Security in the Cloud: A stake holder's perspective

Vivek Shandilya, *Student Member, IEEE*, and Sajjan Shiva, *Fellow, IEEE*

***Abstract*—The cloud computing is a paradigm involving many disparate stake holders. Any system built upon this paradigm and a business run on such system architecture would have similarly disparate scope of access, activities and responsibilities for the stake holders. Depending on the scope of the activities and responsibilities, a stakeholder has to device the security measures to secure his activity space. We formulate the problem formally with this premise. We model and survey, depending upon the generic cloud architecture abstracted from the prominent ones, the actvity space of each stake holder and consequently security measures each stake holder has to take, to ensure the over all security of the system. We survey the recent works related to each facet of the formal model and classify them to present a contemporary perspective.**

***Index Terms*—Coud computing, Formal representation, Security, Activity Space, Best Practices, Stake holders.**

I. Introduction

Cloud computing is becoming popular as the infrastructure solution for many medium and small scale business companies all over the world. This trend is a game changing paradigm shift. Even though the underlying principle of operation of individual constituents is same, since the cloud architectures differ from each other in their construction details, the exact access and action spaces also vary for the stake holders operating on systems built on different clouds.

But considering a generic cloud architecture which absorbs the essential features of most cloud computing infrastructures, we can identify the prominent stake holders in a business system built over such a cloud. Then we can determine the scope of access, activities and controls each of them have. On that basis we can determine who is responsible for what security aspects in the whole operation, and what action each of the stake holder needs to take to ensure security in his own space and eventually the whole system. There are many cloud service providers with varied features. Many of them focus on a set of niche target customers and specialize on the features that are important to such clientle. Though such differences make each cloud service provided by different service providers different, we can form a generic set of features that constitutes a cloud by taking the commonalities of the major cloud services. The major stake holders are the end user of the business, the business organization, the network (Internet) provider facilitating the communication to and from the cloud with the organization, the cloud service provider, the provider of the operating system and other software used to construct the cloud, the hardware manufacturers and the governments who administer and monitor the legalities as applicable to the whole operation. From the systemic point of view, the key issues of security and privacy are identified and is argued to be a problem of risk management in [1]. It is not only important to study the security from the point of view of the systems that functionally constitute the whole operation built on a cloud infrastructure but also from the perspective of the above mentioned stakeholders so that a framework for creating best practices, policies and laws would be facilitated in an informed way. In this paper we study the scope of security measures for each of the stake holders based on the scope of their activity in the cloud based business systems.

The main contributions of this paper are as follows.

1. We formally represent the stake holders and their profiles in a business system based on a generic cloud computing infrastructure.
2. We delineate the security concerns and responsibilities of each stake holder to ensure the overall security of the business, based on the survey of current literature.

The Section II describes a formal representation of the security-activity profile for a generic cloud based system with the perspective of the stake holders and their activity space.The section III describes in detail, the generic architecture of cloud computing services used by the businesses and their security concerns. Section IV describes the activity spaces and profile of the stake holders in the cloud based system. Section V describes the security activity spaces and profile of the cloud based systems. The section VI discusses the related works. The section VII presents the conclusion.

II. Formal representation of the security profile of a cloud

In this section, we formulate the structure of the security problem in a cloud-based system formally.
The cloud based system involves n, where $0 < n < \infty$, different stake holders. The $i^{th}, 1 < i \leq n$ stake holder h_i has access to an unambiguously defined part of the system. This is referred to as the **access space** s_{i_A} of the stake holder h_i.

This access space s_{i_A}, is considered as the set of m areas. $s_{i_A} = \{s_{i_{A_1}}, s_{i_{A_2}}, s_{i_{A_3}}, \ldots, s_{i_{A_j}}, \ldots, s_{i_{A_m}}\}, 1 < j \leq m, 1 < m \leq \infty$.

In each of these areas, the stake holder h_i can choose to do one action, at a time, out of the clearly defined *set of actions*, $s_{i_{a_j}}$ corresponding to j. The ordered pair of this *access area* and the corresponding *set of action* is referred to as the activity area $s_{i_{\alpha_j}} = (s_{i_{A_j}}, s_{i_{a_j}})$.
The union of all such sets of actions available at, that is, corresponding to, each of the areas in the access space is

Vivek Shandilya is with the Department of Computer Science, University of Memphis, Memphis, TN 38152–3240. Phone: +1 901 848–1763, e-mail: vhmsndly@memphis.edu

Sajjan Shiva is with the Department of Computer Science, University of Memphis, Memphis, TN 38152–3240. Phone: + 90 1 678–5465, fax: + 90 1 678–1506, e-mail: sshiva@memphis.edu

referred to as the stake holder's action space s_{i_a} .
$s_{i_a} = \bigcup_{j=1}^{m} s_{i_{a_j}}$
The union of all sets of access areas is the access space of the stake holder h_i.
$s_{i_A} = \bigcup_{j=1}^{m} s_{i_{A_j}}$
The union of all the activity areas of the stake holder h_i, is called the activity space of h_i.
$s_{i_\alpha} = \bigcup_{j=1}^{m} s_{i_{\alpha_j}}$

The sequence of all the activity spaces of the stake holders is referred to as the activity profile S_α of the cloud.
$S_\alpha = (s_{1_\alpha}, s_{2_\alpha}, \ldots, s_{n_\alpha})$
The security measures each stake holder has to take must be accomplish-able with some combination of the legal actions that are available to him. It may involve one or more actions in tandem to be taken in each access area. The security measures in the access area $s_{i_{A_j}}$ the stake holder h_i has to take be the set $r_{i_{A_j}}$,
such that $r_{i_{A_j}} \subseteq s_{i_{a_j}}$.
Thus, the security activity a stake holder does in the access area $s_{i_{A_j}}$ is given by the tuple r_{i_α},
such that $r_{i_{\alpha_j}} = (r_{i_{A_j}}, r_{i_{a_j}})$.
Any practical security measure generally involves a sequence of actions across many activity areas to be effective. And the total security activity of the stake holder h_i is given by r_{i_A},
such that $r_{i_\alpha} = \bigcup_{j=1}^{m} r_{i_{\alpha_j}}$
The sequence of all the security activity spaces of the stake holders is referred to as the security activity profile S_α of the cloud.
$R_\alpha = (r_{1_\alpha}, r_{2_\alpha}, \ldots, r_{n_\alpha})$
A security measure by a stake holder can be cognized as an a priori plan of security actions at each access area. We distinguish security measure from the defense measure which happens, that is the series of executions of actions, *while* defending a system against a malfunction either due to an internal system fault or a malicious attack. Thus, this gives the context to make the plan considering the combined general risks and threats depending on the given system characteristics. Since there are different stake holders with having their own access spaces, either intersecting or not with that of other's, each must take their own security measures. This is described below. A security measure of the stakeholder h_i, is given by a sequences of actions taken at each instant of operation, that is, it has a time stamp in the operations, chosen from the security profile r_{i_α}. This security activity profile gives a formal way to represent quantitatively who can do what and where to defends which assets and how.The above frame work would be useful for the policy makers to confirm what security actions each stake holder would have to take. In the next section, we shall present a survey of the current literature how the activity space and security activity spaces are being used by stake holders in different scenarios.

III. Cloud based systems: architecture and security concerns

The architectures and the security concerns related to them go hand in hand. The more sophisticated the architecture is the more involved will be the security concerns.

A. Architectures

The general security and privacy concerns were identified and discussed along with the direction of research addressing them in [2]. They categorize the concerns as traditional security, availability and thried-party data control concerns. There is a new class of problems that are identified which are *cheap data and data analysis, cost effective defense of availability, increased aunthetication demands and mash-up authorization.* The *cheap data and data analysis* of unheard proportions enable even scantly equipped attacker huge information-advantage enabling a sophistication in the attack.*Cost-effective defense of availability* is a concern dealing with the counter measures against an attacker with the sole motive to sabotage activities. Since any disruption yeilds a positive payoff for the attacker, cloud crystallizes the problem to be that of a single point of failure. *Increased authentication demands* encourage the use of thin client at the client side. This emphasizes increased authentication demands on the cloud side.The cloud model encourages users to mash-up their data. *Mash-up authorization* will lead to problems of data-leaks and in terms of the number of sources of data a user may have to pull data from. To address these concerns *information-centric security, high-assurance remote server attestation and privacy-enhanced business intelligence* are identified as the fertile fields for further research.

The security concerns of each of the components constituting the cloud based system not only are pertinent but also new concerns are emerging. One of them is detectability of the hardware infrastructures hosting virtual machines (VM) delivering the payload of a client, leading to cross-VM side-channel attacks to extract information from another target VM on the same machine.This was explored practically by devising an attack launched over Amazon's EC2 to establish the vulnerability by [3].Its a potential breach to be careful about.

The main cloud computing security issues are fundamentally not new, and are tractable to the concerns in the previous time sharing era. But the complexities of multi party trust concerns, and ensuring the need for mutual audit-ability are distinct to cloud computing. These ideological analyses are done by [4].

An analyses of the major cloud provider for performance for the cost and the types of services offered was done in [5].

The vulnerability of using the standard TCP's congestion control is analyzed and showed to provide opportunities of DOS attacks and as an alternative, a network bandwidth allocation scheme called Seawall is presented in [6].

The configuration of the complex cloud infrastructure is important to be such that, it does not provide any security

holes to be exploited to gain undue information by malicious activity. An automated auditing process is provided to check the configuration in [7]

B. Security concerns

The main security risks concerning operations over cloud were topically pointed out in [8]. The security concerns for an enterprise wanting to move their infrastructure over a cloud, and the resulting risk management are discussed in [9]. The technicalities of the security threat are for most part a reincarnation of the previously known security issues in the older classical computing paradigms. An extension of such previous issues into modern cloud computing security issue is suggested to be mitigated by measures which also are inspired from the extending the previously done counter measures. The distinction of novelty of particular issues is discussed and presented in [10].

IV. Activity spaces

In this section we survey the current literature to get an idea of what the generic activity spaces are in the clouds. It is true that most of the cloud service providers tune up their system architecture to cater some specialized or emphasized services leading to disparate system setups. But we shall take a general consideration and pick the common factors to consider a generic cloud, for our analysis, which can be later customized diligently to any specific architecture with exact details filled in.

The role of the distributed data locations in the cloud architecture is provided and the need for data location compliance is studied in the thesis in [11]. In the Amazon EC2 in [12], Microsoft Azure and other prominent clouds used by many small and medium sized business systems, the cloud service provider takes care of all the hardware, either distributed or not, and the basic operating system that boots those hardware. Some times these hardware are provided by a third party. In that case, both the hardware and the software that boots on those hardware are provided by third parties. Over this operating system a hyper-wiser is used and controlled by the cloud service provider. This is the case in many public and (voluntary and non-profit) community based clouds. Then the cloud service provider provides a actualization through the hyper-wiser and a running operating system over it. This is going to be maintained by the cloud service provider, by installing regular updates and so on. Some of the software applications running on this operating system, as requested by and provided to, the business clients is given as their access space and activity space. Everything below this would be the access space of the cloud service provider if he has not outsourced the hardware and its maintenance to a third party. The business companies will install, run, and configure their applications and that whole space becomes their access area. The end users and clients of the business will be dealing with the companies, by accessing some instances of the software processes they are given, and the data structures they are entitled to access. This forms their access space and activity space.

A. Activity Profile

Activity profile is illustrated in the following works.

The analysis of mutual dependencies and the trustiness resource legitimacy in cloud computing is provided in [13]. Functionally, the activity profile imply the trustiness in an implicit manner. That is, each stake holder has agreed to do his bit and believes the others shall do theirs. This is reflected in many works that discuss how this trust is established, sustained, verified, maintained and actuated. The more complex constructions would be in inevitable but shall provide new challenges. Such moves will alter the activity profiles enormously. One such case is presented here. At the data link layer and network layer of the cloud, the trends of hybrid electrical/optical data-center networks pose many new challenges. An analyses of these with suggestions and directions towards plausible solutions is in [14]. Trusted block as a service in the context of cloud is discussed in [15]. A new trust model for file sharing in the cloud is discussed in [16]. Virtual machines need accounting and monitoring for ensuring authenticity and integrity. Eventually this should lead to bringing reliability, transparency and security in client model for client satisfaction. To do this a mobile agent based architecture is proposed which can dynamically move in the network to accomplish this task. The trust between the stake holders is an important issue. To dynamically assess it and implement decisions based on it, a mechanism is proposed based on mobile agents to collect the information in [17].

As a main concern of security, data integrity in cloud is important. For that, using third party data integrity Management Service (IMS) has its draw backs. To avoid it, a different cloud storage architecture was proposed with services and protocols and implemented on Amazon S3, with favorable results as presented in [18]. To address the problem of secure data transfer a trust-based file sharing is used. There are many open issues related to this approach which are discussed a new model is proposed in [16] Trustworthy clouds underpinning the future Internet from an overarching perspective is discussed in[19]. The data of the end user is kept on the resources of the cloud provider. to make is safe the user could encrypt his data. If the user wants to do any computation using that data on cloud resources itself, then he has to decrypt it and do the computation with the data. This nullifies the privacy of data. To avoid this, a homomorphic encryption scheme is proposed which allows the computations of data in its encrypted form in [20] To ensure the privacy for the data being stored over cloud by the user, the cloud service provider cannot be implicitly trusted. For this a model based upon the principle of dynamic data re-encryption is proposed in [21]. Another work on the business process as service and about remote auditing is presented in [22]. Accountability, Audit-ability and Trust between the stake holders is analyzed in [23]. TrustCloud, a frame work and a system was provided by HP in [23] to establish trust and co-ordinate the stake holders in cloud.

V. Security Activity Spaces

A comprehensive picture of the cross organizational, and the disparate stake holders, and their roles in the security activity is discussed in relation to cross-organizational security settings in [24] and their key roles elaborated in [25]. Public survey was made in two countries and an on line survey in more that 150 countries to identify the perception of the end users about the cloud. The results are discussed in [26], as the impression is a key factor in how the public users eventually adopt and turn out to use it. An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds is discussed in [27] and in [28]. Many parts of the clouds are very convenient to use for attacks leading to breach of privacy and confidentiality of others and unauthorized possession of copyrighted material. An example analysis of Dropbox is done in [29]. [30] reports on legal , privacy, security, access and regulatory issues. This paper raises an awareness of legal, privacy, security, access and regulatory issues that are associated with the advent of cloud computing. An in-depth literature survey is conducted on these and an analysis is drawn from the issues that are identified through the literature survey. Recommendations are then given on how the issues identified in the analysis can be mitigated. The issues of policy interventions, standards, privacy and data protection, traffic and congestion management, business continuity planning, security and regulation are discussed.

Working in various service models ranging from SaaS, PaaS, to IaaS, of cloud computing to mitigate data abuse, encryption is suggested. With data encryption, an issue arises when the data owner who outsourced the data wants to revoke some data-consumers' access privileges, which normally involves key re-distribution and data re-encryption. In this work, a generic scheme was proposed to enable fine-grained data sharing over the cloud, which does not require key-redistribution and data re-encryption whatsoever. The main primitives made use of are attribute-based/predicate encryption and proxy re-encryption, but our construction is not restricted to any specific scheme of its kind. A generic key distribution scheme with a number of advantages over other similar proposals in the literature in given in [31]. The methods of homomorphic encryption and computing on tamper-resistant hardware suffer from high latency. For outsourcing the data and arbitrary computation with lower latency a token based method was proposed in [32].

A. Security Activity Profile

The data availability issues in cloud computing is discussed and a RAID based model is proposed to address these issues along with error correction using parity encoding of the data in [33]. A rule-based-forwarding network design and an access control mechanism CloudPolice implemented in hypervisor to top DoS attacks is discussed in [34] To mitigate the security concern for running an application over cloud, the program is suggested to be run in two pieces as a user and protected program. It was shown to be computationally secure in [35]. The cloud-based infrastructure has to be eventually used by the business community. Those business which need to be ensured about the security can have to work flow certified by the auditors which is then accessible to the users to be ensured of the security. This end user perspective security measure is discussed in [36]. In massive parallel processing scenarios of cloud computing forensics are a challenge.An over view of the cloud Forensics is given in [37]. Technical issues with forensic in cloud is elaborated in [38]. Isolating instances in cloud for forensic is discussed in [39]. A survey on cloud forensics and critical criteria for cloud forensic capability is presented with a preliminary analysis in [40]. Mutual protection of the stake holders is an important security measure and is discussed in [41]. While many works deal with general issues, a specific attack like DoS is addressed in the following work in [42]. Based on the analysis of several recent attack scenarios, a system that enables periodic and necessity-driven integrity measurements and remote attestations of vital parts of cloud computing infrastructures is provided. It was implemented on top of Xen Cloud Platform and trusted computing technology is used to provide guarantees. The work show how system attests the integrity of a cloud infrastructure even in the presence of DoS attack.

VI. Related Work

The trust is an important factor between the many stake holders in cloud computing. The policy-making approaches with control mechanisms in place is discussed in [23] The security challenges and the recommended management models to address them are discussed in [43] An analysis of the cloud computing security problem was done in [44], where the perspective from the architecture of the cloud, services delivery models and the stake holders involved were listed. The analysis showed that the problem has a multi-layered and multi-perspective nature. In our work we are building upon what they identified as the stake holder's perspective and expanding the analysis of what factors affect it.

The cloud is used to provide different services, like infrastructure, services, etc and based on its location is classified as public, private and hybrid. Each of these distinctions get their own identity reflected in distinct security issues. The analysis of the security problem in cloud based systems is done based on the issues that have come up and different security models proposed to mitigate them are listed in [45]. A general discussion of the security challenges were presented in [46] where the information security, network security and the process and data security issues were identified.

VII. Conclusion

The feature of security is resolved in terms of how each stake holder is making secure practices and also how each of them are co-ordinated. An over all regulation is required to channelize the development and thus a need for a regulatory body is discussed in [47]. Thus, just the way the functional scope is now distributed amongst each of the

stake holders, the security or the breach of it depends on each of them. This knowledge is important to decide the best practices and policies for each of the stake holders.

References

[1] W A Jansen, "Cloud hooks: Security and privacy issues in cloud computing," Jan. 2011, pp. 1–10.

[2] *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*. ACM, 2009.

[3] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage, "Hey, you, get of my cloud: Exploring information leakage in third-party compute clouds," *CCS'09: Proceedings of 16th ACM conference on Computer*, 2009.

[4] Yanpei Chen, Vern Paxson, and Randy H. Katz, "What's new about cloud computing security?," *Technical Report No. UCB/EECS-2010-5*, 2010.

[5] Ang Li, Xiaowei Yang, Srikanth Kandula, and Ming Zhang, "Cloudcmp: Comparing public cloud providers," *IMC'10, Melborne, Australia*, 2010.

[6] Alan Shieh, Srikanth Kandula, Albert Greenberg, Changhoon Kim, and Bikas Saha, "Sharing the data center network," *NSDI*, 2011.

[7] Soren Bleikertz, Matthias Schunter, Christian W. Probst, Dimitrios Pendarakis, and Konard Eriksson, "Security audits of multi-tier virtul infrastructures in public infrastructure clouds," *CCSW'10, Chicago, Illinois, USA.*, Oct2010.

[8] Jon Brodkin, *Gartner: Seven cloud-computing security risks*, Retrived on 15 Feb, 2012. InfoWorld.com.

[9] Anthony Bisong and Syed M. Rahman, "An overview of the security concerns in enterprise cloud computing," *International journal of network security & its application*, vol. 3, no. 1, Jan 2011.

[10] F Maggi and S Zanero, "Rethinking security in couldy world," *Technical Report 2010, Departmento do Electronica e Informazione, Politecnico di Milano*, 2010.

[11] J. Noltes, "Data location compliance in cloud computing," M.S. thesis, University of Twente, Aug. 2011.

[12] Amazon.com, "Amazon web services: Overview of security processes," May2011.

[13] J. P. Yoon and Zhixiong Chen, "Service trustiness and resource legitimacy in cloud computing," Jan. 2011, pp. 250–257.

[14] Hamid Hajabdolali Bazzaz, Malaveeka Tewari, Guohui Wang, George Porter, T. S. Eugene Ng, David G. Andersen, Micheal Kamisky, Micheal A Kozuch, and Amin Vahdat, "Switching the optical divide: Fundamental challenges for hybrid electrical/optimal datacenter networks," *SOCC'11, Cascais, Portugal*, 2011.

[15] Jianan Hao and Wentong Cai, "Trusted block as a service: Towards sensitive applications on the cloud," *IEEE TrustCom/IEEE ICESS/FCST, International Joint Conference of*, vol. 0, pp. 73–82, 2011.

[16] Edna Dias Canedo, Robson de Oliveira Albuquerque, and Rafeal Timoteo de Sousa Junior, "Review of trust-based file sharing in cloud computing," *The fourth International Conference on Advances in Mesh Networks*, 2011.

[17] Priyank Singh Hada, Ranjita Singh, and Mukul Manmohan, "Article: Security agents: A mobile agent based trust model for cloud computing," *International Journal of Computer Applications*, vol. 36, no. 12, pp. 12–15, December 2011, Published by Foundation of Computer Science, New York, USA.

[18] S. Nepal, Shiping Chen, Jinhui Yao, and D. Thilakanathan, "Diaas: Data integrity as a service in the cloud," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, july 2011, pp. 308–315.

[19] Rudigger Glott, Elmar Husmann, Ahmad-Reza Sadeghi, and Matthias Schunter, "Trustworthy clouds underpinnning the future internet," *Future Internt Assembly,*, vol. LNCS 6656, pp. 209–221.

[20] Aderemi A Atayero and Oluwaseyi Feyisetan, "Security issues in cloud computing: The potentials of homomorphis encryption," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 10, pp. 546–552, October 2011, CSI Journal.

[21] Pitor Tysowski and M. A. Hasan, "Towards secure communication for highly scalable mobile applications in cloud computing systems," *Centre for Applied Cryptographic Research University of WAterloo, Tech Rep*, vol. CACR2011-33, 2011.

[22] R. Accorsi, "Business process as a service: Chances for remote auditing," 2011.

[23] Ryan K. L. Ko, Bu Sung Lee, and Siani Pearson, "Towards achieving accountability, auditability and trust in cloud computing," in *Advances in Computing and Communications*, vol. 193 of *Communications in Computer and Information Science*, pp. 432–444. Springer Berlin Heidelberg, 2011.

[24] Stefan Thalmann, Daniel Bachlechner, Lukas Demetz, and Ronald Maier, "Challenges in cross-organizational security management," *Hawaii International Conference on System Sciences*, vol. 0, pp. 5480–5489, 2012.

[25] S. Thalmann, D. Bachleehner, R. Maier, and M. Manhart, "Key roles in cross-organisational security settings," *European Security Conference*, 2011.

[26] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Capkun, "Home is safer than the cloud! privacy concerns for consumer cloud storage.," *Symposium on Usable Privacy and Security (SOUPS)*, 2001.

[27] Yogesh Simmhan, Alok Gautam Kumbare, Baohua Cao, and Viktor Prasanna, "An analysis of security and privacy issues in smart grid software architectures on clouds," *International Cloud Computing Conference (CLOUD).IEEE*, 2011.

[28] Alok Kumbhare, Yogesh Simmhan, and Viktor Prasanna, "Designing a secure storage repository for sharing scientic datasets using public clouds," Nov. 2011.

[29] Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar R. Weippl, "Dark clouds on the horizon: Using cloud storage as attack vector and online slack space," 8 2011.

[30] N Dlodlo, "Legal, privacy, security, access and regulatory issues in clod computing," Apr. 2011, Ted Rogers School of Management, Ryerson University.

[31] Yanjiang Yang and Youcheng Zhang, "A generic scheme for secure data sharing in cloud," in *Parallel Processing Workshops (ICPPW), 2011 40th International Conference on*, sept. 2011, pp. 145 –153.

[32] Ahmad-Reza Sadeghi, Thomas Schneider, and Marcel Winandy, "Token-based cloud computing," vol. 6101, pp. 417–429, 2010, 10.1007/978-3-642-13869-0_30.

[33] Anil Gupta, Parag Pande, Aaftab Qureshi, and Vaibhav Sharma, "A proposed solution: Data availability and error correction in cloud computing," *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 4, pp. 405–413, 2011.

[34] Lucian Popa, "Building extensible and secure networks," *Doctoral dissertation in Computer Science, University of California, Berkeley*, 2011.

[35] Kazuhide Fukushima, Shinsaku Kiyomoto, and Yutaka Miyak, "Towards secure cloud computing architecture – a solution based on software protection mechanism," *Journal of Internet Services and Information Securit*, vol. 1, no. 1, pp. 4–17, 2011.

[36] Rafael Accorsi and Yoshinori Sato, "Automated certification for compliant cloud-based business processes," Nov. 2011, vol. 3.

[37] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," *Advances in Digital Frensics*, vol. VII, 2011.

[38] D. Brik and C. Wegener, "Technical issues of forensic investigatinos in cloud computing environments," Tech. Rep., 2011.

[39] Waldo Delport, MS Oliver, and MD Kohn, "Isolating a cloud instance for a digital forensic investigation," in *Information Security for South Africa (ISSA2011) Conference on*, august. 2011, pp. 145 –153.

[40] Keyun Ruan, Ibrahim Baggili, Joe Carthy, and Tahar Kechadi, "Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis," May 2011, number Annual conference of the ADFSL Conference on Digital Forensics, Security and Law.

[41] Aiiad Albeshri and William Caelli, "Mutual protection in a cloud computing environment," in *IEEE International Conference on High Performance Computing and Communications*, 2010, number 12, pp. 308–315.

[42] R Neisse, D Holling, and A. Pretschner, "Implementing trust in cloud infrastructures," 2011, pp. 524–533.

[43] Kresimir Popovic and Zeljko Hocenski, "Cloud computing security issues and challenges," *The Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, pp. 344-349*, 2010.

[44] *An Analysis of the Cloud Computing Security Problem*, Nov. 2010.

[45] Puneet Jai Kaur and Sakshi Kaushal, "Security concerns in cloud computing," *High Performance Architecture and Grid Computing*, vol. 169, pp. 103–112, 2011.
[46] L Ertual, S Singhal, and G. Saldamli, "Security challenges in cloud computing," *WORLDCOMP 2010*, 2010.
[47] Bikramjit Singh, Rizul Khanna, and Dheeraj Gujral, "Cloud computing: A need for a regulatory body," in *High Performance Architecture and Grid Computing*, vol. 169 of *Communications in Computer and Information Science*, pp. 119–125. Springer Berlin Heidelberg, 2011.