A Comprehensive Review on Trust Issues, Security and Privacy Issues in Cloud Storage

K.Suresha
Department of Computer Science and Engineering
D R R Government Polytechnic
Davanagere, Karnataka, India-577004

P.Vijayakarthick
Department of Information Science and Engineering
Sir M Visveswaraya Institute of Technology
Bangalore, Karnataka, India

Abstract:- Now a days everywhere talking about cloud computing paradigm and if you look at business enterprises there are lot of initiatives to put everything on a cloud computing . Most of the IT industries are insisting to adopt cloud computing in their business operations. A Cloud Computing is a one infrastructure which can cater to the need of many people and it can do different varieties of services and functionalities such as ,it can store for you, it can compute for you, importantly it can scale for your need, so cloud computing means a provision of infrastructure which is scalable and it can do different varieties of services. A major challenge today in providing cloud computing is data security, access control and privacy of users data, so first we need to identify what are the security issues, security threats and security vulnerabilities present in cloud computing ,after identifying and analyzing all these issues we have to propose a solution model which will provide data security ,access control and data privacy in cloud computing. Information security is one of the significant imperatives for re-appropriated information in a distributed storage condition.

This paper addresses key concerns that are presumed to have long haul pertinence to distributed computing security and protection on the basis of established concerns and vulnerabilities. The main aim of this paper is to highlight key security , privacy and trust concerns in current cloud computing environments and to help users understand the tangible and intangible risks associated with their use, including those associated with cloud computing. (a)Survey the most important protection, security and trust gives that present dangers to current distributed computing conditions and (b) Analyze how these possible risks to privacy , security and confidence can be handled and provide a high level of security, confidence and reliability in the cloud computing world. In the near future, we will further examine and evaluate privacy, protection and trust problems in the cloud computing environment through a quantifiable methodology, further build and deploy comprehensive security, privacy trust assessment, management system for truly cloud computing environments.

Keywords:- *Access Control, Trust Issues, Security Threats, Vulnerabilities, Multitenancy, Virtualization.*

I. INTRODUCTION

Cloud computing has been characterized as “A Model for enabling Convenient, On-demand Network access to a Shared pool of Configurable Computing resources (e.g., Networks, Servers, Storage, Applications, and Services) that can be Rapidly Provisioned and Released with Minimal management effort or Service Provider Interaction” [61]. Cloud computing should be seen as a digital computing paradigm with implications for greater flexibility and lower cost availability. And of this, cloud computing has attracted a lot of coverage lately. Cloud computing services benefit from economies of scale gained by efficient utilization of infrastructure, specialization and other productivity. However, the evolution of distributed computation is only in its infancy. Today , the term itself is still used for a variety of meanings and interpretations[33]. Three widely cited service models have been built [58, 78, 85] Software-as-a-Service (SaaS) facilitates a software implementation platform in which one or more programmes and computer resources are provided for use on demand as a turnkey service. This will reduce the total costs of hardware and software development, repair and service. Platform-as-a-Service (PaaS) facilitates a software implementation paradigm in which the programming platform is distributed as an on-demand service where applications can be developed and implemented. It will reduce the cost and complexity of buying, housing, and managing the hardware and software components of the network.

Infrastructure-as-a-Service (IaaS) promotes a software delivery paradigm in which the core computing infrastructure of servers, applications and network equipment is provided as an on-demand service on which application development and execution mechanisms can be based. It may be used to avoid common hardware and software infrastructure components from being purchased, stored and controlled.

Cloud computing should be entirely used as a private platform in a corporate computing environment. However, it should be apparent from the service models that the key thrust of cloud computing is to provide the external party with the means to outsource aspects of the setting. And for the outsourcing of information technology resources, there is anxiety about the implications for data security and privacy; In fact, the transfer of sensitive programmes or data from the company's computer center to another organization’s computer center. While cost savings are the primary justification for converting to a cloud provider, there should be no savings in terms of protection or privacy. In the end , the organization is responsible for the overall state of the outsourced operation. Monitoring and resolution of security and privacy problems remain the responsibility of the company; as do other important issues, such as performance, availability, and recovery.

Cloud computing, a long-standing "computing as a service" idea, has opened a new era in future computing, transformed a large part of the IT market, reshaped the buying and use of IT software and hardware, and drawn substantial interest from global and local IT participants, national governments and international agencies[1,3,4].Cloud computing is a large- Cloud computing is a wide scale distributed computing paradigm powered by economies of scale in which a pool of abstracted, virtualized, seamlessly elastic, highly available, configurable and reconfigurable computing services can be quickly generated and published with limited management effort in data centers. Services are delivered on demand via high-speed Internet to external customers with a "X as a Service (XasS)" machine architecture divided into three segments: "applications", "platforms" and "infrastructure." The objective[3][4] is to provide consumers with more flexible installations, more extensible software for computing , storage and networks in a straightforward manner. Similarly, it is no longer sufficient for IT businesses with creative concepts for new application technologies to make substantial capital outlays in hardware and technological infrastructure.

Cloud servers with access to physical files, identification and certificate processing , data authentication, tempering, integrity , security, negligence and information leakage are involved in these problems. To secure private and sensitive data stored in data centres, the cloud customer needs to verify (a) the true truth of the cloud computing system in the world. (b) cloud storage of information; and (c) stability of software in the field of cloud computing. However, in cloud data centres, data and resources control is not safe and accurate.

This paper addresses important cloud infrastructure-related security and privacy challenges as they extend to outsourcing parts of the organizational computing environment. It identifies areas of interest that need extra consideration and makes educated security decisions with the appropriate context. In this paper, trust issues in current cloud computing environments are primarily involved and help users understand the tangible and intangible risks associated with their uses. Our contributions can be summarized as: (a) surveying the most significant privacy, security and trust issues that pose threats in current cloud computing environments; and (b) examining how these potential security, privacy and trust risks can be handled and provide a highly Secure, Trustworthy and efficient cloud storage.

The rest of this paper is arranged as follows. Section II poses data security issues and fixes them. In cloud computing, Section III raises data privacy problems and discusses them. In cloud computing , Section IV raises trust or confidence problems and addresses. Section V raises data availability issues Finally , in Section VI, conclusions and guidance for future work are given.

II. DATA SECURITY ISSUES

Data security is used as a composite term, including 'a mixture of privacy, the prevention of unauthorized exposure of information, integrity of information, the prevention of unauthorized alteration or deletion of information, and the prevention of unauthorized withholding of information'[13]. Data protection is the lack of unwanted access to, or handling of, the state of the system. The main dimensions of security are efficiency, secrecy and integrity. One of the biggest challenges to opening the new era of the long-dreamed view of computers as a service is security.

Cloud computing security issues can be categorized into six sub-categories [5,6,7,11,14], including: (a) how to provide cloud service access or tracking protection measures, (b) how to keep all entities and confidential information secret, (b) how to keep data private, (c) how to deter malicious insiders from illegal actions due to the general lack of transparency in the provider system (d) how to prevent hijacking of networks, where phishing, malware and harassment are well-known IT issues, (e) how to manage multi-instances in multi-tenancy network environments that assume that all instances are completely separated from each other. However, this principle will also break down, allowing attackers to cross virtual machines' side channels, circumvent the sandboxed environment restrictions, and have full access to the host, and (f) how to develop appropriate regulations and implement regulatory jurisdiction, such that consumers, if required, have a chain against their vendors.

In a global network related to data from other consumers, data stored in the cloud typically exists. Organizations that transfer confidential and monitored data to the cloud must therefore take care of the means by which data access is handled and the information is kept secure.

➢ *Data-Isolate:*

Data can take a variety of forms. Cloud-based application development, for instance, requires application programmes, templates, and setup settings, as well as software for development. This includes documentation and other material created or used by apps for deployed apps, as well as account records for application users. One way of keeping data secure from unauthorized users is access controls; encryption is another. Data Access Controls are normally Identity-based, making verification of the User's Identity an important problem in cloud computing.

Database ecosystems that are used in cloud computing can vary greatly. For instance, some settings adopt a multi-instance model, while others adopt a model of multi-intent. For each service customer, the former provides a particular database management system operating on a VM perhaps, granting the customer direct control over job definition, user permission, and other administrative tasks relevant to security. For a cloud service customer, the latter creates a predefined environment that is shared with other users, usually by marking data with a user ID.

For databases, there are various types of multi-tenant arrangements available. A type pools resources differently, delivering varying amounts of separation and utilization of services[26, 65]. Also, other considerations apply. Some features, such as data encryption, for example, are only feasible with agreements that use separate databases rather than shared ones. This forms of tradeoffs imply that the suitability of the data management system with the data concerned be carefully considered. The choice of storage and data organization used in the application is likely to be influenced by criteria in certain fields, such as health care. Data that is responsive to privacy is usually a big problem[52].

When at rest, in transit and in usage, data must be secured and access to data must be controlled. Communication protocol standards and public key certificates allow cryptography to secure data transfers. However, specifications for data storage at rest are not as well standardized, making interoperability an issue due to the predominance of proprietary programmes. Lack of interoperability impacts the availability of data and complicates the portability of applications and data between cloud service providers. Cryptographic key management is currently primarily the responsibility of users in cloud providers. Using hardware authentication modules that do not scale well to the cloud model, key generation and storage is usually done outside the cloud. Research work underway to define extensible and functional Cryptographic secret key manage and interchange techniques to government use that would potentially helping to resolve the obstacles. The security of information usage considered as evolving field of Cryptography with little experimental results to give, confidence technique is the key protection [22].

- *Data-Sanitize:*

There is strong safety ramifications for the data sanitization protocols implemented by the service supplier. Sanitize is the withdrawal from a storage facility of sensitive data in a variety of ways, such as when a storage unit is removed from use or relocated for storage to another venue. It also applies to backup copies made for the service's recovery and restoration and to the residual data left after the service 's termination. Data from one subscriber is physically combined with data from other users in a cloud computing arrangement, which can complicate matters. With sufficient expertise and tools, for example , data may be recovered from damaged drives that are not adequately disposed of by service providers.

- *Data Location:*

This issue is one of the popular complying problems challenging a company as the position of valuable data [30, 51]. The usage of an in-house database center enables the organization to coordinate its processing system and to consider in detail where the information is stored and the safeguards used to safeguard the information. A feature of many cloud storage services, on the other hand, is that precise knowledge about the status of an entity 's data is either unavailable or not disclosed to the service subscriber. This situation makes it impossible to assess whether effective safeguards are in place and whether there is consistency with legal and regulatory enforcement requirements. To a degree, external audits and security certifications may address this problem, but they are not a panacea.

It is incredibly difficult to guarantee protection under international laws and regulations if sensitive data crosses the borders of countries. For instance, the expansive powers of the USA Patriot Act have concerned some foreign governments that the regulations would allow the U.S. government access to private information outsourced to American businesses, such as medical records[5]. The limitations on the trans-border flow of non-classified confidential data and data confidentiality requirements have become the subject of national and international privacy and security laws and regulations[12]. Key concerns related to cross-border data transfers include whether the regulations in the jurisdiction where data is gathered allow data to flow, whether such regulations continue to relate to post-transfer data, and whether there are external challenges to the regulation at the destination[12]. Technical, physical and institutional protections are also implemented, such as access restrictions. For example , European data protection laws may impose additional responsibilities relating to the handling and processing of European data transmitted to the United States[9].

III. DATA PRIVACY ISSUES

Privacy is the privilege of a individual or a group to distinguish themselves or knowledge regarding themselves and, therefore, to reveal themselves selectively, including[15]: (a) where: a participant might be more anxious with the exposure of their present or future information than information from the past; (b) how: a user might be comfortable when friends may inquire for their information manually, but may not want to notify. (c) scope: the user may have their information documented as a generic area rather than a particular point; in the business, consumer and privacy sense, the protection and proper usage of customer information and the satisfaction of the customer's requirements about its use are required. Privacy in organizations requires the application of guidelines, protocols, standards and processes for the management of publicly identifiable information[8].

Depending on the different cloud contexts, privacy issues vary and can be categorized into four subcategories[5][6][8], including: (a) how to keep consumers in charge of their data when collected and processed in the cloud, and how to avoid infringement, misuse and unauthorized resale (b) how to ensure the reproduction of data in a jurisdiction and in a reliable state that it is normally possible to replicate consumer data at a variety of acceptable locations and to avoid data destruction, misuse and unwanted modification or manufacture; (c) which party is responsible for enforcing security requirements for personal information;

IV. TRUST ISSUES

Trust is seen as a measurable faith that uses knowledge to make trustworthy decisions. Originally used in social science to create a connexion between human beings, it is now an important alternative for the development of security mechanisms in distributed computing environments. Since confidence has many soft security features, such as confidentiality, reliability , integrity, fairness, confidence, integrity, protection, competence, and so on.. Indeed, the bond of trust between persons is the most complex since it is extremely contextual, context-dependent, non-symmetrical, uncertain and partly transitive[9,10].

Trust evaluation is a multi-faceted and multi-phase process based on multi-dimensional variables and the length of the trust assessment, and is used to find the answer to the question "What node(s) should I associate with and what should I not associate with?" The observable perception of trust is adapted by [16], "Trust of Party A to Party B to Service X is A's observable expectation that B behaves consistently". Another perception of mathematical confidence is provided in[17],' Confidence (or, symmetrically, distrust) is a simple degree of subjective probability in which an agent determines whether a particular action will be carried out by another agent or a group of agents, both before it is able to monitor such an action (or independently or in its ability to monitor it) and in a way in which it affects its own action.' Standard hard security techniques such as encryption and permission have a stable cloud defence mechanism, but they fail when cooperating entities operate maliciously due to the scale and transient existence of collaborations.

Through mitigating the role of hostile actors in communications and thereby providing a highly trustworthy cloud computing system, Trust will combat such security challenges as a soft social security philosophy. Trust issues can be categorised into four subcategories of cloud computing environments[5][6,8,12], including: (a) how to define and measure trust based on the unique feature of cloud computing environments; b) how to deal with highly sensitive malicious recommended data in cloud computing environments, as cloud trust is variable and unpredictable, (c) how to recognize and provide the extent of difference in service security compared to the degree of trust, (d) how to deal with the change in the degree of trust with touch time and meaning, and how to track, adjust, and completely reflect the complicated change in trust relationship with time and space.

A business relinquishes complete power of some areas of protection under the cloud infrastructure paradigm and, in doing so, confers an unprecedented degree of confidence on the service provider.

➢ *Insider Access*:

Data collected or maintained outside the limits of an entity, the firewall and other security mechanisms are combined with an intrinsic level of risk. For most companies, the insider protection problem is a well-known issue which, beyond its name, often extends to outsourced cloud services[21,54]. Insider risks range to those faced by current or former workers and include company partners, suppliers, and other persons who have had access to the networks, systems , and data of the enterprise to carry out or facilitate activities. It is also possible to cause accidents inadvertently. Moving data and information to an external cloud storage facility improves not only the staff of the service provider, but also likely other business customers, with the possibility of insider protection. For eg, it has been seen that an internal denial of service attack against the Amazon Elastic Compute Cloud (EC2) entails a service user creating an initial 20 accounts and launching instances of virtual machines for each, then these accounts are used to build an additional 20 accounts and system instances to extend and rapidly absorb resources[76].

➢ *Composite Services:*

Nesting and layering of other cloud providers may be made up of cloud services themselves. A SaaS provider might build its services on PaaS or IaaS cloud resources , for example. Issues can emerge from cloud service providers subcontracting their services to third-party service providers, including the scope of third-party management, the duties involved, and the solutions and remedies available. Furthermore, confidence is not transitory, ensuring that third-party arrangements be updated before entering into an arrangement with the service provider and that the terms of certain arrangements be maintained in the course of the relationship or unless fully informed of any planned changes. For composite cloud providers, responsibility and performance expectations may become a serious concern. This situation is illustrated by Linkup, an online storage facility that closed after its 20,000 users lost access to a vast volume of data. The exact responsibility for the cause of the failure was uncertain because another organisation, Nirvanix, hosted the data for The Linkup, and another, Savvis, hosted its application and database[18].

➢ *Visibility:*

Migration to cloud computing provides the service provider with control over the networks on which the enterprise's data and software operate. They must be introduced in accordance with those used by internal organisational systems in order to avoid causing gaps in security, administration, operational and technological controls. The problem is overwhelming, because the metrics used to assess the security of the two computer systems are an evolving research area[27]. Furthermore, the user's network and system level access is typically outside the reach of most service arrangements, explicitly affecting exposure and the means of auditing operations. Service arrangements should have a means of making the compliance protocols and mechanisms implemented by the service provider more visible, as well as their reliability over time , to ensure that policies and procedures are enforced over the device lifecycle.

➢ *Risk Management:*

Some subsystems or subsystem components for cloud-based applications are outside the direct control of an organisation who controls the knowledge and authorises the usage of the software. When they have greater control of the systems and equipment involved, often individuals are more at ease with risk. In the very least, when faced with an event, a high degree of management provides an incentive to weigh choices, set priorities and behave decisively in the company's best interest. The related uncertainties need to be analysed in detail before choosing between an in-house approach versus a cloud-based implementation. It may be a struggle to evaluate and mitigate risk in cloud-based systems. Ideally, the level of trust depends on the degree to which the organisation is able to exert full control over the external service supplier in relation to the use of the security measures necessary for the protection of the operation and the evidence on the effectiveness of those controls[29]. However, the proper operation of the module and the efficiency of security measures can not be tested as closely as in the operational framework, and the degree of confidence must be contingent on other considerations.

V. AVAILABILITY ISSUES

In basic words, availability means an individual has a wide set of accessible and functional computer services at all times. Disponibility can be temporarily or indefinitely compromised and impairment may be partial or absolute. Service denial attempts, system outages and natural disasters are always a challenge to availability.

➢ *Temporary Outages:*

Cloud computing services can and do experience failures and performance slowdowns, despite the use of architectures designed for high service reliability and availability[58]. Amazon's Easy Storage Infrastructure (S3) and EC2 systems experienced a three-hour shutdown in February 2008, which in turn impacted the usage of systems by Twitter and other start-up companies[55,63]. The lightning storm in June 2009 caused a partial EC2 blackout, impacting some users for 4 hours[64]. Similarly, the failure of the Salesforce.com storage cluster prompted a shutdown in February 2008 for several hours and a more brief shutdown in January 2009 due to the failure of the network device[31,37]. Owing to networking problems related to updates, Microsoft's Azure cloud service encountered major loss for approximately 22 hours in March 2009[24].

At a standard 8.76 hours of downtime is expected in one year at a level of 99.999 percent reliability. In the organisation's contingency plans to manage the repair and rehabilitation of disrupted cloud systems and processes using alternate networks, facilities and sites, the extent of stability of a cloud infrastructure as well as its backup and recovery capability should be taken into account. For software stored there, cloud computing systems may be a single point of failure. In such situations, data maintained by the primary provider may be backed up by a second cloud storage provider to ensure that data is available for rapid resumption of critical operations after a sustained disruption or significant disaster at the primary level.

➢ *Prolonged and Permanent Outages:*

A service provider may encounter severe issues, such as bankruptcy or lack of services, disrupting the service for extended periods of time or triggering a full shutdown. The FBI raided data centres in Texas in April 2009, for example, and seized hundreds of computers to pursue fraud claims against a range of businesses working out of the centers[86]. Hundreds of other firms who were not involved in the probe yet had the misfortune of getting their network activities located in the targeted centres were interrupted by the raid. The major data loss suffered by magnolia, the Bookmark archive service and the sudden failure of Omni drive, an online storage company that collapsed in 2008 without warning to its users[37, 58], are other examples.

➢ *Denial of Service*:

Application denial attacks include saturating the target with fake requests to discourage it from responding to genuine requests in a timely manner. Typically, to launch an intrusion, an attacker requires multiple computers or a botnet. In order to defend from and raise costs, even a failed distributed denial of service attack will potentially absorb a large amount of money. In certain cases, complex cloud provision makes it possible for an attacker to do damage. While cloud services are valuable, They could be flooded with enough computers to attack[28]. For example, during an obvious denial of service attack on the underlying Amazon cloud infrastructure, a denial of service attack on Bit Bucket, a code hosting site, culminated in an interruption of more than 19 hours of downtime [19, 62]. There could be denial of service attacks against proprietary networks, such as those used in cloud computing, in addition to publicly available networks. A denial of service attack against the computer programming interface of Amazon Cloud Services, for instance, occurred, involving system instances replicating themselves exponentially[76]. As an attack vector, the centrally assigned non-routable addresses used to manage services within the network of the service provider can also be used. For elements of one cloud, the worse probability is to target that of another or to target all of its own elements[45].

VI. CONCLUSION AND FUTURE WORK

Any of the biggest security issues have receded into the past and remain unanswered while demonstrating the savings and performance gains of the cloud. Several important pieces of technology, such as a federated confidence system, have not been fully implemented yet, impacting successful implementations. A long-standing security challenge that overshadows large-scale computation in general is now deciding the security of sophisticated computer systems. For information protection experts and professionals, the accomplishment of high quality standards in software has been an inescapable goal and is still a work in progress for cloud computing. The reliability of the cloud infrastructure depends on powerful computation and cryptography. Organizational data must be protected in a way compliant with the practises of the service centre of the enterprise or the cloud. There is no clear support arrangement encompassing the breadth of available cloud services and the demands of different entities. A useful starting point[51] is to provide a list of common outsourcing requirements, such as privacy and security guidelines, compliance and compliance issues, service quality criteria and fines, change management procedures, quality of service operation, and the right to cancel. In some ways, conversion to a cloud storage infrastructure is a risk assessment practise. The research makes use of both qualitative and quantitative elements. Risks must be carefully balanced against the safeguards available and future advantages, with the assumption that the organisation is responsible for security. So many restrictions, if the advantages outweigh the costs and associated risks, may be disruptive and risky. Maintaining an appropriate compromise between the strength of the controls and the relative risk associated with each programme and procedure is crucial.

High security remains one of the key obstacles to opening up the modern era of the long-dreamed view of computers as a good. As essential systems and data are migrated to cloud storage centres, they run on virtual computing services in the form of a virtual computer. These unusual aspects, however, introduce many new security concerns, such as accessibility vulnerabilities, virtualization vulnerabilities, and mobile apps vulnerabilities. With the growth of cloud computing and the rising number of cloud users, stability, privacy and trust aspects can continuously grow. Paragraphs L shall be indented. Both the paragraphs, that is, both left-justified and right-justified, must be justified. The cloud user wants to verify (a) the true existence of the world's cloud computing environment; (c) the security of cloud data; and (b) the security of cloud storage services to secure the sensitive and sensitive data contained in data centres.

In this article, we intend primarily to illustrate the main security , privacy and confidence challenges in modern cloud computing environments and help users understand the tangible and intangible threats associated with their use. Two key facets of confidentiality, safety and confidence issues are discussed, including: (a) surveying the most significant data, protection and confidence problems raised by challenges in modern cloud computing environments; (b) identifying how these future technology, privacy and trust risks can be resolved, and creating a highly stable , secure and effective ecosystem for cloud computing.

Future studies will concentrate on the following: (a) reviewing and assessing privacy, security and trust concerns in the cloud computing world from a quantifiable methodology; the survey and review methodology presented in this paper is a first step towards analysing privacy, security and trust concerns (b) introducing maximum defence, faith evaluation of privacy, management's privacy issues and (c) the application of a framework in the actual world of cloud computing.

REFERENCES

[1]. Foster I, Zhao Y, Raicu I, Lu, S. Cloud Computing and Grid Computing 360-degree compared. Proceedings of the Grid Computing Environments Workshop, GCE 2008; IEEE Press, Nov. 2008, 1-10.

[2]. Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009;25(6):599–616.

[3]. Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM; 2010;53(4):50–58.

[4]. Mell P, Grance T. The NIST Definition of Cloud Computing. Communications of the ACM; 2010;53(6):50.

[5]. Paquette S, Jaeger P T, Wilson S C. Identifying the security risks associated with governmental use of cloud computing.Government Information Quarterly; 2010;27(3):245–253.

[6]. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications; 2011;34(1):1–11.

[7]. Vaquero L M, Rodero-Merino L, Morán D. Locking the sky: A survey on IaaS cloud security. Computing; 2011;91(1):93–118.

[8]. Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010; IEEE Press, Nov. 2010, 693-702.

[9]. Ahamed S I, Haque M M, Endadul Hoque M, Rahman F, Talukder N. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments. Journal of Systems and Software ; 2010;83(2):253–270.

[10]. Karaoglanoglou K, Karatza H. Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values. Journal of Systems and Software; 2011;84(3):465–478.

[11]. Takabi H, Joshi J B D, Ahn G. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;8(6):24–31.

[12]. Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments.Communications in Computer and Information Science; 2010;54:255–265.

[13]. Algirdas A, Jean-Claude L, Brian R, Carl L. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing; 2004;1(1):11–33.

[14]. Tchifilionova V. Security and privacy implications of cloud computing - Lost in the cloud. Proceedings of the IFIP WG 11.4 International Workshop on Open Research Problems in Network Security, iNetSec 2010; Springer Verlag Press, Mar.2010,149-158.

[15]. Krumm J. A survey of computational location privacy. Personal and Ubiquitous Computing; 2009;13(6):291–399.

[16]. Shekarpour S, Katebi S D. Modeling and evaluation of trust with an extension in semantic web. Journal of Web Semantics;2010;8(1):26–36.

[17]. Iltaf N, Hussain M, Kamran F. A mathematical approach towards trust based security in pervasive computing environment. Proceedings of the Third International Conference and Workshops, ISA 2009IEEE Press, Jun. 2009, 702-711.

[18]. J. Brodkin, Loss of Customer Data Spurs Closure of Online Storage Service 'The Linkup,' Network World, August 11,2008, http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1

[19]. C. Brooks, Amazon EC2 Attack Prompts Customer Support Changes, Tech Target, October 12, 2009, http://searchcloudcomputing.techtarget.com/news/article/0,289142,sid201_gci1371090,00.html

[20]. M. Calore, Ma.gnolia Suffers Major Data Loss, Site Taken Offline, Wired Magazine, January 30, 2009, http://www.wired.com/epicenter/2009/01/magnolia-suffer/

[21]. D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats,3rd Edition, Version 3.1, CERT, January 2009, http://www.cert.org/archive/pdf/CSG-V3.pdf

[22]. USA Patriot Act Comes under Fire in B.C. Report, CBC News, October 30, 2004, http://www.cbc.ca/canada/story/ 2004/10/29/patriotact_bc041029.html

[23]. R. Chow et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security, Chicago, IL, November 2009

[24]. [24]G. Clarke, Microsoft's Azure Cloud Suffers First Crash, The Register, March 16, 2009, http://www.theregister.co.uk/ 2009/03/16/azure_cloud_crash/

[25]. S. Cocheo, The Bank Robber, the Quote, and the Final Irony, nFront, ABA Banking Journal, 1997 http://www.banking.com/aba/profile_0397.htm

[26]. Safe Harbor Privacy Principles, U.S. Department of Commerce, July 21, 2000, http://www.export.gov/safeharbor/eg_main_018247.asp

[27]. J. E. Dunn, Ultra-secure Firefox Offered to UK Bank Users, Techworld, February 26, 2010, http://news.techworld.com/security/3213740/ultra-secure-firefox-offered-to-uk-bank-users/

[28]. J. E. Dunn, Virtualised USB Key Beats Keyloggers, Techworld, February 22, 2010, http://news.techworld.com/security/3213277/virtualised-usb-key-beats-keyloggers/[29] M. P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions, Hunton & Williams LLP, The Outsourcing Institute, February 15,2005,

[29]. M. P. Eisenhauer, Privacy and Security Law Issues in Off-shore Outsourcing Transactions, Hunton & Williams LLP, The Outsourcing Institute, February 15, 2005, http://www.outsourcing.com/legal_corner/pdf/Outsourcing_Privacy.pdf

[30]. P. Ferrie, Attacks on Virtual Machine Emulators, White Paper, Symantec Corporation, January 2007, http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

[31]. T. Ferguson, Salesforce.com Outage Hits Thousands of Businesses, CNET News, January 8, 2009, http://news.cnet.com/8301-1001_3-10136540-92.html

[32]. S. Frei, T. Duebendorfer, G. Ollmann, M. May, Understanding the Web Browser Threat, ETH Zurich, Tech Report Nr. 288, 2008, http://e-collection.ethbib.ethz.ch/eserv/eth:30892/eth-30892-01.pdf

[33]. G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009

[34]. S. Gajek, M. Jensen, L. Liao, and J. Schwenk, Analysis of Signature Wrapping Attacks and Countermeasures, IEEE International Conference on Web Services, Los Angeles, CA, July 2009

[35]. T. Garfinkel, M. Rosenblum, When Virtual is Harder than Real, HotOS'05, Santa Fe, NM, June 2005

[36]. S. Garfinkel, An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS, Technical Report TR-08-07, Center for Research on Computation and Society, Harvard University, July 2007

[37]. D. Goodin, Salesforce.com Outage Exposes Cloud's Dark Linings, The Register, January 6, 2009, http://www.theregister.co.uk/2009/01/06/salesforce_outage/

[38]. D. Goodin, Webhost Hack Wipes Out Data for 100,000 Sites, The Register, June 8, 2009, http://www.theregister.co.uk/2009/06/08/webhost_attack/

[39]. A. Greenberg, IBM's Blindfolded Calculator, Forbes Magazine, July 13, 2009

[40]. N. Gruschka, L. L. Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited, IEEE International Conference on Web Services, Los Angeles, CA, July 2009

[41]. M. Gunderloy, Who Protects Your Cloud Data?, Web Worker Daily, January 13, 2008, http://webworkerdaily.com/2008/01/13/who-protects-your-cloud-data/

[42]. Twitter Email Account Hack Highlights Cloud Dangers, Infosecurity Magazine, July 23, 2009, http://www.infosecurity-magazine.com/view/2668/twitter-email-account-hack-highlights-cloud-dangers-/

[43]. D. Jacobs, S. Aulbach, Ruminations on Multi-Tenant Databases, Fachtagung für Datenbanksysteme in Business, Technologie und Web, March 2007, http://www.btw2007.de/paper/p514.pdf

[44]. W. Jansen, Directions in Security Metrics Research, Interagency Report 7564, National Institute of Standards and Technology (NIST), April 2009

[45]. M. Jensen, J. Schwenk, N. Gruschka, L. L. Iacono, On Technical Security Issues in Cloud Computing, IEEE International Conference on Cloud Computing, Bangalore, India, September 21-25, 2009

[46]. Guide for Applying the Risk Management Framework to Federal Information Systems, Joint Task Force Transformation Initiative, Special Publication 800-37, Revision 1, NIST

[47]. B. R. Kandukuri, R. Paturi V, A. Rakshit, Cloud Security Issues, IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009

[48]. [48]P. A. Karger, I/O for Virtual Machine Monitors: Security and Performance Issues, IEEE Security and Privacy, September/October 2008

[49]. N. Katz, Austin Plane Crash: Pilot Joseph Andrew Stack May Have Targeted IRS Offices, Says FBI, CBS News, February 18, 2010, http://www.cbsnews.com/8301-504083_162-6220271-504083.html?tag=contentMain%3bcontentBody

[50]. Y. Keleta, J. H. P. Eloff, H. S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf

[51]. S. M. Kerner, Mozilla Confirms Security Threat from Malicious Firefox Add-Ons, eSecurity Planet, February 5, 2010, http://www.esecurityplanet.com/news/article.php/3863331/Mozilla-Confirms-Security-Threat-From-Malicious-Firefox-Add-Ons.htm

[52]. S. King et al., SubVirt: Implementing Malware with Virtual Machines, IEEE Symposium on Security and Privacy, Berkeley, California, May 2006

[53]. B. Krebs, Salesforce.com Acknowledges Data Loss, Security Fix, The Washington Post, November 6, 2007

[54]. E. Kowalski et al., Insider Threat Study: Illicit Cyber Activity in the Government Sector, Software Engineering Institute, January 2008, http://www.cert.org/archive/pdf/insiderthreat_gov2008.pdf

[55]. M. Krigsma, Amazon S3 Web Services Down. Bad, Bad News for Customers, ZDNET, February 15, 2008, http://blogs.zdnet.com/projectfailures/?p=602

[56]. S. Labaton, 2 Men Held in Attempt to Bomb I.R.S. Office, New York Times, December 29, 1995

[57]. 20-Year Term in Plot to Bomb IRS Offices, Nation In Brief, Los Angeles Times, August 10, 1996

[58]. N. Leavitt. Is Cloud Computing Really Ready for Prime Time?, IEEE Computer, January 2009

[59]. R. McMillan, Salesforce.com Warns Customers of Phishing Scam, PC Magazine, IDG News Network, November 6, 2007, http://www.pcworld.com/businesscenter/article/139353/salesforcecom_warns_customers_of_phishing_scam.html

[60]. R. McMillan, Hackers Find a Home in Amazon's EC2 Cloud, Infoworld, IDG News Network, December 10, 2009, http://www.infoworld.com/d/cloud-computing/hackers-find-home-in-amazons-ec2-cloud-742 Hospital, PC Magazine, NewsServiceSept.17,2009,http://www.pcworld.com/businesscenter/article/172185/misdirected_spyware_infects_ohio_hospital.

[61]. P. Mell, T. Grance, The NIST Definition of Cloud Computing, Version 15, October 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing

[62]. C. Metz, DDoS Attack Rains Down on Amazon Cloud, The Register, October 5, 2009, http://www.theregister.co.uk/ 2009/ 10/05/ amazon_bitbucket_outage/

[63]. R. Miller, Major Outage for Amazon S3 and EC2, Data Center Knowledge, February 15, 2008, http://www.datacenterknowledge.com/archives/ 2008/02/15/ major-outage-for-amazon-s3-and-ec2/

[64]. R. Miller, Lightning Strike Triggers Amazon EC2 Outage, Data Center Knowledge, June 11, 2009, http://www.datacenterknowledge.com/archives/2009/06/11/lightning-strike-triggers-amazon-ec2-outage/

[65]. J. Oberheide, E. Cooke, F. Jahanian, Empirical Exploitation of Live Virtual Machine Migration, Black Hat Security Conference, Washington, DC, February 2008

[66]. T. Ormandy, An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments, 2007, http://taviso.decsystem.org/virtsec.pdf

[67]. S. Overby, How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010, http://www.cio.com/article/591629/How_to_Negotiate_a_Better_Cloud_Computing_Contract

[68]. S. Pearson, Taking Account of Privacy when Designing Cloud Computing Services, ICSE Workshop on Software Engineering Challenges of Cloud Computing, May 23, 2009, Vancouver, Canada

[69]. N. Provos et al., The Ghost In The Browser: Analysis of Web-based Malware, Hot Topics in Understanding Botnets (HotBots), April 10, 2007, Cambridge, MA

[70]. N. Provos, M. A. Rajab, P. Mavrommatis, Cybercrime 2.0: When the Cloud Turns Dark, Communications of the ACM, April 2009

[71]. Security Within a Virtualized Environment: A New Layer in Layered Security, White Paper, Reflex Security, retrieved April 23, 2010, http://www.vmware.com/files/pdf/partners/security/security-virtualized-whitepaper.pdf

[72]. T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, ACM Conference on Computer and Communications Security, November 2009

[73]. VMware Vulnerability in NAT Networking, BugTraq, Security Focus, December 21, 2005, http://www.securityfocus.com/archive/1/420017

[74]. A. Shah, Kernel-based Virtualization with KVM, Linux Magazine, issue 86, January 2008, http://www.linuxmagazine.com/w3/issue/86/Kernel_Based_Virtualization_With_KVM.pdf

[75]. T. Shelton, Remote Heap Overflow, ID: ACSSEC-2005-11-25 - 0x1, http://packetstormsecurity.org/0512-advisories/ACSSEC-2005-11-25-0x1.txt

[76]. M. Slaviero, BlackHat presentation demo vids: Amazon, part 4 of 5, AMIBomb, August 8, 2009,http://www.sensepost.com/blog/3797.html

[77]. J.D.Sutter,TwitterHackRaisesQuestions about 'Cloud Computing', CNN, July 16, 2009, http://edition.cnn.com/2009/TECH/07/16/twitter.hack/

[78]. L. M. Vaquero1, L. Rodero-Merino1, J. Caceres, M. Lindner, A Break in the Clouds: Towards a Cloud Definition, Computer Communication Review, January 2009, http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf

[79]. K. Vieira, A. Schulter, C. Westphall, C. Westphall, Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society, August 26, 2009.

[80]. VMware Hosted Products and Patches for ESX and ESXi Resolve a Critical Security Vulnerability, VMware Security Advisory,VMSA-2009-0006, http://www.vmware.com/security/advisories/VMSA-2009-0006.html

[81]. P. Wainewright. Many Degrees of Multi-tenancy, ZDNET News and Blogs, June 16, 2008, http://blogs.zdnet.com/SAAS/?p=533

[82]. J. Wei et al., Managing Security of Virtual Machine Images in a Cloud Environment, ACM Cloud Computing Security Workshop, Nov. 13, 2009, Chicago, IL

[83]. L. Whitney, Amazon EC2 Cloud Service Hit by Botnet, Outage, December 11, 2009, CNET News, http://news.cnet.com/8301-1009_3-10413951-83.html

[84]. Xen Architecture Overview, Version 1.2, Xen Wiki Whitepaper, February 13, 2008, http://wiki.xensource.com/xenwiki/XenArchitecture?action=AttachFile&do=get&target=Xen+Architecture_Q1+2008.pdf

[85]. L. Youseff, M. Butrico, D. D. Silva, Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, held with SC08, November 2008. http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf

[86]. K. Zetter, FBI Defends Disruptive Raids on Texas Data Centers, Wired Magazine, April 7, 2009, http://www.wired.com/threatlevel/2009/04/data-centers-ra/