Enterprise Cloud Adoption: Leveraging on the Business and Security Benefits

Chinedu, Pascal Uchena+, Nwankwo, Wilson+, Eze, Udoka Felista+

+Department of Information Mgt. Technology, Federal University of Technology, Owerri, Nigeria

Abstract

The impact of globalization coupled with the pressure t of the recent economic downturn have stirred increased customers outlook on availability, scalability and efficiency to enterprise information technology (IT) solutions. The increasing interest in cost-effective Information Technology deployment by leaders and organisations centre on how best cloud computing can contain these requirements to reduce or eliminate the huge capital outlay for infrastructure ownership, increase efficiency, ensure higher return on investment (ROI), dynamic provisioning and utility–like pay-as-use services. However, a number of these enterprises along with some information security professionals have expressed fear of the cloud, stating their unflinching consciousness on security, privacy and forensic issues associated with this new computing platform for the next generation of the Internet. As with any emerging technology, cloud computing offers a rare opportunity to rework security and IT controls for a better tomorrow. In an environment where security and privacy has become paramount to enterprise customers, risk of unauthorized access to information in the cloud poses a significant concern to cloud computing stakeholders. This paper defines clouds, describes cloud computing with the different models and characteristics. The paper focuses on unveiling the fear to cloud adoption due to numerous associated security, privacy and forensic concerns in the cloud while also examining both the business and security benefits of this emerging computing paradigm. Finally, as a move in the new direction, appropriate suggestions on measures on how to ameliorate the security issues have been prescribed.

Key Words: Cloud Computing, Cloud Security, Cloud Forensic, Security Benefits, Business Benefits

1.0 Introduction: What is Cloud Computing?

A cloud has been defined as a pool of virtualized computer resources [3]. A cloud hosts a variety of different workloads, quickly through the rapid provisioning of virtual machines or physical machines

- Supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidabl hardware/software failures Monitors resource use in real time to enable rebalancing of allocations when needed [3].

including batch-style back-end jobs and interactive, user-facing applications Allows workloads to be deployed and scaled-out

Boss et al [3] has argued that a cloud is more than a collection of computer resources owing to the fact that it provides a mechanism to manage those resources. Management here includes provisioning, change requests, re-imaging, workload rebalancing, deprovisioning, and monitoring.

Thus, *Cloud computing* is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices [3] Siddiqui [9] had described Cloud Computing as nothing but a way for renting the Software, Platform and/or Infrastructure hosted by a provider. The word *Cloud* in the name refers to the fact that most of the services could be accessed over the Internet. Thus implying that it is *the Cloud Provider that installs, maintains, scales and monitors hardware and/or software services for its customers which access these services via the Internet [9]*. In support of this, Boss et al, [3] added that cloud computing also describes applications that are extended to be accessible through the Internet. These *cloud applications* use large data centres and powerful servers that host Web applications and Web services. According to them, anyone who has the appropriate Internet access or connection with a standard browser could access a cloud application.

Cloud computing environments support grid computing by quickly providing physical and virtual servers on which the grid applications can run [3] . According to his lecture, mid to late '90s, Grid computing was proposed to link and share computing resources [5]. However, Cloud computing should not be confused with grid computing. Grid computing involves dividing a large task into many smaller tasks that run in parallel on separate servers. Grids require many computers, typically in the thousands, and commonly use servers, desktops, and laptops [3].

Clouds also support non-grid environments, such as a three-tier Web architecture running standard or Web 2.0 applications [3]

2.0 Cloud Computing Models and Characteristics

Our understanding and appreciation of the security issues in cloud computing are better grasped through adequate discussion of the three computing models that come under its canopy. These models (also described as delivery models [8] are:

- Software as a Service – SaaS
- Platform as a Service – PaaS
- Infrastructure as a Service – IaaS [9]

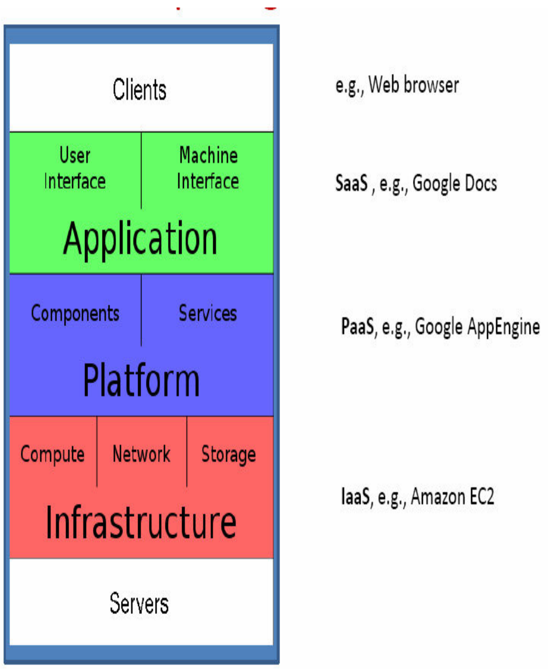

Figure 1: Cloud computing stack showing three delivery models of computing (Source: Hasan, [5])

In highlighting the place of these models, Hasan [5] in a lecture described Cloud computing to mean **selling "X as a service".**

Thus, exerting:

- **IaaS:** Infrastructure as a Service – as "Selling virtualized hardware"
- **PaaS**: Platform as a service – as "Access to a configurable platform/API"

- **SaaS**: Software as a service – as "Software that runs on top of a cloud"

The cloud computing stack (shown below) would be beneficial in revealing the place of these services.

The demonstration of adequate understanding of these three delivery models has significantly shed light on creative ways a few companies had implemented cloud Security at the different levels. Obviously, cloud security has been very broad term with; it is not only composed of the security of data exist in the provider's cloud but also comprises authorization to data access, security of data en route, encryption at the source, and other related aspects.

In order to be considered "cloud" [8] Maintained that these delivery models must be deployed on top of cloud infrastructure that satisfies the following five characteristics:

1. On-demand self-service
2. Ubiquitous network access
3. Location independent resource pooling
4. Rapid elasticity
5. Pay per use [8] 2011).

Thus, the four deployment models are:

1. **Private (internal) cloud**: enterprise owned or leased, behind a firewall
2. **Public (external) cloud**: sold to the public, mega-scale infrastructure (e.g. Amazon EC2)
3. **Hybrid cloud (virtual private cloud)**: composition of two or more clouds (e.g. Amazon VPC)
4. **Community cloud**: shared infrastructure for specific community (e.g. academic clouds) [8]

3.0 Anatomy of Fear- Need For Cloud Security

There have been high levels of comfort and confidence by enterprises (and individuals alike) in storing and maintaining their data on their private computers in their own network environments. The present concern expressed by Siddiqui [9] with the advent of cloud computing where the data storage will be provided (and controlled) by the provider is that the enterprises and individuals would have to part with their data if they want to enjoy the benefits of the cloud; and this is where the concerns
for security originate from.

The concern pinged that we maintain complete control where the data and infrastructure are house within; we could implement any security mechanism we deem fit, we could install any hardware or software to create perimeter around our internal network, we could design "security-by-complexity" by adding multiple layers of security, etc. However, once the data leaves our network into the cloud we lose control over it as well as the security around it. In the cloud we totally depend on the provider to offer these services; meaning that we have lost most of the control [9].

The fears based on the concern of where we are coming from (traditional standalone/ network environment), and where we are going (cloud computing) have been examined and hence outlined by [5] in a lecture, against the following security, privacy and forensic issues:

Confidentiality

- Will the sensitive data stored on a cloud remain confidential? Will cloud compromises leak confidential client data (i.e., fear of loss of control over data)
- Will the cloud provider itself be honest and won't peek into the data? [5]

Integrity

- How do I know that the cloud provider is doing the computations correctly?
- How do I ensure that the cloud provider really stored my data without tampering with it?

Availability

- Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
- What happens if cloud provider goes out of business?

Privacy issues engendered via massive data mining

- Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients

Increased attack surface

- Entity outside the organization now stores and computes data, and so
- Attackers can now target the communication link between cloud provider and client
- Cloud provider employees can be phished

Auditability and forensics

- Difficult to audit data held outside organization in a cloud
- Forensics also made difficult since now clients don't maintain data locally

Legal quagmire and transitive **trust** issues

- Who is responsible for complying with regulations (e.g., SOX, HIPAA, GLBA)?
- If cloud provider subcontracts to third party clouds, will the data still be secure? [5]

These are practical issues are advancing into a perpetual inefficient deployment of technology infrastructure and services, by obviously militate against the adoption of cloud computing. The onus lies with the providers, if they want to win the trust of incredulous potential customers and gain competitive edge in the marketplace, to speedily address the matters of security first.

4.0 The Business Benefits Of Cloud Computing

Cloud computing offers a very attractive enticement by promising high financial savings to enterprises. However, cloud's best opportunity is for enterprises to streamline processes and increase innovation by ensuring increasing productivity and transforming business processes through means that were prohibitively expensive before the cloud. The focus of organizations can be streamlined on their core business, rather than raising concerns on scalability of infrastructure. Through cloud computing, resolving peak business demands for performance can be promptly met—resulting in more reliable backup, increased scalability, more satisfied customers and even higher margins [7]

Some of the key business benefits offered by the cloud include:

- **Cost Containment**

The cloud offers enterprises the option of scalability without the any huge financial obligations required for infrastructure purchase, use and maintenance. ISACA [7] observed that there is usually little to no upfront capital expenditure with cloud services, and that services and storage are availed on demand as they are priced on a pay-as-you-go service bases. Imogokate [6] sustained this assertion while listing his top 10 business benefit of cloud computing by maintaining that there are significant reductions in capital expenditures and IT costs as load and storage shift to the cloud.

Furthermore, the paper appreciated that the cloud model could support with cost savings in terms of wasted resources. Saving on unused server space allows enterprises to contain costs in terms of existing technology requirements and experiment with new technologies and services without a large investment [7]. This suggests that enterprises will match current costs against potential cloud outlays and consider models for TCO to determine whether cloud services will offer the enterprise potential savings.

- **Immediacy**

The ability to provision and utilize a service in a single day has been notably cited as an advantage by many early adopters of cloud computing. This is in contrast with traditional IT projects requiring weeks or months to order, configure and operationalize their necessary resources. This offers significant impact on the agility of a business and the costs reduction associated with time delays [7]

- **Availability**

Cloud providers maintain the necessary infrastructure and bandwidth to cater for business requirements for high speed access, storage and applications. Where redundant paths challenge exist, these providers often take advantage of existing load balancing to ensure that systems are not overloaded and services delayed [7] Concurrently, Imogokate [6] view this under "mobility & accessibility"; arguing that one the greatest advantages of cloud computing is the availability of files and software anywhere with an internet connection. While availability can be promised, ISACA [7] suggested that customers should take care to ensure that they have provisions in place for service interruptions.

- **Scalability**

ISACA [7] observed that with unconstrained capacity, cloud services offer increased flexibility and scalability for evolving IT needs. Provisioning and implementation are done on demand, allowing for traffic spikes and reducing the time to implement new services.

Imogokate [6] concurred by pointing out that service providers may realize this by adding servers or shifting load from one server to another to accommodate additional storage.

- **Efficiency**

Organisations now have the unique opportunity to concentrate efforts on innovation, research and development while reallocating information management operational activities to the cloud. This stimulates business and product growth which may be even more rewarding than the financial advantages offered by the cloud.

Arguing on the "efficient use of resources", Imogokate [6] filed that users are no longer requiring separate or individual servers for different applications if deploying cloud services.

- **Resiliency**

The use of mirrored solutions in case of a disaster scenario and for load-balancing traffic by cloud providers is yet another plus to deployment of their services. In the report, cloud providers insisted that whether there is a natural disaster requiring a site in a different geographic area or just heavy traffic, they will have the resiliency and capacity to ensure sustainability through an unexpected event [7].

- **Software as a subscription**: Imogokate [6] appreciated the fact that software in a cloud resides on a service provider's servers which is external to clients' computers.
- **Reduced Software Maintenance**: Running a list of software in the clouds reduces computer and systems maintenance for the clients.

- **Increased Reliability**: Cloud systems provide back up and redundancy to data which are preserved in provider's data centers [6].
- **Environmentally Friendly**: Cloud IT reduces a business's carbon footprint.
- **Stays Current**: Overhead processing is performed by the provider's servers, muting the need for individual business components.

• **Versionless Software**: Software changes are controlled or eliminated as updates become automatic.

The idea of the cloud is that while providers commit to smarter, faster and cheaper handling of operational activities outsources by enterprises with portions of information management, these enterprises or organisations' workers will focus to improve processes, increase productivity and innovations. Assuming this to be the case, significant changes to the existing business processes will likely be required to take advantage of the opportunities that cloud services offer [7]

5.0 The Security Benefits of Cloud Computing

Haven considered the enormous security concerns of cloud computing, Balding [2] views from a different dimension and focuses on assessing potential security benefits of Cloud Computing. Where the risks are properly managed, some strong technical security arguments in favour of Cloud Computing are in place to substantiate the assessment.

Though the challenges posed by this new paradigm are getting sufficient attention, yet we are not to lose sight of the opportunities. In a blog post Imogokate [6] summarized security advantages of Cloud Computing under the following four (4) outlines:

- Reduces the exposure of sensitive data
- Simplifies security auditing & testing
- Enables automated security management
- Improves redundancy & disaster recovery

Thus, in this paper major focus is on seven technical security benefits some of which are immediate, and others progressively evolving. These presentations highlights some outcomes prevailing today outside of cloud but are either complex; slow to implement (and thus less likely to happen) or prohibitive for capital cost reasons. The benefits discussed do not suggest definitive list but a reflection of the thinking of Balding [2].

Also certain other benefits depend on the Cloud service deployed and so do not apply across the board. A peculiar example includes the absence of any solid forensic benefits with SaaS.

Seven Technical Security Benefits of the Cloud

1. Centralized Data

Reduced Data Leakage: Commonly appreciated among cloud providers is the benefit of reduced data leakage. Balding [2] concurred with this by putting forward the following questions: *How many laptops do we need to lose before we get this? How many backup tapes?* The data "landmines" of today could be greatly reduced by the Cloud as thin client technology becomes prevalent. The idea transporting data buckets in the form of laptops poses more risk than small, temporary caches on handheld devices or Netbook computers. The major challenge is how many laptops in any large company have company 'mandated' controls (e.g. full disk encryption) consistently applied. Despite best efforts around asset management and endpoint security we continue to see embarrassing and disturbing misses. Another concern falls on SMBs, as par how many use encryptions for sensitive data, or even has in place a data classification policy?

Monitoring benefits: Monitoring and Controlling centralized storage is easier to ensure. The flipside is the nightmare scenario of comprehensive data theft. As a security professional, time spent to figure out smart ways to protect and monitor access to data stores in one place are far more justifiable than trying to figure out all the places where the company data resides across a myriad of thick clients. The benefits of Thin Clients are sure available today but Cloud Storage implies faster and potentially cheaper centralize data. What has become the logistic challenge today is getting Terabytes of data into the Cloud in the first place ([2].

2. Incident Response / Forensics

Forensic readiness: Cloud computing services provide quick evidence gathering needed for forensic and investigation purpose. Cloud tweaks (2010) unveiled that *in traditional systems this is attained by turning your server offline, but cloud based servers don't need to be turned down*. The cloud customers have the privilege of now storing logs more cost-effectively, thus enabling comprehensive logging and increasing performance. Also, Balding (2008) suggested that with Infrastructure as a Service (IaaS) providers, a dedicated forensic server can be built in the same Cloud as my company and place it offline, ready for use when needed. According to the report what is needed to be pay for is the storage until an incident occur to with the need to bring it online. With a button at the cloud providers' web interface, the server could be brought ON. Working with multiple incident responders, a copy of the VM can be provided so we can distribute the forensic workload based on the job at hand or as new sources of evidence arise and need analysis. This benefit can be better realized where commercial forensic software vendors could move away from archaic, physical dongle based licensing schemes to a network licensing model.

Decrease evidence acquisition time: In a situation of compromised server in the Cloud (i.e. where server has been broken into), it is now possible to clone that server at the click of a mouse and make the cloned disks instantly available to my Cloud Forensics server. Thus, the need to "finding" storage or have it "ready, waiting and unused" would be completely eliminated – it's just there.

Eliminate or reduce service downtime: Balding [2] noted that in the above scenario there was need to go tell the COO that the system needs to be taken offline for hours whilst dig around in the RAID Array hoping that the physical acquisition toolkit is compatible (and that the version of RAID firmware isn't supported by the forensic software). Abstracting the hardware removes a barrier to even doing forensics in some situations.

Decrease evidence transfer time: According to a testimony, copies in the same cloud are super-fast- made quicker by the replicated, distributed file system Cloud providers have engineered ([2]. Judging from a network traffic stance, it may even be free to make the copy in the same Cloud. Without the Cloud, lots of time consuming and expensive provisioning of physical devices would be required. Payment for only the storage is required as long as I need the evidence.

Eliminate forensic image verification time: Certain Cloud Storage implementations reveal a cryptographic checksum or hash. A typical example includes Amazon S3 which generates an MD5 hash automatically when you store an object. In theory generating time-consuming MD5 checksums using external tools are no longer needful- they are already there.

Decrease time to access protected documents: The Huge CPU power opens some doors. Did the suspect password protect a document that is pertinent to the investigation? A wider range of candidate passwords can now be tested in less time to expedite investigations.

3. Password assurance testing (aka cracking)

Decrease password cracking time: Cloud computing can be used to decrease crack time such that you pay only for what you use if your organisation regularly tests password strength by running password crackers. Ironically, your cracking costs go up as people choose better passwords ;-).

Keep cracking activities to dedicated machines: Rather than use a distributed password cracker where the load is spread across non-production machines, those agents can now be put in dedicated Compute instances - and thus stop mixing sensitive credentials with other workloads.

4. Logging

"Unlimited", pay per drink storage: Consideration for logging usually come as an afterthought. So minimal disk space is allocated and logging is either non-existent or minimal. The reverse is the case with Cloud Storage- no more 'guessing' how much storage you need for standard logs.

Improve log indexing and search: Having your logs in the Cloud leverage Cloud Compute to index those logs in real-time and ensure the benefit of instant search results. What is different here? The Compute instances can be plumbed in and scale as needed based on the logging load - meaning a true real-time view.

Get compliant with extended logging: Extended logging in the form of a C2 audit trail is features characteristics of a number of recent operating systems. Usually, the fear of performance degradation and log size keep it from being enabled often times. Now with cloud computing you can 'opt-in' easily - if you are willing to pay for the enhanced logging, you can do so. Granular logging promotes the acts of compliance and investigations easily.

5. Improve the state of security software (performance)

Drive vendors to create more efficient security software: Billable CPU cycles get noticed. More attention will be paid to inefficient processes; e.g. poorly tuned security agents. Process accounting will make a comeback as customers target 'expensive' processes. Security vendors that understand how to squeeze the most performance from their software will win.

6. Secure builds

Pre-hardened, change control builds: This is primarily a benefit of virtualization based Cloud Computing. Now you get a chance to start 'secure' (by your own definition) - you create your Gold Image VM and clone away. This is achievable today where you can have installed bare-metal OS. However, these usually require additional 3rd party tools, and can be time consuming to clone or include yet another agent to each endpoint.

Reduce exposure through patching offline: Gold images can be kept up securely kept up to date. Offline VMs can be conveniently patched "off" the network.

Easier to test impact of security changes: This is a big one. Spin up a copy of your production environment, implement a security change and test the impact at low cost, with minimal startup time. This is a big deal which eliminates a key barrier to 'doing' security in production environments.

7. Security Testing

Reduce cost of testing security: With SaaS provider only a portion of their security testing costs is passed on. This implies reduction on the expensive security code review and/or penetration test where there is sharing of the same application as a service. Even with Platform as a Service (PaaS) where your developers get to write code, Balding [2] further highlighted potential cost economies of scale (particularly around use of code scanning tools that sweep source code for security weaknesses).

6.0 Suggestions and Conclusion

While cloud security emerges as a critical concern among Information security professionals as well as all those who respond to cloud computing surveys, the basis to understanding security in cloud computing is to realize that the technology is not new, or untested. It signifies the logical evolution to outsourcing of commodity services to many of the same trusted IT providers we have already been using for years.

Cloud computing is the logical move for services to take as more established parts of IT are commoditized. Not moving to cloud computing will imply you are paying more than your competitors for the same commodity [1].

While cloud computing is certainly poised to deliver several benefits, sufficient business impact analyses and risk assessments to inform business leaders of the potential risks to their enterprise should be conducted by information security and assurance professionals. Regular reassessment of risks or reassessment based on event of change should be a part of planned risk management activities which must be managed throughout the information life cycle.

Enterprises that have been considering the utilisation of cloud in their business environment should estimate and match what cost savings the cloud can offer them against what associated and/or additional risks are incurred. Once this analysis is made, enterprises will be better positioned to appreciate how they can leverage cloud services.

Organisations should work with legal, security and assurance professionals to guarantee attainment and sustenance of appropriate levels of security and privacy within this new computing platform. The cloud represents a major paradigm shift in how computing resources will be utilized, and as such requires participation of a broad stream of stakeholders whose governance should initiate its deployment within adopting organizations.

Cloud security has to be a joint-venture between the provider and its customers; it ought to be a two-way street where providers are committed to providing the infrastructure and other services on the server-side and the customers should possess sufficient knowledge to take intelligent and safe cloud decisions on the client-side.

Your organisation is likely to be exposed to higher security risk than your cloud provider, unless you are in the business of implementing security. So ensure you artner with your provider to determine its commitment to security. Match it against your current and actual security levels to ensure the provider is attaining parity or better levels of security.

Understand that proper risk assessment is the key to cloud security. Insist on having the risk assessment provided you by your cloud computing provider with details on how it plans to mitigate any issue identified.

Mandatory discussions with the cloud provider's top security personnel should be on your monthly schedules. This discussion should encourage free flow of ideas from both ways with no hidden items.

The need for improved government regulations around cloud security cannot be over emphasised. Thus, these regulations should be very specific and well-targeted at cloud.

Conclusion

Despite the security privacy and forensic concerns expressed by banks along with other organization, it blows the mind to imagine a world without online banking and other forms of online financial transactions and systems. Correspondingly, the attraction due the economics and convenience of cloud computing (offering enterprises long-term IT savings, including reducing infrastructure costs and offering pay-for-service models) will make this technology innovation a commonplace while cloud computing vendors work vigorously to alleviate customers or market concerns about security … like ecommerce, online banking and other online financial transactions are today.

Obviously, regardless of the convenience and economic benefits, cloud computing may not be for everyone. For critical security and risk reasons, a few organizations with highly classified missions and/or extremely sensitive data may opt out of the idea of cloud computing. However, for most (especially any business looking to enhance IT resources while controlling costs), the business and the security advantages of cloud computing discussed above together with the possibility to deploy private clouds (allowing customers to control who is in the cloud, where data is stored, who has access, etc.) would contain the security assurances required to satisfy these organizations.

With challenges come opportunities, and cloud computing security is surely not an exemption. Just as have been highlighted, these concerns pose huge opportunity that cloud vendors could seize to translate the enormous security ills of cloud computing into solutions to win the trust and the business of potential customers. Therefore, it would not be mind-boggling to assert that through developments in cloud security a cloud provider or vendor could gain a differentiating advantage over others in the global business environment.

Finally, cloud security is part of the foreseeable evolution of IT. Any organisation intending to attain or sustain competitiveness must need to embrace cloud computing and cloud security. Evidently, companies who tackle cloud computing responsibly need not be scared of entering the cloud due to security concerns. The concerns of handling security in the cloud are not as much a nightmare as compared to addressing them in-house.

7.0 Recommendations for Further Research:

It is recommended that the follow-up of this research be conducted with the analysis of how to handle cloud security challenges. The follow-up should identify the challenges and opportunities offerings of cloud computing. Its study should also bring to focus the fears of the cloud with appropriate strategies for demystifying the immediate and future fears within the digitalized and ever changing business environment.

References

[1] Almond, C. (2009). *A Practical Guide to Cloud Computing Security: What you need to know now about your business and cloud security*:Avanade Perspective. Available online at http://www.avanade.com/Documents/Research%20and%20Insights/practicalguidetocloudcomputingsecurity574834.pdf Accessed: 08 June 2011

[2] Balding, C. (2008) Assessing the Security Benefits of Cloud Computing. Available online at http://cloudsecurity.org/tags/forensics.html Accessed: 07 June 2011

[3] Boss et al. (2007). *Cloud Computing*: High Performance On Demand Solutions (HiPODS). Version 1.0, Available online at http://www.ibm.com/developerworks/websphere/zones/hipods/ (Accessed: 20 May 2011).

[4] Cloudtweaks (2010). *The security benefits of cloud computing. Yes, believe it or not there are some!*: Cloud Computing Community- Cloud Computing, Host, IT, Open Source, Security. Available online at http://www.cloudtweaks.com/.../the-security-benefits-of-cloud-computing/ Accessed: 08 June 2011

[5] Hasan, R. (2011). Security and Privacy in Cloud Computing: Johns Hopkins University en.600.412 Spring 2011, Lecture 1, 01/31/2011.

www.cs.jhu.edu/~ragib/sp11/cs412/lectures/600.412.lecture01.pptx (Accessed: 20 May 2011).

[6] Imogokate (2011) Cloud Computing! 4 Security Advantages, 5 Characteristics & 10 Benefits – A Presentation for Business Posted on May 16, 2011. Available online at http://imogoblog.wordpress.com/2011/05/16/cloud-computing-4-security-advantages-5-characteristics-10-benefits-a-presentation-for-business/ Accessed: 07 June 2011

[7] ISACA (2009). Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives: Emerging Technology White Paper. Available online at http://www.isaca.org/...Center/.../Cloud-Computing-28Oct09-Research.pdf Accessed: 08 June 2011

[8] Reilly, D.; Wren, C. & Berry, T. (2011). *Cloud Computing: Pros and Cons for Computer Forensic Investigations:* International Journal Multimedia and Image Processing (IJMIP), Volume 1, Issue 1, March 2011. Available online at http://www.infonomics-society.org/IJMIP/Cloud%20Computing_Pros%20and%20Cons%20for%20Computer%20Forensic%20Investigations.pdf Accessed: 20 May 2011

Siddiqui, M. (2011). *Cloud Computing Security:* Final paper submitted spring 2011. Available online at http://blogs.techconception.com/manny/content/binary/Manny%20Siddiqui%20-%20Cloud%20Computing%20Security.pdf (Accessed: 20 May 2011).