Cloud Security: A Review of Recent Threats and Solution Models

Betrand Ugorji, Nasser Abouzakhar and John Sapsford,
School of computer science, University of Hertfordshire, College lane, Hatfield, UK
b.ugorji2@herts.ac.uk
n.Abouzakhar@herts.ac.uk
j.sapsford@herts.ac.uk

Abstract: The most significant barrier to the wide adoption of cloud services has been attributed to perceived cloud insecurity (Smitha, Anna and Dan, 2012). In an attempt to review this subject, this paper will explore some of the major security threats to the cloud and the security models employed in tackling them. Access control violations, message integrity violations, data leakages, inability to guarantee complete data deletion, code injection, malwares and lack of expertise in cloud technology rank the major threats. The European Union invested €3m in City University London to research into the certification of Cloud security services. This and more recent developments are significant in addressing increasing public concerns regarding the confidentiality, integrity and privacy of data held in cloud environments. Some of the current cloud security models adopted in addressing cloud security threats were – Encryption of all data at storage and during transmission. The Cisco IronPort S-Series web security appliance was among security solutions to solve cloud access control issues. 2-factor Authentication with RSA SecurID and close monitoring appeared to be the most popular solutions to authentication and access control issues in the cloud. Database Active Monitoring, File Active Monitoring, URL Filters and Data Loss Prevention were solutions for detecting and preventing unauthorised data migration into and within clouds. There is yet no guarantee for a complete deletion of data by cloud providers on client requests however; FADE may be a solution (Yang et al., 2012).

Keywords: Cloud Security, Security Threats, Security Solutions.

1. Introduction

Cloud computing is a new technology paradigm that promises huge benefits to its users. It is all about computing resource sharing to increase efficiency while reducing the overhead of administration and other IT costs. Cloud computing avails a convenient and ubiquitous access to highly on-demand elastic computing resource pool in the form of computing infrastructure, platform or software. The NIST has defined cloud computing as a model to enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications and services; that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST, 2012). Amazon Web Service (AWS) launched in 2006 was among the first cloud computing implementations and Eucalyptus was the first open source platform for cloud deployment.

Cloud computing has become very attractive especially to individuals and start-up companies due to its scalability, accessibility, relative inexpensiveness and service oriented Pay-As-You-Use model (Sichao, 2012). This imply that start-up companies get up and running with huge computational resources in a matter of minutes by signing up accounts with cloud computing vendors and may pay only when they utilise those resources. That way, cloud consumers may not have to worry about huge upfront investments in IT Staff, IT infrastructure, software, maintenance etc. depending on their subscription, instead these are taken care of by the Cloud Service Provider (CSP). Many organisations have signed up with CSPs and migrated their data to the cloud and more are considering cloud computing given its promise of numerous benefits (Louis and Andreas 2012). Governments are not left out in this shift to cloud computing. For instance, on the 8th of February 2011, the United States released Federal Cloud Computing Strategy and proposed to commit $20 billion Government spending to cloud computing (Vivek, 2011). In 2009, revenue generated from cloud computing were estimated to be around USD 17 billion and the forecast was that it would amount to USD 44.2 billion by 2013, however, by 2010, the revenues were estimated to be about USD 68.3 billion and to reach USD 148.8 billion by 2014 (Daniele and Giles, 2009) (Christy and Laurence, 2010). This is an indication of how rapidly individuals, organisations and Governments are adopting cloud computing.

There are four types of cloud deployments (Wei et al., 2012).

- **Private cloud**
  The Cloud infrastructure and management is located on a specific organisation's premise or elsewhere and operated for and available to only that organisation.

- **Community cloud**
  A cloud infrastructure shared by specific number of organisations with a common goal (e.g. security enforcement agencies and governments). It may be provided by different CSPs. It may be deployed within either of the participant organisations premise or externally and may be managed internally or externally (Yashpalsinh and Kirit, 2012).

- **Public cloud**
  A public cloud may be owned and provided by a single CSP and is available to anyone who may freely sign-up accounts with the CSP.

- **Hybrid cloud**
  A mix of two cloud deployment types (e.g. a private cloud that accesses public clouds), it may be provided by different CSPs but interoperate for e.g. load balancing (cloud bursting).

Figure 1 shows a model of the cloud deployment types as described above.

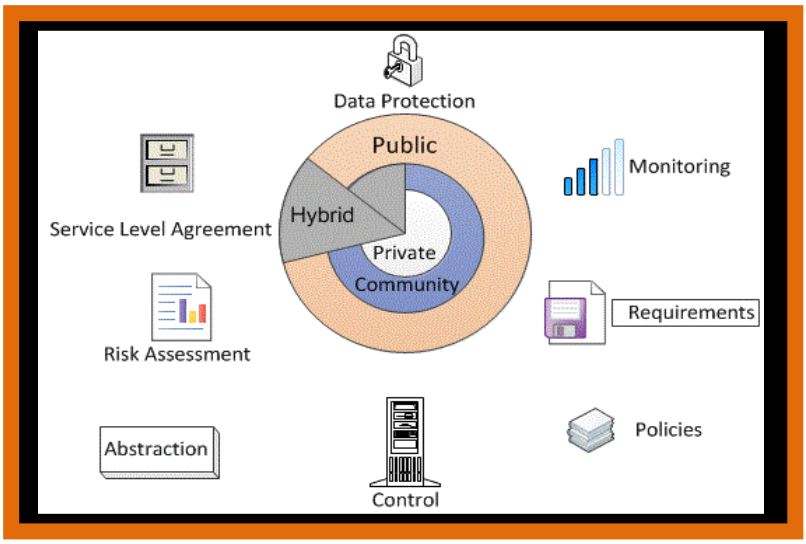

Figure 1: Cloud deployment types.

Cloud deployment types adopt three Service Delivery models (SDM) –

- **Infrastructure as a Service (IaaS)**
  CSP provisions and cloud consumer rents and manages computing storage, networks, operating systems, applications etc. The consumer has no control over the underlying infrastructure.

- **Platform as a Service (PaaS)**
  PaaS provides the capability for a cloud consumer to deploy software and applications on the CSP's cloud platform.

- **Software as a Service (SaaS)**
  A consumer uses applications provided by the CSP such as cloud based emails, spreedsheets, ERPs, UI design applications etc.

Composite as a Service has also been categorised as a cloud SDM in some articles. It is common with CSPs to garnish their products with N + aaS names e.g. Security as a Service (SaaS). Figure 2 shows cloud Service Delivery Models with some cloud service providers and some of their customers.

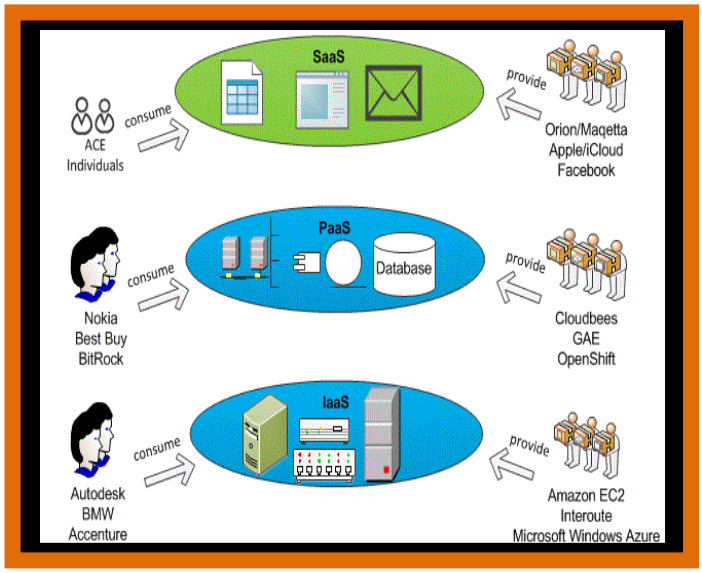

Figure 2: Cloud service delivery models, cloud service providers & their customers

In the early years of cloud computing, there were no cloud computing standards. Therefore, different CSPs used different frameworks and platforms to implement and deploy their cloud offerings mainly based on Service Oriented Architectures, utility computing and Virtualization. However due to the need for cloud interoperability, increased consumer adoption, security and privacy, better service standards; standard organizations such as the Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST), Open Cloud Manifesto (OCM), Federal Information Security Management Act (FISMA) and The Federal Risk and Authorization Management Program (FedRAMP) are now engaged in cloud computing accreditations, certifications or standardizations (Xiang and Bo, 2011) (Kevin, 2011).

In a quest to explore cloud computing paradigm, there is a lot of research going on around cloud computing. However, due to the cost and complexity involved in carrying out some researches within a live cloud computing environment, majority of researches in cloud computing are carried out as simulations using cloud simulation tools such as CloudSim, GreenCloud, Open Cirrus and iCanCloud (Wei et al., 2012). Dr. Lawrence Chung's research team at UT Dallas claim to have found how to build a more efficient cloud and have secured grants from Google to use Google App Engine (GAE) to verify their benchmarking and simulation project in a real cloud environment (LaKisha, 2013).

As common with all new technologies, they come with their advantages and disadvantages. The most significant barrier to the wide adoption of cloud services has been attributed to perceived cloud insecurity (Smitha, Anna and Dan, 2012). According to the IDC, 87.5% of CIO's have security and privacy as top concerns hindering their adoption of cloud computing, also the Government Technology Research Alliance have reported that the major impediment towards adopting cloud computing is security and loss of privacy (Akhil and Kanika, 2012). The security threat posed by cloud computing to individuals and businesses cannot be over-emphasized, as this is evident through some recent cloud computing security events - Amazon cloud failure which caused Distributed Denial of Service to other clouds, web hosting companies, organisations and individuals that depended on it, and the Google and Sony cloud data leakages that affected the confidentiality and privacy of thousands of their customers in 2009, are examples (Murat, Alain and SingRu, 2011) (Xiang and Bo, 2011). Jason Hart, vice-president of cloud solutions at SafeNet reported that 89% of security personnel around the world are not clear on how to keep information in the cloud protected at all times (BCS The Chartered Institute for IT, 2013). With cloud computing in the hands of malicious users, catastrophic malware and virus attacks could be launched against other cloud infrastructures and internet users turning clouds into the biggest botnets. As the clouds pose security threats to cloud customers, these threats are as a result of security threats to the clouds amongst other reasons.

In a view towards addressing increasing public concerns regarding the confidentiality, integrity and privacy of data held in cloud environments, the security industry, CSPs, academia, governments and various stakeholders have continued to work towards a secure cloud environment. For instance, the

European Union invested €3m in City University London to research into the certification of Cloud security services (City University London, 2012). The UK Department for Business, Innovation and Skills together with the Engineering and Physical Sciences Research Council are investing £7.5 Million to train data security experts at University of London and Oxford University (BCS The Chartered Institute for IT, 2013). In an attempt to review this subject, this paper will explore some of the major security threats to the cloud and the security models employed in tackling them.

2. Cloud security threats

In September 2012, the European Network and Information Security Agency (ENISA) top threats publication, lists the following threats against cloud computing as emergent and on the increase –

- Code injection and directory traversal
- Drive by exploits
- Information leakage (especially with increased use of mobile devices)
- Insider threats
- Identity theft (especially with increased use of mobile devices)
- Targeted attacks

There is a basic lack of control over cloud-based environments and uncertainty over how to deal with insider threats, compliance duties and mobile access (BCS The Chartered Institute for IT, 2013).
According to the CSA, the notorious nine cloud computing top threats in 2013 in order of severity are:

- Data Breaches
- Data Loss
- Account Hijacking
- Insecure APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared Technology Issues

Other security threats we identified were:

- Incorrect Hypervisor security implementations in non-private IaaS cloud environments.
- Wrong firewall usages and wrong firewall and access control implementations.
- Predominant use of Vulnerable Distributed Database Systems (DDS).
- Malwares.

The next section will discuss some of the threats listed above under the following headings - Abuse of Cloud Services, Lack of expertise in cloud technology, Inability to guarantee complete data deletion, Message integrity violations, Data leakages, Authentication Issues, Inadequate Monitoring, Insecure interfaces and APIs, Social engineering, drive by exploits and insider threats and Access control violations.

2.1 IaaS threats

- **Abuse of cloud services**
  Currently, there are no physical interactions in purchasing cloud services and most CSP's do not conduct routine inspection on the activities of their IaaS users due to privacy rules, in cases where the latter does not apply, attackers patterns and strategies change over time making attack discoveries and protection even more difficult. Malicious users with forged or stolen bank details could purchase IaaS cloud services and use them to serve malware or perform phishing attacks against other cloud users, as earlier mentioned, turning the cloud into biggest botnet (Eric et al., 2010). This threat is also applicable in PaaS cloud infrastructure.

- **Lack of expertise in cloud technology**
  Research has also shown that there are not enough competent security personnel in securing the volumes of data held in cloud environments. Several cloud security issues have also been attributed to incorrect security configurations in the cloud (BCS The Chartered Institute for IT, 2013) (Nasser, 2013). For instance, (1) defining security configurations on a hypervisor pose

a security threat as VMs completely lose their security when they are relocated (Chris, 2011) and (2) the use of DDS API calls are vulnerable to SQL-Injection attacks (Steve, 2011).

2.2 PaaS threats

- **Inability to guarantee complete data deletion**
  Due to the distributed storage nature of the cloud and collaborations between several cloud service providers (e.g. cloud bursting), guaranteeing the complete deletion of a client's data on the client's request is still an issue. This affects several cloud consumers by causing unwanted vendor lock-ins and privacy issue.

- **Message integrity violations**
  Research has shown that some CSPs do not apply sufficient encryption and some do not encrypt all data stored in the cloud due to the overhead of encryption and the inability to process all encrypted data respectively. This has led to message integrity violations which pose a serious security threat to cloud consumer's privacy (Intel IT Centre, 2011). It is also known that the privacy of cloud consumers files stored in the cloud are threatened by deduplication attacks. Malicious users can easily identify other users file; learn the contents of those files as well as save the files in a remote control centre (Danny, Benny and Alexandra, 2010).

2.3 SaaS threats

- **Inadequate Monitoring**
  As also mentioned earlier, fine grained auditing and traceback is difficult to realise in cloud environments due to shared log files. In networked environments, hardware association could be used to establish traceback however, virtualization makes such association more difficult to establish. Privacy rules also contribute a threat to security as most cloud customers only want their activities to be monitored for charging and accounting purposes only (Sravan and Upendra, 2010).

2.4 Common threats

- **Authentication Issues**
  Existing password-based authentication has an inherited limitation, cause several drawbacks and poses significant risks. Trust propagation for an authenticated user's security context between various interoperating clouds is yet to be fully realised within cloud environments.

- **Data leakages**
  As mentioned previously, the multi-tenancy characteristic of cloud environments pose a significant data leakage threat. There is a good documentation of breaking out of one VM into another within the same host as well as URL traversal making it possible for a malicious tenant to access other tenant's data. Data leakage during cloud bursting is also common due to heterogeneity between different clouds. The different security requirements and trust relations for different tenants is thought as to make a multi-tenant cloud a single point of compromise due to complex security and trust issues (Hassan, James and Gail, 2010).

- **Insecure interfaces and APIs**
  The cause of most application security issues has been attributed to bad application development practices. Cloud environments also use applications which are built for in-house deployments therefore, suffer from any bugs in such applications too (Carl, 2009) (Sravan and Upendra, 2010) (Steve, 2013). DDS systems such as CouchDB, FlockDB, Hive, MongoDB, RavenDB and SimpleDB use API calls (NoSQL) to perform CRUD operations for applications instead of SQL. There are documentations for vulnerabilities in DDS such as limited support for Dynamic Application Testing Tools (DAST), lack of support for native encryption and hashing, SQL-Injection etc. (Steve, 2011).

- **Social engineering, drive by exploits and insider threats**
  The Web is rich with deceptive content that lures users into downloading malware. ENISA and Niels, Moheeb and Panayiotis (2009) express concerns over compromises to cloud servers due to Social engineering attacks, Drive by exploits or Drive-by downloads. Due to the human factor, Social engineering, Drive-by downloads and insider threats still pose a high security threat to cloud computing.

- **Access control violations**
  The ability to emulate hardware via software (Virtualisation) is one of the underlying technologies that drive cloud computing. This provides the ability to run several virtual machines (VM) on the emulation software stack (Hypervisor) which creates the possibility for multi-tenancy and the ability to reallocate resources as needed for elasticity and scalability. However, resource reallocation creates the possibility that sectors containing for instance one tenant's deleted files which have moved into other co-tenants VM can be recovered by those co-tenants. In addition, IP addresses of VM or hosts freed during server relocations which are allowed access into the cloud environment may return to public pools and be used by malicious attackers to access a cloud environment. Heterogeneity in cloud access control interfaces is another serious access control security issue. This makes it difficult for organisations to move their access control policies along when the switch cloud service providers. Existing literature has shown that even though individual domain policies are verified, security violations can easily occur during integration (Hassan, James and Gail, 2010). Access control violations threaten all cloud computing service delivery models. Table 1 shows the various security threats some cloud vendors are concerned about (Intel IT Centre, 2011).

Table 1: Cloud security threats

CSPs	Security Threats
Carpathia	Lack or immature trust extensions in hypervisors and cloud ecosystem.
Cisco	Lack of cloud standards, inadequate security for cloud automation, lack of automation for security service provisioning, inadequate encryption key management and the overhead of encryption.
Citrix	Administrative mistakes and lack of approved workflow.
Expedient	Insufficient end-to-end chains of trust and inadequate encryption key management.
HyTrust	Inadequate virtualization security, authentication and access control.
McAfee	Distributed data storage problems, access control issues, cloud consumer lock-ins and incomplete data deletion.
OpSource	Constantly changing security requirements and lack of cloud security standards.
Trapezoid	Assurance that data is secure irrespective of its constantly changing location.
Virtustream	Incomplete data deletion, software integrity assurance issues, insufficient data encryption in motion and transference of application authentication.

3. Cloud Security Solutions

There are yet no generally accepted security standards for cloud computing however, some cloud security standards by various organisations like CSA, NIST and FISMA are beginning to have widespread adoption by CSPs. Examples of such standards are the Cloud Control Matrix (CCM) and Security, Trust and Assurance Registry (STAR) created by the CSA. Our research findings show that several CSPs are applying different cloud security solutions, however there are similarities in their usage of security mechanism and appliances. Privacy rules are not in favour of proper cloud consumer activity monitoring however Service Level Agreements (SLA) are now used in creating a balance between the responsibilities and expectations of both the CSP and the cloud service consumer. This goes a long way in alleviating the threat posed by the abuse of cloud computing infrastructure and issues of service availability. Defining security policies in the cloud on host-basis is being used as a solution to the threat of hypervisor security level implementation. The advantage of this is that a security configuration remains with a cloud host as it travels (Chris, 2011). Several organisations and governments have invested in training security experts to combat the incompetency problem amongst cloud security experts (The Chartered Institute for IT, 2013). There is yet no

guarantee for a complete deletion of data by cloud providers on client requests however; FADE has shown to be a promising solution to this threat (Yang et al., 2012).

Assigning a random threshold for every file stored in the cloud and performing deduplication only if the number of copies of the file exceeds this threshold, is shown to solve some data integrity violation issues in the cloud (Danny, Benny and Alexandra, 2010). Many CSPs have also deployed Security Information and Event Management (SIEM) Systems within their clouds therefore, are now able to generate and manage log reports. This is largely possible by the use of Big Data for general threat analysis issues (Jennifer, 2012) (Intel IT Centre, 2011) (Chris, 2011). The Cisco IronPort S-Series web security appliance was among security solutions to solve cloud access control issues. 2-factor Authentication with RSA SecurID and close monitoring appeared to be the most popular solutions to authentication and access control in the cloud. Database Active Monitoring, File Active Monitoring, URL Filters and Data Loss Prevention were solutions for detecting and preventing unauthorised data migration into and within clouds (Intel IT Centre, 2011) (Cloud Security Alliance, 2010). Encryption of all data at storage and during transmission, use of hypervisor security at the hardware level as well as use of query re-writers at the database level are being used as solutions to the multi-tenancy and data leakage security threats. Mohemed, John and Amani (2011) demonstrated how to utilise existing security automation efforts to facilitate Cloud Service Security Management Process using a SaaS application to secure multi-tenant cloud environment. Table 2 summarises the security solutions against the cloud security threats identified by CSPs as shown in Table 1.

Table 2: Cloud Security Solutions

CSPs	Security threats	Security solutions
Carpathia	Lack or immature trust extensions in hypervisors and cloud ecosystem.	Use of modern CPUs and chipsets paired with a policy engine controlling orchestration to allow a chain of trust from the hardware to the hypervisor to the operating system by using modern appliances such as the Intel TXT.
Cisco	Lack of cloud standards, automation problems and inadequate encryption key management.	Standardizations as CSA, (ISO) 27001 and 27002 and FISMA, encryption of all data at rest and in transit. Cisco ASA 5585-X Appliance – Firewall, Cisco IronPort S-Series web security appliance and use of SAML to secure SaaS applications.
Citrix	Administrative mistakes and lack of approved workflow.	Enforcement of a workflow enabled administrative solution.
Expedient	Insufficient end-to-end chains of trust and inadequate encryption key management.	Use of Intel Trusted Execution Technology (Intel TXT). Protection of identity through process and governance.
HyTrust	Inadequate virtualization security, authentication and access control.	2-factor authentication with RSA SecurID or smart cards, root password vaulting, accountability and leveraging any pre-existing investment in LDAP or Microsoft Active Directory.
McAfee	Distributed data storage problems, access control issues, cloud consumer lock-ins and incomplete data deletion.	Cloud Identity Manager which auto-provisions and de-provisions cloud accounts, use of Single-Sign-On, policy-based enforcement and 2-Factor-Authentication.
OpSource	Constantly changing security requirements and lack of cloud security standards.	A combination of SAS 70, PCI, SSAE 16, ISO 27001 27002, FISMA and CSA security standards.
Trapezoid	Assurance that data is secure irrespective of its constantly changing location.	Adoption of SecRAMP Security implementations, use of Intel TXT and Cisco Unified Computing System platform.
Virtustream	Incomplete data deletion, software integrity assurance issues, insufficient data encryption in motion and transference of application authentication.	Encryption of all data at rest using the Intel AES-NI (in the CPU) and encryption of data during transmission.

As a solution to security threats due to Insecure interfaces and APIs, cloud API developers validate and sanitize all inputs both on the client and server side of their source code, encrypt or hash data before inserting them into a DDS and adopt secure software development lifecycle (Nasser, 2013) (Steve, 2013). There is yet no fool-proof approach towards tackling the issues of insider threats but sound physical access control procedures, least privilege access, sanctions and proper security and criminal record checks on cloud security personnel is widely practiced. The use of distributed

application firewalls and application-level proxies implemented inside a perimeter firewall, which are based on decentralized information flow control (DIFC) models that supports a decentralized creation and management of security classes at runtime are being used as solution to access control and trust propagation issues (Jennifer, 2012). Intel TXT has been widely adopted by several CSPs as a solution for trust propagation from the hardware to the hypervisor and to the operating system. Multi-threaded IDS deployed across IaaS, PaaS and SaaS cloud infrastructures have proved effective in mitigating malware attacks in cloud environments. Not until recently did Amazon announce that its Hardware Security Module (CloudHSM) is a solution to the problem of proper digital certificate, encryption and cryptographic key management, but this service is relatively expensive and may be unaffordable by individuals and small firms. With AWS CloudHSM, customers maintain full ownership, control and access to keys and sensitive data while Amazon manages the HSM appliances in close proximity to their applications and data for maximum performance (Fahmida, 2013).

4. Conclusion

In this paper we reviewed the recent cloud security threats and solution models. This is a starting point towards identifying and exploring further the security threats facing the cloud. An understanding of recent security threats in the cloud and their current solutions are important in finding lasting solutions to cloud security issues. Solutions to cloud security threats are by far not a single organisation's or industry's responsibility. Security experts in the industry, the academia, various organisations and government need to collaborate towards finding a lasting solution to cloud security problems. Therefore more research is needed in this area for better appreciation of the issues facing cloud security. This review serves as to provide more awareness to the recent security threats in cloud computing and the current solution models employed in tackling them, and most importantly as a scratching surface towards our on-going research into intrusion detection systems (IDS) in cloud based environment. We recommend the adaptation and reuse of standard SOA security frameworks such as SAML and WS-Trust in authenticating and federating trust in securing cloud environments. Perhaps the only way to guarantee the security of data at all times is to invest in the latest solutions on the market that can be used to ensure it is not breached by hackers or other unauthorised individuals (BCS The Chartered Institute for IT, 2013).

References

Smitha, S., Anna, C.S. and Dan, L. (2012) Ensuring Distributed Accountability for Data Sharing in the Cloud. *IEEE Transactions on Dependable & Secure Computing,* Vol. 9, No. 4, July/August 2012, pp 555-567.

Yang, T., Patrick, P.C.L., John, C.S.L. & Radia, P. (2012). Secure Overlay Cloud Storage with Access Control and Assured Deletion. *IEEE Transactions on Dependable and Secure Computing,* Vol. 9, No. 6, November/December, pp 903-916.

Peter, Mell and Timothy, Grance. (2011) The NIST Definition of Cloud Computing. National Institute of Standard and Technology US Department of Commerce, Special Publication 800-145. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [accessed on 31st March 2013]

Sichao, Wang (2012) Are enterprises really ready to move into the cloud? An analysis of the pros and cons of moving corporate data into the cloud, https://cloudsecurityalliance.org/wp-content/uploads/2012/02/Areenterprisesreallyreadytomoveintothecloud.pdf [accessed on 11th May 2013]

Vivek, Kundra. (2011) Federal Cloud Computing Strategy. The White House Washington, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf [accessed Feb. 23rd 2013]

Daniele, Catteddu and Giles, Hogben. (2009) Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA (European Network and Information Security Agency).

Christy, Pettey and Laurence, Goasduff (2010) Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010, Press Release, 22 June, Gartner Stamford, Connecticut.

http://www.gartner.com/newsroom/id/1389313

Wei, Z., Yong, P., Feng, X. and Zhonghua, D. (2012) Modeling and Simulation of cloud computing: A Review, *2012 IEEE Asia Pacific Cloud Computing Congress (APCloudCC),* November, pp 20-24.

Yashpalsinh, Jadeja and Kirit, Modi (2012) Cloud Computing - Concepts, Architecture and Challenges, *2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]*, pp 877-880.

Xiang, Tan and Bo, Ai (2011) The Issues of cloud computing security in high-speed railway. *2011 International Conference on Electronic & Mechanical Engineering and Information Technology,* August, pp 4358-4363.

Kevin, McCaney. (2011) Amazon cloud service gets approval under fisma. GCN, 16 September, http://gcn.com/articles/2011/09/16/amazon-ec2-cloud-fisma.aspx.

LaKisha, Ladson. (2013) The University of Texas at Dallas News Centre. Cloud Computing Project Wins First-of-its-Kind Google Award. 4 March, http://www.utdallas.edu/news/2013/3/4-22431_Cloud-Computing-Project-Wins-First-of-its-Kind-Goo_article-wide.html

Akhil, Behl and Kanika, Behl. (2012) An Analysis of Cloud Computing Security Issues, *2012 World Congress on Information and Communication Technologies*, October-November, pp 109-114.

Murat, K., Alain, B., SingRu, C. H. (2011) Impact of Security Risks on Cloud Computing Adoption, *Forty-Ninth Annual Allerton Conference Allerton House, UIUC, Illinois, USA,* September, pp 670-674.

BCS The Chartered Institute for IT. (2013) Cloud computing 'poses daunting challenge to security chiefs', BCS Latest Industry News, 8 May, http://www.bcs.org/content/conWebDoc/50504?utm_medium=email&utm_source=BCS+The+Chartered+Institute+for+IT&utm_campaign=2493324_securityspecialmay13&dm_i=9U7,1HFV0,9QGEZI,51JJQ,1

City University London. (2012) City University London wins European Union grant for Cloud security research, City University News 27 September, http://www.city.ac.uk/news/2012/sep/city-university-london-wins-european-union-grant-for-cloud-security-research

BCS The Chartered Institute for IT. (2013) Data security experts 'to be trained at university', BCS Latest Industry News, 9 May, http://www.bcs.org/content/conWebDoc/50515?utm_medium=email&utm_source=BCS+The+Chartered+Institute+for+IT&utm_campaign=2493324_securityspecialmay13&dm_i=9U7,1HFV0,9QGEZI,51JJQ,1

Cloud Security Alliance. (2013) “The notorious nine cloud computing top threats in 2013” https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_nine_Cloud_Computing_Top_Threats_in_2013.pdf. [Accessed on 7th April 2013]

Eric, G., John, H., James, R., Jim, R. and Steve, S. (2010) Cloud Computing Roundtable, *IEEE Security and Privacy*, Vol. 8, No. 6, 3 December, pp 17-23.

Nasser, S. Abouzakhar. (2011) Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations.

Chris, Brenton. (2011) Hypervisor vs. Host-based security, A comparison of the strengths and weaknesses of deploying cloud security with either a hypervisor or agent based model,
Cloud Security Alliance, https://cloudsecurityalliance.org/wp-content/uploads/2011/11/hypervisor-vs-hostbased-security.pdf

Steve, Markey. (2011), Auditing Distributed Databases, How to assess risk posture and secure distributed databases. Cloud Security Alliance, https://cloudsecurityalliance.org/wp-content/uploads/2011/11/CSA_Distributed_Dbs_v2.pdf

Niels, P., Moheeb, A. R. and Panayiotis, M. (2009) Cybercrime 2.0: When the Cloud Turns Dark. *ACM QUEUE*, February/March, Vol. 9, No. 2, pp 48-53. http://delivery.acm.org/10.1145/1520000/1517412/p46-provos.pdf

Intel IT Centre. (2011) Cloud Security: Vendors Answer IT's Questions about Cloud Security, Intel IT Centre Vendor Round Table, October, pp 2-44.

Danny, H., Benny, P. and Alexandra, S. (2010) Side Channels in Cloud Services: Deduplication in Cloud Storage, *Security and Privacy, IEEE,* Vol. 8, No. 6, November/December, pp 40-47.

Hassan, T., James, B.D. Joshi and Gail, A. (2010) Security and Privacy Challenges in Cloud Computing Environments, *Security and Privacy, IEEE,* Vol. 8, No. 6, November/December, pp 24-31.

Sravan, K. D. and Upendra, K. M. (2010) Designing Dependable Service Oriented Web Service Security Architectures Solutions, *International Journal of Engineering and Technology*, Vol. 2, No. 2, pp 81-86.

Carl, Armond (2009) Avanade Perspective: A Practical Guide to Cloud Computing Security. What you need to know now about your business and cloud security, Accenture and Microsoft. http://www.avanade.com/Documents/Research%20and%20Insights/practicalguidetocloudcomputingsecurity574834.pdf

Steve, Markey. (2013) Extend your secure development process to the cloud and big data, IBM developerWorks, http://www.ibm.com/developerworks/cloud/library/cl-extenddevtocloudbigdata/ [accessed 14th April 2013].

Jennifer, Marsh. (2012) Effective Measures to Deal with Cloud Security. CIO Update, 14 September, http://www.cioupdate.com/technology-trends/effective-measures-to-deal-with-cloud-security.html [accessed 14th April 2013].

Mohemed, A., John, G. and Amani, S.I. (2011) Collaboration-Based Cloud Computing Security Management Framework, *2011 IEEE 4th International Conference on Cloud Computing*, Washington DC, pp 364-371.

Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing V3.0, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf [accessed 4th May 2013].

Fahmida, Y. R. (2013) Amazon Offers Appliance-based Encryption Key Management Solution, 28 March, http://www.securityweek.com/amazon-offers-appliance-based-encryption-key-management-solution [accessed 4th May 2013].

Louis, Marinos and Andreas, Sfakianakis. (2012) ENISA Threat Landscape: Responding to evolving threat Environment.

BCS The Chartered Institute for IT. (2013) Employees may pose data breach threat, BCS Latest Industry News, 14 May, http://www.bcs.org/content/conWebDoc/50546 [accessed 15th May 2013].