Cloud Computing Security, Reliability And Availability

To make cloud computing suitable for use in business, where customers need to be assured of supply of the business product/service at all times, and business need to operate at full potential at all times, three pertinent issues need to be addressed for cloud computing to fulfill its roles. These issues are security, availability and reliability, and without them, cloud computing cannot fulfill its role of being the best alternative in data and information storage.

1. Security

Due to the increasing popularity of cloud computing, emerging concerns users are having to contend with include undesirable internet invaders such as worms, viruses, hackers and financially motivated cyber-terrorists. As more people move into the cloud computing avenues, these undesirables take advantage of vulnerabilities and exploit them for personal gain. Providers will therefore need to up their protection systems to ensure that their clients' data is safe, which will in turn lead to skyrocketing of costs of cloud computing prices.

The main types of applications that are available are classified according to the service being offered. The different types of services also have different security concerns that stem from the structures that are put in place to make them accessible to multiple users.

Saas, Iaas and Paas

Software as a Service (Saas)

The main security concern for users of SaaS is denial of service attacks that may be made towards them directly, or that might affect them when their provider it attacked. In denial of service attacks malware may be injected into the servers that generate useless traffic to the server that slows down access of service by genuine users. Another way that is done is by hackers giving multiple commands to servers that slow it down and make it hard for other users to be able to enjoy the service sufficiently.

Platform as a Service (PaaS)

PaaS has some underlying security concerns associated with it, which emerge mostly from the activities of the provider such as third-party relationships they may have with other providers. Combinations of these elements from numerous sources create mash-ups, whose security is suspect, and which also brings the security concerns into the entire platform.

Another security issue with PaaS is the requisite frequent upgrading of features contained in the platform. As the providers strive to keep up with the upgrading requirements of features, applications may get developed too quickly to give sufficient time to seal all security loops and bugs in them. Once the applications have been integrated into the platform, the whole platform becomes susceptible to the bugs.

Infrastructure as a Service (IaaS)

IaaS providers make storage facilities, servers, networks and other computing resources available to their users by creating virtualized systems. The security concerns experienced by IaaS therefore come from the virtualization feature of their services such as the hypervisor, which oversees the performance of all virtual machines. The hypervisor therefore becomes a very crucial component of the IaaS that must be secured, as its breach is passed on to the whole system.

Other weak points of the IaaS include Virtual Machine image repositories which are made public for all users. These repositories, when infected images are uploaded onto them, could potentially spread the infection to the whole cloud.

Threats to cloud computing applications as attributed to by Bisong and Rahman (2011) include the abuse of cloud computing by third parties who might be looking to benefit from information stored in the clouds, use of programming interfaces that are not fully secure, which might expose users to various forms of possibly catastrophic attacks, abuse by insiders with malicious intents and vulnerabilities that develop out of sharing of technologies between numerous people in different places and with different needs.

Others include loss or leakage of data during transit into the cloud, during transfer from one point of the cloud to the other, such as from the provider to the cloud or from the cloud to the user's computers. Hijacking of service provisions is another detrimental threat, which is mostly perpetrated by hackers in order to illegally access other people's data for personal gain; the last threat to cloud computing is the unknown risk factor, the ever present factor to every business decision in a business on the unpredictability of events out of the entrepreneur's control.

To manage risks, businesses need to respond to issues that could lead to breach of confidentiality, integrity or uninterrupted and reliable availability of an Information system, Bisong and Rahman (2011). Among businesses that have intellectual property and trade secrets stored in their clouds, securing of this information is of critical importance, as it sustains business activities on the day to day basis. The fact that the business is not able to verify the integrity of devices used to store their information by their cloud computing provider makes it absolutely necessary to ensure total confidence in the selection of a provider, such that the information placed in their servers is secure and always accessible.

Bisong and Rahman (2011) also advice users to ensure that their data is segregated from other users online to prevent mix-up with other data, which could bring about more complications in form of insecurity and virus infections, which might turn out to be destructive. The service provider should demonstrate sufficient proof of encryption schemes that actually protect user data from theft and malicious attacks from other users.

In the event of an attack in which loss of data or information happens, the provider ought to have sufficient forensic examination capacity to find the fault in their system and also the capability to rectify them to avoid such incidents in the future. This is the risk assessment that every business should conduct on a

potential provider of their cloud computing services, not only on their own systems, but more importantly, on the provider's systems.

On vulnerability, the Bisong and Rahman (2011) define them as those weaknesses that exist in the system that can be exploited to cause harm to the business. The most harmful forms of weaknesses in a system are those that can allow a third party to eavesdrop, access databases by hacking or cracking, or conduct malicious attacks meant to cause harm, or outages in services reception or provision.

Businesses and users of cloud computing services are ultimately responsible for their own security, as they stand to lose most in case of loss of information they store in the cloud. According to Bisong and Rahman (2011), it is important that businesses realize that the loose structure in which the cloud is organized in also creates an impact on the data that is sent to its servers for storage. In-depth knowledge of the structure of your provider is encouraged to avoid pitfalls that may turn out to be very harmful to the business.

2. Service Availability in Cloud Computing

The end means of cloud computing services and the reason why most people are shifting towards cloud computing applications as a means of storing their data is because of the universality of the internet. By hosting the data deposited in the windows on the World Wide Web platform, providers assure the users that they can gain access to their files/data from whatever location. Being placed in a virtual space, with encryption codes and authorization limitations, the users can gain access to their data from any place, which is convenient to many users.

Such services as public clouds, a cheaper, much more accessible and available type of cloud, have been made popular by the widespread attractiveness and demand for cloud applications. Public clouds are suitable for individual users as they allow for people to scale up or down on their storage allocations according to their needs. The users are also able to access their data remotely, with back-ups available in an as-needed basis. Some of the social websites function as a cloud of sorts, allowing people to access a limited amount of data in a given database from any location, with back-up and security support assured.

The benefits of public cloud storage, according to Ricky & Magalhaes, 2014 include the increased agility in access and storage of data. With the ability to remote-access data, people do not have to be using the devises in which their data is physically stored, instead using their credentials with their provider to access their data freely and with limited limitation.

Back-ups that are automatically available in many clouds are very important in the recovery of information and data that is lost for whatever reason. It also allows users to archive information they do not require instant access for a later time when the access might become necessary. Public clouds are also way cheaper than private ones, as the costs of handling data stored in cloud are distributed to a larger group of people.

Concerns that come with public cloud usage for storage of data include the loss of control of data placed in the cloud. As providers need to keep the amount of data load on their systems, restrictions are often placed

on the quality of data that can be stored online. Users often need to downgrade their data to match the storage requirements of providers, which affects the general value of the data.

Other concerns come from the fact that the user is just a statistic in a large multi-tenancy infrastructure, with little to no specialization of services provided being available. Due to having many people access databases at once, some type of denial of service concerns in accessibility may exist, making it rather unreliable. With networks of data and information sharing in a domain established, changing a vendor may mean that users will not be able to access to pertinent information. This means that the user has limited control on the vendor they use to get cloud services.

Due to the important role played by the provider of cloud computing services, users are advised to ensure that sufficient disaster recovery infrastructure has been put in place, which will save them from the worry of events to follow after the loss of data in the cloud. Another important quality to vet in the provider is their long-term availability, and the fate of cloud data stored in their servers in the event of failure that leads to bankruptcy, or in case the company become absorbed into another. Enough assurance should be given that the data stored in the cloud will be accessible to users independent of the provider.

Businesses should avoid rushing into cloud computing without conducting their due diligent cross-examination of the pros and the cons. The switch to cloud computing ought to be well planned, and over time, piloted and good governance systems set up to manage and ensure its sustainability. Only then should the business make the strategic move into cloud computing, with all security concerns mitigated and back-up plans put in place.

3. Cloud Computing Reliability

Users are also advised to demand for transparency on the security infrastructure of the cloud computing provider to ensure that they are capable of fulfilling the needs for which cloud computing services are being sought. On this vein, a potential user of a provider's services should check that they have a record of regular audits on the security of their cloud. Businesses should ensure that the auditor is an independent third party, or more preferably a federal agency, as they are incorruptible and less easily manipulated.

Users should also put to mind the legal implications of what is sent into the cloud, and its relationship with the law. The fact that the cloud is supposed to be a vault that is secret and safe from interference does not remove the supremacy of the law, and should the information being stored be declared illegal, a business or individual would be susceptible to the rules of the land in a court of law, should it come to that.

To ensure the safety of data stored in the cloud, a user is also advised to monitor any changes in technologies or advancement and development of new and/or better means of doing things. In the ever evolving world of the internet, both the security and the convenience of data stored in the cloud will forever be evolving for the better. The service provider should pass all confidence tests that assure prospective users, beyond all reasonable doubt, that they are capable of providing satisfactory and uninterrupted services.

Sabahi F. (2012) touches on the operational procedures of clouds, and the systems that are put in place to enable the numerous users who enjoy the services of clouds to do so with confidence. It also addresses issues that affect the effectiveness of a cloud system, which need to be properly monitored to ensure that clouds conform to the highest set standards of the service. These include virtualization, hypervisor installation among others.

Virtualization is described as systems that are put in place by IT companies to optimize the performance of virtual machines, the systems that are created by providers to meet the clients' computer needs without having to purchase thousands of them for each customer. They are controlled by a hypervisor, which exists in a superior level to monitor the performance of these virtual machines. By creating a virtual hardware, the features of this hardware are duplicated to satisfy customer needs.

Information security policies are other issues that providers have to adhere to in creating their products. These assure users that they shall have privileged user access to preserve the sanctity of their data from unauthorized access. This is especially important when sensitive data is being handled. The providers are also held responsible by regulations placed by legislative bodies, while also receiving some protection from certain types of client caused losses, which makes the client as responsible for the security of their data as their provider.

Even with the requirement to create virtual machines to enable segregation of user data, virtualization machines are susceptible to attacks, such as those that are aimed directly at the hypervisors. The hypervisor hardware may be susceptible to attacks on location or to the OS, when the attacks are being conducted from within the providers' ranks. Expanded network surfaces are other spaces where the virtualization software may be susceptible, due to their placement outside the firewall of hypervisors.

Intrusion of clouds, in which client's data is susceptible to malicious attack, is an issue that cloud providers have had to face decisively to avoid loss in confidence by their customers. The most prominent way in which this is made possible is by the use of Intrusion Detection (ID) software. This type of software helps in detecting and stopping malicious behavior in networks, and it is also usable for SaaS, PaaS and IaaS providers' protection.

These are the measures put in place by the industry and the providers of cloud computing applications to increase the performance of their servers, and to assure their users that they can be able to trust them to provide cloud services at all times. Reliability means that users are able to completely forget about the other issues of their data being secure and available in the cloud without them having to be at risk of personal loss.

Users should realize that the ultimate responsibility of securing their own data rests with them and that even with all the steps taken by the applications providers to ensure that the sanctity of data stored in cloud is safe, the responsibility of selecting their service provider who meets the parameters of a competent provider rests with them. One of the safest routes to take in choosing a cloud provider is by choosing one

with enough experience in the field, because they are the ones most likely to have the know-how of solving issues that arise on the day-to-day basis, and ensuring that service provision is not disrupted.

Cloud Computing Applications

When making a decision to use cloud computing applications, every person ought to first understand what it entails. Information is as important in cloud computing applications as the applications themselves, as the suitability of the application will be informed by the knowledge the purchaser has on their requirements. Convenience of cloud computing applications is important, but the three most important issues still remain to be availability, reliability and security.

Security is the most pertinent issue in cloud computing applications that are available for customer use. The primary and most common reason for users purchasing cloud computing services is to secure their data from storage risks in their servers. Due to the crucial and sensitive nature of information to business and individuals, security concerns are most important consideration, both for the providers, and for the users. This is made especially important by the existence of numerous undesirable elements in the internet that are focused solely on wrecking havoc on other users to gain personal financial gain.

Protection from worms, viruses, hackers and cyber-terrorist is an issue that has led to numerous regulations from governments and industry norms put in place by players in the industry to reassure users that the sanctity of their data will be preserved in the cloud.

Security plays an equally important role in ensuring that cloud services are available and reliable; when breaches in security of whatever kind occur in the cloud, the availability of data is invariably affected, and in most cases, made virtually impossible. The greatest issue in availability of cloud computing services is security.

When security breaches are common in an application, users cannot be sure that they will be able to access their data at the times when they need to. Yet even on the cloud, worms, viruses and hackers could create data loss perpetuated by attackers which make data inaccessible, making it an unreliable storage for operational data in business. Accessing applications when they are available and being unable to do so when a security concern takes out the service causes unreliability.

Availability is the most important tenet of cloud computing applications for any business or individual using them. The technology was generated in order to bridge the gap between users and their data by allowing remote access from any internet enabled terminal. The other means of data storage clouds replace is physical storage in devices such as flash disks, hard disks, in-built computer and device memory among others.

These forms of storage are susceptible to loss, destruction, malware and other such challenges. Cloud computing is there to answer the question of what happens when data stored in a device is no longer accessible. With back-ups being equally as vulnerable to attack, the ultimate security is to place the data online and entrusting a provider to provide the back-up and protection necessary to keep that data safe.

That is the one way in which the availability of data can be assured, as long as the provider has been vetted and found to have all the measures in place that will keep data secure and accessible. Confidence in the provider means that the user data will be available even in the event of risk; the ultimate responsibility to make data ever-accessible ultimately lay on the user.

Reliability is an equally important issue to consider in purchasing cloud computing applications. A reliable application is one that the user can be sure of its availability at all times, and one that assures users that their data will always be secure from any forms of attack or interference. In a nutshell, it is the trust that a user has on their provider to give them quality services and a nod to their abilities in making coud computing services accessible to them at all times.

Users should check on their providers to be sure that they have put in pace all measures assuring them of both security and availability of their data. Reliable cloud providers are those that have some experience in the provision of the services, which gives them the ability to provide superior, uninterrupted services at all times.

Businesses seeking computing services should make several considerations in choosing the most suitable product, the greatest of which should be the storage capacity available, and the scalability of the same for future needs, as well as the bandwidth allocation. In this world of all things internet, bandwidth plays a vital role in the accessibility of data from trillions of gigabytes of other data online. Bandwidth also protects from the debilitating security concern of the most common form of cyber-bullying- denial of service attack- by absorbing the extra meaningless traffic being generated into the spare bandwidth. It is also a common remedy that providers resort to when a client suffers from this form of attack.

As the most widely available cloud computing application, cloud computing is a great consideration for individuals and small businesses aiming to keep costs low while still enjoying cloud computing applications. Users should choose carefully when selecting public clouds to avoid the pitfalls that come with it, by planning carefully and vetting providers to be sure that they match their needs. In most cases, the more expensive software is would mean that more people use it, which might guarantee its performance more than any other assurances by the distributer.

For individuals seeking cloud computing services, conducting research, risk assessment and suitability and feasibility tests is necessary, as joining a cloud service is a crucial business decision that is not to be taken lightly. Individuals and businesses are also expected to choose the best service to purchase from the cloud out of the SaaS, PaaS and IaaS available. The choice is supposed to be the one most suited to their needs, and for business, the one that will best ensure that profit maximization is possible.

Conclusion

Cloud Computing is often regarded as the future of business and the future of storage and transmission of data. With the freedom that it gives users also comes risks and shortfalls, most of which are related to the all important factor of information safety while in cloud. Both the users and the providers of clouding services are charged with the safety of the service, with users being guided by their best interests to ensure that prudence is practiced in selecting a provider and the best type of service. Providers are regulated by governments, and self-regulate as an industry, to provide the best possible cloud services to their clients. Ultimately, cloud computing is made secure, reliable and available at all time by the diligence of both the user and the provider.

References

Bisong A. and Rahman S. M. (2011) An Overview Of The Security Concerns In Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1,

https://www.researchgate.net/publication/48197685_An_Overview_Of_The_Security_Concerns_In_Enterprise_Cloud_Computing

Hashizume K., Rosado G. D., Fernández-Medina E. and Fernandez B. E. (2013) An analysis of security issues for cloud computing Journal of Internet Services and Applications

http://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5

Ricky M. & Magalhaes L. M. (2014) Stability and Reliability of Public Cloud Storage"

http://www.cloudcomputingadmin.com/articles-tutorials/public-cloud/stability-and-reliability-public-cloud-storage.html

Sabahi F. (2012) Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges. International Journal on Advances in ICT for Emerging Regions (ICTer) 4(2)

http://icter.sljol.info/articles/abstract/10.4038/icter.v4i2.4673/