VOL. 2, NO. 10, October 2011 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Security Issues in Cloud Computing: *The Potentials of Homomorphic Encryption*

Aderemi A. Atayero*, Oluwaseyi Feyisetan**

*Covenant University, Nigeria, Email: atayero@ieee.org
** Kings College, United Kingdom, Email: oluwaseyi.feyisetan@kcl.ac.uk

ABSTRACT

The prominence of the place of cloud computing in future converged networks is incontestable. This is due to the obvious advantages of the cloud as a medium of storage with ubiquity of access platforms and minimal hardware requirements on the user end. Secure delivery of data to and from the cloud is however a serious issue that needs to be addressed. We present in this paper the security issues affecting cloud computing and propose the use of homomorphic encryption as a panacea for dealing with these serious security concerns vis-à-vis the access to cloud data.

Keywords : *Cloud computing, Cryptography, Data security, Homomorphic encryption, RSA*

1. INTRODUCTION

Cloud computing as a concept is the result of the natural evolution of our everyday approach to using technology delivered via the Internet. Cloud computing came into the foreground as a result of advances in virtualization (e.g. VMWare) [1], distributed computing with server clusters (e.g. Google) [2] and increase in the availability of broadband Internet access. Industry leaders describe cloud computing simply as the delivery of applications or IT services, which are provided by a third party over the Internet (Rackspace, Microsoft, IBM) [3, 4, 5]. Ironically, the recent global economic recession served as a booster for interest in cloud computing technologies as organizations sought for ways to reduce their IT budget, while keeping up with performance and profits [6]. The cloud computing buzz began in 2006 with the launch of Amazon EC2, gaining traction in 2007 as seen in the Figure 1.

The National Institute of Standards and Technology defines cloud computing as follows: "*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.*" [7]

Cloud computing is currently characterized by having an on demand access to elastic resources via a tenancy model. It typifies the holy grail of no-worries in computing, allowing a company to focus on its core business, paying for all its IT resources as a service.

The rest of the paper is divided into the following sections. Section II describes the three major cloud computing service models. In section III we present the four cloud computing deployment models vis-à-vis infrastructure ownership. The main thrust of this paper – cloud computing security issues is introduced in section IV, while homomorphic encryption is discussed in sections V, VI and VII. The paper concludes in section VIII by proposing a novel approach of adding an encryption layer on top of the encrypted files to be stored on the cloud.

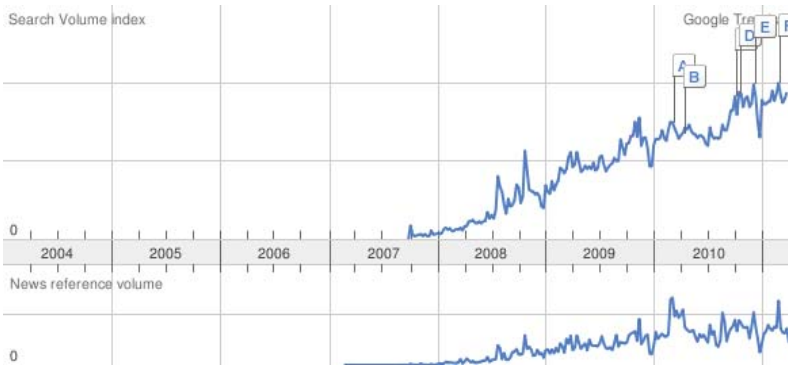

Figure 1: Search and News Volume for Cloud Computing as at April 2011 [Source: Google Trends]

2. CLOUD COMPUTING SERVICE MODELS

In cloud computing, everything is delivered *as a Service* (*XaaS*), from testing and security, to collaboration and metamodeling [8]. The cloud was rapidly becoming a conflagration of buzzwords "as a service". Today there are three main service models, which are agreed on and defined in the NIST document [9].

1. *Software as a Service* {*SaaS*} - this simply means delivering software over the Internet. It is the most widely known model of cloud computing. *SaaS* has been around since early 2001 when it was commonly referred to as the Application Service Provider (ASP) Model [8]. Software as a Service consists of software running on the provider's cloud infrastructure, delivered to (multiple) clients (on-demand) via a thin client (e.g. browser) over the Internet. Typical examples are Google Docs and Salesforce.com CRM.

2. *Platform as a Service* {*PaaS*} - this gives a client (developer) the flexibility to build (develop, test and deploy) applications on the provider's platform (API, storage and infrastructure). *PaaS* stakeholders include the *PaaS* hoster who provides the infrastructure (servers etc), the *PaaS* provider who provides the development tools and platform and the *PaaS* user [10]. Examples of *PaaS* are Microsoft Azure and Google AppEngine.

3. *Infrastructure as a Service* {*IaaS*} - rather than buy servers and build a datacenter from ground up, and consequently having to worry about what happens when the

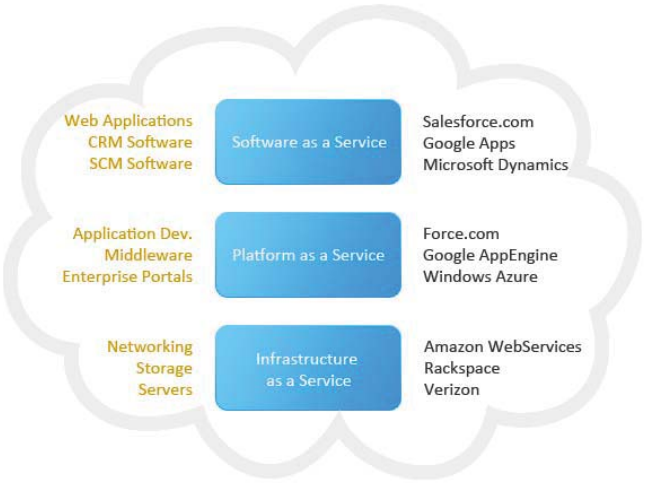

Figure 2: Cloud Computing Service Models

website hits a million users, *IaaS* offers users elastic on-demand access to resources (networking, servers and storage), which could be accessed via a service API. The underlying infrastructure is transparent to the end user, while s/he retains control over the platform and software running on the infrastructure. *IaaS* runs on a tenancy model, which employs a usage-based payment approach allowing users to pay for only those resources they actually use.

3. CLOUD COMPUTING EPLOYMENT MODELS

Depending on infrastructure ownership, there are four deployment models of cloud computing each with its merits and demerits. This is where the security issues start.

1. *The Public Cloud* - this is the traditional view of cloud computing in every day lingua. It is usually owned by a large organization (e.g. Amazon's EC2, Google's AppEngine and Microsoft's Azure). The owner-organisation makes its infrastructure available to the general public via a multi-tenant model on a self-service basis delivered over the Internet. This is the most cost-effective model leading to substantial savings for the user, albeit with attendant privacy and security issues since the physical location of the provider's infrastructure usually traverses numerous national boundaries.

2. *The Private Cloud* - refers to cloud infrastructure in a single tenant environment. It defers from the traditional datacenter in its predominant use of virtualization. It may be managed by the tenant organization or by a third party within or outside the tenant premises. A private cloud costs more than the public cloud, but it leads to more cost savings when compared with a datacenter as evidenced by Concur Technologies (est. savings of $7million in 3 years from 2009) [11]. The private cloud gives an organization greater control over its data and resources. As a result, the private cloud is more appealing to enterprises especially in mission and safety critical organizations.

3. *The Community Cloud* - according to NIST, the community cloud refers to a cloud infrastructure shared by several organizations within a specific community. It may be managed by any one of the organizations or a third party. A typical example is the Open Cirrus Cloud Computing Testbed, which is a collection of Federated data centers across six sites spanning from North America to Asia [12].

TABLE 1: CLOUD DEPLOYMENT MODELS AND ISSUES

Model	Cost Issues	Security Issues	Control Issues	Legal Issues
Public	Setup: highest Usage: lowest	Least secure	Least control	Jurisdiction of storage
Private	Setup: high	Most secure	Most control	
Community	Relatively low	Less secure	Less control	
Hybrid				Jurisdiction of storage

4. *The Hybrid Cloud* - comprises of a combination of any two (or all) of the three models discussed above. Standardization of APIs has lead to easier distribution of applications across different cloud models. This enables newer models such as "Surge Computing" in which workload spikes from the private cloud is offset to the public cloud. A comparison of the different issues of cloud computing vis-à-vis deployment models is given in Table 1.

4. SECURITY ISSUES IN CLOUD COMPUTING

Security has always been the main issue for IT Executives when it comes to cloud adoption. In two surveys carried out by IDC in 2008 [14] and 2009 [15] respectively, security came top on the list (see Figure 3). However, cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualization, each fraught with inherent security issues. For example, browser based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing. There are potentials for a new wave of large-scale attacks via the virtualization platform. Chow et al. [16] described the "Fear of the Cloud" by categorizing security concerns into three traditional concerns, availability and third party data control. Research firm Gartner [17] posited seven security risks ranging from data location and segregation to recovery and long-term viability. The European Network and Information Security Agency [18] also published a list of 35 issues in cloud computing in 4 categories. Organizations such as ISACA and Cloud Security Alliance publish guidelines and best practices to mitigate the security issues in the cloud [19, 20].

Before delving into all the security ills of cloud computing, worthy of note are some of the cloud security

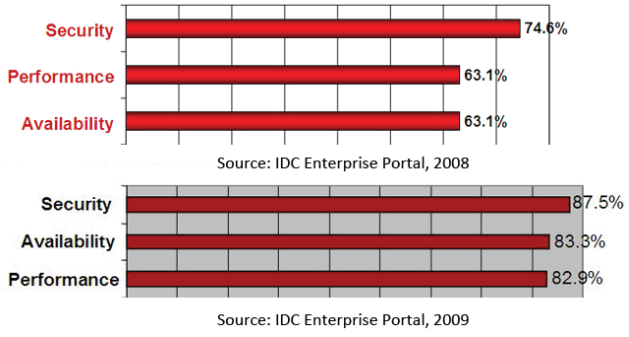

Figure 3: Top 3 issues with the cloud/on-demand model

advantages, which were pointed out by Peter Mell and Tim Grance of NIST in [21]. The cloud offers data redundancy - through automated replication and simpler auditing - due to cloud homogeneity. Cloud companies are also able to afford a dedicated security team and invest more in security infrastructure. Other benefits noted in [18] include rapid smart scaling of resources, standardized security interfaces and an overall benefit of scale (security measures are cheaper on a large scale). Some of the pressing security issues in cloud computing include:

1. *Availability* - This borders on data being available whenever it is required. This is one of the prime concerns of mission and safety critical organizations. Availability concerns also extend to the need to migrate to another provider, uptime periods of current provider or long-term viability of the cloud provider as noted in [16, 17]. Some well-known outages of leading cloud providers are shown in Table 2.

TABLE 2: CLOUD SERVICE OUTAGES

Cloud Service	Outage Duration	Dates
Google Gmail	30 hours	Oct. 16-17, 2008 [22]
Google Gmail, Apps	24 hours	Aug. 11, 2008 [23]
Windows Azure	22 hours	Mar. 13-14, 2009 [24]
FlexiScale	18 hours	Oct. 31, 2008 [25]
Amazon S3	7 hours	Jul. 20, 2008 [26]
Salesforce.com	40 minutes	Jan. 6, 2009 [27]

2. *Data Security* - This risk stems primarily from loss of physical, personnel and logical control of data. Issues include virtualization vulnerabilities [28], *SaaS* vulnerabilities (e.g. a case in which Google Docs exposed private user files) [29], phishing scams [30] and other potential data breaches. Other data security risks mentioned in [18] include data leakage and interception, economic and distributed denial of service and loss of encryption keys. Unique risks also arise due to the multi-tenancy and resource-sharing models as pointed out in [17, 18, 20, 31]. The inability to fully segregate data or isolate separate users can lead to undesired exposure of confidential data in the investigation of a situation involving co-tenants. Hypervisor vulnerabilities can also be leveraged to launch attacks across tenant accounts. Data containing social and national insurance details, health data and financial information raise issues about authorization, rights management, authentication and access controls.

Furthermore, Abadi [32] pointed out that it is hard to maintain ACID (atomicity, consistency, isolation, durability) properties of during data replication over large geographic zones. Data remembrance or persistence remains an issue due to replication and distribution of data even after a user has left a cloud provider. A data security lifecycle

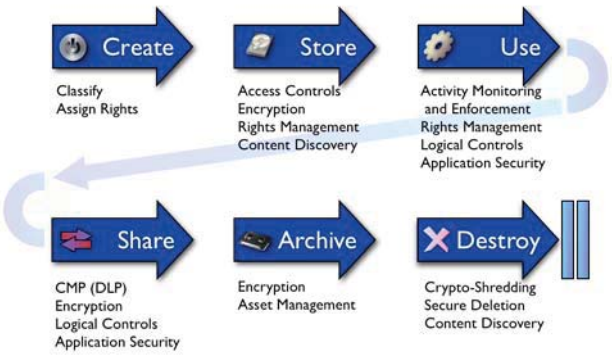

Figure 4: Data Security Lifecycle [20]

model is shown in Figure 4.

3. Third-Party Control: this is probably the prime cause of concern in the cloud. With the growing value of corporate information, third party access can lead to a potential loss of intellectual property and trade secrets. There is also the issue of a malicious insider who abuses access rights to tenant information. The fear of corporate espionage and data warfare also stems from third party control. Provider compliance with regulations such as those on auditing also raise questions on how that can be effected on site in a globally distributed multi tenant environment [16]. A situation can also arise in which the user becomes locked-in to a particular vendor. This can be due to a difficulty in migrating data to a new vendor. Other risks might arise from the terms of service being obsolete following the merger or acquisition of the cloud provider. A final note on prompt disaster recovery also arises due to third party data control.

4. Privacy and Legal Issues - data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Pearson [33] summarized the main privacy issues of cloud computing. Users are made to give away their personal information without knowing where it is stored or what future purpose it might serve. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks. Some legal compliance issues in cloud computing include the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 which prevents disclosure of individually identifiable health information. Similarly, the Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, 123 Stat. 258-263 laid regulations requiring notifications of breaches in health data. The Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338, also has similar requirements with regards to financial data. Similarly, the EU Data Protection Directive (Directive 95/46/EC) seeks to secure the privacy and protection of personal data.

5. HOMOMORPHIC ENCRYPTION AND ITS POTENTIALS IN THE CLOUD

If all data (personal, health, financial etc) stored in the cloud were encrypted, that would effectively solve issues 2, 3 and 4. However, a user would be unable to leverage the power of the cloud to carry out computation on data without first decrypting it, or shipping it entirely back to the user for computation. The cloud provider thus has to decrypt the data first (nullifying the issue of privacy and confidentiality), perform the computation then send the result to the user. What if the user could carry out any arbitrary computation on the hosted data without the cloud provider learning about the user's data - computation is done on encrypted data without prior decryption. This is the promise of homomorphic encryption schemes which allow the transformation of ciphertexts *C(m)* of message m, to ciphertexts *C(f(m))* of a computation/function of message m, without disclosing the message.

The idea was first suggested by Rivest, Adleman and Dertouzos in 1978, referred to as privacy homomorphisms [34]. RSA (invented by Rivest, Shamir and Adleman '78) [35] had multiplicative homomorphism (you could compute a ciphertext which is the product of plaintexts) and over the next 30 years, researchers such as Yao '82 [36], Goldwasser and Micali '82 [37], ElGamal '85 [37 - 38] and Paillier [39] came up with partially homomorphic cryptosystems. A survey of homomorphic encryption schemes can be found in [40,41].

An encryption scheme can be said to be fully homomorphic if:

$$E(m_1 \ \Theta \ m_2) \leftarrow E(m_1) \ \Theta \ E(m_2) \ ; \ \forall \ m_1 \ , \ m_2 \ \in \ M \qquad (1)$$

Where M is the set of plaintexts, Θ - represents any arbitrary function and $\leftarrow$ means computation is done without the plaintexts being decrypted.

The first fully homomorphic encryption system was proposed by Craig Gentry in 2009 [42] using ideal lattices. Gentry's approach employed devising a somewhat homomorphic scheme, and then bootstrapping it to get a fully homomorphic scheme. Since then researchers have

proposed variants and improvements to Gentry's model. Smart and Vercauteren [43] presented a specialization of Gentry's scheme which yielded a smaller ciphertext size. Dijk, Gentry, Halevi, and Vaikuntanathan [44] introduced the first variant of Gentry's using arithmetic operations over integers. Stehle and Steinfield [45] also proposed a faster improvement of Gentry's model.

6. GENTRY'S FULLY HOMOMORPHIC ENCRYPTION USING IDEAL LATTICES

An encryption scheme has the following three step algorithm:

1. *KeyGen - creates two keys i.e. the secret key sk and the public key pk.*
2. *Encrypt - encrypts the plaintext m with the public key pk to yield ciphertext c.*
3. *Decrypt - decrypts the ciphertext c with the secret key sk to retrieve the plaintext m.*

Gentry introduced a fourth step called *Eval* to the algorithm:

4. *Eval - outputs a ciphertext c of f(m) such that Decrypt (sk,m) = f(m).*

The scheme becomes homomorphic if *f* can be any arbitrary function, and the resulting ciphertext of *Eval* is compact (i.e. it does not grow too large regardless of the complexity of function *f*). The *Eval* algorithm in essence means that the scheme can evaluate its own decryption algorithm (i.e. the scheme is *bootstrappable*).

It can be shown that any arbitrary function is made up of an aggregate of addition, subtraction and multiplication functions (i.e. AND, OR and NOT gates). Gentry employed ideal lattices which provide additive and multiplicative homomorphism and low circuit complexities (for the decryption algorithm) in creating his fully homomorphic scheme. More on lattice based cryptography can be found in [42 - 40]. Further, in order to prevent the ciphertext (as well as the inherent noise/error) from becoming too large, Gentry introduced a *Recrypt* function which refreshes a ciphertext *c'* to produce a new ciphertext *c* using a different key. *Recrypt* is a two-step procedure:

1. *Encrypt (pk2, c1)* to yield *c1'*, then
2. output a new ciphertext *c* by *Eval (pk2, Decrypt, sk2', c1')*.

This is the process behind bootstrapping to yield the fully homomorphic encryption.

7. VAN DIJK ET AL, FULLY HOMOMORPHIC ENCRYPTION OVER THE INTEGERS

A much more conceptually simple and true variant of Gentry's scheme was proposed by van Dijk et al [44]. It follows Gentry's method of starting with a somewhat homomorphic scheme, then bootstrapping to a fully homomorphic scheme. However, the scheme is conceptually simpler, employing simple addition and multiplication over integers. The algorithm is as given below:

KeyGen

- The secret key *p*, is an odd number

Encrypt - to encrypt a 1-bit message *m*

- A large multiple of the secret key e.g. *pq*
- A small even number e.g. *2r* where *r* is the noise and $r < p/4$ or $2r < p/2$
- The ciphertext is $c = pq + 2r + m$

Decrypt - to decrypt ciphertext *c*

- $c = pq + 2r + m$
- $c \pmod p = 2r + m \pmod p$
- $(c \bmod p) \bmod 2 = r + m$,

since the noise has the same parity as the message, simply read off the least significant bit (LSB) to retrieve the message. As long as the noise stays small, this can yield a fully homomorphic scheme – the onus is in proving that it supports additive and multiplicative homomorphism.

Given, $c_1 = pq_1 + 2r_1 + m_1$; $c_2 = pq_2 + 2r_2 + m_2$

Additive Homomorphism implies:

$c_1 + c_2 = p(q_1 + q_2) + 2(r_1 + r_2) + m_1 + m_2$

$[(c_1 + c_2) \bmod p] \bmod 2$,

reading off the LSB gives us $m_1 + m_2$

Multiplicative Homomorphism:

$c_1 . c_2 = p.(c_2q_1 + c_1q_2 - q_1q_2) + 2.(r_1r_2 + r_1m_2 + r_2m_1) + m_1m_2$

$[(c_1 . c_2) \bmod p] \bmod 2$,

reading off the LSB gives us m_1m_2

The main issue with both schemes above is the ciphertext and noise growth (especially w.r.t. function complexity).

8. AUGMENTING AN *SHE* SCHEME WITH A MULTI-USER SEARCHABLE SYMMETRIC ENCRYPTION

The main issue with the fully homomorphic schemes described above is the amount of time and computational resource required for their execution. What if we could assist the cloud in locating the information for computation while maintaining semantic security? Searchable Symmetric Encryption permits a user to selectively search the data that the user hosted in the cloud. Constructions and definitions can be found in [45, 46, 47].

This paper proposes an encryption layer on top of the encrypted files to be stored on the cloud. This extra layer would be an encrypted search index layer, which can be searched by using secure indexes such as is discussed in [45]. Furthermore, Park et al described in [48] a method of secure index search for groups that can be used to allow a dynamic set of users search based on predefined access levels.

Searching the index will be possible only via a security token which could be generated for each search/computation. To prevent the server from learning the file content of each segment or what words are being searched by monitoring the user's search pattern, the scheme has to be stochastic in nature. This also lends to a semantically secure system, as such, many tokens can be used to search for a single keyword. Each token would contain a timestamp, security credentials of the user, the index key and the next origin. The next origin is proposed to allow the index layer to be reset, as such, a different token would have to be generated to make a search for the same keyword.

REFERENCES

[1] Virtualization Overview. White Paper. Vmware. Retrieved April 6, 2011, available at: http://www.vmware.com/pdf/virtualization.pdf

[2] Web Search For A Planet: The Google Cluster Architecture. Retrieved April 6, 2011, available at: http://labs.google.com/papers/googlecluster-ieee.pdf

[3] What is Cloud. Retrieved April 6, 2011, available at: http://www.rackspace.co.uk/cloud-hosting/learn-more/what-is-cloud/

[4] What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.microsoft.com/business/en-gb/solutions/Pages/Cloud.aspx

[5] What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.ibm.com/developerworks/cloud/newto.html#WHATIS

[6] Recession is good for cloud computing - Microsoft agrees - http://www.cloudave.com/2425/recession-is-good-for-cloud-computing-microsoft-agrees/

[7] National Institute of Standards and Technology - Computer Security Division http://csrc.nist.gov/groups/SNS/cloud-computing/

[8] Bhaskar P., Admela J·, Dimitrios K·, Yves G.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. J. Grid Computing 9(1), 3-26 (2011)

[9] What the Hell is Cloud Computing. Retrieved April 6, 2011, available at: http://www.youtube.com/watch?v=0FacYAI6DY0

[10] Boniface, M., Nasser, B., Papay, J., Phillips, S., Servin, A., Zlatev, Z., Yang, K. X., Katsaros, G., Konstanteli, K., Kousiouris, G., Menychtas, A., Kyriazis, D. and Gogouvitis, S., "Platform-as-a-Service Architecture for Real-time Quality of Service Management in Clouds", Fifth International Conference on Internet and Web Applications and Services, ICIW 2010, May 2010, Barcelona

[11] LEMOS, R. 2009. Inside One Firm's Private Cloud Journey. Retrieved April 7, 2011, from http://www.cio.com/article/506114/Inside_One_Firm_s_Private_Cloud_Journey

[12] Campbell , R. et al. Open Cirrus Cloud Computing Testbed: Federated Data Centers for Open Source Systems and Services Research. In Proc. HotCloud, 2009.

[13] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A Berkeley view of Cloud computing. Technical report UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, USA, February 2009.

[14] IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=210

[15] New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved April 8, 2011 from http://blogs.idc.com/ie/?p=730

[16] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. In ACM Workshop on Cloud Computing Security, 2009

[17] J. Brodkin. Gartner: Seven cloud-computing security risks. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853, 2008.

[18] Catteddu, D. and Hogben, G. Cloud Computing: benefits, risks and recommendations for information security. Technical Report. European Network and Information Security Agency, 2009.

[19] Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. White Paper. Information Systems Audit and Control Association, 2009.

[20] Brunette, G. and Mogull, R. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Technical Report. Cloud Security Alliance, 2009.

[21] Mell, P. and Grance, T. Effectively and Securely Using the Cloud Computing Paradigm. NIST Information Technology Lab, 2009.

[22] Perez, J. C. Extended Gmail outage hits Apps admins. Retrieved April 8, 2011 from http://www.computerworld.com/s/article/9117322/Extended_Gmail_outage_hits_Apps_admins

[23] Jackson, T. We feel your pain and we are sorry. Retrieved April 8, 2011 from http://gmailblog.blogspot.com/2008/08/we-feel-your-pain-and-were-sorry.html

[24] The Windows Azure Malfunction This Weekend. Retrieved April 8, 2011 from http://blogs.msdn.com/b/windowsazure/archive/2009/03/18/the-windows-azure-malfunction-this-weekend.aspx

[25] FlexiScale Suffers 18-Hour Outage. Retrieved April 8, 2011 from http://www.thewhir.com/web-hosting-news/103108_FlexiScale_Suffers_18_Hour_Outage.

[26] Amazon S3 Availability Event: July 20, 2008. Retrieved April 8, 2011 from http://status.aws.amazon.com/s3-20080720.html.

[27] Ferguson, T. Salesforce.com outage hits thousands of businesses. Retrieved April 8, 2011 from http://news.cnet.com/8301-1001_3-10136540-92.html

[28] VMware Shared Folder Bug Lets Local Users on the Guest OS Gain Elevated Privileges on the Host OS. Retrieved April 9, 2011 from http://securitytracker.com/alerts/2008/Feb/1019493.html

[29] Google Docs Glitch Exposes Private Files. Retrieved April 9, 2011 from http://www.pcworld.com/article/160927/google_docs_glitch_exposes_private_files.html

[30] Salesforce.com Warns Customers of Phishing Scam. Retrieved April 9, 2011 from http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html

[31] Maggi, F. and Zanero, S. Rethinking security in a cloudy world. Technical report, Dipartimento di Elettronica e Informazione, Politecnico di Milano, 2010

[32] Abadi, D.J.: Data management in the cloud: Limitations and opportunities. IEEE Data Eng. Bull. 32(1), 3–12 (2009)

[33] Pearson, S. Taking account of privacy when designing cloud computing services. In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, 2009.

[34] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180, 1978.

[35] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In Comm. of the ACM, 21:2, pages 120–126, 1978

[36] A. C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.

[37] S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984

[38] T. ElGamal, "A prublic key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology (CRYPTO '84), vol. 196 of Lecture Notes in Computer Science, pp. 10–18, Springer, New York, NY, USA, 1985.

[39] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (EUROCRYPT '99), vol. 1592 of Lecture Notes in Computer Science, pp. 223–238, Springer, New York, NY, USA, 1999.

[40] C. Fontaine , F. Galand, A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security, 2007, p.1-15, January 2007

[41] D. Micciancio and O. Regev. Post-Quantum Cryptography, chapter Lattice-based

Cryptography. Springer, 2008

[42] C. Gentry. Fully homomorphic encryption using ideal lattices. In Proc. of STOC, pages 169178. ACM, 2009

[43] N. P. Smart and F. Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. Lecture Notes in Computer Science, 2010, Volume 6056/2010, 420-443.

[44] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In Advances in Cryptology – Eurocrypt 2010, Springer LNCS 6110, 24–43, 2010.

[45] Goh, E.-J.: Secure indexes. Technical Report 2003/216, IACR ePrint Cryptography Archive (2003), http://eprint.iacr.org/2003/216

[46] Chang, Y., Mitzenmacher, M.: Privacy preserving keyword searches on remote encrypted data. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 442–455. Springer, Heidelberg (2005)

[47] Curtmola, R., Garay, J., Kamara, S., Ostrovsky, R.: Searchable symmetric encryption: Improved definitions and efficient constructions. In: Juels, A., Wright, R., De Capitani di Vimercati, S. (eds.) ACM Conference on Computer and Communications Security (CCS 2006), pp. 79–88. ACM, New York (2006)

[48] Hyun-A. Park, J.W.Byun, and D.H.Lee, Secure Index Search for Groups, TrustBus 2005, LNCS3592 pp.128-140, 2005