IBIMA Publishing
Communications of the IBIMA
http://www.ibimapublishing.com/journals/CIBIMA/cibima.html
Vol. 2013 (2013), Article ID 655710, 12 pages
DOI: 10.5171/2013.655710

Research Article

Cloud Computing: Security and Reliability Issues

Farhad Ahamed, Seyed Shahrestani and Athula Ginige

University of Western Sydney, School of Computing, Mathematics and Engineering, Sydney, Australia

Received 1 October 2012; Accepted 10 October 2012; Published 19 February 2013

Academic Editor: Abdul Razak Ibrahim

Abstract

Security and reliability of cloud computing services remain among the dominant concerns inhibiting their pervasive adaptation. The distributed and the multi-tenancy nature of the cloud computing paradigm can be considered as the root causes for their increased risks and vulnerabilities. Resource sharing and virtualization can also be mentioned as additional main factors contributing to or augmenting cross-site scripting and other cloud vulnerabilities. Cloud are also exposed to the risks and liabilities faced by other networked systems. Poorly designed APIs that may cause security problems or distributed denial of services attacks are the examples of this category that are considered in this paper. Public key infrastructure provides the foundations for provision of some essential security services. These include services such as confidentiality, authentication, and privacy that are of vital importance for establishing trust and confidence between the cloud providers and their clients. In this work, we will discuss the potential flaws of this infrastructure and examine how they may deteriorate the security and reliability levels of the cloud environments. To enable a comprehensive study of the challenges in security and reliability of the cloud computing environments, we categorize the risks and vulnerabilities they face. Traditional techniques, based on cryptography, can address some of these challenges to a certain degree. We will argue that they may not be efficient for use in cloud environments. We then focus on data-centric and homomorphic encryption methods that may provide more appropriate solutions in addressing the challenges in cloud computing security and reliability.

Keywords: Cloud computing; cryptography; data-centric security; network security.

Introduction

Cloud computing is a heterogeneous architecture, benefitting from a range of technologies to provide several remote services. National Institute of Standards and Technology (NIST) has identified five widely accepted characteristics, common to all cloud systems (Vaquero et al., 2008, Mell and Grance, 2009, Hogan et al., 2011). These are on-demand self-service, broad network access and diversity of client devices, resource pooling, rapid elasticity and measured service with the pay-per-use business model. Resource pooling allows the cloud providers to serve multi-tenant clients by managing resource utilization efficiently using virtualization, resource partitioning

 Contact author: Farhad Ahamed E-mail: 17368113@student.uws.edu.au

How to Cite this Article: Farhad Ahamed, Seyed Shahrestani and Athula Ginige, "Cloud Computing: Security and Reliability Issues," Communications of the IBIMA, vol. 2013, Article ID 655710, 12 pages
DOI: 10.5171/2013.655710

and workload balancing. Rapid elasticity scales the needed resources in a dynamic manner. Other important features include the heterogeneity on both the provider and the client sides, and multi-provider services.

Cloud computing is considered as one of the major shifts in contemporary computing. The Internet, web applications, cluster computing, terminal services and virtualization have all contributed to cloud computing. They have set the grounds for the remote service clients to utilize distributed computing, resource sharing and pay-as-you go models needed in the cloud architecture (Youseff et al., 2008). Three major parts construct the bulk of services in cloud computing environments (Vaquero et al., 2008, Youseff et al., 2008). One part is referred to as Software-as-a-Service (SaaS). This service enables the cloud client machines to use the software on a cloud server, as if it were within their local work environments. Platform-as-a-Service (PaaS) provides software development platforms for clients. This can reduce the overheads associated with maintenance and infrastructure. Infrastructure-as-a-Service (IaaS) is the third part. Essentially, IaaS provides software, hardware, and network devices, as virtual but apparently on-demand services. For instance, enterprises can get all the benefits associated with a data center, without actually owning and operating one.

Although the benefits of these services are obvious, widespread adaptation of cloud computing depends on properly addressing the relevant security challenges. Many studies and surveys have already established this, for instance see (Hayes, 2008, Takabi et al., 2010, Catteddu and Hogben, 2009). Many of the attacks on cloud computing are related to their distributed and shared environments. Such attacks may target any networked system. They may be considered as the more traditional threats that are also of concern in cloud environments (Takabi et al., 2010). Denial of Service (DoS) attacks or Cross Site Scripting (CSS) threats are examples on this category (Chen et al., 2010). On the other hand, some threats are specific to cloud environments. This may for instance be related to multi-tenancy nature of the cloud server or to virtual machines (VM) that form the basis of the cloud computing paradigm (Chen et al., 2010). In either of these cases, traditional cryptography and its evolutions play dominant roles in addressing some the underlying challenges (Kamara and Lauter, 2010). The issues related to certifying authorities and Public Key Infrastructure (PKI) system as well as privacy and authentication management require special attention, More recent approaches like data-centric security and Homomorphic cryptography are making substantial progress in addressing cloud security challenges (Gentry and Halevi, 2011). However, to achieve secure remote computing environments, utilization of Homomorphic encryption must be limited to schemes that avoid bootstrapping techniques. That is because, bootstrapping techniques can lead to chosen ciphertext attacks (Chunsheng, 2012, Chun-sheng and Ji-xing).

Clearly, the challenges in securing the cloud and the potential solutions encompass many old and new ideas. These are very active research areas and the resulting publications can be overwhelming. This work is an attempt to categorize the security challenges in cloud computing environments and to identify systemic ways for addressing them. The main aims of this work include identifying the current research directions and perhaps more importantly to determine the areas that require more research in securing the cloud.

To discuss these points further, this paper is organized as follows. More traditional security threats relevant to confidentiality, privacy, and authentication in cloud computing are discussed in the following section. The more contemporary security and reliability concerns, which are rather specific to cloud computing environments and architecture, are discussed in the part after that. The next section covers PKI related

issues that may be of concern in cloud computing environments. It also covers some of the proposed solutions that can provide data integrity and privacy services in cloud environments. It also covers some of the shortfalls of such solutions. In particular, data-centric approaches and homomorphic cryptography that can facilitate the computational operations on encrypted information, including data secured in cloud servers, are examined in that part. The concluding remarks constitute the last part of the paper.

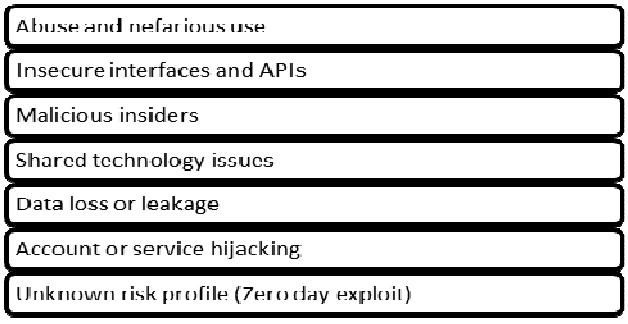

Fig 1. Cloud Security Alliance Identified Threat Domains in Cloud Computing

Common Risks and Threats

Cloud Security Alliance (CSA) has identified seven domains of security threat (Cloud Security Alliance, 2011, Cloud Security Alliance, 2009). Fig 1 summarizes these threat domains. Data integrity in cloud environment is also a challenge for cloud service providers (CSP). Either traveling of data in clusters, in virtual machines, in databases, or into third party storages, data ownership should be always attached to the end users or they should have mechanism to audit the data and verify the logs of data access. Encrypted data can provision these characteristics.

There is ongoing research to address how to perform operation on encrypted data without decrypting it. Additionally, it is required to conduct further research to investigate how to sort, search over encrypted data and metadata. These are also discussed in later sections. Data security on remote resources with multiple shared users, security on network transmission protocol, encrypted information, and multiparty data or service provision are examples of conventional or more traditional security threats.

However, by manipulating conventional mechanisms or simply by exploiting poorly designed Application Programming Interface (API) of the cloud software vendors, attacks on cloud environment can be intensified. Poorly designed API may present another set of issues. Such APIs usually lack the security measures and can cause servers crashing or they may gain execution privileges for unauthorized users (Henning, 2007). Fig 2 is a summary of the major security threats that has been recently reported (Web Hacking Incident Database, 2011). From this figure, it is clear that a large percentage of attacks are still in the category of traditional threats. The major attacks in this category, namely malware, CSS, and DoS are discussed in the remainder of this section.

Malicious software (malware) refers to a range of hostile software that by character are intrusive. Their variations have been considered to pose major threats since internetworking gained popularity. Despite various antivirus programs and firewall set-ups, sophisticated malware is still reported

to gain access to various computing systems. For example, recent attacks by Stuxnet and Flame have shown how vulnerable cloud computing environments to sophisticated malware are (Essers, 2011, ICANN).

A zero-day exploit is an attack that takes advantage of security vulnerability on the same day that it becomes commonly known. It is a process that widely used by smart malwares for spreading the malicious code through some network. To mitigate the effects of these codes, some vendors provide lightweight architecture that incrementally update the systems of their clients in near real-time (TechWeb, 2006). It needs to be noted that, there is no known mechanism to identify the relevant security issues, before the attack happening and in a pro-active manner. There has been some progress in addressing these issues through for instance, by analyzing the behavior of network users or by sophisticated intrusion detection systems. But the research in this area is ongoing (Lahiri, 2012).

Some studies have indicated that attacks on web services constitute more than 60% of the total attempts at exploiting online vulnerabilities (SANS Institute, 2009). It has also been shown that injection flaws and cross-site scripting are among the most common liabilities of these services (Open Web Application Security Project, 2010, Lloyd et al., Mar, 2001). This is further complicated by noting that some vendor sites, like Amazon use Simple Object Access Protocol (SOAP) based cloud control interface to monitor, add, and remove virtual machine instances. SOAP provides for the exchanges of structured information needed for the use of such web services and is reliant on XML. XML signature wrapping attacks on public SOAP interface in the cloud have been reported to cause the formation of new instances of VM as well as starting and stopping of existing VM (Somorovsky et al., 2011). Code injection in web applications poses an ongoing threat due to immature coding and lack of preventive measures (Johns, 2009). To prevent injection flaws and cross-site scripting, automatic approaches to detect vulnerabilities have been suggested (Bello and Russo, 2012). In these approaches, rather than modifying interpreters or compilers, a taint analysis of could-related web applications that consider persistent storage, opaque objects and security policies, are to be used.

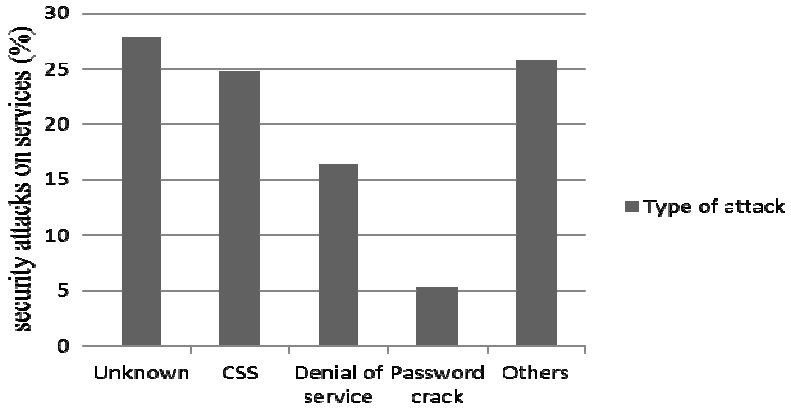

Fig 2. Major Attack Types on Cloud Services

Botnet is a collection of compromised computers or bots. Botnets attackers may utilize cloud resources to expand their network and processing power, posing a threat to the very shared resources they are using on the same host (Kandula et al., 2005).

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on shared resources or on the cloud server can cause devastating impacts in provisioning of the cloud services. The semantic and flooding DDoS attacks are well known and the associated risks are well researched (Mirkovic and Reiher, 2004). Fraudulent Resource Consumption (FRC) attack on cloud servers are analogous to an application-layer DDoS attack. As the name implies, FRC attacks fraudulently consume bandwidth and other resources of the cloud services resulting in financial liabilities for the cloud clients (Idziorek and Tannian, 2011). Utility computing in cloud environments is particularly vulnerable to such attacks, where the attackers seek to exploit the utility pricing model to harm the victim financially. It has also been shown that DoS attacks on cloud systems can cause the OS kernel to crash and for some systems, the crash can be sustained in the VM level (Kurmus et al., 2011).

Cloud-Specific Security Liabilities

Some of the security and reliability concerns are more specific to clouds and are more contemporary. In this sense, these can for instance be due to the inherent sharing of resources, virtualization, and other underlying technology-related issues. These are discussed in this section. In the cloud model, virtualization and VMs are at the heart of providing remote desktop capabilities. Some clients may require a large number of VMs to cover their development, integration, testing, and deployment needs. Obviously, the security protections of all these VMs need to be current to prevent security breaches and leaks. Given the scale of the task, this can be a serious challenge (Garfinkel and Rosenblum, 2005). Maintaining the integrity of saved images can also be challenge for virtualization vendors (Wei et al., 2009). It has been demonstrated how a malicious insider can obtain passwords, cryptographic keys, files and other confidential data of the cloud users from the data stored in virtual machines (Rocha and Correia, 2011).

One of the major benefits of cloud computing is the capability of providing storage and processing power at lower costs in comparison to locally arranging for these. But as a side effect, this may be of benefit to so-called hacker community or to occasional hackers (Homeland Security News Wire, 2011). Identity theft and stolen credit cards can help the hackers to register with false identities for cloud resources. With the VM model and sharing of the resource in cloud environments, their fraudulent monitoring is of concern. These may for example relate to observing CPU usage, caches and network activity, disk writing timing, and in more serious cases, retrieving the passwords or other information from the servers (Bilge et al., 2009). The security characteristics that is required from cloud services and surrounding attacks types are shown in Fig. 3 Multi-tenancy system is prone to disclosing CPU cache memory, timing analysis and tracking of hardware resources. These can open the door to side channels that passively observe the information, or to covert channels that actively send data (Xu et al., 2011, Aviram et al., 2010). An attacker can detect the target VM in a server using the techniques like measuring cache usage, load-based co-residence detection and estimating traffic rates on network address (Ristenpart et al., 2009). When the target virtual instance and malicious instance are in the same physical machine, monitoring the CPU, memory, network utilization, and other behavior patterns can lead to cross VM information leakage. It has been proposed that new systems with secure cache be designed to overcome some of these issues (Wang and Lee, 2007).

In public cloud environments, the data owner does not normally have full physical control over their data. To ensure the integrity of data, periodic audit is necessary. To address the growing concerns about the associated loss of control over private data hosted in the cloud, an architecture for a secure data

repository service, motivated by the smart power grid domains has been proposed (Kumbhare et al., 2011). The system masks file names, user permissions and access patterns while providing auditing capabilities with provable data updates. Providing and managing end user access in the cloud while enforcing the security policies is an ongoing research issue. If the security of a VM is compromised, the rest of the VM holders, at least those on the same physical machine, will be concerned. To monitor these attacks, while preserving data privacy, some security and access management framework has been proposed (Almorsy et al., 2011). A cloud vendors, CloudPassage, claims to be capable of securing the servers across public, private and hybrid clouds and give real-time detection for a wide range of security events and system states (Hickey and McCarthy, 2012). However, this type of monitoring requires autonomic intelligent alarm systems and self-defense capabilities.

A major issue in cloud computing relates to establishing trust between the servers and the clients. Some argue that such trust relations must be formed dynamically (Demchenko et al., 2011). Many services, like Google email, Orkut mail services, and some social networking services, use trust or referral-based information filtering to protect mail servers from spammers (Golbeck, 2004). In cloud environments, it is not easy to establish trust when a server shares data with another server. This is particularly true when the source server does not have control over the destination server to enforce data sharing rules on that server (Khan and Malluhi, 2010). At any case, it remains a challenge to enforce predefined security policies across the servers and services. To ensure confidentiality and privacy in the cloud, several issues need to be addressed (Kretzschmar et al., 2011). These include, management of identities, credentials, privileges, cryptographic keys, and other security information.

Cloud Security and Cryptography

Given the diversity of threats discussed in previous parts, the classical security approaches lead to focusing on solutions based on encryption techniques. These techniques can be used for storing the encrypted data on remote severs and sharing them with legitimate users or groups. Most encryption systems for secure transaction and communication over Internet rely on PKI, either directly or indirectly. The functioning of PKI is dependent on trustworthy Certifying Authorities (CA). There are over 600 CAs around the globe (Eckersley, 2011). Managing trustworthiness for all these certificate-issuing authorities, has become a major challenge in its own right. For instance, in 2011, DigiNotar CA was compromised. They could not provide any information regarding the number of fraudulent certificates issued or any information about the nature of the data leakage (Whitney, 2011). To resolve the problem, major browsers blocked DigiNotar CA, and all their clients had to revoke their certificates. A similar incident with Comodo, a major CA, raised concerns among the cloud community (ICANN, Open Web Application Security Project, 2010). The incident occurred in late 2010, where login credential of an employee of Comodo was compromised. Subsequently, fraudulent digital certificate of cloud service providers like Google and Yahoo were generated. These resulted in many man in the middle attacks using the fraudulent certificates over several months with an unknown number of email accounts monitored.

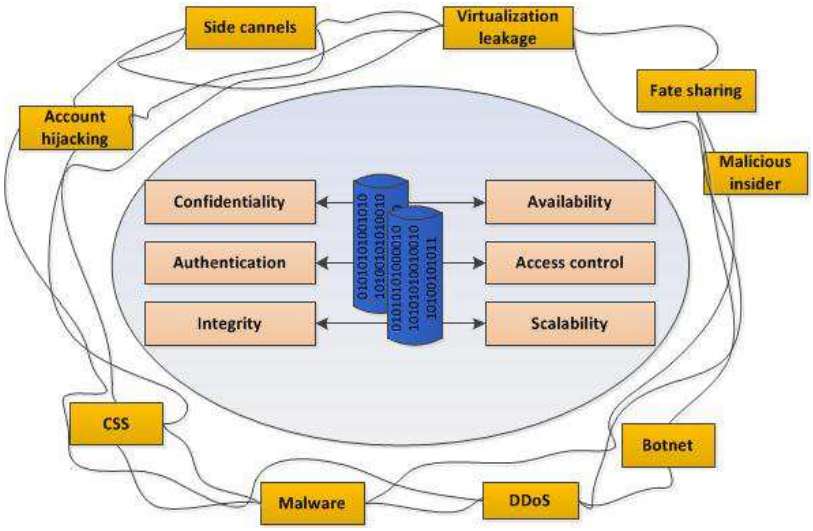

Fig 3. The Required Security Characteristics Surrounded by the Security Threats

To minimize the impact of fraudulent certificates, DNSSEC protocol has been introduced to mitigate the effects of the man-in-the-middle attack (ICANN). DNSSEC leverages PKI and CA into DNS level, protecting the local user. DNSSEC on the other hand does not provide any solution on DoS attacks. It actually makes the problem more complex by including itself in the list of prime targets in the network. Cross certification and interoperability issues within PKI infrastructure may lead to trust management chaos as it is impractical to have a singular trusted CA for all the countries, domains and businesses (Stock et al., 2007, SANS Institute, 2009). Revoking the fraudulent certificates is not an easy task, as the Certificate Revocation List (CRL) is not maintained by all the involved parties due to cost and processing overhead for their system. There are suggestions that alternate authentication, confidentiality and privacy provisioning architecture that avoid PKI are needed (Ekert and Jozsa, 1996, Childs and Van Dam, 2010).

Another widely used approach is to encrypt the data by a symmetric key. This approach is not scalable. An extension of it though, creates meta-data from the information and sends semantics or keywords within the encrypted meta-data. When the user gets matching of encrypted meta-data, selected data will be downloaded to local machine. The data can only be decrypted, if the user has the required key. Clearly, this approach avoids the overhead of unnecessary decryption of the data to be searched (Kui et al., 2012).

To preserve data confidentiality on the cloud, the data is encrypted in one way or another. Consequently, traditional data utilization services that are based on plain text keyword search lose their usefulness. Data-centric approach is one way of overcoming this problem and providing access to legitimate users. The users get access to data encrypted with the secret key that is associated with the data itself. There are several issues with data sharing among the applications hosted on clouds based on this approach (Idziorek and Tannian, 2011, Zhou et al., 2010). Another approach to overcome the problem is based on using fuzzy keyword search over encrypted cloud data using symmetric searchable encryption (Cong et al., 2011).

A more aspiring solutions that aims to achieve computations on encrypted data is referred to as homomorphic encryption scheme (Rivest et al., 1978). Partial

Homomorphic Encryption (PHE) generally provides for homomorphic addition or multiplication on ciphertext. Some useful applications that utilize PHE are becoming available (Jurik and Nielsen, 2003, Aditya et al., 2004, Bringer et al., 2007). An example of these applications is an additively homomorphic encryption to perform secure electronic voting (Cohen and Fischer, 1985). Fully Homomorphic Encryption (FHE) can help with providing Secure Computing Outsourcing (SCO) (Gentry, 2010, Gentry, 2009). FHE is shown to enable Turing machines to run algebraic operations on encrypted data without decrypting them (Vaikuntanathan, 2011).

Utilizing FHE, trust is not a prerequisite for allowing an entity to carry out computational operations on the data, as the operations are carried out on encrypted data and result in ciphertext. As such, public cloud servers for instance, can be employed without any concerns for compromising data privacy or confidentiality (Mitchell et al., 2012). Clearly, an efficient and fully homomorphic cryptosystem will be of substantial advantage for outsourcing of private computations (Gentry, 2010, Naone, 2011). That is a long time away. There have been some attempts to develop FHE system, however further theoretical improvement is required (Gentry and Halevi, 2011). But several schemes that aim to formulate a method for Somewhat Homomorphic Encryption (SWHE) first, and apply bootstrapping techniques later to decipher the text have been proposed (Van Dijk et al., 2010, Coron et al., 2011, Gentry, 2009, Gentry and Halevi, 2011, Smart and Vercauteren, 2010, Chunsheng, 2011). FHE is not yet ready for building applications and requires extensive computation capabilities (Naehrig et al., 2011). FHE operations on integers or using ideal lattice can be the target of a Chosen Ciphertext Attack (CCA) (Chunsheng, 2012, Chun-sheng and Ji-xing, 2012). Overcoming CCA issue and avoiding bootstrapping are the essential requirements for FHE being prosperous in provisioning SCO (Zhang et al., Brakerski et al., 2012).

Conclusion

In this work, we have categorized and presented potential security threats and risks in cloud computing environments. The risks may be either common to many distributed systems or are of more contemporary nature that is more specific to cloud environments. In either case, they are amongst the main obstacles in widespread adopting of cloud computing. Due to their inherent multi-tenancy and virtualization architecture, cloud computing environments are prone to threats in addition to those relevant to any distributed system. Cryptographic solutions provide to some of these threats. Noting that most cryptosystems rely on PKI in one way or another, this work has detailed some of the deficiencies of using this infrastructure in cloud security. In this work, we have also argued that the more traditional cryptosystem-based solutions may not have all the capabilities needed for efficiently securing the cloud. However, the more contemporary cryptography-based solutions are more applicable to issues and risks encountered in cloud environments. For instance, homomorphic encryption techniques and data-centric approaches offer many interesting solutions to computing on ciphertexts or preserving the client anonymity in clouds. However, the implementation and full development of such methodologies still require extensive research. In our future research, we plan to work on these issues.

References

Aditya, R., Boyd, C., Dawson, E., Lee, B. & Peng, K. (2004). Multiplicative Homomorphic E-Voting.

Almorsy, M., Grundy, J. & Ibrahim, A. S. (2011). Collaboration-Based Cloud Computing Security Management Framework, Cloud Computing (CLOUD), 2011 IEEE International Conference on.

Aviram, A., Hu, S., Ford, B. & Gummadi, R. (2010). Determinating Timing Channels in

Compute Clouds, Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop. *Chicago, Illinois, USA: ACM.*

Bello, L. & Russo, A. (2012). Towards a Taint Mode for Cloud Computing Web Applications, Proceedings of the 7th Workshop on Programming Languages and Analysis for Security. *Beijing, China: ACM.*

Bilge, L., Strufe, T., Balzarotti, D. & Kirda, E. (2009). All Your Contacts are Belong to Us: Automated Identity Theft Attacks on Social Networks, *ACM.*

Brakerski, Z., Gentry, C. & Vaikuntanathan, V. (2012). Fully Homomorphic Encryption without Bootstrapping, *Innovations in Theoretical Computer Science.*

Bringer, J., Chabanne, H., Pointcheval, D. & Tang, Q. (2007). Extended Private Information Retrieval and Its Application in Biometrics Authentications, *Springer-Verlag.*

Catteddu, D. & Hogben, G. (2009). 'Cloud Computing Risk Assessment,' *The European Network and Information Security Agency (ENISA).*

Chen, Y., Paxson, V. & Katz, R. H. (2010). What's New about Cloud Computing Security?, *EECS Department, University of California, Berkeley.*

Childs, A. M. & Van Dam, W. (2010). Quantum Algorithms for Algebraic Problems, *Reviews of Modern Physics,* 82, 1.

Chunsheng, G. (2011). New Fully Homomorphic Encryption over the Integers. *Cryptology Eprint Archive,* Report 2011/118, 2011.

Chunsheng, G. (2012). Attack on Fully Homomorphic Encryption over the Integers.

Chun-Sheng, G. & Ji-Xing, G. (2012). Attack on Fully Homomorphic Encryption over Principal Ideal Lattice [Online]. Available: http://onlinepresent.org/proceedings/vol1_2012/9.pdf.

Cloud Security Alliance. (2009). Top Threats in Cloud Computing V 1.0 [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

Cloud Security Alliance. (2011). Security Guidance for Critical Areas of Focus In Cloud Computing V 3.0 [Online]. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

Cohen, J. D. & Fischer, M. J. (1985). A Robust and Verifiable Cryptographically Secure Election Scheme, *Foundations of Computer Science,* 1985., 26th Annual Symposium on.

Coron, J. S., Mandal, A., Naccache, D. & Tibouchi, M. (2011). "Fully Homomorphic Encryption over the Integers with Shorter Public Keys," *Advances in Cryptology–CRYPTO 2011,* 487-504.

Damgård, I., Jurik, M. & Nielsen, J. B. (2003). A Generalization of Paillier's Public-Key System with Applications to Electronic Voting. Citeseer.

Demchenko, Y., Ngo, C., De Laat, C., Wlodarczyk, T. W., Rong, C. & Ziegler, W. (2011). Security Infrastructure for On-demand Provisioned Cloud Infrastructure Services, Cloud Computing Technology and Science (Cloudcom), 2011 IEEE Third International Conference on.

Eckersley, P. (2011). How Secure is HTTPS Today? How Often is It Attacked? [Online]. Available: https://www.eff.org/deeplinks/2011/10/how-secure-https-today.

Ekert, A. & Jozsa, R. (1996). "Quantum Computation and Shor's Factoring Algorithm," *Reviews of Modern Physics,* 68, 733-753.

Essers, L. (2011). Dutch Government Struggles to Deal with DigiNotar Hack [Online]. Available: http://www.pcworld.com/businesscenter/article/239639/dutch_government_struggles_to_deal_with_diginotar_hack.html.

Garfinkel, T. & Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments, *In Proceedings of the 10th Hotos.*

Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices, Proceedings of the 41st Annual ACM Symposium on Theory of Computing. *Bethesda, MD, USA: ACM.*

Gentry, C. (2010). "Computing Arbitrary Functions of Encrypted Data," *Communications of the ACM,* 53, 97-105.

Gentry, C. & Halevi, S. (2011). "Implementing Gentry's Fully-Homomorphic Encryption Scheme," Advances in Cryptology – EUROCRYPT 2011. In: Paterson, K. (ed.). *Springer Berlin / Heidelberg.*

Golbeck, J. (2004). Trust Networks for Email Filtering [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.6090&rep=rep1&type=pdf.

Hayes, B. (2008). "Cloud computing," *Commun ACM,* 51, 9-11.

Henning, M. (2007). "API Design Matters," *Queue,* 5, 24-36.

Hickey, A. R. & Mccarthy, J. E. (2012). '20 Coolest Cloud Security,' *CRN, 24-n/a.*

Hogan, M., Liu, F., Sokol, A. & Tong, J. (2011). NIST Cloud Computing Standards Roadmap.

Homeland Security News Wire. (2011). Hackers Using Cloud Networks to Launch Powerful Attacks [Online]. Available: http://www.homelandsecuritynewswire.com/hackers-using-cloud-networks-launch-powerful-attacks.

Icann. (DNSSEC Standards [Online]. Available: http://www.icann.org/en/news/in-focus/dnssec/standards.

Idziorek, J. & Tannian, M. (2011). Exploiting Cloud Utility Models for Profit and Ruin, Cloud Computing (CLOUD), 2011 IEEE International Conference on.

Johns, M. (2009). Code Injection Vulnerabilities in Web Applications - Exemplified at Cross-Site Scripting, *University of Passau.*

Kamara, S. & Lauter, K. (2010). Cryptographic Cloud Storage, Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security. Tenerife, Canary Islands, *Spain: Springer-Verlag.*

Kandula, S., Katabi, D., Jacob, M. & Berger, A. (2005). Botz-4-Sale: Surviving Organized DDos Attacks that Mimic Flash Crowds, Proceedings of the 2nd Conference on Symposium on Networked Systems Design \& Implementation - Volume 2. USENIX Association.

Khan, K. M. & Malluhi, Q. (2010). "Establishing Trust in Cloud Computing," *IT Professional,* Vol. 12, Pp. 20-27.

Kretzschmar, M., Golling, M. & Hanigk, S. (Eds.) (2011). Security Management Areas in the Inter-Cloud.

Kumbhare, A. G., Simmhan, Y. & Prasanna, V. (2011). Designing a Secure Storage Repository for Sharing Scientific Datasets Using Public Clouds, Proceedings of the Second International Workshop on Data Intensive Computing in the Clouds. *Seattle, Washington, USA: ACM.*

Kurmus, A., Gupta, M., Pletka, R., Cachin, C. & Haas, R. (2011). A Comparison of Secure Multi-Tenancy Architectures for Filesystem Storage Clouds, Proceedings of the 12th ACM/IFIP/USENIX International Conference on Middleware. Lisbon, Portugal: Springer-Verlag.

Lahiri, B. (2012). 'Detecting Exploit Patterns from Network Packet Streams,' Ph.D. 3511430, *Iowa State University.*

Lloyd, S., Fillingham, D., Lampard, R., Orlowski, S. & Weigelt, J. (Mar, 2001). CA-CA Interoperability, *PKI Forum.*

Mell, P. & Grance, T. (2009). A NIST Definition of Cloud Computing [Online]. *National Institute of Standards and Technology.* Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Mirkovic, J. & Reiher, P. (2004). "A Taxonomy of Ddos Attack and Ddos Defense Mechanisms," *SIGCOMM Comput. Commun.* Rev., 34, 39-53.

Mitchell, J. C., Sharma, R., Stefan, D. & Zimmerman, J. (2012). Information-Flow Control for Programming on Encrypted Data, *Computer Security Foundations Symposium (CSF),* 2012 IEEE 25th.

Naehrig, M., Lauter, K. & Vaikuntanathan, V. (2011). Can Homomorphic Encryption Be Practical?, Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. Chicago, *Illinois, USA: ACM.*

Naone, E. (2011). Homomorphic Encryption: Making Cloud Computing More Secure, *Technology Review (Cambridge, Mass.).*

Open Web Application Security Project. (2010). OWASP Top 10 Risks [Online]. Available: http://www.owasp.org/index.php/Top_10_2010.

Ren, K., Wang, C. & Wang, Q. (2012). "Security Challenges for the Public Cloud," *Internet Computing, IEEE,* 16, 69-73.

Ristenpart, T., Tromer, E., Shacham, H. & Savage, S. (2009). Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, Illinois, USA: ACM.

Rivest, R. L., Adleman, L. & Dertouzos, M. L. (1978). "On Data Banks and Privacy Homomorphisms," *Foundations of Secure Computation,* 32, 169-178.

Rocha, F. & Correia, M. (2011). Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud, Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on.

Sans Institute. (2009). 'The Top Cyber Security Risks,' [Online]. *SysAdmin, Audit, Network, Security Institute.* Available: http://www.sans.org/top-cyber-security-risks.

Smart, N. & Vercauteren, F. (2010). "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes," *Public Key Cryptography–PKC 2010,* 420-443.

Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L. L. (2011). All Your Clouds are Belong to Us: Security Analysis of Cloud Management Interfaces, Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. *Chicago, Illinois, USA: ACM.*

Stock, A. V. D., Williams, J. & Wichers, D. (2007). OWASP Top 10 Risks [Online]. Available: http://www.owasp.org/index.php/Top_10_2007.

Takabi, H., Joshi, J. B. D. & Ahn, G. J. (2010). "Security and Privacy Challenges in Cloud Computing Environments," Security & Privacy, IEEE, 8, 24-31.

Techweb. (2006). 'Exploit Prevention Labs Ships Zero-day Exploit Blocker,' *TechWeb. Manhasset, United States, Manhasset.*

Vaikuntanathan, V. (2011). Computing Blindfolded: New Developments in Fully Homomorphic Encryption, *Foundations of Computer Science (FOCS),* 2011 IEEE 52nd Annual Symposium on.

Van Dijk, M., Gentry, C., Halevi, S. & Vaikuntanathan, V. (2010). "Fully Homomorphic Encryption over the Integers," *Advances in Cryptology–EUROCRYPT 2010,* 24-43.

Vaquero, L. M., Rodero-Merino, L., Caceres, J. & Lindner, M. (2008). "A Break in the Clouds: Towards a Cloud Definition," *SIGCOMM Comput. Commun.* Rev., 39, 50-55.

Wang, C., Wang, Q. & Ren, K. (2011). Towards Secure and Effective Utilization over Encrypted Cloud Data. Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on.

Wang, Z. & Lee, R. B. (2007). "New Cache Designs for Thwarting Software Cache-Based Side Channel Attacks," *SIGARCH Comput. Archit.* News, 35, 494-505.

Web Hacking Incident Database. (2011). Available: http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database.

Wei, J., Zhang, X., Ammons, G., Bala, V. & Ning, P. (2009). Managing Security of Virtual Machine Images in a Cloud Environment, Proceedings of the 2009 ACM Workshop on Cloud Computing Security. *Chicago, Illinois, USA: ACM.*

Whitney, L. (2011). Comodohacker Returns in Diginotar Incident [Online]. Available: http://news.cnet.com/8301-1009_3-20102027-83/comodohacker-returns-in-diginotar-incident/.

Xu, Y., Bailey, M., Jahanian, F., Joshi, K., Hiltunen, M. & Schlichting, R. (2011). An Exploration of L2 Cache Covert Channels in Virtualized Environments, Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. *Chicago, Illinois, USA: ACM.*

Youseff, L., Butrico, M. & Da Silva, D. (2008). Toward a Unified Ontology of Cloud Computing, *Grid Computing Environments Workshop, 2008.* GCE '08.

Zhang, Z., Plantard, T. & Susilo, W. (Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes, Zhou, W., Sherr, M., Marczak, W. R., Zhang, Z., Tao, T., Loo, B. T. & Lee, I. (2010). Towards a Data-Centric View of Cloud Security. Proceedings of the Second International Workshop on Cloud Data Management. *Toronto, ON, Canada: ACM.*