company servers, but to visit computing infrastructure via the Internet [22]. A large-scale Cloud Computing service provider can sufficiently meet the demands from various clients on more computing functions. Those small and medium enterprises without large data center can utilize the powerful processing function from Cloud Computing provider so as to effectively reduce IT costs [23][24]. As a new technology that is expected to cut costs greatly, Cloud Computing is increasingly recognized by many enterprises.
From the perspective of academic research, problems to be addressed in the field of Cloud Security include: how to encrypt data storage and transmission; the replacement of research and algorithm of new encryption algorithm in Cloud Computing; authentication among cloud service application components; criteria and application of platform security evaluation of Cloud Computing; management of users authorized to access to the exotic cloud services and access manners; the security and access control of cloud service application program interfaces; a new generation of Cloud Computing Network Security Technology needed in Service Cloud Computing; the research and establishment of a complete Cloud Computing QoS system; and the integration research of Cloud Computing and trusted computing technology [25].

Under the mode of Cloud Computing, all of the business process will be completed on the server-side, and in the case that some problems occur in the server, the user application will be hampered from normal operation and data access [26]. The time to solve cloud breakdown is not long, yet sufficiently enough as a warning of Cloud Computing [27]. After all, the scale of cloud services is practically huge. In the event of any breakdown, the doubt of Cloud Computing Model among netizens may be triggered easily, undermining the confidence of users for cloud services [28] [29] [30]. Thus, if the weakness in reliability and safety of Cloud Computing cannot be properly solved, the popularity of Cloud Computing still requires more efforts.

ACKNOWLEDGMENT

The authors wish to thank anonymous reviewers for their valuable comments. Funding for this research was provided in part by the Scientific Research Program of Zhejiang Educational Department under Grant No.20071371, National Natural Science Foundation of China (Grant No.61070153), Natural Science Foundation of Zhejiang province (Grant No.Y1080831).

REFERENCES


**Jiyi Wu** was born in Zhejiang, China. He received the B.Eng. degree in 2002 and M.Eng. degree in 2005 both from Zhejiang University, Hangzhou China, all in computer science. He is currently a PhD candidate in the School of Computer Science and Technology, Zhejiang University, and associate professor of the Key Lab of E-Business and Information Security, Hangzhou Normal University. He is a senior membership of China Computer Federation (CCF). His main research interests include peer-to-peer network, cloud computing and virtualization, network information security.

**Qianli Shen** is a lecturer at Alibaba Business School, Hangzhou Normal University. He received Master's degree in computer science and technology from Zhejiang University in 2004. His research interests include Cloud Computing, SaaS and information security. Shen Qianli was born in 1978. He received B.S degree from Zhejiang University in 2001.

**Tong Wang** is an associate professor at Information and Communication Engineering College, Harbin Engineering University. He received Doctor's degree in Computer Application from Harbin Engineering University in 2006. His research interests include Cloud Computing, SaaS and information security. He was born in 1977. He received Master's degree from Harbin Engineering University in 2003.

**Ji Zhu** is a teaching assistant at Alibaba Business School, Hangzhou Normal University. He received B.S degree in computer science and technology from Wenzhou University in 2009. His research interests include Cloud Computing, SaaS and information security.

**Jianlin Zhang** is a professor at Alibaba Business School, Hangzhou Normal University. He received Master's degree in Computer Application from Zhejiang University in 1998. His research interests include Cloud Computing, SaaS and information security. Prof. Zhang was born in 1966. He received B.S degree from Zhejiang University of Technology in 1989.