Adoption of Secure Cloud Computing Environment to Sri Lankan Organizations

Aiman M M Athambawa
Department of Information technology, Hardy Advanced Technological Institute,
Sri Lanka Institute of Advanced Technological Education (SLIATE), Ampara, Sri Lanka
matheeh@yahoo.com

Abstract - Cloud computing is the new and latest word in the field of computing. The idea of cloud computing is more of a combination of many technologies rather than a single technology. Its element mirrors the earlier computing era's but differs in that it incorporates advances in virtualization, storage, connectivity, and processing power to synthesize modern technical ecosystem for cloud computing. Many organizations moving their data to the cloud due to huge benefits it offers to range from flexibility, scalability, centralized data management, cheap in terms of cost, no downtime or infinitesimal downtime, and most importantly the architecture stresses on the benefits of shared services over isolated products; thus increasing the adoption of cloud computing services. A recent study has shown that security, privacy and legal issues are the main obstacles to the adoption of cloud services. As an outcome of this research user can constantly place a check on the cloud service provider with respect to data security and in cases where there has been a breach of the security agreement, how this breach can be traced using forensic tools by the provider. we implement a virtual environment to showcase proposed solution and configure security and test out deployment using a forensic tool (Forensic Tool Kit)

Keywords - Cloud Computing, Security, Privacy, Legal issues, Adoption of Cloud

I. INTRODUCTION

As we blaze on in this jet age where speed and time are a key concern to everyone especially in the IT industry, technological advancement has come to help us make work and living easy by affording tangible products and also services that helps us undertake the various task in more organised and easy way. These products and services help us keep pace with major logical and technical challenges we face daily; and as a result makes work easier, faster, cheaper, and better. Amongst these services is cloud computing.

The idea of cloud computing is more of a combination of many technologies rather than a single technology. Its element mirrors the earlier computing eras, but differs in that it incorporates advances in virtualization, storage, connectivity, and processing power to synthesize modern technical ecosystem for cloud computing. Many organizations including private sector, public sector, and the governmental organization are moving their data to the cloud via cloud service providers amongst which are: Microsoft, VMware, Google, Amazon etc due to the huge benefits it offers to range from flexibility, scalability, centralized data management, cheap in terms of cost, no downtime or infinitesimal downtime, and most importantly the architecture stresses on the benefits of shared services over isolated products; thus increasing the adoption of cloud computing services. This research focuses on the private cloud infrastructure deployment, and how the service renders security of data because moving data to the cloud, to a large extent exposes users of this cloud service to privacy attack by hackers. However, one of the branches of this research focuses on ways in which these data stored in the cloud is kept secured. Cloud computing, as a matter of fact, has come to make productivity quite easier by offering users of these services the ability to stay connected and at the same time maintain essential security and control required. This gives everyone a better platform and endless ways to work and collaborate from anywhere, anytime, and on a variety of devices.

II. RESEARCH MOTIVATION

Owing to the fact that cloud services could either be a public cloud service or a private cloud service; whichever the case may be, we adopt this service base on the many benefits it promises but not really putting into consideration the fact that as we adopt cloud services, confidential data is outsourced in a sense, this therefore raises the question of data protection, as data protection policies varies in different countries. Many cloud service providing organisations may not even have proper controls in place in terms of security, hence we only hope that our data is kept secured based on trust and also when in transit as we call for them. This piece of work looks at how a cloud service user can constantly place a check on the cloud service provider with respect to data security through auditing, and in cases where there has been a breach of the security agreement, how this breach can be traced using forensic tools by the provider.

Similarly, there has been a slow adoption of cloud service as a result of issues arising base on the security of data in the cloud; hence this piece of work in a sense has come to present the concept of cloud computing not just as migration, but a transformation. It's just like saying the aim of marriage is not just to change your surname but more so for companionship.

It is important to draw to mind the fact that we are still in the early stage of cloud adoption owing to the fact that transferring one's organisation's sensitive data to a third-party cloud-based vendor raises serious security concerns we can't really overlook; amongst which is untraceable data breaches. Unto this end, we shall deploy the cloud infrastructure in a virtualized environment for the sake of this research.

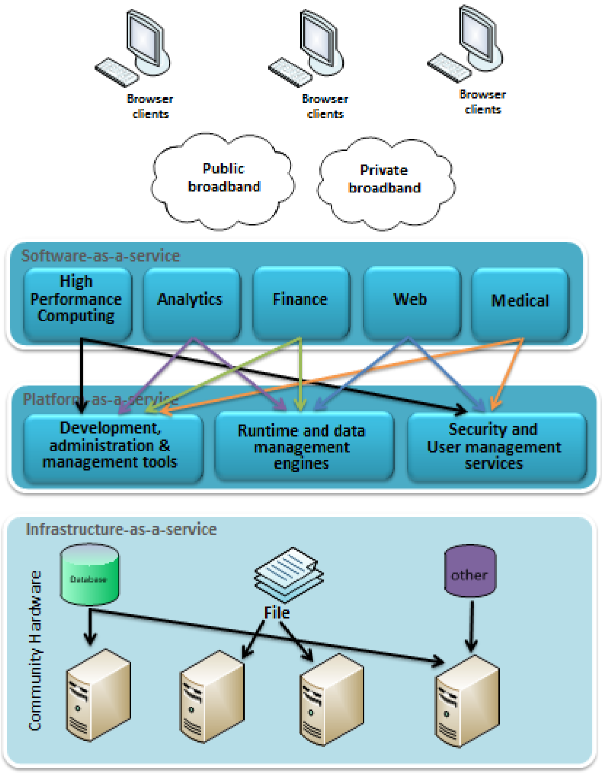


Figure: Architecture for relevant technologies

III. WHAT IS CLOUD COMPUTING.

The concept of cloud computing is based on these five essential characteristics according to National Institute of Standards and Technology (NIST) Information Technology Laboratory

1. Scalable (Aggregate): The property of a system or service whereby an increase in resources leads to a proportional increase in performance.
2. Elasticity: The capability of cloud services to expand and reduce in order to handle fluctuations in demand for resources.
3. On-Demand Self-Service: Characteristic of cloud computing whereby a user can setup and use a cloud service with human interaction with the cloud service provider and can gain access to the computation power and storage they require.
4. Ubiquitous access: The cloud inherited from its web ancestry. Ubiquitous access refers to the concept whereby all of an entity's capabilities are open and accessible from anywhere using any supported device or service (application)
5. Complete Virtualization: Irrespective of the degree of scaling of a particular cloud, the simplicity of working with it does not change i.e. it stays easy to operate and easy to develop applications for as if it was a single server.

IV. BENEFITS: ADOPTION OF CLOUD COMPUTING

1. Reduction/ Maximization of IT cost:
   The adoption of cloud computing can provide an organization with means for reducing IT infrastructure costs and offering ways to maximize the available IT capacity through a variety of schemes. For instance, cloud computing can avail an organisation with 'prepay' capacity such that they only pay for what they need and when they need it. This also eliminates unnecessary capital expenditure with the associated cost of maintaining an extensive IT infrastructure. Cloud computing affords organisation a reduced cost of

operation since operations can easily be centralized when virtualized thereby requiring less IT resources in terms of software, hardware and peopleware.

2. More efficient IT asset utilization:
   Cloud computing provides leverage for storage and infrastructure virtualization which can significantly improve server and storage utilization to the tune of 50-65%. Such asset utilization reduces the associated fixed overhead cost, maintenance cost and the total number of staff required to manage the assets. Furthermore, cloud computing can allow an organization easily decouple its IT infrastructure and assets in such a way that makes outsourcing seamless so that IT staff can focus on more strategic aspects of the organization which leads to a better return on people assets.
3. Business agility:
   To a large extent, the adoption of cloud computing in a business can shed some weight of the business to leave room for flexibility in the business model. When cloud models such as infrastructure as a service (IaaS), platforms as a service (PaaS) or software as a service (SaaS) are adopted by a business, the business is given the freedom to easily react to market changes without its infrastructure holding it back. In addition, the business can easily experiment with infrastructure or service architectures without costing it so much money or time.

V. Risks of Cloud Computing

According to Gartner in the article “Seven Cloud computing risks”, there are specific issues that should be raised with cloud services vendors regarding the security of the service being provided.

1. User access: Access control is a big concern when referring to cloud computing services due to insider attacks. The user of the cloud service has no control over the physical and logical access controls at the end of the service provider as well as the hiring policies. Hence the user is at risk of compromise from the same individuals who provide the service.
2. Regulatory compliance: The responsibility of ensuring security and integrity of their data is still placed on the cloud user even though it is held by the service provider. Hence customers have to ensure these providers are able to meet the regulatory requirements or run the risk of being prosecuted.
3. Data location: When using cloud services, a customer is at risk of their data being stored in a different country. And different countries have different requirements and controls which are to be placed on data access.
4. Data segregation: When using a cloud service, the user runs the risk of having their data stored in a shared environment along with data from other customers. Encryption may or may not be provided and during transit and at rest is data encrypted. Although encryption is effective, availability is compromised.
5. Recovery: Disaster recovery is a key factor when using cloud services. Users may not know where their data is located, but where ever that is, it is physically located somewhere which is subject to threats such as fire, floods, natural disasters etc. Hence not knowing what could happen to your data is a big concern for customers.
6. Investigative support: In event of a security breach, accessing logs and data is usually difficult as multiple customers are usually co-located and the customer’s information may be spread across different servers and data centres, thus, making it difficult to carry out an investigation.
7. Long-term viability: The viability of a cloud service provider is a risk a customer has to face as they could go out of business and the customer would be left stranded.

VI. Forensic Analysis of Cloud Services

Prosecution of computer crime perpetrators is possible with the provision of computer forensic evidence. Computer forensics refers to the use of scientific methods on computing resources in order to validate the occurrence or not of a suspected event. The process of gathering forensic evidence involves analysing storage devices such as hard drives or CDs.

The forensic analysis involves the following steps:

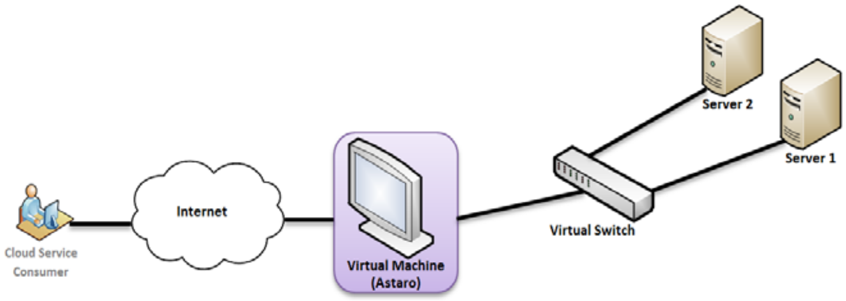
- Verifying that an incident has indeed taken place
- Gathering evidence and ensuring that the chain of custody of the evidence is maintained using tools developed specifically to maintain evidence integrity
- Investigating and analysing the evidence
- Reporting results

Computer forensics has to be carried out in a manner that ensures that it maintains the standards of evidence which can be admissible in a court of law.

VII. PROPOSED SOLUTION

In order to achieve the aims of this research, we propose a solution provides for security of the cloud service user's data by implementing Intrusion prevention and detection using Astaro Security gateway virtual and also using Forensic toolkit to trace data security breach at the cloud service provider's end when such incident(s) present themselves.

This solution is to be implemented on VMware server 2.0 running three (3) virtual machines. Two of the virtual machines are running Windows XP operating systems and have been set up to run in a Client-Server manner. The third virtual machine is the Astaro security gateway virtual appliance which is set up to ensure the security of the cloud deployment. The forensic toolkit was installed on the client –side to analyse digital evidence from the server.



Proposed Solution Architecture

Software Components Used

1. VMware Server 2.0

VMware server is a free virtualization offering that allows for quick deployment of several virtual machines on a physical server.

VMware Server supports the following hardware and software:

- Any standard x86compatible or x8664compatible personal computer
- Windows, Linux, Solaris, and other guest operating systems (both 32-bit and 64-bit)
- Twoway Virtual SMP
- Intel Virtualization Technology (Intel VT)
- AMDVirtualization (AMTV)

2. Astaro Security Gateway

Astaro Security Gateway is a virtual appliance designed to run in VMware environments. It was the first unified threat management product designed as VMware ready. It provides for easy deployment of an all-encompassing security solution. ANS includes a configurable firewall, Intrusion detection and prevention system, web security etc.

3. Forensic Tool Kit

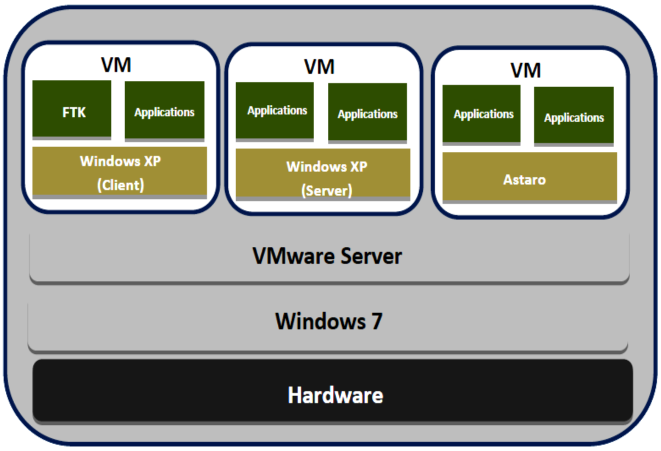
Forensic Toolkit (FTK) is a computer forensics software that delivers excellent computer forensic analysis, decryption and password cracking. It is a court-validated digital investigations platform built for speed, analytics and enterprise-class scalability.

VIII. IMPLEMENTATION OF SOLUTION

A. SOLUTION DESIGN

The idea of this solution is to provide a secure cloud infrastructure which allows for Forensic analysis of the server from the client side. This solution is setup in a client-server fashion which is representative of the cloud infrastructure. We then deploy the different components of the design which are the VMware Server 2.0, the two (2) Windows XP Virtual machines, Astaro Security Gateway 8 and Forensic Tool Kit.

The design of the solution is described in the figure.



DDesign overview

B. SETUP & CONFIGURATION

Deploying VMware SERVER 2.0

1. The first step taken was to log in to the Microsoft Windows 7 host as the Administrator. Then from the Start menu, the directory containing the downloaded installer file was selected. Then permission to run the installer was granted through the User Account Control dialogue box.
2. When the installation wizard opens and finished computing space requirements, the license agreement was accepted and destination folder specified.
3. On the Server configuration page, the FQDN, Server HTTP Port, and Server HTTPS Port were specified and on that same page “Allow virtual machines to start and stop automatically with the system” was selected.
4. On the Configure shortcuts page, the shortcuts we wanted were specified and at the ready to install page, install was clicked to begin the installation.
5. The final wizard prompts were followed to complete the installation and the computer rebooted.

Logging In to VMware Server Using VI Web Access

In order to manage our deployment, we setup the VMware server to allow access via the VI Web Access management interface. To do this we did the following:

1. Launched the Web browser and entered the URL of the VMware Server installation in the format of http://<host_name>:8222 or https://<host_name>:8333
2. The VI Web Access login page appears and then the username and password used to log in to the host were entered to Log In.
3. After the username and password are authorized, the main application page appears.

Deploying the Virtual Machines

To deploy the virtual machines on VMware Server, the virtual machine had to be first created using the virtual machine wizard and the operating system was then installed.

To create a new virtual machine

1. After logging on to the VI Web Access management interface, on the commands section of the host workspace, create virtual machine was clicked.
2. On the Name and Location page, the name of the virtual machine was entered and a datastore from the list of existing datastores was selected.
3. On the Guest Operating System page, the type of operating system that is to be installed on the new virtual machine and the version was selected.
4. Under the Product Compatibility heading, hardware version 7 (the default) was selected as this allows the virtual machine to use new VMware server 2.
5. On the Memory and Processors page, the default memory setting was kept and the number of processors for the virtual machine was selected.
6. On the Hard Disk page, to configure the virtual disk create a New Virtual Disk was selected to add a new blank hard disk to the virtual machine.
7. On the Network Adapter page, a network adapter was added. „
8. On the Ready to complete page, the finish was clicked to create the virtual machine.

DEPLOYING THE TWO WINDOWS XP VIRTUAL MACHINES ON VMWARE SERVER 2

1. After logging into the VI web access interface, the virtual machine that was created was selected.
2. In the Hardware section of the Summary tab, the CD/DVD drive's icon was edited to Connect at power on.
3. The ISO Image was selected from the existing datastore.
4. The SCSI or IDE device node in the Virtual Device Node section was also selected.
5. The changes were saved and the virtual machine powered
6. To complete the guest operating system installation using VMware Remote Console the Console tab was clicked.
7. The instructions specific to Windows XP O.S. was followed to complete the installation.

DEPLOYING ASTARO ON VMWARE SERVER 2.0

1. After unzipping the downloaded package in the VMachines directory, the Infrastructure Client was opened to log in to the management interface of the VMware Server 2.0.
2. Under the datastore section where the virtual ASG is located and the VMX file of the ASG was selected and added to the Inventory from the context menu
3. The VMware Add to Inventory Wizard then opened and a name for the ASG entered.
4. Then the VMware server was specified to run the virtual machine and the Add to Inventory Wizard was completed.
5. The necessary IP address configurations were then carried out
6. The URL of https://192.168.0.1:4444 was entered into the web browser and the SSL certificate was accepted
7. As this was the first time ASG's web frontend (called WebAdmin) was started, a strong password and valid e-mail address for the administrator account was entered.
8. The Perform Basic System Setup button was clicked to continue logging in and the admin Username and password specified was entered.
9. After logging in, the Dashboard of WebAdmin appeared, providing us with all system status information of the Astaro Security Gateway unit.

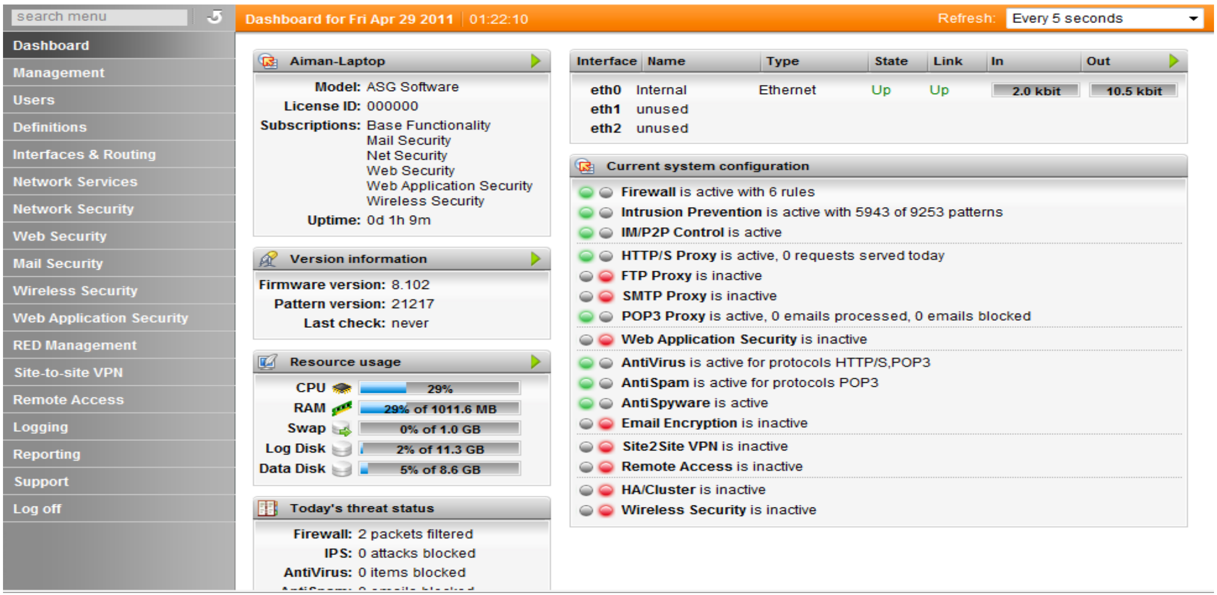
Network configuration information

WinXP-VM1 - 192.168.10.1

WinXP-VM2 - 192.168.10.2

Astaro - 192.168.0.1:4444

Configuring Astaro for security



Dashboard for Fri Apr 29 2011 | 01:22:10

Refresh: Every 5 seconds

Aiman-Laptop

Model: ASG Software
License ID: 000000
Subscriptions: Base Functionality
Mail Security
Net Security
Web Security
Web Application Security
Wireless Security
Uptime: 0d 1h 9m

Version information

Firmware version: 8.102
Pattern version: 21217
Last check: never

Resource usage

CPU 29%
RAM 29% of 1011.6 MB
Swap 0% of 1.0 GB
Log Disk 2% of 11.3 GB
Data Disk 5% of 8.6 GB

Today's threat status

Firewall: 2 packets filtered
IPS: 0 attacks blocked
AntiVirus: 0 items blocked

Interface	Name	Type	State	Link	In	Out
eth0	Internal	Ethernet	Up	Up	2.0 kbit	10.5 kbit
eth1	unused					
eth2	unused					

Current system configuration

Firewall is active with 6 rules
Intrusion Prevention is active with 5943 of 9253 patterns
IM/P2P Control is active
HTTP/S Proxy is active, 0 requests served today
FTP Proxy is inactive
SMTP Proxy is inactive
POP3 Proxy is active, 0 emails processed, 0 emails blocked
Web Application Security is inactive
AntiVirus is active for protocols HTTP/S,POP3
AntiSpam is active for protocols POP3
AntiSpyware is active
Email Encryption is inactive
Site2Site VPN is inactive
Remote Access is inactive
HA/Cluster is inactive
Wireless Security is inactive

Web security

HTTP/S

The tab of the HTTP/S was used to configure Astaro Security Gateway Software as an HTTP/S caching proxy. The HTTP/S of Astaro Security Gateway provides simple caching services, web filtering etc. It also prevents viruses and spyware infections using its virus scanning engines.

FIREWALL

The Packet Filter was used to define and manage packet filter rules of the firewall.

INTRUSION PREVENTION

On the Intrusion Prevention tab, the IPS rules of the firewall were defined. The Intrusion Prevention System (IPS) is a signature-based IPS that analyses the complete traffic and then automatically blocks attacks before they can reach the network to compromise it.

LOGGING

Logging was enabled in Astaro through the logging tab. The machine was enabled to log all interactions on the system including FTP Data connections, Admin notifications, Intrusion prevention system alerts etc.

C. ENABLING AUDITING ON WINDOWS XP:

To allow for forensic analysis local auditing/logging has to be enabled in Windows XP and was done as follows:

1. After Logging on as administrator and opening the control panel, the local security policy was expanded to display the individual policy settings.
2. The type of auditing required was then enabled

Deploying FTK

In order to install and run FTK, the following steps were taken:

INSTALL CODEMETER

The installation wizard was launched to Install CodeMeter Software and the directions were followed and all defaults were accepted to complete the installation

INSTALL FTK

Following the installation of CodeMeter Software, FTK was then installed by clicking on Autorun. 1.

The Access Data License Agreement was read and accepted before selecting the location for the FTK components.

The screen prompts were followed to successfully install the application.

RUN FTK:

FTK was run next, to add the schema to the database.

IX. CONCLUSION

In this research, I am able to conduct an in-depth research into cloud computing and this paper presents the results of this research. We found out that cloud computing is a rapidly developing area in the IT services industry. Despite the excitement around cloud computing, most specialists have a different definition of the term. We were also able to present a report on the emergence of cloud computing by looking into the history and stages of development of cloud computing. This report also presents the different cloud deployment models and service models.

The challenges of ensuring security by cloud adopters are the main focus of this research and we presented a prototype solution which attempts to solve this issue for cloud adopters. This research was concerned with how to provide a secure cloud service by presenting a client-server virtual deployment which is representative of the cloud infrastructure and the cloud adopters. We then went on to deploy a virtual security gateway which provides intrusion detection and prevention, firewall and web security. In addition, to be able to trace breaches we adapted the Forensic toolkit to carry out forensic analysis in the cloud.

In the process of carrying out this research, we faced a lot of challenges, ranging from the software to be used to achieve the aims of the research to acquire the technical know-how in order to successfully carry it out.

Adoption of cloud computing environment to Sri Lankan organisations is easier, secure and anytime accessible with existing solutions in the current market.

X. REFERENCES

[1] Brodkin, J. (2018). Gartner: Seven cloud-computing security risks. [online] InfoWorld. Available at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1 [Accessed 28 Mar. 2018].

[2] Cloudsecurityalliance.org. (2018). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. [online] Available at: https://cloudsecurityalliance.org/csaguide.pdf [Accessed 28 Mar. 2018].

[3] Hurwitz, J. (2010). Cloud computing for dummies. Hoboken, N.J.: Wiley Pub.

[4] Irving Wladawsky-Berger. (2018). Cloud - the Emergence of a New Model of Computing. [online] Available at: http://blog.irvingwb.com/blog/2009/04/cloud-the-emergence-of-a-new-model-of-computing.html [Accessed 28 Mar. 2018].

[5] L. Krutz, R. and Dean Vines, R. (2010). Cloud security: a comprehensive guide to secure cloud computing. 1st ed. Indianapolis, IN: Wiley.

[6] Lozano, B. and Marks, E. (2013). Executive's guide to cloud computing. Hoboken, N.J.: Wiley.

[7] Mather, T., Kumaraswamy, S. and Latif, S. (2010). Cloud security and privacy. Beijing: O'Reilly.

[8] Qamar, S., Lal, N., Singh, M., (2010). Internet Ware Cloud Computing: Challenges. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.

[9] Rittinghouse, J. and Ransome, J. (2016). Cloud Computing. Boca Raton: CRC Press.