Secrecy of Data in Cloud Computing – Trends & Research

Ms. Charanpreet Kaur

Mr. Amandeep Singh

Dr. Shalu Tandon

Associate Professor, Don Bosco Institute of Technology

Ms. Poonam Arora

Assistant Professor, Don Bosco Institute of Technology

Dr. Vikas Rao Vadi

Professor, Don Bosco Institute of Technology

ABSTRACT

Cloud computing environment is a new way in which web base enable applications provide as a service for the users with low computational cost through internet. As we store data and it also provide services in distributed environment. Cloud ease its users by providing virtualization technology of resources through internet. Cloud computing is the emerging field, due to this reason the various new techniques are still developing. At current scenario new security challenges were increases for cloud professionals. Due to lack of security in cloud computing environment user of cloud lost it trust in cloud. Multi-tenancy, elasticity, Security Performance and Optimization, etc. are various security issues in cloud computing. In this paper we will discuss some of the issue incloud. This paper also discusses some of the existing security technique for securing a cloud and help researchers and professionals to know about various security threats.

Keywords

Cloud Computing; Security; Trusted Computing; Data integrity, confidentiality; survey.

1. INTRODUCTION

Cloud computing is fast becoming a popular option for renting of computing and storage infrastructure services (called Infrastructure as a Service or IaaS) for remote platform building and customization for business processes (called Platform as a Service or PaaS)]; and for renting of business applications as a whole (called Software as a Service or SaaS) The economic casefor cloud computing has gained widespread acceptance.Cloud computing providers can build large datacenters at low costdue to their expertise in organizing and provisioning computationalresources. The economies of scale increase revenue for cloudproviders and lower costs for cloud users. The result in on-demandmodel of computing allows providers to achieve better resource utilization through statistical multiplexing, and enables users to avoid the costs of resource over-provisioning through dynamic scaling. At the same time, security has emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing. This view originates from perspectives as diverseas academia researchers, industry decision makers, and governmentorganizations. For many business-critical computations, today’s cloud computing appears inadvisable due to issues such as service availability, data confidentiality, reputation fate sharing, and others.To add to the confusion, some have coitized the term “cloud computing” as too broad. Indeed, cloud computing does include established business models such as *Software as a Service*, and the underlying concept of on-demand computing utilities goes back as far as early time-sharing systems. At the same time, the lack of consistent terminology for cloud computing has hampered discussions about cloud computing security. Thus, security criticisms of cloud computing have included a murky mix of ongoing and new issues. This context frames the genesis of our paper.We recognize that security poses major issues for the widespread adoption of cloud computing. However, secure or not, cloud computingappears here to stay. Thus, our ambition is to get past terminology issues and attempt to sort out what are actually new security issues forcloud computing, versus broader and more general security challengesthat inevitably arise in the Internet age. Our goal is to advance discussions of cloud computing security beyond confusion, and to some degree fear of the unknown, by providing a comprehensive high-level view of the problem space. We ground the development of our viewpoint in a survey of contemporary literature on cloud computing security, coupled with are view of historical work on early time-sharing systems and virtual machine monitors. Contemporary discussions reveal security concerns that are indeed “new” relative to computing ofthe past decade; however, looking back several decades, many contemporary challenges have quite similar historical counter parts. We build the case that few of the security problems arising in cloud computing are in fact new, even though satisfactory solutions for many still will require significant development. The combined contemporary and historical viewpoints allow us to identify a number of research topics that deserve more attention. On the other hand, we argue that two facets are to some degree new and fundamental to cloud computing: the complexities of multi-party trust considerations, and the ensuing need for mutual auditability.

There is a growing body of work dealing with various cloudcomputing security issues. Authors have mostly discussed about singular aspects of cloud security such as vulnerabilities in platform layer (virtualization, network, or common software stacks); vulnerabilities with co-located user data and multi- tenancy; access control; identity management and so on. However, barring a few there has not been a holistic treatment on cloud security issues and state of research in eachof these issues. In this paper we provide a concise but all-round surveyon cloud security trends and research. We observe that data, platform, user access and physical security issues; although accentuated in cloud computing; are generally applicable in other enterprise computing scenario as well. For example, hypervisor related threats such as cross channel attacks will be present in any virtualized environment not specific to cloud. Two of the great virtues of cloud computing are service abstraction and location transparency. However, from security point of view these two points in conjunction with third-party control of data can create challenging security implications. The paper outlines how research around Trusted Computing, Information Centric Security and Privacy Preserving Models may provide answer to some of these difficult challenges. Since private clouds are operating inside enterprise firewalls, we exclude them from this discussion.

2. COMMON CONCERNS ABOUT CLOUD SECURITY AND IMPLICATIONS

We divide the common security issues around cloud computing across four main categories:

a) Cloud infrastructure, platform and hosted code. This comprises concerns related to possible virtualization, storage and networking vulnerabilities. We cover vulnerabilities that may be inherent in the cloud software platform stack and hosted code, which gets migrated to cloud. We also discuss the physical data-center security aspects here.

b) Data. This category comprises the concerns around data integrity, data lock in, data remanence, provenance, and data confidentiality and user privacy specific concerns.

c) Access. This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management.

d) Compliance. Because of its size and disruptive influence, cloud is attracting attention from regulatory agencies, especially around security audit, data location; operation trace-ability and compliance concerns.

We believe that through this categorization we cover almost all common cloud security issues. To provide a perspective on why these issues are important; from cloud consumer (enterprises), providers, and third party points of view; we first lay out the paramount top-level security concerns (mainly on part of consumers and third party agencies) and sub-levels thereof with anecdotal evidences. We then discuss the technologicalimplications (mainly on part of the cloud providers) of each of these concerns and related research issues. We defer discussion onsome of the “cloud specific” advance research discussion to the next section.

Enterprise customers looking at public and hybrid clouds are generally accustomed to elaborate security arrangements in their data centers in forms of single sign-on technologies, identity management, and VLAN to separate different customer domains, storage appliances, VPN technologies etc. These provide a strong infrastructure for role-based access, logical partitioning of networks, controlled data and application, secure remote access etc. The situation with cloud gets fuzzy.

2.1 Concern C1: Is my cloud-services providers’ physical and software infrastructure secured?

A recent survey carried out by Novell [7], 87% enterprise respondents looked as hybrid clouds as a future data center evolution while 92% say that internal IT will eventually get migrated to public cloud. However, *nine* out of *ten* respondents have also voiced their concerns on security. Migrating applications to cloud and hosting those in remote multi-tenant environment raise concerns like:

C11: *Are the cloud data centers physically secured against security breaches?*

C12: *How is my application secured in shared virtualized infrastructure (VMs, storage, network) against malicious attacks?*

Implication I1*:* Secure physical computing, storage and network access environment.

Typical data-center related security measures related to physical access, layouts of racks, servers and network redundancy and isolation, intrusion detection and prevention systems, backup and disaster recovery contingency, HVAC related issues are required. The TIA-942: Data Center Standards Overview [8] describes the requirements for the data center infrastructure. It is expected for sensitive and critical customers to come into public cloud, the cloud must meet these criteria adequately to address concern C11. It is often noted that major security breaches and threats come from internal staff. A stringent set of checks and audit processes are required for this purpose.

To tackle C12, the IaaS cloud providers should ensure that virtualized infrastructure is secure against anyone exploiting known and emerging vulnerabilities. These are vulnerable to exploitations and attacks. Malicious code can detect presence of a hypervisor and launch attacks such as denial of service or even exit from the protected environment to garner higher privileges [9]. A group of researchers have exploited network topology and VM placement strategy in Amazon cloud. They have taken recourse to *who is* queries, TCP synch messages, and other internal / external probes and fairly static internal IP allocations of EC2 availability zones to map and target physical hosts of specific guest VMinstances. They then “planted” malicious VMs in a co- located manner and exploited shared zones and covert channels such as time-shared catches to gain processing information [10]. Service providers also need to guard against general and common OS and VM vulnerabilities such as reported vulnerabilities like in insecure named pipes, SSL related issues in the type 1 (emulated hypervisors) and HVM (hardware virtualization) monitors, reported serious flaws etc.

2.2 Concern C2: What happens to my data in cloud?

In today’s competitive economy, data is the primary asset enterprises and individuals possess. In cloud computing, foremostconcern is about data integrity, confidentiality and privacy, and provenance. There is a growing worry about the confidentiality of data stored in public cloud server-side infrastructure. Additionally, mechanisms facilitating intermittent connectivity,like Google Gears [14], cache data on the devices. Unless the cached data is effectively secured and purged regularly, it can become a treasure trove for data theft.

It is mandated that providers like Google, Yahoo, and AOL retain search data for 18 months before anonymizing it (removing specific client info like IP addresses and cookies) for internal purpose, if any. However, there have been instances where even anonymized data has been compromised. Perhaps the most famous case is when anonymized health records fromMassachusetts Group Insurance Commission were analyzed to reveal the medical history of the Governor of that state [5]! This case proved that injecting innocuous and neutral data such as ZIP code, gender, birth-date into anonymized data can reveal sensitive information. Other concerns are those around data lock-in and data location. To cite an example on data lock-in [15], 45% users of an online storage service company Link up suffered when their locked data with a third-party storage provider called Nirvanix gotlost.

Implication I2: Ensure proper access control and identity management.

Synchronizing enterprise and external cloud services access control lists in the context of C31 to ensure right access roles is a very important challenging issue as PaaS and SaaS platforms have complex hierarchies and many fine-grained access capabilities (tenant org level, sub-tenant, and individual user levels). This assumes importance as users, who are no longer part of an enterprise, may still potentially exploit access provided in cloud; unless those credentials are revoked quickly. However, we recognize this as more of a process issue than a technology one. Use of standard languages like Service Provisioning Markup Language promoted by OASIS, can enable faster user account provisioning and de-provisioning.

Cloud service authentication presents some interesting problems. Cloud services are increasingly getting accessedthrough browsers and thin mobile devices running new set of applications like HTML-5. Browsers do not have direct means of handling XML signatures and XML encryption, and rely on the underlying SSL layer for handshake. Hence this channel maybecome a potential threat if not secured properly. This may push enterprises to use VPNs while communicating to cloud. The Cloud Security Alliance [20] recommends cloud provider to provide stronger authentication mechanism and also (optionally) allow users to use third party identity management and single sign-on platforms like Microsoft Passport. This may lead to an added set of authentication complexity. Online open identity management communities like OpenID [21], OAuth [35] etc. are proliferating and each brings its own set of integration challenges for cloud providers.

There is a growing chorus on “inter cloud” hand-offs and federated identity management possibly through assertion tokens like Security Assertion Markup Language (SAML) or privilege management infrastructure based on x.509 certificates. The ongoing standardization work WS-federation may provide some help in this aspect. Cloud federations need to establish a set of common security token services and identity providers. But in dynamic cloud scenario these trust relations maynot work. We need to develop more flexible cases of identity federation.

3. ADVANCED ISSUES IN CLOUD COMPUTING SECURITY

In the previous section, we have discussed generic set of security concerns observed in public and hybrid clouds. We now turn our focus to some atypical cloud specific security issues. In particular,cloud does bring out a set of unique challenges like:

- Abstraction: Cloud provides an abstract set of service end-points. For a user, it is impossible to pin-point in which physical machine, storage partition (LUN), network port MAC address, switches etc. are actually involved. Thus, in event of security breach, it becomes difficult for a user to isolate a particular physical resource that has a threat or has been compromised.
- Lack of execution controls: The external cloud user doesnot have fine-gained control over remote execution environment. Hence the critical issues like memory management, I/O calls, access to external shared utilitiesand data are outside the purview of the user. Client would want to inspect the execution traces to ensure that illegal operations are not performed.
- Third-party control of data: In cloud, the storage infrastructure, and therefore, the data possession is also with the provider. So even if the cloud provider vouches for data integrity and confidentiality, the client may require verifiable proofs for the same.
- Multi-party processing: In multi-cloud scenario, one party may use part of the data which other party provides. In absence of strong encryption (as data is being processed), it becomes necessary for participating cloud computing parties to preserve privacy of respective data.

To build a strongly secure cloud computing model and tackleissues such as above, we postulate that cloud groups will need to address the issues of trust, create context specific access model within data and preserve privacy. In this section, we discuss three specific areas of security research; namely; *Trusted Computing*, *Information Centric Security* and *Privacy Preserving Models* and show the implications for cloud computing.

Trusted computing: It is a set technology being developed andpromoted by Trusted Computing Group (TCG). To tackle theconcern of un-trusted execution environment, trusted platform modules enable a strong endorsement key to attest users to a host and host to users. This is called *remote server attestation*. All subsequent execution on an attested host-user pair can then be validated through *trusted path* mechanism. Trusted virtual machine monitors like *Terra*] allow strong isolation at VM layer. Integrity and confidentiality of data stored in cloud can either be secured through sealed storage [27] or by making authenticity checks when accessing data. Checksums are useful mechanisms for this. However, checksums are costly to compute and can only be used after transmission of full data to the client (costly for network). New techniques such as Provable Data Possession (PDP) in untrusted cloud may be a more efficient mechanism as it generates a probabilistic proof for data integrity based on only a small portion of the file [29]. Similarly there are research works around Proof of Retrievability (PoR) to give customer some semblance of assurance that once data is stored ina public cloud, it will be eventually retrievable proof carrying codes is another mechanism through which the cloud provider host can verify user applications through formal proofs.

Information centric security (ICS): As information in the public cloud is stored outside of organizational boundaries, we need to insert context specific access metadata in the information itself. Strong encryption of the entire data may not be useful as thedata is often processed in cloud in un-encrypted form which makes it vulnerable. One way of achieving ICS would be to use Policy based or Role based access controls which can be defined in a language like Extensible Access Control Markup Language (XACML) which governs context-based access rules in policy enforcement point of the data. Any access request to the data can then be verified through an assertion or by checking with central server. Another way could be to add access control metadata in the form of Cryptographic Message Syntax (CMS) It is more compact than XML, and is flexible enough to freely add users to the “read” list as long as each user possesses a cryptographic key pair. .

Privacy preserving models: In cloud computing data processing collaboration is often required across sources which have complementary sources of data (like distributed data mining). In multi-party processing, the data hosting parties may even be passive adversaries – they trust each other and fulfill the contracts, but may want to gain “extra” information out of other party data. Research around secure multi-party computation [32]seeks to create a randomized bit-level partition scheme for the data. The random data, even if aggregated (using XOR or other method) at the other party site, does not elicit any useful information. Yet another scenario is where content originated from a customer and encrypted with customer’s public key meant for cloud A is passed / routed through cloud B (which is providing a gateway service). It may be necessary for cloud provider B to carry out some select keyword search activity to process the request better. For example, searching for and finding the keyword “urgent” in the message may mean a different processing logic. Research in “searchable encryption” models is useful here. When a cloud tenant downloads / updates privatedata from a cloud database, it may be possible for another “curious” database user to trace back what the user is up-to and gain information about the data set. In other words, in spite of partitioning techniques and access control mechanisms; nodatabase is *private* in information theoretic sense unless a user gets the full copy of the private database and makes update – which is impractical. Recent research around using replicated and distributed copies of databases shows that a query can however beformed across the sets which can’t be guessed with reasonable computational complexity by another party. These privacy preserving models and research are increasingly becoming important in multi-cloud information processing cases.

4. MORE ISSUES

With such a wide spectrum of concerns, an enterprise has to be very careful in assessing potential security threats to its applications on a cloud. A three steps approach will help in rigorous security assessment:

Cloud computing has various cloud security issue. In most applications, confidential data is stored at servers. Securing data is always vital importance. So many challenges regarding security. Leakage of confidential data fatal many computing systems today. For example, last year marks a peak in data breaches about 740 million records were exposed, the largest number till now.

A. Multi Tenancy

Multi tenancy is built for reasons like allocation of resources sharing of memory, storage and distributed computing. It provides effective utilization of hardware components, and maintain cost is very low. It gives distribution of resources, services and application with other components residing on same physical/logical platform at service providers. Thus, it breaches the confidentiality of data and leakage of information and this causes the possibility of attacks.

B. Insider Attacks

Cloud computing is a multitenant based model that is provided by the service provider. So, the threat of leakage of formation arises within the organization. There are no rules for hiring cloud employees. So, an organization can easily hack by the third-party vendor, due to this the data of one organization cannot be safe. It’s leads loss of information of user, confidentiality, integrity and security. This attack is difficult to defend and the solution of this attack is no found yet.

C. Outsider Attacks

This is also one of the major issues in an organization. Data are resided in server and this confidential data of an organization in open to other. In Clouds there many interfaces, so cloud is differed from a private network. One of the disadvantages is that hackers and attackers to exploiting the API, weakness and this result breaking in connection.

D. Elasticity

When a system is adaptable to changing environment. In this resource are provisioned by the user as their requirement. In this synchronization of available resources and current demand occurs. It implies scalability, and users are able to scale up and down as requirement. Due this scaling tenants use a reusable resource.

E. Network level attacks

During resource pooling process all data or services flow over the network needs to be secured from attacker to prevent the breaching of sensitive information or other susceptibilities.

a) Man, in the Middle attack: It is also a category of eavesdropping. The attacker set up the connection between both victims and makes conversation. Attacker making they talk directly but infect the conversation between them is controlled by attack.

b) Brute force attack: In this attack when attacker want to find the password it will try all possible combination of password until correct password not found.

c) Distributed denial of service attack: In this attack, servers are down due to huge amount of network traffic. This attack is classified into two broad categories based on protocol level which they targeted one is Network level attack and another is application level attack.

F. Hardware Based Attack

It is one of the most frequently discovered vulnerabilities in cloud which direct result of language and programs that are as follows.

a) Trojan horses/Malware: They are the unauthorized program that are contained or injected by malicious user within valid program to perform unknown and unwanted function. Unlike viruses it does not replicate themselves.

b) XML Signature wrapping Attack: Protocol like SOAP that use XML format to transfer the request for services are attack by this type of attacks. In this, attack moves the original body of SOAP message to newly inserted wrapping element writing within SOAP header attack perform in new body.

5. TECHNIQUE TO SECURE DATA IN CLOUD COMPUTING

Cloud computing as a platform for outsourcing and remote processing of application and data is gaining rapid momentum. Security concerns; especially those around platform, data and access; can prove to be hurdles for adoption of public and hybrid clouds. In this paper, we have tried to categorize the key concerns and discuss the related technical implications and research issues, including some advanced security issues specific to cloud. We have also discussed some issues regarding security-related regulatory compliance in cloud. Additionally, we have presented few high-level steps towards a security assessment framework.

We made several observations in current cloud security landscape. Firstly, the security standardization activities, under aegis of manystandard bodies and industry forums like CSA, OGF, W3C, SNIA etc. are fragmented. Proliferation of open community, based identity management solutions also makes cloud identity management and integration difficult. Second, quick provisioning of the users in cloud and mapping of their roles between enterprise and cloud has become somewhat complicated. Third, Data anonymization and privacy preserving techniques will increasing assume greater importance and more mainstream research is required in this area. Fourth, migrating generic in- house software code to public cloud require through understanding of potential security risks. Finally, adherence to the regulatory compliance by the cloud providers and better disclosure norms from them is imperative for commercial success of cloud. On the other hand, we observe the virtualization related security risks are not specific to cloud, but risks related to open- source shared application server, DB and middleware components definitely are; and a Trusted Computing Platform to execute / isolate client run-times in cloud will definitely help.

We believe that this survey, though short, provides a broad-level overview of important current and emerging security concerns in cloud and delineate main research challenges. As a subsequent work a more elaborate survey can be undertaken. We also plan to flesh out the assessment framework further, supported by tools – to aid migration of enterprise applications to cloud.

6. STEPS TOWARDS AN SECURITY ASSESSMENT FRAMEWORK

With such a wide spectrum of concerns, an enterprise has to be very careful in assessing potential security threats to its applications on a cloud. A three steps approach will help in rigorous security assessment:

Step 1: Characterize the application's security requirements: Each application has different security requirement. E.g. security requirements for an e-commerce portal hosted on an IaaS are quite different from a hybrid cloud scenario where a cloud-hosted data analytics application interacts with databehind the enterprise firewall. It is important to identify if the current application requires compliance to domain-specific security and data protection policies like HIPPA, SAS 70 etc. Further, one should determine if the application requires a fully encrypted communication and if the application's interaction withother applications (cloud hosted or on-premises) requires secure communication (e.g. HTTPS / SSL). Furthermore, the use Single Sign-on using SAML or non-SAML techniques need to be determined. Security requirements become stringent when applications require role-based access, particularly in a multi- cloud scenario or a hybrid cloud scenario. Access modes to the application characteristics – whether web, mobile, or mixed – also determine the additional security protocols the application needs to support. It is important to perform a security vulnerability analysis of the application to identify security loopholes. In a typical web-application, one should assess all three tiers – web application tier assessment for loopholes in CGI scripts, HTML/JSP/JavaScript loopholes etc., source code analysis of the business tier and database security assessment. For example, clear-text passwords and configuration files, often overlooked in secure enterprise computing, should be avoided in cloud

Step 2: Characterize and review cloud provider's security strengths and vulnerabilities: Based on a mix of techno-commercial factors, the enterprise can decide on various cloud environments – IaaS, PaaS and SaaS – for potential hosting of applications. In selection of the cloud environment, security becomes an important factor. Similar to Step 1, it is essential to characterize provider's security offering. In doing so, it is good to perform an in-depth security analysis across infra and platform, data, and access layers of the provider; on concerns depicted in section 2 of this paper. Such an analysis can be done by going through published documentation (security controls, protocol compliance and standard operating procedures) or by employing services of commercial / open-source cloud auditing agencies (such as *http://www.cloudaudit.org)*. Further, published audit reports and case studies, if available, provide an analysis of the provider's „on-ground‟ adherence to security best-practices and techniques. One also needs to keep the local cyber-security and data location laws in mind. Cloud Security Alliance has also created a cloud Governance, Risk Management and Compliance (GRC) toolkit, supported by checklists and questionnaire, for cloud migration audit.

Step 3: Map application's security characteristics and cloud security characteristics to perform a fit analysis: Once the application and cloud provider assessments are performed, a fit analysis can be done to determine the best cloud- services provider for an application or class of applications from asecurity perspective. For enterprises that publish applications to cloud, as well as for the cloud providers, protocols like Security Control Automation Protocol (SCAP), promoted by NIST [39], should be a good choice for organizing, expressing, and measuring security-related information in standardized ways.

7. TECHNIQUE TO SECURE DATA IN CLOUD COMPUTING

A. Encryption Algorithm

We that cloud service provider encrypt user's data using a strong encryption technique but, in some circumstances, encryption accidents can make data completely useless and on the other side encryption it also complicated. As this task is challenging cloud provider must provide proof that encryption technique was design and properly tested by knowledgeable and experience authority.

B. Authentication and Identity

The most common method of authentication of users is cryptography. Through cryptography, authentication is provided between communicating systems. Passwords is one of most common form of authentication of users individually.

Other form authentication is security token, or in the form a biometric like fingerprint etc. This traditional identity approaches are not sufficient respect to cloud environment,when the enterprise uses multiple cloud service providers (CSPs). In this synchronizing of identity information not scalable. Infrastructure is also one of major concern when we shifting toward traditional approach to cloud-based.

C. Scrutinize Support

Checking of illegitimate activities is a difficult task. When users store their data in the provided cloud, they store data in server and they don't have the information where the data is stored. Therefore, cloud service provider must provide inspection tools to the users to scrutinize and control various policy implementation.

8. CONCLUSION AND FUTURE WORK

Cloud computing is the effective technology which depend on cost, time and performance. It gives benefit to the users of cloud and of course the practice of cloud computing will surely will increase more in next few years. In this paper we have discussed and examine thebasic of cloud computing and issues regarding securities in the cloud computing. Some security issues are the very crucial in the cloud computing. Privacy and integrity of data are the especially key concern security issues. In the cloud as data is stored in server and we don't know the exact location of the data resided, due to this data stored in the cloud has a threat of being accessed or theft by unauthorized person during transmission.

.

9. REFERENCES

[1] Amazon Elastic Compute Cloud web services at *http://aws.amazon.com/ec2*

[2] Sales Force Force.com Platform as a service at *http://developer.force.com*

[3] NetSuite SaaS portal at *http://www.netsuite.com*

[4] Gartner Data Quest Forecast on Public Cloud Services Doc

IDG00200833, June 2, 2010

[5] Chow,R.,Gotlle,P.,Jakobsson, E.S.,Staddon,J., Masuoka,R., and Molina,J.;2009, Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009.

[6] Gellman, R., Privacy in the Cloud: Risks to Privacy andConfidentiality in Cloud Computing. *Technical Report prepared for World Privacy Forum*, 2009

[7] C. Hong, M. Zhang, and D. Feng, AB-ACCS: A cryptographic access control scheme for cloud storage, (in Chinese), Journal of Computer Research andDevelopment, vol. 47, no. 1, pp. 259–265, 2010.

[8] Enrique Jimenez Domingo and Minguel LagaresLemos, CLOUDIO: A Cloud Computing-oriented Multi-Tenant Architecture for Business Information Systems In Proc. of the 23rdInternational Conference on Cloud Computing pages 532-533.IEEE, 2010.

[9] D. Feng, Y. Qin, D. Wang, and X. Chu, Research on trusted computing technology, (in Chinese), Journal of Computer Research and Development, vol. 48, no. 8, pp. 1332–1349, 2011. [13] Naresh vurukonda and B. Thirumala Rao, in 2nd International Conference on Intelligent Computing, Communication & Convergence,ICCC 2016**.**

[10] Raj Kumar Buyya, Rajiv Ranjan, Rodrigo N. Calheiros,"Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities", in the 2009 International Conference on High Performance Computing and Simulation, HPCS 2009, pp:1-

[11] Telecommunication Industry Association, TIA-942: Data Center Standards Overview at *http://tiaonline.org*

[12] Carpenter, M., Liston, t., and Skoudis, E, Hiding Virtualization from Attackers and Malware. *IEEE Security and Privacy Magazine*, 2007

[13] Ristenport, T., Tromer, E., Shacham, H., and Savage, S., Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *Proceedings of the16th ACM conference on Computer and Communication Security*, 2009

[14] MIT Exo-kernel operating system. Documentation at *http://pdos.csail.mit.edu/exo.html*

[15] Czajkowski, G., Application Isolation in the Java Virtual Machine. *ACM SIGPLAN Notices, vol 35, issue 10*. Oct 2000

[16] M. Jensen, N. Gruschka, and R. Herkenh¨oner, A survey of attacks on web services, *Computer Science Research and Development (CSRD), Springer Berlin/Heidelberg*. 2009.

[17] Google Gears at *http://gears.google.com*

[18] http://www.zdnet.com/blog/projectfailures/mediamax-the-linkup-when-the-cloud-fails/999

[19] IBM Homomorphic Encryption research page at *http://domino.research.ibm.com/comm/research_projects.nsf /pages/security.homoenc.html*

[20] Plank, J.S., Erasure codes for Storage Applications,Tutorial given at *FAST-2005: 4th Usenix Conference on File and Storage Technologies* San Francisco, CA. December, 2005

[21] Zhong, S., Yang, Z., and Wright, R., Privacy-Enhancing *k* – anonymization of Customer Data, *Proceedings of the 24th ACM Symposium on Principles of Databases*. 2005

[22] Storage Network Industry Alliance at *http://www.snia.org*

[23] Cloud Security Alliance at *http://www.cloudsecurityalliance.org*

[24] OpenID foundation website at *http://www.openid.net*

[25] http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

[26] http://epic.org/privacy/cloudcomputing/google /ftc031709.pdf

[27] http://ciocoo.com/clouds-and-data-jurisdiction-282/.

- Ruan, K., Cloud Forensics : Challenges and Opportunities, *Presentation from Center of Cybercrime and Investigation*. University College, Dublin

[28] Open Grid Forum‟s OCCI specification at *http://www.occi-wg.org/*

[29] Trusted Computing Group at *http://www.trustedcomputinggroup.org*

[30] Garfinkel, T., Pfaff,B., Chow, J., Rosenblum, M., and Boneh,D., Terra: A Virtual Machine-Based Platform for Trusted Computing, *Proceedings of ACM Symposium on Operating Systems Principles*. 2003

[31] Ateniese, G., Burns, R., and Curtmola, R., Provable Data Possession in Untrusted Stores, *Proceedings of the 14th ACMconference on Computer and Communication Security*,2007

[32] Necula, G., C., Proof-carrying code, *Proceedings of 24th ACM SIGPLAN-SIGACT symposium on Principles of Programming Languages*, 1997

[33] Cryptographic Message Syntax standard at *http://www.ietf.org/rfc/rfc2630.txt*

[34] Lindell, Y., and Pinkas, B., Privacy Preserving Data Mining, *Proceedings of 20th Annual International Cryptology Conference*. 2000

[35] Boneh, D., and Crescenzo, G., D., Public Key Encryptionwith Keyword Search, *Proceedings of Advances in Cryptology, EuroCrypt 2004*. Lecture Notes in ComputerScience, Springer

[36] Chor, B., Goldreich, O., Kushilevitz, E., and Madhu Sudan,*Proceedings of the 36th Annual 1EEE conference on foundation of Computer Science*. 1995

[37] OAuth community site at *http://www.oauth.net*

[36] *http://blogs.wsj.com/digits/2009/03/08/1214/*

[37] Reddy, K.K.M, Macko, P., and Seltzer, M., Provenance forthe cloud, *Proceedings of the 8th USENIX conference on File and storage technologies*, 2010

[38] http://www.oasis-open.org/committees/provision/

[39] National Institute of Standards and Technology at *http://www.nist.gov.*