Towards Distributing Multimedia Applications on a Virtualized Cloud Infrastructure

Mak Shama
Birmingham City University
Birmingham, UK
mak.shama@bcu.ac.uk

David Newell
Software Systems Research Group
Bournemouth University
Bournemouth, UK
dnewell@bournemouth.ac.uk

Philip Davies
Faculty of Technology
Bournemouth and Poole College
Bournemouth, UK
pdavies@bpc.ac.uk

Benjamin Todd
Postgraduate Research Student
Bournemouth University
Bournemouth, UK
bwtodd@gmail.com

***Abstract*—We examine some technological aspects of cloud computing, focusing on virtualization applied to various data types including multimedia and identify the benefits & security concerns for a modern IT infrastructure. An experiment to migrate a live company server consisting of Microsoft Exchange e-mail and file server to a cloud infrastructure is conducted. The initial findings are that each process step needed to overcome security issues of server migration.. The writers will propose improved approaches for modelling cloud-hosted multimedia applications, semantics and abstract data models.**

Keywords – Multimedia, Virtualization; Cloud Computing; Server Migration; Security.

INTRODUCTION

In a previous paper [1], we evaluated an adaptive multimedia presentation system with contextual supplemental support media. In this paper we will be considering the requirements for operating this adaptive system from a cloud based infrastructure. 'Cloud Computing' is a term for a multitude of online services allowing in-house computing services to migrate to rented online infrastructures. 'Software, Platform or Infrastructure as a Service' are concepts for processing, developing or hosting application and data on demand. Improved speed and reliability of network connections fuel the explosion of portable, hand-held devices by reducing organisational IT costs.

The Virtualization and Evolution to the Cloud Survey [2] found that 75% of global organisations are positively considering migration to a virtualized /hybrid cloud environment. However, 44% of CEOs and 46% of CFOs still have concerns about migrating their applications and services. It was also suggested that once organisations move their critical applications to virtualized or hybrid cloud environments then they find many benefits.

The current ad-hoc methodology to migrate a company server or application to the cloud uses an infrastructure, storage vendor, or a software service provider. The security aspects are built around the vendor, measures built into the customers own systems and how the data centres operates, for example, on a multi-tenant basis [3]. There are additional security measures that need to be implemented over virtual, public cloud networks that are discussed in this paper.

A small survey of ten local SMEs was undertaken by the writers to find out what services they run. Results confirm the industry trend towards virtualization and migration to the cloud raised security concerns for organisations. The main findings are summarized in Fig. 1.

Most businesses run four essential business applications: e-mail, file storage & printing, application serving and databases. It was found that these businesses have a desire to migrate to the cloud but their primary concerns are confidence in security compared with their on-premises solution, and worry about overall control of business data when required. It is clear from these results that companies, including those involved in multimedia data types, need to be shown how their data is secure in the cloud and the many advantages to be gained from migration.

The structure of this paper is as follows: Section 2 gives a brief survey of current methodological approaches to virtualisation. Section 3 reports on a case study of an actual small company migration. Section 4 discusses findings, including use of a novel multimedia application in an educational setting and finally, Section 5 concludes with a discussion of future work.

METHODS AND APPROACHES

Virtualization is a term given to the creation of a virtual computer within a larger more powerful computer. The more powerful computer is often known as a Virtual Machine (VM) host that runs software known as a hypervisor [4].

The hypervisor is a layer of software that controls and monitors the resource allocation of the host hardware - memory, processor and drive space - to the VMs that run on it. The VMs on the hypervisor are called instances; many of these instances can be run on one hypervisor, limited only by the hardware of the host system, which is usually designed to run multiple guest VMs. This has been illustrated in Fig. 2.

 ISBN: 978-1-61208-195-3

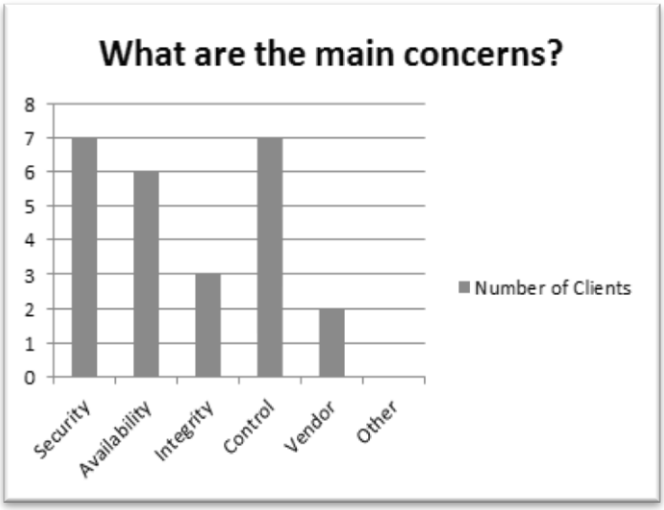

Figure 1. Summary of Survey Results

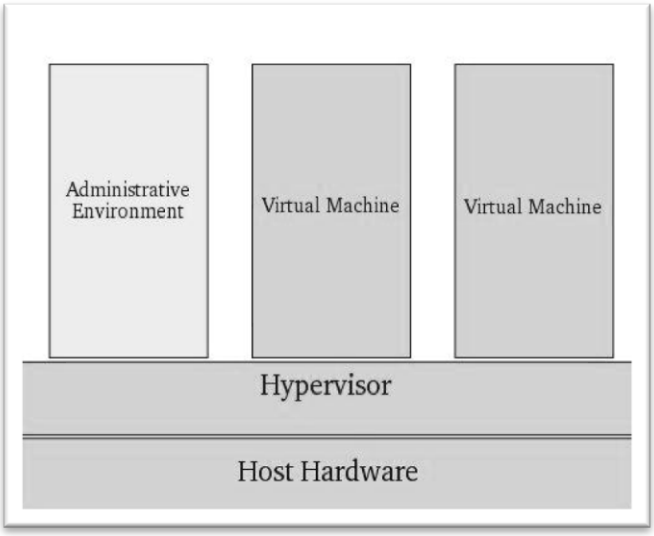

Figure 2. Virtualization Hypervisor Layer (Source: Virtuatopia, 2009)

There are many virtualization platforms available. The most commonly used are compared in Fig. 3. They offer comparable features, run on different specification hardware and are available for use on different physical computer system such as Windows, Linux or Macintosh host server platforms. [5].

Virtualization offers organisations advantages such as reduced operating costs, freeing up resources so users can instantly launch new servers within minutes, improving the flexibility of IT architectures [4].

Modern organisations are moving to a functioning cloud computing model where applications are virtualized and become 'always available' online, rather than the traditional systems, where all IT infrastructures are stored and maintained within a physical location of an organisation.

The general approach to migration to the cloud initially, is for an organisation to migrate to server virtualization followed by other types of virtualization such as storage and desktop/endpoints, and then finally private storage-as-a-service and private/hybrid clouds [6].

Virtualization is an important factor of modern day computing that has three distinct benefits to organisations. Firstly, it offers substantial cost reductions. Using virtualization allows organizations to consolidate their data centres and non-mission critical applications down to less than a quarter of their current data centre requirements, moving servers that are running at 20% capacity to shared servers that run at 70% capacity. Secondly, it offers speed of deployment and scalable resources to an organisation needing to launch IT infrastructure. For example, to go with the launch of a new product, increases in customer demands can easily be achieved in a matter of hours instead of weeks on the old model. Finally, it offers organisations a way to manage expertise and skill sets to easily manage multiple different applications with reduced staff to maintain the network[2].

A small organisation may virtualize just the servers in their office for consolidation, which becomes a small private cloud that they can access internally and externally. Larger organisations can go so far as to create complete virtual networks, using multiple VMs on different cloud infrastructure providers, and create virtual switches and connections with VLANs for their networks. As complexity increases, so may security concerns. With a network that is so complex, there needs to be a way to monitor all VMs that are running correctly [2].

Virtualization Platform	Provider	Host OS
Citrix Zen	XenSource	NetBSD, Linux, Solaris
Virtual Server / Hyper-V	Microsoft	Windows Server
Virtual PC	Microsoft	Windows
Parallels	Parallels	Macintosh
Virtual Box	Sun Microsystems	Windows, Linux, Macintosh, Solaris
VMware / ESX Server	VMware	Windows, Hardware (no host OS)

Figure 3. Comparison of Virtualization Platforms

 ISBN: 978-1-61208-195-3

There are benefits of virtualization in large organisations with thousands of computers otherwise requiring hardware rollouts, patching and maintenance [7]. Each desktop no longer needs individual licences for antivirus or productivity software as this will reside on the main hypervisor desktop virtualization server.

Virtualization is also eco-friendly and saves money in the long run. In the future, organisations will move more towards a virtualized desktop, and some examples of this can already been seen in third-world counties developing Virtual Learning Environments (VLE's) that allow students access to online resources without the need for a powerful local computer [8].

Terminal services such as Citrix have had a multi-user operating system environment for some time. Virtual Desktop Infrastructure (VDI) works in a very different way. Instead of having a server which can be used by multiple users at the same time, the server is running many virtualized single user operating systems which all act independently of each desktop system due to the function of the hypervisor [7].

An example of desktop virtualization using VDI is shown in Fig. 4. It makes use of a thin client at each user work desk. The virtual desktops are stored in a secure environment on the server. Thin clients use less energy, need less maintenance, and updates can all be performed much quicker on the VDI server. VDI is designed to allow the use of desktop operating systems such as Windows as well as Linux in a virtual environment that is easy to deploy, secure and manage with everything stored in the data centre [7].

Virtualisation can be extended to cloud computing. [9] Broadly, there are three levels of service that cloud computing provide:

A. Software as a Service (SaaS)

Applications are available online. For example, e-mail, online file storage, web hosting image banks, online software to perform virtually any task on multimedia data and more. Google Docs, or Sales-Force.com are current examples. There is not much control other than over data, but with no control over routers, firewalls, IPS or WAFs.

B. Platform as a Service (PaaS)

Application platform used for development of online services. For example, client relations management database, online developer tools, web site creation services and more. Combinations of different components managed by someone else allow use of databases or application services. Microsoft Azure is an example.[10]

C. Infrastructure as a Service (IaaS)

Provision of an online infrastructure. For example, online server hosting, virtual servers, direct access to physical servers in the cloud, web hosting and data centre. Amazon EC2 and Savvis (enterprise cloud) are examples that give users a lot more control. Raw virtualization with a good service layer could move a WAF or Gateway to this service. Users themselves start to assert a level of control of the cloud.

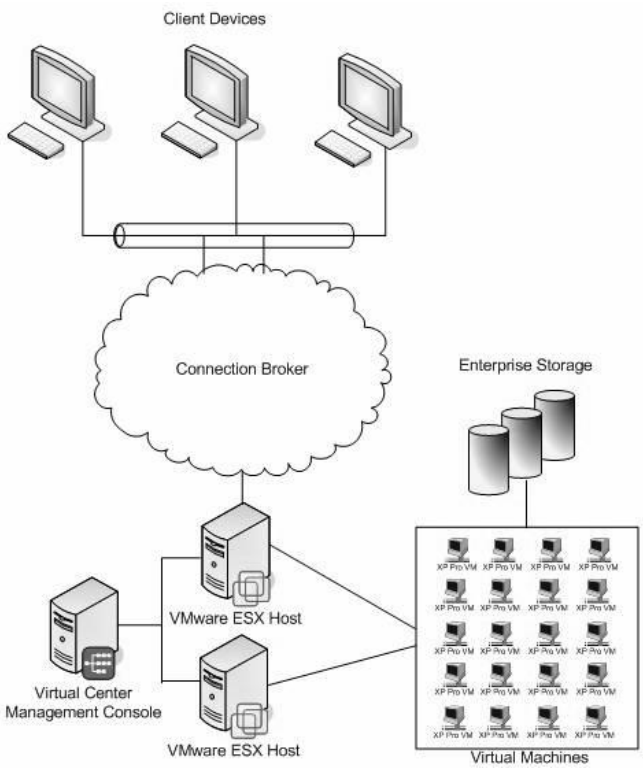

Figure 4. Virtual Desktop Infrastructure (Image Source: [7])

THE CASE STUDY

We perform an experiment to observe the migration of a company e-mail and file server to a cloud infrastructure to evaluate a strategy for transfer and to analyse the security implications. E-mail is moved over to a cloud service to be available on all devices everywhere and reduces costs. The experiment will test the migration of the Exchange Server from a physical server and make a comparison of options.

We consider the case of a local business which has an e-mail server at their head office in Bournemouth and they would like to move to cloud services. Their current server configuration is Microsoft Exchange for e-mail and the same server to store files. This server has anti-virus software for which the licence needs to be renewed each year. The desired result is to remove this server completely. Microsoft offer Exchange online as an alternative to hosted exchange, the web interface to migrate the exchange to online services. A second option is to migrate to Google Apps for business online that offers E-mail, Calendar, Contacts and Notes. It also offers file storage. A third option is to image the entire server, which currently stands at 200Gb of data, to a file and then upload this image to an online virtual server. The same software that was on the physical server will continue to be run on the online virtual server.

Some minor network re-configuration is needed and a redirect of the MX record for the e-mail domain. The shared drives can be mapped using Virtual Private Network (VPN) tunnelling. A drawback with this method is that the 200GB file will take a long time to upload at current upload speeds of 1.5 Mbps.

 ISBN: 978-1-61208-195-3

An alternative solution is an online service with a plug in application for the physical server. [11] This plug in application would selectively upload and replicate the data over to the online vendor with application integrity checking to ensure that the data is transferred correctly. Fig 5 illustrates how this application would function.

Currently, the organisation has Exchange for e-mail and VPN access for file shares. Email access is available through Outlook Web Access, IMAP or Exchange Message Application Programming Interface (MAPI) – one of the benefits of using Microsoft MAPI is that you also can use Calendar, Contacts, Tasks and E-mail all together with one protocol. A cloud provider should be able to support these extra functions. Google Apps for business supports this with an application that synchronises the contacts, calendar and tasks to Google cloud servers. Microsoft Exchange online simply performs all the exchange features that a local Exchange server would perform.

The methods available are to virtualise the server, upload it in its entirety and then make some small adjustments to the network connectivity, or to export the database then import it into an online providers system.

The server migration options are shown in the comparison table in Fig. 6 including security issues.

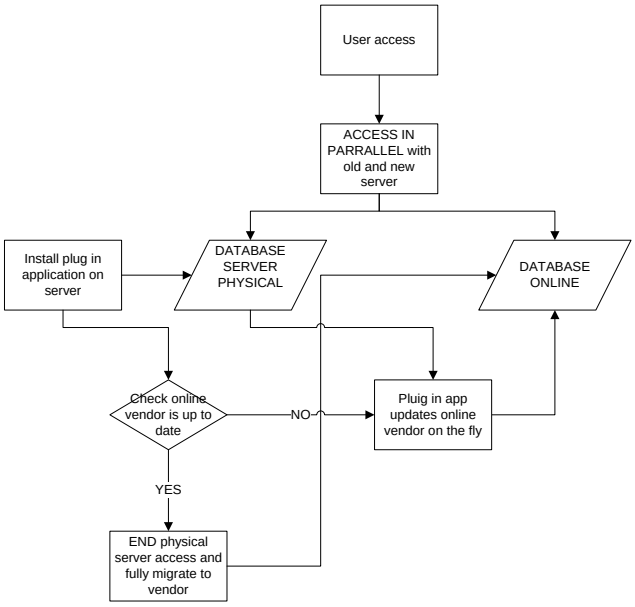

Figure 5. Server Upload Application Flowchart

FINDINGS

The experiment was performed with the server migrated online with all three options evaluated. Although it was found that Exchange Online and Google Apps were good choices, it ultimately depends on individual organisation preference. All e-mail features are available to computers at the office and to all portable devices with very little reconfiguration. However, the virtualized server resulted in a very large data file of 200 GB which takes a long time to upload. The user file is relatively efficient to upload as it is not sending a copy of the entire computer system to the cloud provider but there could still be compatibility issues with the image file when it reaches the online provider. The customer data was exported. For 100 users, the size of the exported file was quite small at 100MB. This file is very fast to upload to the online provider. Import problems could still arise with correct allocation of data fields. The data would need to be looked at to ensure its integrity.

Mission critical applications, as well as data are migrating to the cloud. A recent example of small cloud application is canp.me. [8] Providing a virtual desktop and storage facility using the local desktop processing power, the application provides synchronising data with the application. Hence it is possible to load an application to any PC from the cloud and authenticate the user from data stored on a USB key/dongle. Only one software copy is needed and one license. [12] Deployment times are greatly reduced as the cloud will only contain the latest data and latest copy of the application state. When a cloud based application is called, a minimum set of the appropriate Data Link Libraries (DLLs) are loaded and the remaining application is not loaded until it is required.

The fundamentals of the technology are based around the application's ability to compress, encrypt and transmit desktop applications into smaller parts to the cloud, and then to intelligently rebuild them from the cloud on the virtual desktop in real-time. This saves on bandwidth, because the application and data both reside locally until the data is to be saved and the.

Action	**Method**	**Security Concern**
Hardware Server	Stay at the physical server and update all components.	Security can always be improved: firewalls, IPDS, WAF all cost extra money to run and maintain.
Exchange Online	Install the client exchange transfer connecter module from Microsoft and it will upload automatically.	Security depends on Microsoft, however, they are a large vendor and their reputation is dependent on security for their service.
Google Apps for Business	Install the Google transfer module and exchange mailboxes are sent to Google.	As secure as Google cloud. Google has introduced a 2 step verification to add extra security. Also security features can be managed by Organisation Google accounts over and above individual Google accounts.

Figure 6. Comparison of Migration and Security Issues

 ISBN: 978-1-61208-195-3

application closed. Similar to Citrix XenDesktop, users can appear to travel with their virtual desktop anywhere by creating widgets

In summary, the applications such as cnap.me [8] offers users the possibility of a virtual desktop, synchronised storage, and updated software application, i.e. a low cost managed cloud solution.

EVALUATION

As cloud computing evolves and bandwidth increases, the nature of network connections change. The demand for migrating critical applications including multimedia into a cloud infrastructure will increase rapidly, as will services demanded of online security vendors.

This paper has presented evidence that migrating and storing data in the cloud can be as secure as retention on premises. [13] However, adequate attention to security measures is needed. It is recommended that any organisation considering migration should so do so at the earliest opportunity and take advantage of enhancing security provision.

Users concerned about cloud vendor failure should deploy a solution with failover between different cloud providers to provide access if one provider goes down or has lower costs. This may also be useful for a large organisation that wishes to separate applications in the event of partial failure. [14] Clearly, service level agreements are required for cloud provision. Therefore, each individual case will require evaluation and assessment as a superior service will attract a premium, however, failover, recovery and backup should be provided.

The cloud can offer many advantages over on-premises IT infrastructure. It has the potential to be flexible and cost effective for organisations to use. Security concerns raised can be solved using methods that secure the core aspects of data, identities and devices on an infrastructure. Using this across virtualization platforms will provide a secure network IT infrastructure.

Cloud infrastructure has the potential with appropriate security implementation, to be a better architecture than the old physical model. Virtual security should be much better than physical security.

Security issues are wide ranging and should include securing printer ports that are connected to networks possibly using mac-address based port security authentication. VLANS on virtual networks play a role in the security solution. Access control lists need to function across multiple segments of the network but only allow users access to authorised areas.

NAT, PAT, DNS and DHCP and security are critical network components that still need to be configured locally.

A necessary start for business executives for deployment of virtualized networks is to conduct a full requirements analysis and audit of the current infrastructure, and build a network to provide a future path for migration of physical networks to cloud ones. Plans have to include data, applications and infrastructure.

A major advantage of cloud based solutions is the rapid deployment of a reconfigured service or set of services such as cnap. For example, in the rapidly changing educational environment when a new department is set up, users can be simply added to an existing group policy or set up as a new group. Each user will have access to the applications already present with the inherent security privileges. If a separate server is required for this department, no new hardware is needed; the IT team can request or create a new virtual server within minutes ready to be deployed [15] [16].

CONCLUSIONS AND FUTURE WORK

A variety of methods and approaches have been identified to achieve a successful migration producing a documented strategy for implementation in an organisation with minimum disruption to business functions.

Using physical servers takes up valuable resources and requires a team of technicians to configure monitor and apply patches. There are clear financial and environmental advantages in the use of virtualization and migration to the cloud. A major advantage is rapid time for infrastructure deployment because there is no need to purchase additional hardware.

As more infrastructures are moved into the cloud, organisations can make use of additional services such as multimedia rich media streaming, sharing, and similar services. The reducing costs of infrastructure will open up new markets and opportunities for collaboration.

Plans by the writers will clarify requirements of the network, applications and data to take specific account of ubiquity and the pervasive nature of future multimedia applications & data.

Future goals will be identified for multimedia data models for applications and infrastructure hosted in the cloud. For example, experiments will be undertaken concerned with infrastructure performance to host cloud applications such as cnap.me [8], as a large scale multimedia Virtual Learning Environment (VLE) vehicle in a University. The vision is to clarify data models and requirements for a Cloud-based Virtual learning Environment (CAVE) as a logical evolution of the writers' current research area [1]. Future work will explore migration of a multimedia presentation system to the cloud by combining centralised with cloud-based Virtual Learning Environment (VLE) applications

REFERENCES

[1] Cutts, S., Davies, P., Newell, D. and Rowe, N., (2009) 'Evaluation of an Adaptive Multimedia Presentation System (AMPS) with Contextual Supplemental Support Media'. Proceedings of the MMEDIA 2010 Conference, Athens, Greece.

[2] Symantec. 2011. Virtualization and Evolution to the Cloud Survey: Global Results.https://www4.symantec.com/mktginfo/whitepaper/Virt_and_Evolution_Cloud_Survey_060811.pdf [September 2011]

[3] Morrison, K. S., Chenxi W., Managing the Cloud: An Enterprise Migration Roadmap. Layer 7 Webcast. June 2011.

[4] Rule, D,. and Dittner, R. 2007. The Best Damn Server Virtualization Book Period: Including Vmware, Xen, and Microsoft Virtual Server. Burlington:Syngress.

[5] Virtuatopia. 2009. An Overview of Virtualization Techniques. Available from http://www.virtuatopia.com/index.php/An_Overview_of_Virtualization_Techniques [Accessed December 2011]

[6] VMware,. 2011.VMware Overview. California: VMware. Available from: http://www.vmware.com/files/pdf/VMware-Company-Overview-DS-EN.pdf [Accessed September 2011].

[7] Rouse, P,. 2010. Virtual Desktop Infrastructure (VDI) Overview. Quest Software. Available from: http://www.virtualizationadmin.com/articles-tutorials/vdi-articles/general/virtual-desktop-infrastructure-overview.html [Accessed December 2011].

 ISBN: 978-1-61208-195-3

[8] CNAP. 2011. About cnap.me. Available from: http://www.cnap.me/content/about [Accessed October 2011]
[9] IBM. N.d,.Cloud computing: Paradigm shift or just hype? Available from: https://www-304.ibm.com/businesscenter/cpe/html0/158782.html[Accessed October 2011]
[10] MSDN,. 2011. Definition of Federated Security. Available from: http://msdn.microsoft.com/en-us/library/ms730908.aspx [Accessed December 2011].
[11] InfoTech Spotlight, 2011. Gizmox Debuts Instant CloudMove, an Automated Tool-Based Solution. Available from: http://it.tmcnet.com/topics/it/articles/136729-gizmox-debuts-instant-cloudmove-an-automated-tool-based.htm [Accessed September 2011].
[12] Lombardi, F,. Di Pietro, R,.2010. Secure Virtualization for Cloud Computing. Elsevier Ltd.
[13] Global Knowledge., 2010. Top 10 Security Concerns for Cloud Computing. Available from: https://www.infosecisland.com/blogview/5300-Top-10-Security-Concerns-for-Cloud-Computing.html [Accessed September 2012].
[14] ISO/IEC 27001. 2005. Information Technology Security Techniques: Information security management systems requirements.
[15] ISSAUK. 2011. Information Systems Security Association – UK Chapter. Available from: http://www.issa-uk.org/ [Accessed October 2011].
[16] Miller. 2008. Confidentiality, Integrity and Availability (CIA). Available from: http://it.med.miami.edu/x904.xml [Accessed December 2011]

 ISBN: 978-1-61208-195-3