TimeTec Cloud Security

FACING SECURITY CHALLENGES HEAD-ON

- by Mr. Daryl Choo, Chief Information Officer, FingerTec HQ

Cloud usage and trend

Cloud Computing is getting more common nowadays and eventually almost everybody will need to consume this technology daily either for leisure purposes or for critical ones such as enterprise business solution. With the rapid enhancement and improvement in the Cloud Computing technology, it is now a mature technology for enterprise to adopt and implement.

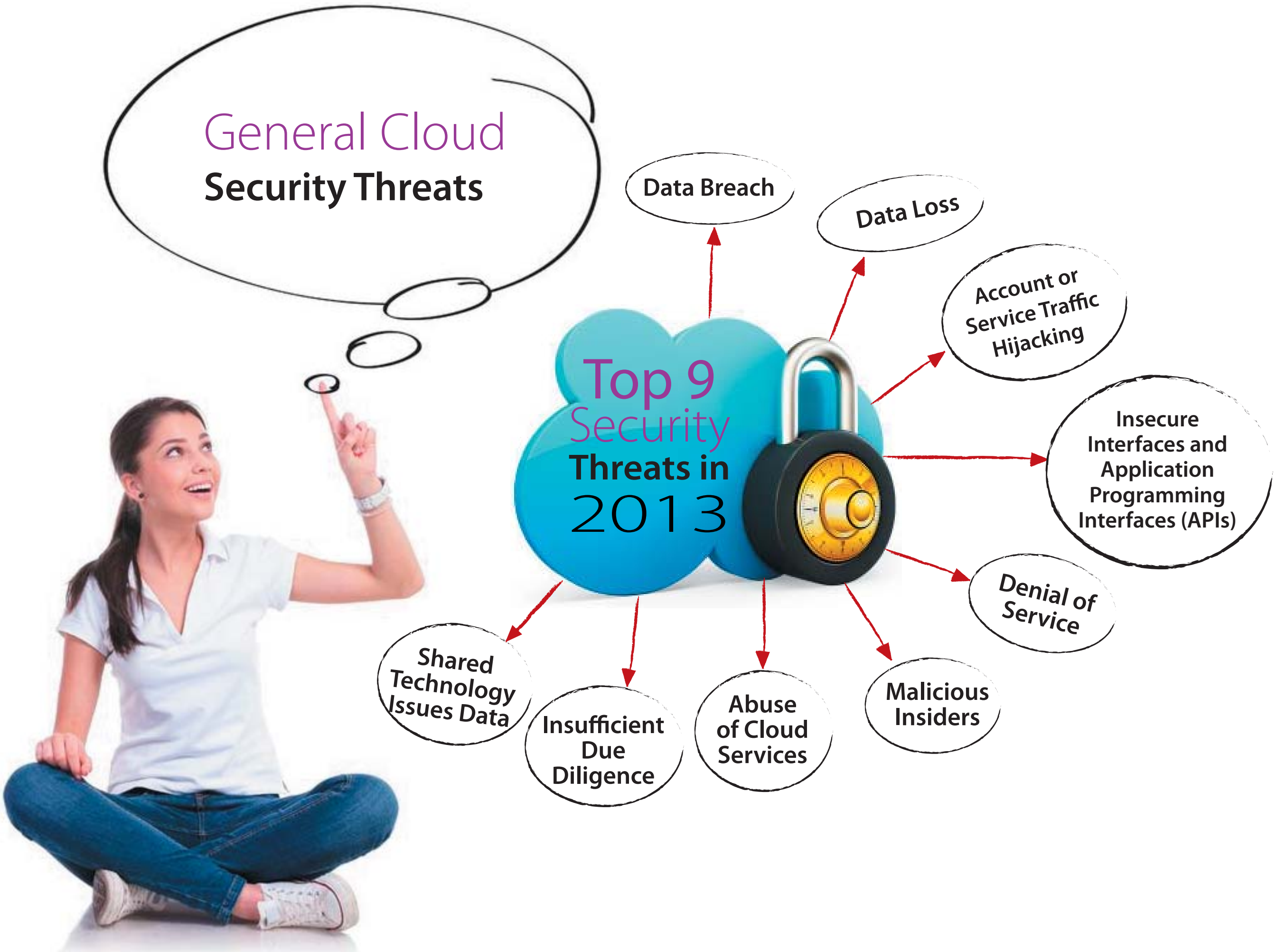
Based on the market analysis conducted by both Gartner and IDC, the Cloud market is estimated to increase from $40B to $109B in 2012 and to grow at around 19% on a compounded basis from 2010-2015 [1]. In early January 2013, another research carried out by Gartner anticipated that most of the uncertainty in global business is nearing resolution and IT spending will grow at 4.2% in 2013 [2]. Based on their statistics as well, Data Center Systems and Enterprise Software, which are the major components of Cloud Computing, are having constant growth rates.

Cloud Computing is definitely the technology of the future but the question is, what are the obstacles waiting for the Cloud implementors and Cloud users, and are we up to the challenge that might come our way?

Challenges

Despite the positive outlook in Cloud Computing, the latest survey done by KPMG on Cloud Computing implementation highlights a major concern and challenge for Cloud adoption at an enterprise level: Cloud security [3]. The risks of intellectual property theft and data loss are among the top areas of concern for Cloud implementation.

In the PwC IT Outsourcing and Cloud Computing Survey 2011, which compares data and system portability, IT governance, etc., data security is getting the most attention [4]. Therefore, early identification of the potential Cloud security issues during implementation and deployment is crucial to roll out a secure and successful Cloud Application for the market. More recently, PwC has again conducted a research on security, The Global State of Information Security® Survey 2013 [5], which highlighted that information security is still a very tough challenge in the business world but with more understanding about the security risks onvolved, organizations can improve and manage the security issue better.


General Cloud
Security Threats
Top 9 Security Threats in 2013
Data Breach
Data Loss
Account or Service Traffic Hijacking
Insecure Interfaces and Application Programming Interfaces (APIs)
Denial of Service
Malicious Insiders
Abuse of Cloud Services
Insufficient Due Diligence
Shared Technology Issues Data

This paper will discuss all the existing and possible security issues based on the many researches conducted by the leading Cloud agencies in order to provide a complete overview of the Cloud security matters. We shall also highlight some risk management and mitigation plan within our Cloud Strategy to offer a reliable and secure Cloud environment to our customers.

1• Data Breach

When we are moving from physical to Cloud or consuming Cloud Service, data breach is arguably the most frequently asked question. Besides the Cloud Virtual Machine (VM), the data that resides on Cloud solutions will need to be protected in order to prevent the organization's sensitive internal data to fall into the hands of their competitors. In a more complex and complicated environment like multitenant applications, a single flaw might cause another client's data to be compromised.

It was published in AWS Security Whitepaper [7] the remedy for data breaches taken by them, that all the virtual machines and the data that resides on AWS are isolated and the data is wiped off completely before it is made available to the next customer to prevent any information leak to their competitors.

For TimeTec Cloud, we offer a centralized authentication layer to verify all user access prior to granting any user any access permission.

2 • Data Loss

Apart from the deliberately deleting action by a user, data loss could also be caused by malicious attacks, physical catastrophes, Cloud service provider problems, and etc. The Cloud backup would be a very important task for both the Cloud service provider and the Cloud application provider. Both of them will need to ensure that multiple copies of backups are in place and reside on different locations to ensure data can be recovered in case of any hardware failure or service outage. These backups are in place for databases, server, storage and etc.

TimeTec Cloud is running in a Multi Availability Zone (Multi-AZ) concept, which means that if one availability zone is having problem, TimeTec Cloud will not be affected, as the second availability zone will immediately take over. This is almost identical with the Fail-Over concept.

3 • Account or Service Traffic Hijacking

Besides the Cloud infrastructure and Cloud instance, the Cloud-based application also plays a very important role in Cloud implementation. Most of the time, system engineers are able to secure the Cloud environment and its infrastructure through Firewall and Intrusion Detection System (IDS) but a minor bug or a backdoor entry to the Cloud application might cause a user account to be hijacked by an unscrupulous user. Once an account or a service is hijacked, the attacker will be able to gain access into your account and 'eavesdrop' on your transactions and activities. The common way of this exploit is via SQL injection attack and Cross-Site Scripting.

TimeTec Cloud has a dedicated and experienced software testing team to run detailed testing procedures on the product. Load testing, penetration testing and functionality testing are thoroughly conducted prior to any software release. Inserting a captcha code is also required at the login process to increase login security and to reduce the potential of break-ins by brute force.

4 • Insecure Interfaces and Application Programming Interfaces (APIs)

In a Cloud Computing environment, we are often exposed to an API either internally or externally with our third party vendor. It might be at the infrastructure level, application level and database level. Without a proper plan or a complete design to consolidate all these interfaces prior to giving access to our client, the system access control or the client data might be compromised and this will increase the risk of the entire Cloud Infrastructure.

TimeTec Cloud does not offer API integration directly from our Cloud infrastructure or database level. However, we have created an in-house API layer on Secure Socket Layer (SSL) to communicate with a third party application for information exchange and processing. The API access is fully controlled by another set of encrypted key and this feature shall be available to the customer soon for integration with a third party application.

5 • Denial of Service (DOS)

Not only for Cloud Application, but DOS attacks can happen a lot of time in our typical web hosting application. A DOS attack aims to consume inordinate amounts of finite system resources, which causes an intolerable system slowdown and failed to response to the user's request. The common attack method is via Ping Flood, SYN flood and etc. On a larger scale, the Distributed Denial of Service (DDoS) attack might complicate the incident, as large numbers of infected machine from different locations will be working together to bring down the Cloud Service.

To minimize the risk of DOS attacks, all unrelated services inclusive of ping service has been turned off and blocked by the firewall on TimeTec Cloud. Furthermore, the TimeTec Cloud application is also running on the SSL Layer that further complicates the DOS attack process while the Enterprise Load Balancer installed at the background can greatly minimize the risk of DOS attack.

6 • Malicious Insider

Apart from technology and security risks, human resources and personnel could also be another threat to Cloud Implementation. Current or formal employees, contractors or business partners who have access to a Cloud service might, intentionally or otherwise, obtain organization or system data if the user access rights are not properly defined. This shows that it's important to have a mechanism to block or disable user access rights in order to prevent any data leakage from the organization.

In TimeTec Cloud, we practiced different user access levels control. From the system level, application level and database level, all the login credentials are unique and limited to their own scope of data to prevent information leakage from one to another. In further securing access control, only a trustworthy person within the organization infrastructure itself can manage TimeTec Cloud.

7 • Abuse of Cloud Services

With the introduction of Cloud Computing, one can easily own tens of thousands of virtual servers in a jiffy, an otherwise impossible task with a physical server. One can switch on or off the virtual server that they want after their task or workload is completed. It has become the responsibility of the Cloud Service Provider to ensure that their Cloud customers do not misuse the system for email spamming, malware distribution, denial of service attack, pirated software distribution and etc. If this is not well managed, it might affect all the Cloud customers who are running their Cloud Solution on its platform.

TimeTec Cloud runs on AWS infrastructure, where a lot of security measurements have been taken care off. A lot of value-added services have been added, such as Simple Email Service (SES), Content Delivery Network (CDN), and Database Service (RDS), to cater for all type of customers whereby they can scale up and down depending on their capacity without affecting the overall usage of the entire Cloud Service.

8 • Insufficient Due Diligence

Since Cloud Computing is getting more common and stable, a lot of businesses and enterprises have started to adopt Cloud services for their business solutions. Unlike their existing on-premise architecture approach, the Cloud computing is rather more complicated for network and user level security access control. It is also very important to have capable resources, either technical or non-technical, to oversee the entire risks and Cloud Service Provider's due diligence before adopting the Cloud Computing model.

The AWS is committed to Service Level Agreement [8] of at least 99.95% uptime. It has also maintained a high level of security and data protection via it AWS Compliance program [9]. Apart from conducting our research and development on AWS infrastructure and services, we do work together with AWS consulting partners during the whole planning and implementation process in order to get the best performance and optimization of user experience on TimeTec Cloud.

9 • Shared Technology Vulnerabilities

Cloud computing exists for the sharing service model. With the virtualization technology used on server, storage and network, it is very crucial to have strong isolation properties for multi-tenanted architecture. If system vulnerability is detected in a Cloud server but cannot be isolated, it might potentially affect the entire Cloud provider operation. We must ensure that all Cloud solutions operate at its sandbox without interfering with other client's system.

Based on AWS Security Whitepaper [7], its network, instances, storages have enforced secure user access control. On top of that, all the instances are isolated from each other via the Xen Hypervisor to ensure other hosts would not jeopardize the instance performance.

Cloud Security Challenges by Type

For a clearer overview of the security issues for different types of Cloud services, like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), they are represented in the following schematic diagram based on the hierarchy of Cloud computing [10].

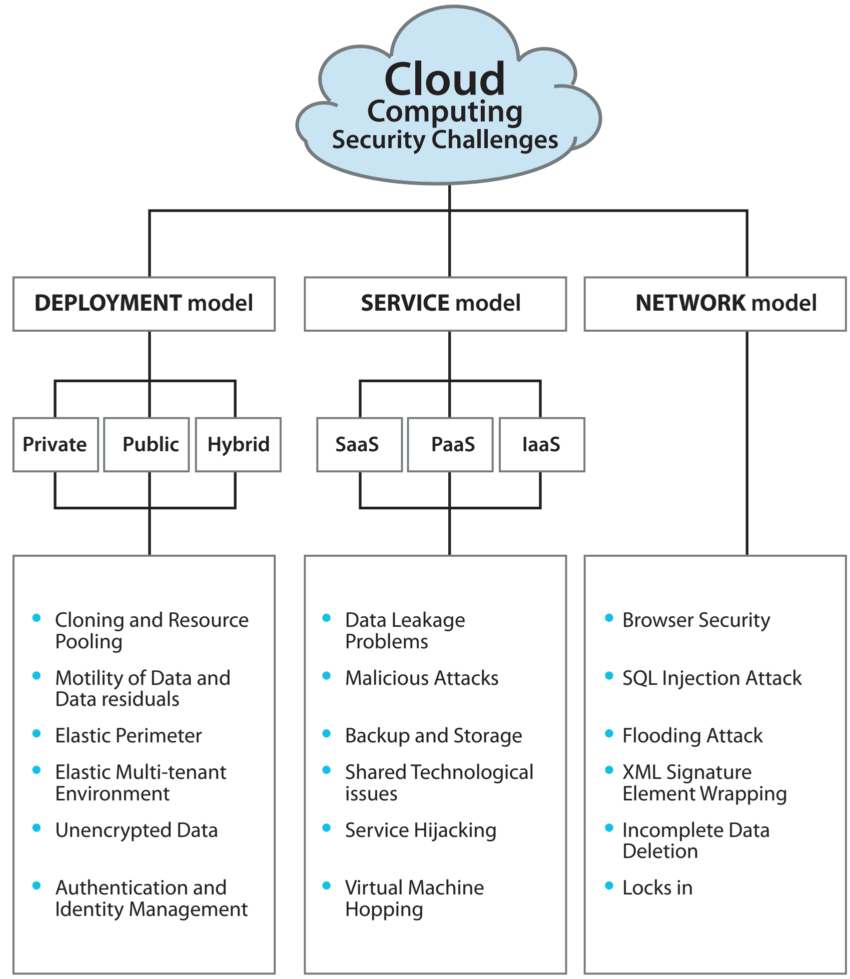


Figure 1: Classification of Security Challenge

Based on the paper, An Analysis of Security Challenges in Cloud Computing [10], it emphasizes that security challenge exists in all phases along the Cloud Implementation. Some challenges have been discussed earlier and other challenges only exist on Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) models. The decision on a deployment model is also required, whether it is on Private Cloud, Public Cloud or Hybrid Cloud as they all offer different pros & cons to our Cloud Solution. A secure Cloud solution is one thing, but more importantly the Cloud Service Provider must be able to cater to your needs and expansion in the future.

Cloud Strategy

A lot of security risks have been highlighted and it might become a deterrent for some organization to continue their journey on the Cloud application. Nevertheless, Cloud based application is definitely THE trend for current and future development and deployment. As long as we have done thorough upfront planning and follow the best practice available, the risks can be minimized and we can prevent any unforeseen circumstances on the Cloud Application.

Based on the recommendation by PwC in The Global State of Information Security® Survey 2013 [5], businesses seeking to strengthen their security practice must:

- Implement a comprehensive risk-assessment strategy and align security investments with identified risks.
- Understand their organization's information, the people who wants it, and what tactics adversaries might use to get it.
- Understand that information security requirements — and, indeed, overall strategies for doing business — have reached a turning point.
- Embrace a new way of thinking in which information security is both a means to protect data and an opportunity to create value to the business.

During our TimeTec Cloud development and deployment, we have adhered to the best practices in setting up the Cloud Solution based on all points discussed earlier and designed the TimeTec Cloud architecture [11] accordingly to offer high reliability and high availability to our customers.

References

1 Martin Tantow. October 30, 2012. The Future of Cloud and SaaS: Forecasts and Prospects. http://Cloudtimes.org/2012/10/30/future-Cloud-saas-forecasts-prospects/

2 Gartner, Inc. January 2, 2013. Forecast Alert: IT Spending, Worldwide, 4Q12 Update. http://www.gartner.com/resources/229800/229878/forecast_alert_it_spending_w_229878.pdf

3 KPMG International. February 6, 2013. Taking a sober look at security http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Cloud-service-providers-survey/Pages/sober-look-at-security.aspx

4 PwC. November 2011. The future of IT outsourcing and Cloud computing. http://www.pwc.com/gx/en/technology/Cloud-computing/charticles/the-big-dilemma.jhtml

5 PwC. 2013. The Global State of Information Security® Survey 2013. http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

6 Cloud Security Alliance (CSA). February 2013. The Notorious Nine Cloud Computing Top Threats in 2013. https://downloads.Cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

7 Amazon Web Services. June 2013. Amazon Web Services: Overview of Security Processes. http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

8 Amazon Web Services. June 01, 2013, Amazon EC2 Service Level Agreement. http://aws.amazon.com/ec2-sla/

9 Amazon Web Services. June 01. 2013. Amazon-Web Services: Risk and Compliance. http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

10 Ms. Disha H. Parekh & Dr. R. Sridaran. 2013. An Analysis of Security Challenges in Cloud Computing. http://www.thesai.org/Downloads/Volume4No1/Paper_6-An_Analysis_of_Security_Challenges_in_Cloud_Computing.pdf

11 FingerTec Worldwide. June 2012. TimeTec Cloud Technology White Paper. http://sales.fingertec.com/download/info/TTC-whitepaper-E.pdf