ANALYTICAL STUDY ON PRIVACY AND RELIABILITY OF CLOUD COMPUTING

Omkar Ramesh Ghatage[1], Dr.Mona Dwivedi[2]

[1]Research Scholar Opjs University Churu Rajasthan
[2]Professor, Computer Science Department Mansarovar Global University

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 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 datacentric 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.

CLOUD SERVICE DEPLOYMENT AND CONSUMPTION MODELS

Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are four primary ways in which cloud services are deployed (CSA Security Guidance, 2009). Cloud integrators can play a vital role in determining the right cloud path for a specific organization.

Public cloud: Public clouds are provided by a designated service provider and may offer either a single tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is generally owned by and managed by the designated service provider and located within the provider's data centers (off premises). All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.

Private cloud: Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds: (i) on-premise private clouds and (ii) externally hosted private clouds. The on-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider.

Hybrid cloud: Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third party cloud providers in a full or partial manner, thereby increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Managed cloud: Managed clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is owned by and/or physically located in the organizations' data centers with an extension of management and security control planes controlled by the designated service provider. The notion of public, private, managed and hybrid when describing cloud services really denotes the attribution of management and the availability of service to specific consumers of the

services. Table 1 summarizes various features of the four cloud deployment models. When assessing the impact a particular cloud service may have on one's security posture and overall security architecture, it is necessary to classify the assets/resource/service within the context of not only its location but also its criticality and business impact as it relates to management and security. This means that an appropriate level of risk assessment is performed prior to entrusting it to the vagaries of the cloud (CSA Security Guidance, 2009). In addition, it is important to understand various tradeoffs between the various cloud service models:

• Generally, SaaS provides a large amount of integrated features built directly into the offering with the least amount of extensibility and in general a high level of security (or at least a responsibility for security on the part of the service provider).

• PaaS offers less integrated features since it is designed to enable developers to build their own applications on top of the platform, and it is, therefore, more extensible than SaaS by nature. However, this extensibility features trade-offs on security features and capabilities.

• IaaS provides few, if any, application-like features, and provides for enormous extensibility but generally less security capabilities and functionalities beyond protecting the infrastructure itself, since it expects operating systems, applications and contents to be managed and secured by the customers.

CLOUD COMPUTING SECURITY AND PRIVACY ISSUES

This section addresses the core theme of this chapter, i.e., the security and privacy-related challenges in cloud computing. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable for malware detection in the clouds – an approach which is usually adopted in intrusion detection systems (IDSs). As shown in Figure 1, there are six specific areas of the cloud computing environment where equipment and software require substantial security attention (Trusted Computing Group's White Paper, 2010).

These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication of users/applications/ processes, (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response.

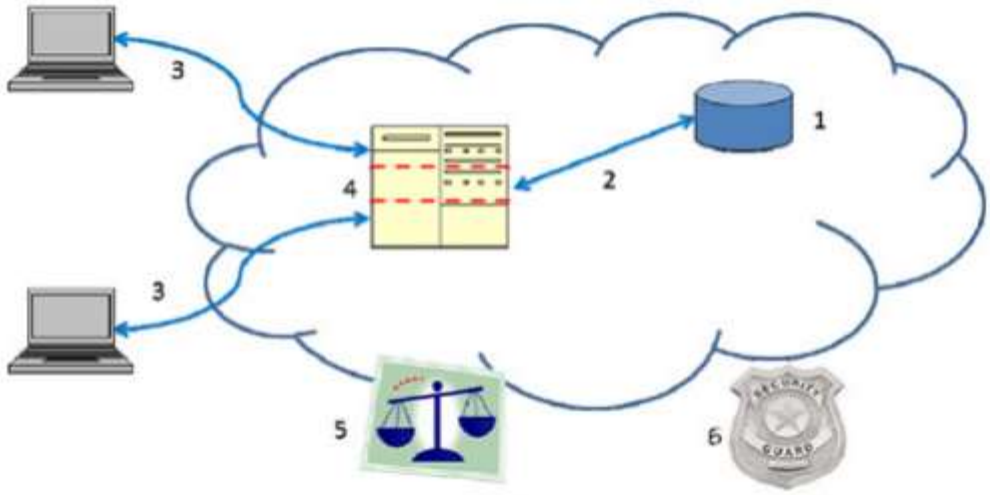

Figure 1: Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, (3) authentication, (4) separation between customers, (5) cloud legal and regulatory issues and (6) incident response.

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group (Trusted Computing Group's White Paper, 2010). These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.

COMMON RISKS AND THREATS

Cloud Security Alliance (CSA) has identified seven domains of security threat (Cloud Security Alliance, 2011, Cloud Security Alliance, 2009). 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). 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 setups, 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).

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).

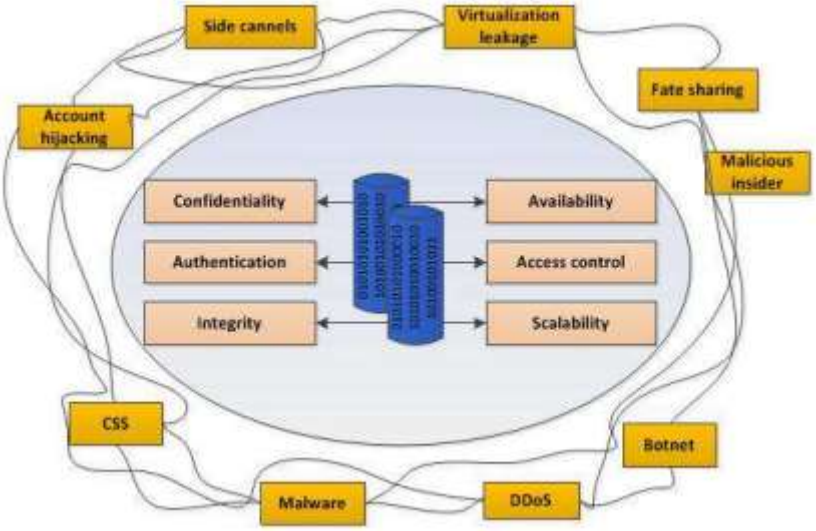

Fig 2. The Required Security Characteristics Surrounded by the Security Threats

The security characteristics that is required from cloud services and surrounding attacks types are shown in Fig. 2 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, loadbased 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).

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.

To minimize the impact of fraudulent certificates, DNSSEC protocol has been introduced to mitigate the effects of the manin-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).

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 multitenancy 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 cipher texts 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.

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 Ondemand 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/ho w-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/ar ticle/239639/dutch_government_struggles_t o_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.