Cloud Computing Report

BUSINESS-CRITICAL INFRASTRUCTURE MIGRATION

Pklm51 | Software, Systems and Applications | Cloud Computing

PKLM51

Contents

Introduction

The Organization- ITSB

Information Technology Systems for Businesses (ITSB) are a small-scale Organization, who offer IT-based business solutions for other small-scale companies. They offer a range of services, including software development of bespoke systems, and IT management through monitoring and security.

ITSB currently have around 15 members of staff, and have roughly doubled their revenue each year since their start-up 8 years ago. They aim to continue this trend over the coming years and wish to employ another 15 members of staff by the end of 2020, opening a second office to handle the increase in size. ITSB currently have around 100 clients, who they offer around the clock support for, ensuring the services they are offering are working correctly and to a high standard, matching that of the ISO 9001 quality standards [1]

The need for a change in infrastructure

To help manage the predicted increase in size, ITSB feel moving their business-critical infrastructure to the cloud may be a workable solution. They want a truly scalable solution so that they can easily adapt to change, whether it be above, below or on target to their projections.

The company also wish to be able to host web-servers as a product for clients who want to make use of web-services, which will be ran and monitored by ITSB as part of their IT management services.

ITSB staff have also requested to be able to work fluidly between both offices as they may be changing workplace daily depending on client demands, with the ability to access all the same accounts, documents and software at both locations.

This document

This document aims to best advise ITSB, by providing information on what would be needed in terms of infrastructure and security, to offer maximum uptime for an around the clock operation, and to meet the projected business model with an effortlessly scalable system.

Infrastructure Management

Deployment techniques

ITSB have 3 main options for how they wish to deploy their cloud infrastructure:

- Private Clouds- Invest in company's infrastructure, deploying datacenters and virtual environments for internal and client use.
- Public Clouds- Lease 3rd party infrastructure and services to meet the company's evolving demands.
- Hybrid Clouds- Use a mixture of private and public clouds, managing the load between the two.

Each Infrastructure has its own advantages and disadvantages, generalized in the table below:

TECHNIQUE	ADVANTAGE	DISADVANTAGE
PRIVATE	More control over infrastructure Easier internal development (sandboxing)	More difficult to scale than other two Difficult to load balance
PUBLIC	No Capital expenditure Easily scalable to adapt to change in load	Long term total cost Don't own the hardware so no sale able assets
HYBRID	Easy to deal with compliance standards Ability to scale Business critical components	Integration management between the two may be difficult due to complex network infrastructure

For ITSB's current situation, I feel a hybrid cloud set-up would be the best to deploy. Using a private cloud for operational aspects and a public cloud for business-critical aspects would allow ITSB to scale seamlessly for the projected increase in number of clients, whilst giving the company better control of internal operations, such as software development on sandbox virtual machines.

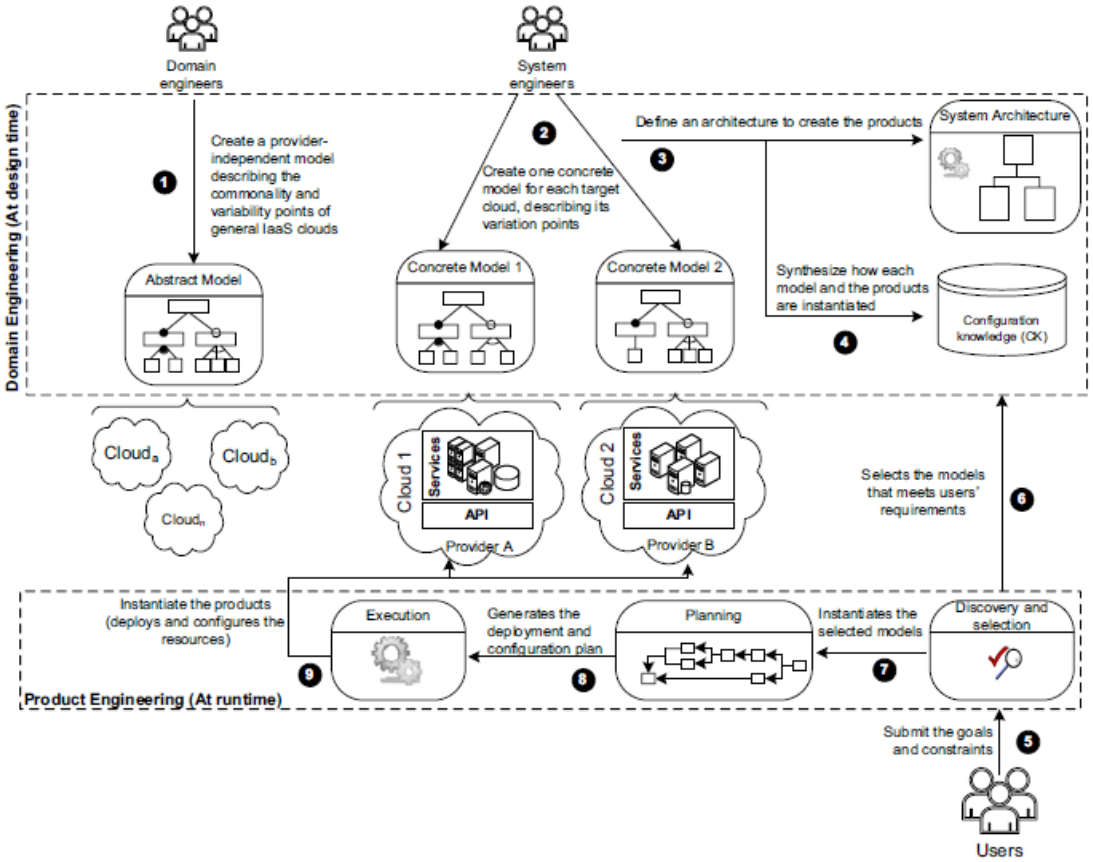
Though a full private cloud would put the company in full control of their infrastructure, I feel for a company of their size, the demand to own and manage all the required assets would be too much of a demand, with the initial cost of set up being too large for the small company [2]

Autonomic management

Due to the variability in demand from both internal staff and external clients on the network, the cloud infrastructure should be able to deal with the load balancing automatically, and without constant shadowing from a member of staff. Each user accessing the different services available should be able to do so consistently, with minimal interruption/delay regardless of the time or day.

A simple solution to the issue would be monitoring each of the different services (potentially through in-house built custom software), and allocating additional hardware, such as number of CPU's or increasing Memory size, to help cope with the load on struggling services. This is a naïve approach however, and in practice, wouldn't work effectively within ITSB's set up. In practice, the load will be varying too much to efficiently reallocate physical hardware manually and would take up more staff time than required.

A more sophisticated autonomic management could be deployed however. For example, A feature-based engineering method to automate resource allocation and configuration in inter-cloud environments, could be an effective solution. This would require predefined company standards, but would allow consistent, fair and effective resource management, with the ability to prioritise more critical services.



[3]

The purpose of the automation should be to ensure the three types of services (Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)) are delivered with a high of Quality of Service (QoS) to meet Service Level Agreements (SLAs) [4], such as that the company embodies in ISO 9001. An effective autonomic management method would help ensure these services are delivered to a good level, but most important, consistently.

Scalability under constraints

ITSB's current internal infrastructure would soon run into obvious scalability constraints. There is a physical limit on how much hardware can be used on-site, with equipment and space being a key issue, and the time taken to re-adjust to scale increases/decreases costing the company money.

A cloud-based infrastructure helps loosen constraints on scalability, though doesn't open the doors to scale infinitely with no extra operations expenditure (OPEX) cost. As the scale of operations increases, so does the cost. For example, a simple online calculator (found here: https://www.planforcloud.com/) demonstrates how the Base Hourly Cost increases as the required hardware does, and how the difference in service provider and server type can also make a significant difference. For example, for a 512 server (0.5GB RAM, 20GB HDD) with Rackspace costs $0.022 as a Base Hourly Cost, where as a Web/Worker Role server (0.75GB RAM, 20GB HDD) with Windows Azure costs $0.02 as a Base Hourly Cost. This is a potential $175 difference a year.

Disregarding operational expenditure however, services that ITSB wish to deploy in the public cloud should not face scalability constraints. The company's supplying the service are built with an infrastructure capable of handling spikes in an increase in demand, allowing for dynamic scalability to guarantee scaling and elasticity features [5]. In contrast however, the internal private cloud features will only be able to scale to a maximum of the physically available hardware to the organization.

Product offerings from different providers

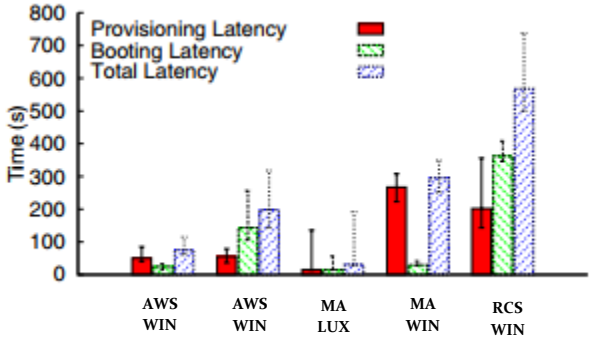
One way that ITSB could handle their hybrid cloud based infrastructure is through using AWS, Microsoft Azure or Rackspace CloudServers for the business-critical public components, whilst using VMware vSphere for server virtualization of their private cloud elements [6].

For the private cloud elements, the majority of decision making is within the company themselves and how they wish to handle their datacenters and internal infrastructure, where the public cloud elements offer more choice and variability which will be analysed further below.

There are a wide range of providers that could be selected, and selection would be affected by the exact requirement from ITSB, but the following comparisons are going to be based from Amazon AWS, Microsoft Azure and Rackspace CloudServers.

One key contributing factor is cost. For example, for a single core VM with Amazon AWS the price pre-hour is $0.085 compared to that of $0.12 from Rackspace CloudServers. Amazon AWS also offer the cheapest price per hour for a quad core VM at $0.68, with Microsoft Azure and Rackspace CloudServers costing $0.28 more per hour. [7]

Another contributing factor is latency time, which varies between latency type and provider as shown below:



[7]

As well as choosing between providers, ITSB will need to choose a service model. One option is to use a Service Oriented Architecture which entails using policies, practices, frameworks that enable application functionality to be provided and consumed as sets of services published at a granularity relevant to the service consumer [8]. Another is to use the self-explanatory and industry standard Pay-As-You-Go model where ITSB would pay for the exact resources they use/require.

Security

Data management and protection

As with all IT services, personal data should be handled carefully, with every effort to protect personal information, upholding to legal and company standards.

Data security is extremely important when using cloud computing at all levels (Iaas, PaaS, SaaS) [10], and the public cloud computing provider has to offer a level of security that the enterprise is confident with, for their data, during its life in the Cloud. ITSB should consider how they can ensure that data is secure and protected during the following [11]:

DATA SECURITY ASPECT	EXPLANATION	DATA THREAT	DATA MANAGEMENT /PROTECTION	EXAMPLE IN ITSB
DATA – IN – TRANSIT-	Transferring of data across the internet	Unauthorized Access	Encryption algorithm on data	Sharing custom bespoke software written for clients through FTPS
DATA – AT –REST	Data stored in a cloud based application	Unclear ownership and responsibility of data protection	Encryption- though can cause problems when searching data	Customer details stored in a database
PROCESSINGOF DATA	Processing of unencrypted data in the cloud	Data Inconsistency	IBM homomorphic encryption scheme [9]	Private queries on search engines
DATALINEAGE	Recording the path that data takes	Inadequate authentication and authorization	Used for tracing/debugging	Tracking which VM's the different customer's services use
DATAPROVENANCE	The ensuring of data integrity and accuracy of manipulated data	Audit difficulty	Encryption of input and output data, with through testing of data calculations	In-house functions to calculate cost of projects for functions
DATAREMANENCE	The remains of data in the storage media	Data theft	Ensure full and thorough wiping of unwanted sensitive data	Deleting archived customer details after a set period of time

An example of a level of data management that the company should uphold to is the ISO 27001 [12]. This is a specification for an information security management system (ISMS). And is a framework of policies and procedures that includes all legal, physical and technical controls.

LIABILITY:

Ultimately, the responsibility for data management and protection would lie with ITSB, though any problems that may occur during the processing, transferring or storing of data from the Cloud Service Providers would be their liability. The following paper discussing in more depth the responsibilities of the different parties, and how the different services being provided affect the situation: "Liability for non-compliance with data protection obligations" [13]

Potential threat vectors and mitigation techniques

There are many potential threats to a cloud computing infrastructure, however in this document the top 12 threats of 2016 will be reviewed to help ITSB prepare for and prevent the most likely causes of threat. [14]

THREAT VECTOR	DESCRIPTION	SERVICE MODEL EFFECTED	THREAT MITIGATION
1. DATA BREACHES	A breach of sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so	IaaS, PaaS, SaaS	Information Management and Data Security
2. WEAK IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT	Data breaches from weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates	IaaS, PaaS, SaaS	Encryption and Key Management
3. INSECURE APIS	Insecure authentication and access control to encryption and activity monitoring of interfaces and API's	IaaS, PaaS, SaaS	Application Security

4. SYSTEM AND APPLICATION VULNERABILITIES	Exploitable bugs in programs that attackers can use to infiltrate a computer system for stealing data, taking control of the system or disrupting service operations	IaaS, PaaS, SaaS	Governance and Enterprise Risk Management
5. ACCOUNT HIJACKING	Methods such as phishing, fraud and exploitation of software vulnerabilities still achieve results	IaaS, PaaS, SaaS	Traditional Security and Incident Response
6. MALICIOUS INSIDERS	A malicious insider could be a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data	IaaS, PaaS, SaaS	Identity, Entitlement, and Access Management
7. ADVANCED PERSISTENT THREATS (APTS)	APTs are a parasitical form of cyberattack that infiltrates systems and smuggle data and intellectual property	IaaS, PaaS, SaaS	Data Center Operations and Virtualization
8. DATA LOSS	Data stored in the cloud can be lost for reasons other than malicious attacks. An accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, can lead to data being lost	IaaS, PaaS, SaaS	Business Continuity and Disaster Recovery, physical back-ups of data
9. INSUFFICIENT DUE DILIGENCE	Developing a poor roadmap and checklist for due diligence when evaluating technologies and CSPs	IaaS, PaaS, SaaS	All the aforementioned
10. ABUSE AND NEFARIOUS USE OF CLOUD SERVICES	Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.	IaaS, PaaS, SaaS	Legal Issues: Contracts and Electronic Discovery

11. DENIAL OF SERVICE	DoS attacks are attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources	IaaS, PaaS, SaaS	Data Center Operations and Application Security
12. SHARED TECHNOLOGY ISSUES	Comprising the infrastructure supporting cloud services for deployment may cause integration issues	IaaS, PaaS, SaaS	Cloud Computing Architectural Framework and Encryption and Key Management

LIABILITY:

ITSB should take as much responsibility to ensure that each of the 12 threat vectors above are reduces to as small of a probability as possible. The likelihood of most of the threats can be reduced internally with sufficient management and delivery of information to staff. Considering the drastic effects that the treats could have to the organization, ITSB should make taking the suggested pervasive actions as an essential step in migrating the business-critical components to the cloud.

Contemporary Trends in Cloud Computing

Though the above information should be sufficient to allow ITSB to deploy an effective cloud based solution, they may want to consider the following leading areas of research and trends within cloud computing to be better prepared for future developments.

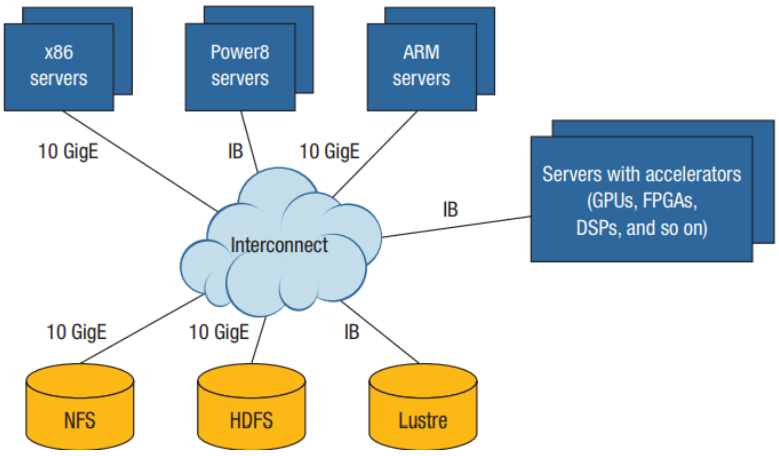
Infrastructure development

One new trend that ITSB may consider adopting is the option to change the cloud infrastructure from the 'normal' standard set up of having dedicated compute and storage resources located in data centers [15]. This could be achieved by implementing any of the following:

- **Federated cloud**- A model for business-driven federation of cloud computing providers, where each provider can buy and sell, on-demand, capacity from other providers [16]. Although this is not something that ITSB can adopt until further progress is made, they can encourage its development by registering interest and showing their support for the proposed solution for Cloud Computing.

- **Microcloud and cloudlet**- A sustainable alternate low power and low-cost model, achieved by decentralizing computing towards the edge of the network for making computing possible closer to where user data is generated [17]. This can be further developed by adapting an Ad hoc cloud technique by adopting a variety of underutilized resources (servers) from a range of locations for a more efficient and elastic infrastructure [18]

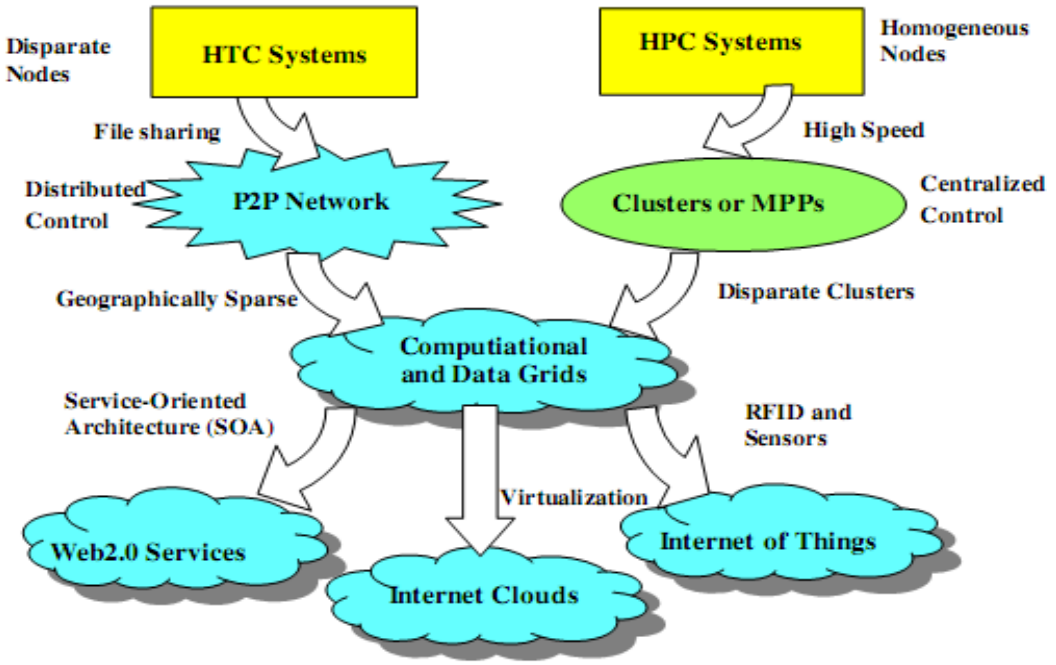
- **Heterogeneous cloud**- Heterogeneity at the infrastructure level, combining several types of processors to offer VMs with heterogeneous compute resources. For example:



[19]

Internet of Things

Another emerging trend within Cloud Computing is the use of the Internet of Things. With almost anything being able to connect to the internet, from dishwashers to automobiles, a large amount of data could be used, and processed with the correct architecture. Computational and Data Grids could be used to utilize HPC (High-Performance Computing), HTC (High-Throughput Computing) P2P (Peer to Peer) and MPP (Massively Parallel Processors). The infrastructure could look as follows:



[20]

Big Data

Finally, there is currently a lot of research into Big Data, and how it could potentially be effectively utilised within Cloud Computing. With data being created at a record rate [21], a huge challenge is creating platforms that can process and interpret the intensive workloads. One way that this could be handled within the cloud is through using MapReduce in clouds [22]. This accelerates the processing of enormous amounts of data in a cloud by robotically performing scalable distribution and also provides an interface that allows for parallelization and distributed computing in a cluster of servers.

References

[1] ISO, Quality management principles, 2015.

[2] Marston and Et.Al., Cloud computing — The business perspective, 2010.

[3] A. Leite and Et.Al., Autonomic Provisioning, Configuration, and Management of Inter-cloud Environments Based on a Software Product Line Engineering Method, 2016.

[4] S. Singh and Et.Al, STAR: SLA-aware Autonomic Management of Cloud Resources, 2017.

[5] V. Casola and Et.Al., Automatically Enforcing Security SLAs in the Cloud, 2016.

[6] vmware, VMware Solutions for Small and Midsize Business, 2013.

[7] L. Ang and Et.Al., CloudCmp: Comparing Public Cloud Providers, 2010.

[8] D. Sprott and L. Wilkes, Understanding Service-Oriented Architecture, 2004.

[9] C. Gentry, A fully homomorphic encryption scheme, 2009.

[10] T. Sathyanarayana and I. S. L, Data Security in Cloud Computing, 2013.

[11] T. Mather and S. Kumaraswamy, Cloud Security and Privacy, 2009.

[12] ISO, Information technology — Security techniques — Information security management systems — Requirements, 2005.

[13] M.-C. Roques-Bonnet and L. Neto Galvao, liability for non-compliance with data protection obligations, 2014.

[14] C. S. Alliance, The Treacherous 12 Cloud Computing Top Threats in 2016, 2016.

[15] B. Varghesea and R. Buyya, Next generation cloud computing: New trends and research directions, 2017.

[16] B. Rochwerger and Et.Al., An architecture for federated cloud computing.

[17] B. Varghese and Et.Al., Challenges and opportunities in edge computing, 2016.

[18] G. McGilvary and Et.Al., Proceedings of the IEEE 8th International Conference on Cloud Computing.

[19] S. Crago and J. Walters, Heterogeneous Cloud Computing: The Way Forward, 2015.

[20] K. Hwang, G. Fox and J. Dongarra, Distributed and Cloud Computing, 2012.

[21] R. Villars, C. Olofson and E. M, Big data: what it is and why you should care, 2011.

[22] I. Hashem and Et.Al., The rise of "big data" on cloud computing: Review and open research issues, 2015.