2011 IEEE World Congress on Services

Cloud Computing Security - Trends and Research Directions

Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma
Accenture Technology Labs
Accenture
Bangalore, India
Email: {shubhashis.sengupta, vikrant.kaulgud, vibhu.sharma}@accenture.com

***Abstract*—Cloud Computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud adoption is real and perceived lack of security. In this paper, we take a holistic view of cloud computing security - spanning across the possible issues and vulnerabilities connected with virtualization infrastructure; software platform; identity management and access control; data integrity; confidentiality and privacy; physical and process security aspects; and legal compliance in cloud. We present our findings from the points of view of a cloud service provider, cloud consumer, and third-party authorities such as Govt. We also discuss important research directions in cloud security in areas such as Trusted Computing, Information Centric Security and Privacy Preserving Models. Finally, we sketch a set of steps that can be used, at a high level, to assess security preparedness for a business application to be migrated to cloud.**

***Keywords*-Cloud Computing; Security; Trusted Computing; Data integrity and confidentiality; Survey;**

I. Introduction

Cloud computing is fast becoming a popular option for renting of computing and storage infrastructure services (called Infrastructure as a Service or IaaS)[1]; for remote platform building and customization for business processes (called Platform as a Service or PaaS)[2]; and for renting of business applications as a whole (called Software as a Service or SaaS)[3]. The cloud infrastructure has been further sub-divided into, Public cloud - where the infrastructure resides totally outside of the tenant / enterprises? firewall; Hybrid cloud - where the infrastructure and business processes reside partly within the enterprise and partly consumed from third party; and Private cloud - where IT services are mounted on top of large-scale conglomerated and virtualized infrastructure within enterprise firewall and consumed in "per transaction" basis. Technology consulting firm Gartner has estimated market size of $59 billion for Public and Hybrid cloud and has predicted it to grow to $149 billion by 2014 with a compounded annual growth rate of 20[4] . However, real and perceived security concerns remain one of the greatest inhibitors for adoption of Cloud computing. The primary concerns for cloud security are around cloud infrastructure, software platform and user data; as well as access control and identity management. Researchers also include broader issues of data integrity and compliance under security. Additionally, physical data center security and processes play an important role.

There is a growing body of work dealing with various cloud computing 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. Recently, a draft report by NIST [40] discusses some security challenges and considerations that organisations planning to utilze a public cloud environment should be aware of. However, barring a few [5], [6], there has not been a holistic treatment on cloud security issues and state of research in each of these issues. In this paper we provide a concise but all-round survey on cloud security trends and research.

We recognize that there are three major groups involved in cloud security. First group is the providers of Public and Hybrid clouds. Second group is the individuals / organizations which use cloud services - either by migrating and hosting their applications binaries / data to cloud, or by having an interface or a "pipe" connected to an external cloud to do some activities (like downloading cloud public data / modules or to route messages through cloud). The third group is the Government and other third-party regulatory entities that may have fiduciary roles (audit, forensic etc.). In our paper, we have tried to map security concerns and obligations of each of these groups.

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.

978-0-7695-4461-8/11 $26.00 © 2011 IEEE
DOI 10.1109/SERVICES.2011.20

Finally, we present a high-level framework to assess security preparedness for application migration to cloud.

The paper is organized as follows: in section 2, we talk about the categories of cloud security concerns and implications. In section 3, we discuss advanced security issues of cloud computing. In section 4, we briefly present the assessment framework. We conclude by summarizing the paper's contribution and scoping further work.

II. COMMON CONCERNS ABOUT CLOUD SECURITY AND IMPLICATIONS

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

1) 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.
2) Data. This category comprises the concerns around data integrity, data lock in, data remanence, provenance, and data confidentiality and user privacy specific concerns.
3) Access. This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management.
4) Compliance. Because of its size and disruptive influence, the 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 technological implications (mainly on part of the cloud providers) of each of these concerns and related research issues. We defer discussion on some 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.

A. Concern C1: Is my cloud-services provider's 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:

1) C11: Are the cloud data centers physically secured against security breaches?
2) C12: How is my application secured in shared virtualized infrastructure (VMs, storage, network) against malicious attacks?
3) C13: Since my application is hosted with common software stack (PaaS and SaaS), how does potential common-stack vulnerability affect me?
4) C14: In hybrid cloud my internal applications may interact with cloud-based ones in a common workflow. How do I ensure security isolation?
5) C15: Can I trust the APIs and interfaces provided by cloud providers?
6) C16: Since I relinquish execution control, how can it be ensured that no illegal operations happen?

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 whois 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 VM instances. 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.

Concerns (C13, C14) around shared resources and workflow are particularly important for hybrid PaaS and SaaS providers. The Cloud Security Alliance [20] terms it as 'shared technology vulnerability'. Active monitoring of any unexpected configuration changes (however small) and vulnerability scanning of any shared resources (OS, global caches, multiplexed channels etc.) are required for this. OS level isolations such as exo-kernels [11] have not found much adoption; but JVM and process level isolation techniques are increasingly getting popular [12]. Newer platforms like APEX from Force.com [2] use components and meta-data that are shared across tenants. These have strong session management, object scoping and data filtering mechanisms. The proliferation of usage of open-source provisioning tools, application servers, DBs, scripting languages, Web services protocols in cloud create the issues of security risks like SQL injection, cross site scripting , Database row-level security, and Web 2.0 specific security vulnerability (Ajax keeps on pinging pages for infinitesimal changes) etc. Researchers have provided examples of metadata spoofing attacks [13] where an adversary can overwrite WSDL metadata and the compromised client can generate un-warranted actions. These concerns and C15 can potentially be addressed by a key based digest and integrity verification of all cloud open interfaces and APIs. C16 is an advanced issue, and we defer it to next section.

B. 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, foremost concern 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 from Massachusetts 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 LinkUp suffered when their locked data with a third-party storage provider called Nirvanix got lost. The concerns are listed as below:

1) C21: What ensures integrity and prevents loss of my data in cloud?
2) C22: Will my business data remain confidential? How do I protect privacy of my users?
3) C23: How do I prevent my data getting locked out in case the provider is likely to fail?
4) C24: How do I ensure that data is not remanent in storage (i.e., bits are really wiped-out when delete operation is performed)?
5) C25: How do I know that updates to my data are tracked properly and I get the correct copy each time a request is made?
6) C26: How to maintain data confidentiality and integrity where multiple cloud parties are involved in processing?

Implication I2: Ensure effective data management including integrity, confidentiality and privacy

Data governance, including all the issues above, perhaps has most important implications for providers. C21 is relatively straightforward to address through strong encryption mechanisms like AES and DES. The management can be done through common PKI infrastructure. Labels are placed on repositories (basically file servers) encrypted with a public key that is associated with each user. The user possesses the private part of the key and is the only one that can decrypt the labels encrypted with the public part. This form of encrypted data in cloud is good for storage or archival but is rather costly to process. However, a new form of encryption, called Homomorphic Encryption [16] enables the ciphertext to be processed in public cloud without decrypting it. Service providers need to ensure storage integrity against loss of non-volatile data due to failure of storage sub- system and bit rots. Distributed data coding like Erasure Coding and network coding has been studied and used extensively [17], especially for fault tolerant and highly available storage in cloud. Transport level security (TLS) measures ensure secure data transfer over networks.

The common procedure of masking data for individual customer record confidentiality (C22) is data anonymization. In the context of risks such as health, research is being performed to better common anonymization techniques like k-anonymization with distributed anonymization [18]. Several concerns like C23 can be resolved by publishing and maintaining a standard set of data interfaces and transformation logic. Storage Network Industry Association (SNIA) [19] has suggested a set of remedial mechanism for data remanence problem C24. One of the suggestion is to encrypt

the data and then shred the key! Finally, device management becomes a critical function in data remanence. Things like remote management of mobile devices, remote wipe-out or remote disabling of a device need to be factored into the cloud eco-system.

C25 essentially highlights the important issue of data provenance. Cloud employs identifier based data objects such as S3 objects in Amazon cloud. Due to multiple concurrent access and latency in persistence and in absence of a proper file-system for journaling, the data queries may get inconsistent result and data lineage / update history may get lost. Researchers have proposed provenance aware storage system (PASS) wrapper layer [37] on top of simple cloud storage.

Multi-cloud information processing activities (C26) like distributed data mining would require sophisticated privacy preserving models, and we defer the treatment to section 3.

C. Concern C3: Are users accessing cloud- services really mine and can all my genuine users get seamless and secure accessibility?

Another fundamental cloud security concern is that of user authentication, authorization and access control (AAA). The first question is that of access management - mapping of traditional enterprise directory structure like LDAP and Active Directory for providing organizational role-based access to a cloud PaaS or SaaS provider. The second question is that of identity management like authentication, identity theft and phishing. Of particular importance will federated identity management in multi cloud scenario. Some such concerns are:

1) C31: How do I ensure that there is no un-authorized access to my cloud by a disgruntled employee, who has left the organization or by an identity thief?
2) C32: How to ensure proper levels of authentication to cloud services? How do I manage multi-device access?
3) C33: In multi-cloud scenario, how do I ensure that I provide / delegate access to users to different security domains so that the end-to-end workflow is seamless? Similarly, in hybrid cloud, how do I create a minimum common access control and identity structure?

Implication I3: 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 [38] promoted by OASIS, can enable faster user account provisioning and de-provisioning.

Cloud service authentication (C32) presents some interesting problems. Cloud services are increasingly getting accessed through 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 may become 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 (C33), 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 [22] 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 may not work. We need to develop more flexible cases of identity federation.

D. Concern C4: Are cloud providers compliant with regulation?

Various forms of compliance exist in cloud computing. Industry initiatives on compliance like accounting (Sarbanes-Oxley, Basel), health information privacy (HIPAA), and credit card data safety (PCI) are important for different verticals. Similarly standards around outsourcing auditing (SAS70) govern cloud based outsourcing vendors. US Federal and other international laws such as the Electronic Communication Privacy Act (ECPA) can govern concerns for data privacy in cloud. Transparency of data location is a fundamental premise of cloud computing. In reality, different geographical data locations may come under different jurisdictions, each with its own set of laws that govern data privacy and security.

Regulations and national security matters require effective auditing and sharing of audit reports with relevant authorities. Today, it is not clear if Govt. agencies have enough trust in cloud security preparedness. Federal Trade Commission (FTC) of US, in a recent filing, has stated that they are investigating security implications of cloud based remote data processing [23]. Some laws also mandates that critical Financial and Defense related data does not leave the perimeter of the country. Easy accessibility to data 'on

demand' for audit purpose is also mandated. For example, in many jurisdictions the government has the power to access any data residing within their limits for a "reasonable" cause. Data can even be seized if the service provider comes on the wrong side of the law enforcement agencies [24]. Note that compliance concerns are no longer limited to existing regulations, but extend to newer ones specific to cloud computing.

Implication I4: Ensure proper regulatory compliance

Cloud providers generally follow legal compliance and contractual obligations. However, there have been instances, like the case of Google Docs in March 2009, where full security and data safety audit reports have not been made public and data integrity was allegedly compromised by improper access [36]. This made ECPA petition to FTC to initiate action [23]. Furthermore, providers should be open to forensics [25] such that data provenance can be achieved and whenever required, mala- fide actions can be traced back to the origins. Many compliance specific concerns, in the minds of enterprises, are perceived (fear of the un-known) than real; and better disclosers on part of providers will dispel some of the fear.

Due to serious concerns regarding the location of data and processing entities within the cloud, some sort of location awareness is required, the primary aim being the ability to enforce and establish requirements like "at any time data should only reside within these jurisdictions". Current standardization efforts like the Open Grid Forum's cloud computing interface (OCCI) specification, which is meant to provide mechanisms of querying the implementations for information, do not yet provide infrastructure-based location awareness and there are certainly discussions and efforts going on around this area [26].

III. 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:

1) 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.
2) Lack of execution controls: The external cloud user does not have fine-gained control over remote execution environment. Hence the critical issues like memory management, I/O calls, access to external shared utilities and data are outside the purview of the user. The client would want to inspect the execution traces to ensure that illegal operations are not performed.
3) 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.
4) 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 tackle issues 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 and promoted by Trusted Computing Group (TCG) [27]. To tackle the concern 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 [28] 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 in a public cloud, it will be eventually retrievable. Proof carrying codes [30] 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 the data 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 [31].

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 parties 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 methods) 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 [33]. When a cloud tenant downloads / updates private data 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; no database 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 be formed across the sets which can't be guessed with reasonable computational complexity by another party [34]. These privacy preserving models and research are increasingly becoming important in multi-cloud information processing cases.

IV. 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 step approach will help in rigorous security assessment:

1) 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 data behind 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 with other 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.
2) 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 infrastructure and platform, data, and access layers of the provider; on concerns depicted in the 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.
3) 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 a security 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, as well as related reference data such as unique identifiers for vulnerabilities.

V. CONCLUSION AND FUTURE WORK

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 the cloud. We have also discussed some issues regarding security-related regulatory compliance in the cloud. Additionally we presented a 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 many standard 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 increasingly assume greater importance and more mainstream research is required in this area. Fourth, migrating generic in-house software code to public cloud require thorough 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.

REFERENCES

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

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

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

[4] Gartner DataQuest Forecast on Public Cloud Services *DocID G00200833, June 2, 2010*

[5] Chow,R.,Gotlle,P.,Jakobsson, E.S.,Staddon,J., Masuoka,R., and Molina,J. *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 and Confidentiality in Cloud Computing.* Technical Report prepared for World Privacy Forum, 2009

[7] Novell Inc. survey on cloud computing, *http://www.novell.com/news/press/novell-survey-reveals-widespread-and-accelerating-enterprise-adoption-of-private-clouds*

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

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

[10] 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 the 16th ACM conference on Computer and Communication Security, 2009

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

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

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

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

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

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

[17] 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

[18] 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

[19] Storage Network Industry Alliance, *http://www.snia.org*

[20] Cloud Security Alliance, *http://www.cloudsecurityalliance.org*

[21] OpenID foundation website, *http://www.openid.net*

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

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

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

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

[26] Open Grid Forum's OCCI specification, *http://www.occi-wg.org/*

[27] Trusted Computing Group, *http://www.trustedcomputinggroup.org*

[28] 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

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

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

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

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

[33] Boneh, D., and Crescenzo, G., D., *Public Key Encryption with Keyword Search*, Proceedings of Advances in Cryptology, EuroCrypt 2004. Lecture Notes in Computer Science, Springer

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

[35] OAuth community site, *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 for the 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 (NIST), *http://www.nist.gov*

[40] NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, *http://csrc.nist.gov/publications*. 2011