Academic City University College – Accra Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART) Africa
Tony Blair Institute for Global Change
FAIR Forward – Artificial Intelligence for All - Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Accra Bespoke Multidisciplinary Innovations Conference (ABMIC)

& The Africa AI Stakeholders' Summit 14th December, 2021

Standardization Issues and Associated Collaterals In Cloud Computing

Sarumi, Jerry. Abayomi (PhD)[1] & Aderibigbe, Stephen Ojo (PhD)[2]
Department of Computer Science
Lagos State University of Science & Technology
Ikorodu, Lagos State, Nigeria
E-mail: jerrytechnologies@yahoo.co.uk[1], aderibigbe2000@gmail.com
Phone: +2348023408122

Proceedings Citation Format

Sarumi, Jerry. Abayomi & Aderibigbe, Stephen Ojo (2021): Standardization Issues and Associated Collaterals In Cloud Computing.. Proceedings of the Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. December 2021. Pp 289-306 www.isteams.net/ghanabespoke2021.

Standardization Issues and Associated Collaterals In Cloud Computing

Sarumi, Jerry. Abayomi (PhD)[1] & Aderibigbe, Stephen Ojo (PhD)[2]

ABSTRACT

This paper presents a discussion on the various activities been undertaken by different standard development organizations (SDOs) in the world, at the domain of cloud application and service deployments, particularly concerning security and privacy issues. For each standard development organization (SDO), we identify the focus on cloud computing related works particularly with regard to security and privacy issues and conclude with some propositions for the standardization of cloud computing security.

Keywords: Standardization, Issues, Collaterals, Computing, Cloud, Security Standards.

1. INTRODUCTION

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulation exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing. Trust is a critical issue in cloud computing since an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider.

However, public cloud computing manifests itself as a thought-provoking paradigm shift from conventional computing to an open deperimeterized organizational infrastructure – at the extreme, displacing applications form one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate. The security and privacy issues which are identified by NIST to be relevant in cloud computing are: (i) governance, (ii) compliance, (iii) trust, (iv) hardware and software architecture, (v) identity and access management, (vi) software isolation, (vii) data protection, (viii) availability, and (ix) incident response. Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.

At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency. In addition, the organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data.

2. NIST CLOUD STANDARDS

NIST is a key organization in defining various standards for cloud computing. With regard to security and privacy aspects of cloud computing NIST has released standard guidelines for public clouds (Badger et al., 2011). The primary focus of the report issued by NIST is to provide an overview of public cloud computing and the security and privacy considerations involved.

It discusses the threats, technology risks, and safeguards surrounding public cloud environments, and their suitable defense mechanisms. The report observes that "since the cloud computing has grown out of an amalgamation of technologies, including service oriented architecture (SOA), virtualization, Web2.0, and utility computing, many of the security and privacy issues involved in cloud computing can be viewed as known problems cast in a new setting" (Badger et al., 2011).

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. Many cloud-based applications require a client side to initiate and obtain services. However, many of the simplified interfaces and service abstractions on the client, server, and network belie the inherent underlying complexity that affects security and privacy. Therefore, the NIST report recommends that it is important to understand the technologies the cloud provider uses to provision services and the implications the technical control involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to access and manage risk. The hypervisor or virtual machine monitor is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines and is common to IaaS clouds. Compared with traditional, non-virtualized implementation, the addition of hypervisor cause an increase in the attack surface in cloud computing, i.e., there are additional methods (e.g. application programming interfaces), channels (e.g., sockets), and data items (e.g., input strings) an attacker can use to cause damage to the system.

The report of NIST recommends that care should be taken to provision security for the virtualized environments in which the images of various applications run. It also recommends the use of virtual firewalls to isolate groups of virtual machines from other hosted groups, such as production systems from development systems or development systems from other cloud-resident systems. Another aspect of security that is critical in cloud computing is the client-side protection. Since the services from different cloud providers, as well as cloud-based applications developed by the organization, can impose stringent demands on the client-side, which may have implications for security and privacy that need to be taken into account for system design. Likewise, the web browsers, which are key elements for many cloud computing services and various plug-ins and extensions available for them are notorious for their security problems.

The growing availability and use of social media, personal webmail, and other publicly available sites also have associated risks that a concern, since they increasingly serve as avenues for social engineering attacks that can negatively impact the security of the browser, its underlying platform, and cloud services accessed. Since data sensitivity and privacy of information have become increasingly an area of concern for organizations in the paradigm of cloud computing, preventing unauthorized access to information resources in the cloud is a critical requirement. The NIST report recommends the use of identity federation as one solution to the complicated authentication requirements in cloud computing. Identity federation allows an organization and a cloud provider to trust and share digital identities and attributes across both domains, and to provide a means for single sign-on.

For such federation to succeed, identity and access management transactions must be interpreted carefully and unambiguously and protected against attacks. There are several ways in which an identity federation can be accomplished such as with the security assertion markup language (SAML) standard or the OpenID standard (Badger et al., 2011). A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to application and data. SAML request and response messages are typically mapped over SOAP, which relies on the eXtensible Markup Language (XML) for its format. SOAP messages are digitally signed. In a public cloud, for instance, once a user has established a public key certificate with the service, the private key can be used to sign SOAP requests. However, SOAP message security validation is complicated and must be carried out carefully to prevent attacks. XML wrapping attacks have been successfully demonstrated against a public IaaS cloud (Gajek et al., 2009; Gruschka & Iacono, 2009). XML wrapping involves manipulation of SOAP messages.

A new element (i.e., the wrapper) is introduces into the SOAP security header: the original message body is then moved under the wrapper and replaced by a bogus body containing an operation defined by the attacker (Gajek et al., 2009; Gruschka & Iacono, 2009). The original body can still be referenced and its signature verified, but the operation in the replacement body is executed instead. Since SAML alone is not sufficient to provide cloud-based identity and access management services, the NIST report recommends the use of eXtensible Access Control Markup Language (XACML) by a cloud provide to control access to cloud resources. XACML focuses on the mechanism for arriving at authorization decisions, which complements SAML's focus on the means for transferring authentication and authorization decisions between cooperating entities.

Since multi-tenancy in IaaS cloud computing environments is typically done by multiplexing the execution of virtual machines from potentially different consumers on the same physical server, applications deployed on guest virtual machines remain susceptible to attack and compromise, much the same as their non-virtualized counterparts (Badger et al., 2011). However, regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms. This becomes an especially challenging proposition since multi-tenancy in virtual machine-based cloud infrastructures, together with the subtleties in the way physical resources are shared between guest virtual machine, can give rise to new sources of threat. The most serious threat is that malicious code can escape the confines of its virtual machine and interfere with the hypervisor or other guest virtual machines. Live migration, the ability to transition a virtual machine between hypervisors on different host computers without halting the guest operating system, and other features provided by virtual machine monitor environments to facilitate systems management, also increase software size and complexity and potentially add other areas to target in an attack.

Since the data stored in a public cloud typically resides in a shared environment collocated with data from other customers, the NIST report strongly recommends that access to the data should be controlled and the data should be kept secure (Badger et al., 2011). These requirements are also applicable for the data that is migrated within or between clouds. In addition, data can take many forms in the cloud. For example, for cloud-based application development, data may include the application programs, scripts, and configuration settings, along with the development tools.

For developed applications, it includes records and other content created or used by the applications, including deallocated objects, as well as account information about the users of the applications. The NIST report recommends two methods for keeping data away from unauthorized users: (i) access controls, and (ii) encryption.

NIST is currently undertaking the Cryptographic Key Management Project for identifying scalable and usable cryptographic key management and exchange strategies for use by government, which would help to alleviate the problem eventually (Cryptographic Key Management Project). NIST also recommends that before proceeding in cloud environments where the cloud provider provides facilities for key management, the organization must fully understand and weigh the risks involved in the processes defined by the cloud provider for the key management lifecycle (Badger et al., 2011). Hence, the cryptographic operations performed in the cloud become part of the key management process and, therefore should be managed and audited by the organization.

In a public cloud, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Hence, NIST recommends that sufficient measures should be taken to ensure that data sanitization should be performed appropriately throughout the system lifecycle. The NIST report also observes that availability of services is a critical requirement for cloud service providers. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. In most of these cases, the downtime is unplanned and can adversely affect the mission of the organization. Despite employing architectures designed for high service reliability and availability, cloud computing services can and do experience outages and performance slowdowns (Leavitt, 2009). NIST recommends that the level of availability of a cloud service and its capabilities for data backup and disaster recovery need to be addressed in the organization's contingency and continuity planning to ensure the recovery and restoration of disrupted cloud services and operations, using alternate services, equipment, and locations, if required.

NIST report points out the fact that a cloud service provider's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Each layer in a cloud application stack, including the application, operating system, network, and database, generates event logs, as do other cloud components, such as load balancers and intrusion detection systems; many such event sources and the means of accessing them are under the control of the cloud service provider. The report also observes that availability of relevant data from event monitoring is essential for timely detection of security incidents.

However, the cloud customers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments and the service providers have insufficient access to event sources and vulnerability information, inadequate interfaces for accessing and processing event data automatically, and do not have the capability to add detection points within the cloud infrastructure, and have difficulty in directing third-party reported abuses and incidents effectively back to the correct customer or the cloud provider for handling.

The report also observes that an incident should be handled in a way that limits damage and minimizes recovery time and costs. Hence, collaboration between the cloud consumer and provider in recognizing and responding to an incident is vital to security and privacy in cloud computing. In summary, the NIST report on security and privacy issues in public cloud computing provides an overview of the public cloud and describes the threats, technology risks, and safeguards that are surrounding the public cloud environment. It also provides detailed guidelines for the service providers and the consumers to handle various security and privacy issues in cloud computing.

Cloud Security Alliance (CSA)

This non-profit organization provides security guidance for critical areas of focus in cloud computing (CSA Homepage). The alliance covers key issues and provides advice for both cloud computing customers and providers within various strategic domains. CSA has published a report on cloud computing that outlines the areas of concern and guidance for organizations adopting cloud computing with an objective to provide the security practitioners with a comprehensive roadmap for being proactive in developing positive and secure relationships with cloud providers. The CSA guide on cloud computing deals with fifteen broad domains of cloud computing: (i) cloud computing architectural framework, (ii) governance and enterprise risk management, (iii) legal aspects of cloud computing, (iv) electronic discover, (v) compliance and audit, (vi) information lifecycle management, (vii) portability and interoperability issues, (viii) traditional security, business continuity and disaster recovery, (ix) data center operations, (x) incident response, notification and remediation, (xi) application security, (xii) encryption and key management, (xiii) identity and access management, (xiv) storage, and (xv) virtualization.

From security perspective, the CSA report recommends that a portion of the cost savings obtained by cloud computing services must be invested into the increased scrutiny of the security capabilities of the provider and ongoing detailed audits to ensure requirements are continuously met. It also recommends the following: (i) the service providers should have regular third party risk assessment and these should be made available to the customers, Iii) the cloud provider’s key risk and performance indicators must be understood clearly and methods must be designed to monitor and measure these indicators from the perspective of the customers, (iii) the onus should be on the customer to perform due diligence of a cloud provider for usage in mission critical business functions or hosting regulated personally identifiable information, (iv) the cloud providers should adopt as a security baseline the most stringent requirements of any customer, (v) centralization of data implies the risk of insider threats from within the cloud provider is a significant concern, (vi) any data classified as private for the purpose of data breach regulations should always be encrypted to reduce the consequences of a breach incident and the customer should stipulate encryption requirements (algorithm, key length and key management at a minimum) contractually, (vii) IaaS, PaaS and SaaS create differing trust boundaries for the software development lifecycle, which must be accounted for during the development, testing and production deployment of applications, (viii) securing inter-host communications must be the rule, there can be no assumption of a secure channel between hosts, whether existing in a common data center or even on the same hardware platform, (ix) application providers who are not controlling backend systems should assure that data is encrypted when being stored on the backend, (x) segregate the key management from the cloud provider hosting the data, creating a chain of separation. This protects both the cloud provider and customer from conflict when being compelled to provide data due to a legal mandate.

Distributed Management Task Force (DMTF)

DMTF develops standards for interoperable IT management solutions (DMTF Homepage). From this perspective DMTF is working on several topics like (1) open virtualization format (OVF) that formats for packaging and distributing software to run over virtual machines (2) Open Cloud Standards Incubator, for interactions between cloud environments by developing cloud resource management protocols. The activity was moved to Cloud Management Working Group (CMWG) and (3) Cloud Audit Data Federation (CADF) working group that develops solutions that allows sharing of audit information / logs. For security issues in cloud computing, DMTF have established a partnership with CSA to promote standards for cloud security as part of DMTF Open Cloud Standard Incubator. The Open Cloud Standard Incubator group is charged with first formulating a series of management protocols, packaging formats and security tools to foster interoperability between cloud, followed by specifications that will foster cloud service portability and cross-cloud management consistency.

Storage Networking Industry Association (SNIA)

SNIA has created the Cloud Storage Technical Work Group for the purpose of developing SNIA architecture related to system implementations of cloud storage technology (SNIA Homepage). It is promoting cloud storage as a new delivery model that provides elastic, on-demand storage billed only for what is used. The initiative, known as the Cloud Data Management Interface (CDMI), lets the customer to tag his/her data with special metadata (data system metadata) that the cloud storage provider what data services to provide that data (backup, archive, encryption etc.). These data services all add value to the data the customer stores in the cloud and by the implementation of the standard interface of CDMI, the customer can freely move his/her data from one cloud vendor to another without experiencing any pain of recoding to different interfaces.

SNIA is also involved in storage network security related activities. Although storage network security is a new subject, it is rapidly gaining in importance in the minds of both users and product developers. The increase is born of a general realization of the increasing importance and value of the information held in on-line systems, and of the separation of processing and storage functions enabled by the development of storage area networks (SANs). SINA's mission is "to ensure that storage networks become efficient, complete, and trusted solutions across the IT community". However, to achieve this goal, SNIA will have to develop new standards and technologies in storage network security. While storage network security seeks to learn from the application of similar techniques to communications security in general and to network security in particular, it has some unique requirements that will necessitate the development of new and specialized techniques. Currently, the development of such techniques is in its infancy.

Open Grid Forum (OGF)

OGF's Open Cloud Computing Interface (OCCI) (OCCI Homepage) group creates practical solutions to interface with cloud infrastructures exposed as a service. The focus is on a solution which covers the provisioning, monitoring and definition of cloud infrastructure services. The Open Cloud Computing Interface comprises a set of open community-led specifications delivered through the Open grid Forum. OCCI is a protocol and API for all kinds of management tasks. OCCI was originally initiated to create a remote management API for IaaS model based Services, allowing for the development of interoperable tools for common tasks including deployment, autonomic scaling and monitoring. It has since evolved into a flexible API with a strong focus on integration, portability, interoperability and innovation while still offering a high degree of extensibility.

The current release of the Open Cloud Computing Interface is suitable to serve many other models in addition to IaaS, including e.g., PaaS and SaaS. The security group of OGF is concerned with technical and operational security issues in the grid and cloud environments, including authentication, authorization, privacy, confidentiality, auditing, firewalls, trust establishment, policy establishment, and dynamics, scalability and management aspects of these issues. The purpose of the Certificate Authority Operations (CAOPS) working group is to develop

Open Cloud Consortium (OCC)

OCC (OCC Homepage) is a member driven organization that: (i) supports development of standards, (ii) supports development of benchmarks, (iii) supports reference implementations of cloud computing, preferably open source, and (iv) sponsors workshops and other events related to cloud computing. OCC has four working groups: (i) large data clouds working group, (ii) open cloud test-bed working group, (iii) standard cloud performance measurement (SCPM) working group, and (iii) information sharing and security working group.

The SCPM working group is responsible for establishing benchmarks appropriate for four use cases: (i) moving an application between two clouds, (ii) obtaining burst instances from multiple cloud service providers for a private/public hybrid application, (iii) moving a large data cloud application to another large data cloud storage service, and (iv) moving a large data cloud application to another large data cloud computing service.

Organization for the Advancement of Structured Information Standards (OASIS)

OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards (OASIS Homepage). The consortium produces more web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and application-specific markets. In cloud computing domain, OASIS has the following technical committees, each having its clearly defined objectives and goals.

1. Advanced Message Queuing Protocol (AMQP) TC: it defines a ubiquitous, secure, reliable and open ended Internet protocol for handling business messaging.
2. Cloud Application Management for Platforms (CAMP) TC: it is responsible for standardizing cloud PaaS management API.
3. Cloud Authorization (CloudAuthZ) TC: it focuses on enabling contextual attributes and entitlements to be delivered to Policy Enforcement Points in real-time.
4. Identity in the Cloud TC: it is involved in developing profiles of open standards for identity deployment, provisioning and management in cloud computing.
5. Open Data Protocol (OData) TC: its goal is to simplify data sharing across disparate applications in enterprise, cloud and mobile devices.
6. Privacy Management Reference Model (PMRM) TC: it is responsible for providing a guideline for developing operational solutions to privacy issues.
7. SOA Reference Model TC: it is involved in developing a core reference model to guide and foster the creation of specific service-oriented architecture (SOA).
8. Topology and Orchestration Specification for Cloud Applications (TOSCA) TC: it is responsible for enhancing the portability of cloud applications and services.
9. Transformational Government Framework TC: it is advancing an overall framework for using IT to improve delivery of public services.

TM Forum

TM Forum (TM Forum Homepage) – an association that includes technology vendors such as HP and IBM, as well as more than 750 of the world's largest service providers in the communications, media and cloud service markets – has delivered what it calls the industry's first set of enterprise-grade external compute Infrastructure as a Service (IaaS) requirements. Put together by the association's Enterprise Cloud Leadership Council (ECLC), the document includes guidelines for technology; requirements for external private clouds in commercial, technical and operational terms; the business case for external private clouds; and sample use cases.

It also details how business and technical agreements between enterprise customers and cloud service providers should be defined and managed to maximize benefits for both parties. Focused on enabling best-in-class IT for service providers in the communications, media, defense and cloud service market, TM Forum created ECLC in 2009 to provide a forum for enterprise cloud users to share requirements and drive the development of best practices and standards that will remove the barriers to development and adoption of cloud services.
Its list of members includes Deutsche Bank, Boeing, ING, Dassault Systems and Northrop-Grumman. Incorporating the input from the top cloud innovators and thought leaders, this document of TM Forum intends to create a way forward for the industry that separates out the vital needs from the minor and secondary requirements. Based on end users' experience and requirements the document is intended to assist cloud service providers and technology suppliers to determine customer demands, drive direction on standards and best practices, and remove barriers to adoption. The vendors need to map their product and service offerings against those requirements.

The cloud services initiative of TM Forum, therefore, intends to deliver the following:

a. An ecosystem of enterprise customers, cloud service providers and technology suppliers that enable the commercialization of this major business opportunity.
b. Business guidance including benchmarks and service quality metrics.
c. Technical agreements in collaboration with other industry groups.

The a particular focus on developing standards in cloud computing, the Enterprise Cloud Leadership Council (ECLC) of the TM Forum has the following programs in its agenda of activities:

Defining service level agreements (SLAs) for cloud services

a. Data-as-a-Service (DBaaS) reference architecture
b. Cloud API requirements
c. Business process and information frameworks for cloud
d. Secure virtual private cloud reference architecture
e. Standard service definitions/SKUs (Taxonomy of services)
f. Cloud SDO liaisons
g. eTOM and ITIL; how to combine them in a cloud context?
h. Cloud service provider benchmarking and metrics
i. Billing engine, client billing and partner revenue sharing for cloud services
j. Common definition of commercial terms (business contract language)

The TM Forum has created a Cloud Services Initiative with the purpose to define a range of common approaches, processes, metrics and other key service enablers (TM Forum Homepage).

International Telecommunication Union (ITU)
The International Telecommunications Union-Telecommunications Standards Group (ITU-T) (ITU-T

Homepage) has formed a focus group on cloud computing (FG Cloud) to further ITU-T TSAG (Telecommunication Standardization Advisory Group) agreement at its meeting in Geneva during 8-11 February 2010. The focus group, established in accordance with Recommendation ITU-T A.7, from the standardization view points and within the competencies of ITU-T contributes to telecommunication aspects, i.e., the transport via telecommunications networks, security aspects of telecommunications, service requirements, etc.,

In order to support services/applications of cloud computing making use of telecommunication networks, specifically in the following activities:

a) Identify of potential impacts on standard development and priorities for standards needed to promote and facilitate telecommunication/ICT support for cloud computing
b) Investigate the need for future study items for fixed and mobile network in the scope of ITU-T
c) Analyze which components would benefit most from interoperability and standardization
d) Familiarize ITU-T and standardization communities with emerging attributes and challenges of telecommunication/ICT support for cloud computing
e) Analyze the rate of change for cloud computing attributes, functions and features for the purpose of assessing the appropriate timing of standardization of telecommunication/ICT in support of cloud computing

The focus group on cloud computing in ITU-T collaborates with worldwide cloud computing communities (e.g., research institutions, laboratories, forums, and academia) including other SDOs and consortia. The group has also identified its specific tasks and deliverables in cloud computing standards development activities.

The identified deliverables are: (i) identification of the benefits of cloud computing from telecommunication/ICT perspectives, (ii) gap analysis of ITU-T standards for telecommunication/ICT to support cloud computing, (iii) collection and summarization of vision and value propositions of cloud computing with a focus on telecommunication/ICT aspects, (iv) leveraging expertise within the ITU-T in building telecom networks to take advantage of cloud concepts and capabilities, (v) Analysis of telecommunication/ICT networking requirements functions and capabilities to support cloud computing services/applications (for both fixed and mobile devices), (vi) use case of services and reference models for telecommunication/ICT to support cloud computing, (vii) Designing the roadmap to guide further development of relevant ITU-T recommendations.

The European Telecommunications Standards Institute (ETSI)

ETSI (ETSI Homepage) Technical Committee (TC) GRID, now known as TC CLOUD, has been formed to address issues associated with the convergence between IT (Information Technology) and Telecommunications. The focus is on scenarios where connectivity goes beyond the local network. This includes not only grid computing but also the emerging commercial trend towards cloud computing which places particular emphasis on ubiquitous network access to scalable computing and storage resources. Since TC CLOUD has particular interest in interoperable solutions in situations which involve contributions from both the IT and Telecom industries, the emphasis is on the Infrastructure as a Service (IaaS) delivery model. The focus of the ETSI TC Cloud is on the following issues: (i) to complement progress being made elsewhere with a networking perspective and a more formal approach to standards and test specifications, (ii) introduce new requirements into networking (e.g., next-generation networks) standards to support new kinds of application such as grid and cloud, (iii) achieving the desired level of interoperability needed in next-generation networks, grids and clouds, (iv) collaborate with other SDOs in developing standards in cloud computing.

Object Management Group (OMG)

OMG is an international, open membership, not-for-profit computer industry standards consortium. OMG Task Forces (TFs) develop enterprise integration standards for a wide range of industries. In cloud computing standardization, OMG's focus is on modeling deployment of applications and services on clouds for portability, interoperability and reuse (OMG Homepage). The standardization activities in cloud computing in OMG are mainly focused on the following broad areas:

- Meta-element association: for defining distributed and non-deterministic computing from the cloud and SOA perspective.
- Governance: there is a services governance domain and a cloud governance domain. The key is how to integrate these two points of view for governing distributed and non-deterministic computing.
- SLAs: developing SLAs for services delivered over the cloud
- SOA, events, and agents: defining communication among and within clouds between services enabled in these clouds.

Association for Retail Technology Standards (ARTS)

ARTS (ARTS Homepage) is an international membership organization dedicated to reducing the costs of technology through standards. ARTS has been delivering application standards exclusively to the retail industry. ARTS released a white paper on cloud computing in 2009 that offers unbiased guidance for achieving maximum results from this relatively new technology. The version 1.0 of the whitepaper represents a significant update to the draft version released in October 2009. The document seeks to identify the characteristics of cloud computing that makes it compelling for retailers, and attempts to highlight areas in which a cloud-based solution offers strong benefits to retailers. It also discusses the key obstacles to adopting cloud-based solutions, including reliability, availability, and security. It also covers issues relating to portability, manageability, and interoperability.

Institute of Electrical and Electronics Engineers (IEEE)

Hoping to propel cloud computing to new heights, the IEEE (IEEE Homepage) has launched a design guide and a standard for interoperable cloud services. According to IEEE, these two initiatives are by far the first ever attempt by any formal standards body to address the issues hounding cloud services. In order to enable transfer of customer data from one provider to another in a seamless standardized manner, the IEEE P2301 draft guide is being designed to provide an intuitive roadmap for application portability, management, and interoperability interfaces, as well as for file formats and operating conventions. The standard is expected to be completed in 2014 and will help vendors, service providers, and consumers involved in every aspects of procuring, developing, building, and using cloud computing.

In addition, IEEE is involved in preparation of another draft standard – IEEE P2302 draft standard for intercloud interoperability and federation. There is a growing demand from the consumers for the same kinds of global roaming, portability, and interoperability capabilities for storage and computing as with voice and text messaging. To meet this requirement, IEEE P2302 is defining the topology, protocols, functionality, and governance required for cloud-to-cloud interoperability. The term “intercloud” refers to an interconnected mesh of clouds that depends on open standards for their operation. “Federation” allows users to move their data across internal and external clouds and access services running on other clouds according to the business and application requirements. The IEEE P2302 working group is also focusing on building a system among cloud product and service providers that would be transparent to users. The group plans to address transparent interoperability and federation in much the same way that standards do for the global telephony systems and the Internet.

Alliance for Telecommunications Industry Solutions (ATIS)

ATIS (ATIS Homepage) is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. ATIS’ Cloud Services Forum (CSF) facilitates the adoption and advancement of cloud services from a network and IT perspective. Its primary focus is on the basic APIs in the control plane layer of the network rather than on the services on the network. Drawing upon business use cases that leverage cloud services’ potential, CSF addresses industry priorities and develops implementable solutions for this evolving marketplace. CSF is working to ensure that services are quickly put into operation to facilitate the delivery of interoperable, secure and managed services. Current priorities of CSF include content distribution network interconnection, cloud services framework, intercarrier tele-presence, virtual desktop, virtual private network, and development of a cloud services checklist for onboarding. The current initiatives of CSF include the following activities:

a) Develop video service specifications as a component of a unified communications framework (e.g., telepresence, mobility etc.).
b) Advance a trusted information exchange (TIE) solution to address the directory, routing, privacy, and accessibility.
c) Progress the next phase of content distribution network-interconnection (CDN-I) – building on initial use cases to address more complicated models and additional content types. CSF currently leads the market in standardization aspects of CDN-I for content delivery, for example Multicast.
d) Define virtual desktop functional requirements to take advantage of cloud resources to reduce management costs and support ay-device, any-network access to desktops by end-users.

Internet Engineering Task Force (IETF)

IETF (IETF Homepage) has established the Cloud OPS WG (working group on cloud computing and maintenance) which is currently discussing cloud resource management and monitoring, and Cloud-APSBOF which has focused on cloud applications. There are several existing working groups within the IETF that are also working in the technical areas that could be useful to cloud computing activities. Among these working groups are Decade working group within IETF application area, nfsv4 working group within TSV application area, and netconf working group within OPS application area. Similarly, IRTF (Internet Research Task Force) has been working on the technical issues related to cloud computing as part of P2PRG working group and VNRG research group. While the above working groups have been in existence for some time, in the last year, there has been some renewed effort to focus on providing cloud services. Currently, there is an effort underway in the form of birds of feather (BOF) to discuss various contributions related to cloud computing. Most of the work being discussed as part of this effort would hopefully be very useful to the service providers.

3. PROPOSITIONS FOR SECURITY IN CLOUD COMPUTING

In this section, we discuss some novel security approaches that may be utilized in cloud computing deployments. The core issue is that with the advent of the cloud, the cloud provider also has some control of the cloud users' data. In this section, some propositions have been made in such a way that the current capabilities of the cloud are not curtailed while limiting the cloud provider control on data and enabling all cloud users to benefit from the cloud.

Information-centric security: In order for enterprises to extend control of data in the cloud, it may be worthwhile to take an approach of protecting data from within. This approach is known as information centric security. This self-protection technique requires intelligence be put in the data itself. Data needs to be self-describing and defending, regardless of its environment. When accessed, data consults its policy and attempts to recreate a secure environment that is verified as trustworthy using the framework of trusted computing (TC).

High-assurance remote server attestation: At present, lack of transparency is discouraging businesses from moving their data to the cloud. Data owners wish to audit how their data is being handled at the cloud, and in particular, ensure that their data is not being abused or leaked, or at least have an unalterable audit trail when it does happen. Currently, customers must be satisfied with cloud providers using manual auditing procedures like SAS-70. A promising approach to address this problem is based on trusted computing. In a trusted computing environment, a trusted monitor is installed at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide proof of compliance to the data owner, guaranteeing that certain access policies have not been violated. To ensure integrity of the monitor, trusted computing also allows secure bootstrapping of this monitor to run beside (and securely isolated from) the operating system and applications. The monitor can enforce access control policies and perform monitoring/auditing tasks. To produce a proof of compliance, the code of the monitor is signed, as well as a statement of compliance produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run, and that the cloud server has complied with access control policies.

Privacy-enhanced business intelligence: A different approach for retaining control of data is to require the encryption of all cloud data. The problem in this approach is that encryption limits data use. In particular, searching and indexing the data becomes problematic, if not impossible. For example, if data is stored in clear-text form, one can efficiently search for a document by specifying a keyword. This is impossible to do with traditional, randomized encryption schemes. The state-of-the-art cryptographic mechanisms may offer new tools to solve these problems. Cryptographers have invented versatile encryption schemes that allow for operations and computations on the cipher-texts. For example, searchable encryption (also referred to as predicate encryption) (Song et al., 2000) allows the data owner to compute a capability from his secret key.

A capability encodes a search query, and the cloud can use this capability to decide which documents match the search query. The cloud can use this capability to decide which documents match the search query, without learning any additional information. Other cryptographic primitives such as homomorphic encryption (Gentry, 2009) and private information retrieval (PIR) (Chor et al., 1998) perform computations on encrypted source data without decrypting them. As these cryptographic techniques mature, they may open up new possibilities and directions for research, development and deployment of cloud security protocols and algorithms.

While in many cases more research is needed to make these cryptographic tools sufficiently practical for the cloud, they present the best opportunity for a clear differentiator for cloud computing since these mechanisms can enable cloud users to benefit from one another's data in a controlled manner. In particular, even encrypted data can enable anomaly detection that is valuable from a business intelligence standpoint. Apart from ensuring privacy, applied cryptography also offers tools to address other security problems related to cloud computing. For example, in proofs of retrievability (Shacham & Waters, 2008), the storage server can show a compact proof that it is correctly storing all of the client's data.

Table 1 summarizes some important security issues in cloud computing and their possible defense mechanisms.

Table 1: Some Important Security Issues In Cloud Computing

Security threats	Possible defense mechanisms
Spoofing identity	Authentication Protect secrets Don't store secrets
Tampering with data	Authorization
	Hashes Message authentication codes Digital signatures Tamper-resistant protocols
Repudiation	Digital signatures Time-stamps Audit trails
Information disclosure	Authorization Privacy-enhanced protocols Encryption Protect secrets Don't store secrets
Denial of Service (DoS)	Authentication Authorization Filtering Throttling Quality of service (QoS)
Elevation of privilege	Run with least privilege

Table 1. Cloud computing threats and suggested defense mechanisms for these threats

4. CONCLUDING REMARKS

In ensuring standards in the cloud domain, acccess controls that are typically identity-based, which makes authentication of the user's identity an important issue in cloud computing arena must also be looked into. Sincere Clouds lack physical control over the storage of information, encryption is the only way to ensure that it is truly protected. In addition, data must be secured while at rest, in transit, and in use, and access to the data must be controlled. The standards for communication protocols and public key certificates allow data transfers to be protected using cryptography and can usually be implemented with equal effort in SaaS, PaaS, and IaaS environments (Badger et al., 2011). The NIST report observes that the security of a system that employs cryptography depends on the proper control of central keys and key management component. Currently, the responsibility for cryptographic key management falls mainly on the cloud consumer. Key generation and storage is usually performed outside the cloud using hardware security modules, which do not scale well to the cloud paradigm.

REFERENCES

1. Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. (2003). Xen and the Art of Virtualization. Technical Report, University of Cambridge. Available online at: www.cl.cam.ac.uk/research/srg/netos/papers/2003-xensosp.pdf (Accessed on: January 23, 2013).
2. Bhattacherjee, B., Abe, N., Goldman, K., Zadrozny, B., Chillakuru, V. R., Del Caprio, M., and Apte, C. (2006). Using Secure Coprocessors for Privacy Preserving Collaborative Data Mining and Analysis. In Proceedings of the 2nd International Workshop on Data Management on New Hardware (DaMoN'06), Chicago, Illinois, USA, June, 2006 Article No 1, New York: ACM Press.
3. Boneh, D., and Waters, B. (2007). Conjunctive, Subset, and Range Queries on Encrypted Data. In Proceedings of the 4th Conference on Theory of Cryptography (TCC'07), pp. 53-534.
4. Brandic, I., Music, D., Leitner, P., Dustdar, S. (2009). VieSLAF Framework: Enabling Adaptive and Versatile SLA-Management. In Proceedings of the 6th International Workshop on Grid Economics and Business Models (GECON'09), pp. 60-73, August 25-28, 2009, Delft, The Netherlands.
5. Cavoukian, A. (2008). Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet. Available online at: http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf.
6. Chappel, D. (2008). Introducing the Azure Services Platform. Available online at: http://download.microsoft.com.(Accessed on: January 23, 2013).
7. Chong, F., Carraro, G., and Wolter, R. (2006). Multi-Tenant Data Architecture. Available online at: http://msdn.microsoft.com/en-us/library/aa479086.aspx. (Accessed on: January 23, 2013).
8. Cloud Computing Security: Making Virtual Machines Cloud Ready. Available online at:
9. http://www.techrepublic.com/whitepapers/cloud-computing-security-making-virtual-machines-cloudready/1728295. (Accessed on: January 23, 2013).
10. Creeger, M. (2009). Cloud Computing: An Overview. ACM Queue- Distributed Computing, Vol 7, Issue 5, p. 2, June 2009. New York: ACM Press.
11. DeCandia, G., Hastorun, D., Jampani, M., Kakulapati, G., Lakshman, A., Pilchin, A., Sivasubramanian,
12. S., Vosshall, P., and Vogels, W. (2007). Dynamo: Amazon's Highly Available Key-Value Store. In Proceedings of the 21st ACM SIGOPS Symposium on Operating Systems Principles (SOSP'07), pp. 205220, Stevenson, WA, USA, October 2007.
13. Desisto, R. P., Plummer, D. C., and Smith, D. M. (2008). Tutorial for Understanding the Relationship between Cloud Computing and SaaS. Stamford, CT: Gartner, April 2008.
14. Emig, C., Brandt, F., Kreuzer, S., and Abeck, S. (2007). Identity as a Service- Towards a ServiceOriented Identity Management Architecture. In Proceedings of the 13th Open European Summer School and IFIP TC6.6 Conference on Dependable and Adaptable Network and Services (EUNICE'07), pp. 1-8, July 2007, Twente, The Netherlands.
15. Everett, C. (2009). Cloud Computing- A Question of Trust. Computer Fraud & Security, Vol 2009, Issue 6, pp. 5-7 June 2010.
16. Gellman, R. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing.
17. World Privacy Forum (WPF) REPORT, February 23, 2009. Available online at: http://www.worldprivacyforum.org/cloudprivacy.html (Accessed on: January 23, 2013).

18. Golden, B. (2009). Capex vs. Opex: Most People Miss the Point about Cloud Economics. URL: http://www.cio.com/article/484429/Capex_vs._Opex_Most_People_Miss_the_point_About_Cloud_Econ omic.
19. Heritage, T. (2009). Hosted Informatics: Bringing Cloud Computing Down to Earth with Bottom-Line Benefits for Pharma. Next Generation Pharmaceutical, Issue 17, October 2009.
20. Itani, W., Kayssi, A., and Chehab, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. In Proceedings of the 8th IEEE International Conference on Dependable, Automatic and Secure Computing (DASC'09), pp. 711-716, Chengdu, China, December 2009.
21. Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. IEEE Security & Privacy, Vol 7, Issue 4, pp. 61-64, July-August 2009.
22. Messmer, E. (2009). Gartner on Cloud Security: 'Our Nightmare Scenario is Here Now.' Network World October 21, 2009. URL: http://www.networkworld.com/news/2009/102109-gartner-cloud-security.html. (Accessed on: January 23, 2013).
23. Open Cloud Manifesto. http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf. (Accessed on: January 23, 2013).
24. Pearson, S. (2009). Taking Account of Privacy when Designing Cloud Computing Services. In Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing (CLOUD'09), pp. 44-52, Vancouver, British Columbia, Canada, May 2009.
25. Pearson, S. and Charlesworth, A. (2009). Accountability as a Way Forward for Privacy Protection in the
26. Cloud. In Proceedings of the 1st International Conference on Cloud Computing (CloudCom'09), pp. 131144, December 2009, Beijing, China.
27. Petry, A. (2007). Design and Implementation of a Xen-Based Execution Environment. Diploma Thesis, Technische Universitat Kaiserslautern, April 2007.
28. Price, M. (2008). The Paradox of Security in Virtual Environments. IEEE Computer, Vol 41, Issue 11, pp. 22-38, November 2008.
29. RightScale Inc. (2009). RightScale Cloud Management Features. URL: http://www.rightscale.com/products/cloud-management.php. (Accessed on: January 23, 2013).
30. Rochwerger, R., Caceres, J., Montero, R. S., Breitgand, D., Elmroth, E., galls, A., Levy, E., Llorente, I. M., Nagin, K., and Wolfsthal, Y. (2009). The RESERVOIR Model and Architecture for Open Federated Cloud Computing. IBM Systems Journal, September 2009.
31. Schubert, L., Kipp, A., and Wesner, S. (2009). Above the Clouds: From Grids to Service-Oriented Operating Systems. In G. Tselentis, Jet al. (Eds.), Towards the Future Internet-A European Research Perspective, pp. 238-249, Amsterdam: IOS Press.
32. Sims, K. (2009). IBM Blue Cloud Initiative Advances Enterprise Cloud Computing. URL: http://www03.ibm.com/press/us/en/pressrelease/26642.wss. (Accessed on: January 23, 2013).
33. Sotomayor, B., Montero, R. S., Llorente, I. M., and Foster, I. (2009). Virtual Infrastructure Management in Private and Hybrid Cloud. IEEE Internet Computing, Vol 13, Issue 5, pp. 14-22, September-October 2009.

34. Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Linder, M. (2009). A Break in the Clouds: Towards a Cloud Definition. ACM SIGCOMM Computer Communication Review, Vol 39, Issue 1, pp. 50-55, January 2009.
35. Vouk, M. A. (2008). Cloud Computing – Issues, Research and Implementations. In Proceedings of the 30th International Conference on Information Technology Interfaces (ITI'08), pp. 31-40, Cavtat, Croatia, June 2008.
36. Vozmediano, R. M., Montero, R. S., and Llorente, I. M. (2011). Multi-Cloud Deployment of Computing Clusters for Loosely-Coupled MTC Applications. IEEE Transactions on Parallel and Distributed Systems, Vol 22, Issue 6, pp. 924-930. (Accessed on: January 23, 2011).