ENFORCING SECURITY ON CLOUD COMPUTING NETWORK: A THEORETICAL FRAME WORK

Mughele E.S.
Department of Science and Technology
Computer Science Option
Delta State School of Marine Technology
Burutu, Delta State, Nigeria
prettysophy77@yahoo.com

Ibitola A.
Department of Computer Science
Lead City University
Ibadan, Nigeria
ibitolaayobami@yahoo.com

Okunoye, A.
Williams College of Business
Xavier University
Cincinnati Ohio. USA.

ABSTRACT
Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability as well as providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service(PaaS), and Infrastructure-as-a-Service (IaaS). The paper highlighted various threats in cloud computing networking, and also proffered solution by discussing extensively various security measures to be enforced on the system to achieve security to a large extent. This paper presents a security architecture that enables a user of cloud networking to define security requirements and enforces them in the cloud networking infrastructure.

Keywords: Cloud Computing, Infrastructure, Abstraction, Services, Security & Framework.

1. INTRODUCTION

Cloud computing is a technology which provide you a service through which you can use all the computer hardware and software sitting on your desktop, or somewhere inside your network but they are not actually installed on your computer, it is provided for you as a service by another company and accessed over the Internet [Priya, 2011]. Cloud computing, or computing as a utility, is a new computing paradigm. It allows third party service providers (i.e. cloud service providers) to provide a centralized pool of configurable computing resources to end-users. The end-users (individuals and enterprises) could make on-demand accesses to these resources and use them to implement their services according to their ever-changing requirements. In this way, the end-users do not need to deploy and manage their own computing services thus enabling fast deployment and minimum operational and management overheads [Ren et al, 2011].

Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends information technology‘s existing capabilities. Cloud computing promotes availability, zero maintenance, subscription based service [Asha, 2012].

In cloud computing, remote servers are being entrusted with users’ data, software and computations, thus, making it open up to a new world of opportunities. Moreover, consumers still have control over the deployed applications. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies [Wayne, 2011]. However, it is an emerging form of distributed computing still in its infancy which stipulates that cloud computing is still a work in progress. While Cloud computing brings promising benefits, it also introduces some challenging security and privacy issues that need to be considered and addressed prior to committing to a cloud computing strategy. Understanding who is responsible for what is vital before moving to cloud [Asha, 2012]. These issues include how data owners (i.e. entities which have outsourced their data) could be assured that their data are used in an authorized manner, how the confidentiality of outsourced data be protected while still allowing legitimate accesses of data, or allowing computations being performed on the data, how the trustworthiness of service metering be assured so that end-users are not charged unfairly, etc.

In computing generally, there is a trade-off between functionality and achieving better security [Adkins et al, 2003]. Consider a set of primitives required to implement some functionality. As the functionality of a system increases, we usually need more primitives to implement them. The probability that none of the primitives has a security flaw decreases (security is often an all-or-nothing game, as a single flaw can render the entire system vulnerable). Thus, simplicity and less functionality (fewer primitives) usually contribute to increased security [Schneier, 1997].
Contrary to this popular belief, this research provides an overview of the security and privacy challenges relevant to cloud computing and points out measures that should taken when outsourcing data, applications, and infrastructure to a public cloud environment.

1.1 Research Problem
Due to the advantages of greater flexibility and availability in obtaining computing resources at lower cost, the interest in cloud computing has grown rapidly in recent years. However, security and privacy are a concern for end-users (individuals and enterprises) considering transitioning applications and data to cloud computing environments, and form the impetus behind this paper. Cloud computing is more than simply a technical challenge. By putting our personal data on remote servers, we risk losing control over that data. Security is an essential component of strong privacy safeguards in all online computing environments, but security alone is not sufficient. Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure [Priya 2011].

These issues include how data owners (i.e. entities which have outsourced their data) could be assured that their data are used in an authorized manner, how the confidentiality of outsourced data be protected while still allowing legitimate accesses of data, or allowing computations being performed on the data, how the trustworthiness of service metering be assured so that end-users are not charged unfairly, etc.

Researchers have shown that users should have a well defined methodology before migrating to cloud computing. The less control you have for your data means more you have to trust the providers'security policies. Security and privacy issues have to be addressed from the initial phase, considering after the deployment will be more complicated, expensive and risky [Asha 2012].
The usual security norm in public cloud is service level agreements (SLAs) which talks about the expected level of services provided by the cloud provider to the cloud consumer. Consumers make sure that the contract they sign have reference to the security measures that the provider have in mind and also make sure that the contract meet the expected security norms from their business perspective [Asha 2012]. The complete terms and conditions for a cloud service agreement are usually stipulated in multiple documents, which can typically include a Service Level Agreement (SLA), privacy policy, acceptable use policy, and terms of use [Bradshaw et al, 2010].

Two types of service agreements exist: predefined non-negotiable agreements and negotiated agreements [Wayne & Timothy, 2011]. Non-negotiable agreements are in many ways the basis for the economies of scale enjoyed by public cloud computing. The terms of service are prescribed completely by the cloud provider. They are typically not written with attention to federal privacy and security requirements. Furthermore, with some offerings, the provider can make modifications to the terms of service unilaterally (e.g., by posting an updated version online) without giving any direct notification to the cloud consumer [Bradshaw et al., 2010].
End- users who want to deploy critical applications can think about private clouds over public clouds which offer better insight and control over security and privacy [Asha 2012].

1.2 Research Objectives
The objectives of this research are to provide an overview of cloud computing and the security and privacy challenges involved. This paper discusses the threats, technology risks, and protective measures for cloud environments, and provides the insight needed to make informed information technology decisions on their treatment.

1.3 Research Questions
Many of the features that make cloud computing attractive, however, can also be at odds with traditional security models and controls [Wayne & Timothy, 2011].
Cloud computing does raise a number of important policy questions concerning how end-users (people, organizations, and governments) handle information and interactions in this environment. The key questions of Cloud Computing as it is shared and its on-demand nature include but limited to the following;

- how data owners (i.e. entities which have outsourced their data) could be assured that their data are used in an authorized manner,
- how the confidentiality of outsourced data can be protected while still allowing legitimate accesses of data, or allowing computations being performed on the data,
- how the trustworthiness of service metering be assured so that end-users are not charged unfairly, etc.

1.4 Scope
This paper provides an overview of public cloud computing and the security and privacy challenges involved; discusses the threats, technology risks, and protective measures for cloud computing environments, and provides the perceptiveness needed to make essential information technology decisions on their treatment. The paper does not recommend any specified cloud computing service, service arrangement, service agreement, service provider, or deployment model. Each end-user (individuals and enterprises) must perform its own analysis of its needs, and assess, select, engage, and oversee the public cloud services that can best fulfill those needs.

1.5 Research Significance
Cloud computing presents IT organizations with a funda-mentally different model of operation, one that takes advantage of the maturity of web applications and

networks and the rising interoperability of computing systems to provide IT services. The essence of this paper is to make more highlights on cloud computing and the security and privacy challenges involved; discusses the threats, technology risks, and protective measures for cloud computing environments, and provides the perceptiveness needed to make essential information technology decisions on their treatment and as well provide basis/ platform for further research. Fundamentally, the researcher believes that further research is needed to enhance the security features of these cloud computing technologies.

2. RELATED WORKS

Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [Mell, 2011]. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other practicable efficiencies. However, cloud computing is an emerging form of distributed computing that is still undergoing evolution and standardization. The term itself is often used today with a range of meanings and interpretations [Fowler, 2009]. Much of what has been written about cloud computing is definitional, aimed at identifying important paradigms of deployment and use, and providing a general taxonomy for conceptualizing important aspects of service [Wayne & Timothy, 2011].

2.1Deployment Models

Deployment models broadly characterize the management and disposition of computational resources for delivery of services to consumers, as well as the differentiation between classes of consumers. They include

1. **Public cloud computing:** is one in which the infrastructure and computational resources that it comprises are made available to the general public over the Internet. It is owned and operated by a cloud provider delivering cloud services to consumers and, by definition, is external to the consumers' organizations.
2. **Private cloud computing:** is one in which the computing environment is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it. A private cloud has the potential to give the organization greater control over the infrastructure, computational resources, and cloud consumers than can a public cloud.
3. **Community cloud computing:** falls between public and private clouds with respect to the target set of consumers. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization.
4. **Hybrid cloud computing**: are more complex than other deployment models, since they involve the composition of two or more clouds (private, public or community). Each member remains a unique identity, but is bound to others through standardized or proprietary technology that enables application and data portability to them.

While the choice of deployment model has implications for the security and privacy of a system, the deployment model itself does not dictate the level of security and privacy of specific cloud offerings [Wayne & Timothy, 2011].

2.2 Service Models

Just as deployment models play an important role in cloud computing, service models are also an important consideration. A service model can be actualized as a public cloud or as any of the other deployment models. Three well-known and often-used service models are the following:

- **Software-as-a-Service.** (SaaS) provides a software services to end users. Web-based email and Google Documents are perhaps the best-known example of SaaS. End user gets the access to use the software utility but he has no rights to change or to modify it. Software is not installed on end user computer it is configured in cloud. End user has to pay for the service according to their requirements.
- **Platform-as-a-Service.** (PaaS) provides an end user a facility to develop his own application which will run on the platform or environment provided by the cloud service of some other company. The end users may or may not know that the application is hosted on the cloud. The storage space for user data may be increased or decreased per the requirement of the applications. A typical example is the Google App Engine.
- **Infrastructure-as-a-Service.(I**aaS) provides an access to hardware resource such as storage or raw computing hardware . Since you buy what you need and pay-as-you-go, this is often referred to as utility computing. A simple example of IaaS: you pay a monthly subscription or a per-megabyte/gigabyte fee to have a hosting company serve up files for your website from their servers.

2.3 Scope and Control Among Cloud Service Models

[Extracted from Wayne Jansen, Timothy Grance, The NIST Guidance on security and privacy in public cloud Computing, January 2011.]

The figure below illustrates scope and control between the cloud consumer and cloud provider for each of the service models discussed above. Five conceptual layers of a generalized cloud environment are identified in the centre diagram and apply to public clouds, as well as each of the other deployment models. The arrows at the left and right of the diagram denote the approximate range of the cloud provider's and cloud consumer's scope and control over the cloud environment for each service model. In general, the higher the level of support available from a cloud provider, the more narrow the scope and control the cloud consumer has over the system.

The two lowest layers shown denote the physical elements of a cloud environment, which are under the full control of the cloud provider, regardless of the service model. Heating, ventilation, air conditioning (HVAC), power, communications, and other aspects of the physical plant form the bottom layer, the *facility layer*, while computers, network and storage components, and other physical computing infrastructure elements form the *hardware layer.*

The remaining layers denote the logical elements of a cloud environment. The *virtualized infrastructure layer* entails software elements, such as hypervisors, virtual machines, virtual data storage, and virtual network components used to realize the infrastructure upon which a computing platform can be established.
While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded.

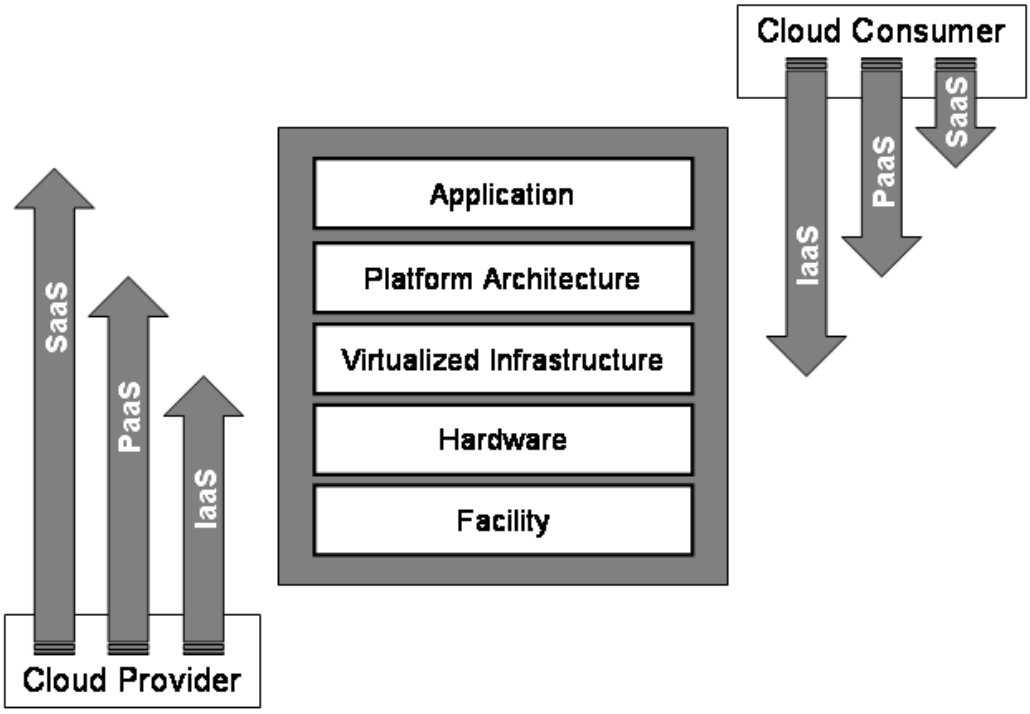

Figure 1: Scope and Control among Cloud Service Models

Similarly, the *platform architecture layer* entails compilers, libraries, utilities, middleware, and other software tools and development components needed to implement and deploy applications. The *application layer* represents deployed software applications that are targeted towards end-user software clients or other programs, and made available via the cloud.

Some have argued that the distinction between IaaS and PaaS service models is fuzzy, and in many commercial offerings, the two are more alike than different [Armbrust et al., 2010]. Nevertheless, these terms do serve a purpose, distinguishing between very basic support environments and environments having greater levels of support, and accordingly different allocations of control and responsibility between the cloud consumer and the cloud provider.

3. DESIGN METHODOLOGY

A well configured cloud computing architecture is a hacker's worst nightmare. Conversely, a poorly configured cloud computing architecture is a hacker's best dream. You cannot build secure systems until you understand your threats [Priya et al., 2011].

Moreover, considering the questions of Cloud Computing as it is shared and its on-demand nature which includes the following; how data owners (i.e. entities which have outsourced their data) could be assured that their data are used in an authorized manner, how the confidentiality of outsourced data can be protected while still allowing legitimate accesses of data, or allowing computations being performed on the data, how the trustworthiness of service metering be assured so that end-users are not charged unfairly, etc., a model with combination of different techniques has to be developed and implemented to prevent threats and to keep data on cloud secure and private.

The major disparity between cloud computing and the traditional information technology systems is the increased complexity and difficulty in providing adequate supervision to maintain accountability and control over deployed applications and systems.
Before the highlighted problems can be tackled, the threat or jeopardizes have to be briefly considered.

3.1 Threats

The dangers to keep data secure and private include but not limited to the following:

- **Abusive and scandalous use of cloud computing**
  The cloud environment offers several added utilities to the users including unlimited bandwidth and storage capacity to run the applications smoothly. Some providers even allow other benefits like free limited trial periods and additional usage. These user models frequently come under the security threats and malicious attacks. The areas of concern of these attacks include decoding and cracking of the password, launching potential attack points and executing malicious commands.
- **Breach in interfaces and APIs**
  Cloud computing users have smooth access of a comprehensive set of software interfaces or APIs manage and execute internal communication with cloud services. These APIs play an integral part during provisioning, management, orchestration, and monitoring of the processes running in the cloud environment. The failure to monitor the authentication and access control and other associated encryption and activity monitoring policies provides a pathway for malicious attack.

- **Insider threat and attack**
  These kinds of attacks and breaches are done due to the lack of transparency into the cloud provider s delivery mechanism and procedure. Any superficial command over the level of access could lead to various adversaries like corporate hacking and organized business threats in the domain of business verticals [Priya, 2011]. The insider security threat is a well-known issue for most organizations and, despite the name, applies as well to outsourced cloud services [Kowalski, 2008]. Insider threats go beyond those posed by current or former employees to include contractors, organizational affiliates, and other parties that have received access to an organization's networks, systems, and data to carry out or facilitate operations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information. Incidents may also be caused unintentionally—for instance, a bank employee reportedly sent out sensitive customer information to the wrong Google mail account [Zetter, 2009].
  Moving data and applications to a cloud computing environment operated by a cloud provider expands the circle of insiders not only to the cloud provider's staff and subcontractors, but also potentially to other customers using the service, thereby increasing risk. For example, a denial of service attack launched by a malicious insider was demonstrated against a well-known IaaS cloud [Slaviero et al., 2009].

3.2 Mitigation Techniques

After the various threats of security and privacy issues have been comprehensively analysed, mitigation techniques/ strategies can be designed to evaluate solutions.

1. **Enforcing An Effective Service Agreement**
   A service agreement defines the complete terms and conditions for access and use of the services offered by the cloud provider. It also establishes the period of service, conditions for termination, and disposition of data (e.g., preservation period) upon termination. The complete terms and conditions for a cloud service agreement are usually stipulated in multiple documents, which can typically include a Service Level Agreement (SLA), privacy policy, acceptable use policy, and terms of use [Bradshaw et al., 2010]. That is, the service agreement is the primary means for an organization to enforce control and maintain accountability over the computing environment [Wayne & Timothy, 2011].

   Thus, it is essential the terms of the service agreement fully meet the needs of the end-user, since responsibilities normally held by the end-user are given over to the cloud provider and, without sufficient provisions; the consumer would have little recourse to address problems and resolve to its satisfaction issues that may arise.
   Considering the growing number of public cloud providers and the broad range of services offered by them, organizations must exercise due diligence when selecting and moving functions to a public cloud. Decision making about services and service arrangements entails striking a balance between benefits in cost and productivity versus drawbacks in risk and liability. An organization may be able to employ compensating security and privacy controls to work around identified shortcomings in a public cloud service. Non-negotiable service agreements generally limit the range of risk-mitigation activities available to an end-user, while negotiated service agreements, which provide greater range and flexibility, necessitate careful scrutiny and prioritization of requirements that are incorporated into the terms of service in order to be cost effective.

Therefore, in outsourcing to a cloud provider an end-user should carry out prescribed activities to remain accountable and mitigate the above-mentioned security and privacy issues. This involves specifying the requirements when planning the initiative [Leng, 2003].The end-user must identify its security, privacy, and other requirements for cloud services, as a criterion for the selection of a cloud provider. Common security requirements include coverage for the following areas [Leng, 2003]:

- Personnel requirements, including clearances, roles, and responsibilities
- Regulatory requirements
- Service availability
- Problem reporting, review, and resolution
- Information handling and disclosure agreements and procedures
- Physical and logical access controls
- Network access control, connectivity, and filtering
- Data protection
- System configuration and patch management
- Backup and recovery
- Data retention and sanitization
- Security and vulnerability scanning
- Risk management
- Incident reporting, handling, and response
- Continuity of operations
- Resource management
- Certification and accreditation
- Assurance levels
- Independent auditing of services.
- Service metering procedures/ measures

Part of the requirements analysis should narrow the choice among IaaS, PaaS, and SaaS service models to a single selection that is appropriate for the end-users's specific needs and objectives. The responsibilities of both the end-user and the cloud provider vary depending on the service model.

Establishing an exit strategy is an important part of the planning process and should be factored into the requirements analysis. It also relates to the organization's contingency and continuity planning activities. The exit strategy should cover a normal termination, such as that at expiration of the service agreement, and also an unexpected termination, such as that due to service provider bankruptcy or poor performance [Grance, 2003]. The ability to export all of the organization's data in a usable format through a secure, reliable, and efficient means, and in a timely manner, is a vital aspect of an exit strategy. Other aspects include addressing application dependencies on proprietary programming interfaces, system calls, and database technologies, as well as the recovery of useful metadata that may have accumulated within the cloud environment [Wayne & Timothy, 2011].
However, include clause regarding data ownership and protection of intellectual property in SLA agreement.

2. **Client Side Security**
Cloud computing encompasses a client and a server, nonetheless, the client side security is always over looked. The first step towards a secure data management business is strengthening the client side security. To provide physical and logical safety to client machine is a big challenge. Built in security measures can be eluded by an erudite person without much difficulty. To maintain secure client, end- users should review existing security practices and employ additional ones to ensure the security of its data. Clients must consider secure VPN to connect to the provider.

Web browsers are majorly used in client side to access cloud computing services. Cloud providers usually provide the consumers with APIs which is used by the latter to control, monitor the cloud services. It is vital to ensure the security of these APIs to protect against both accidental and malicious attempts to evade the security. The various plug-ins and applications available in the web browsers also causes a serious threat to the client systems used to access the provider. Many of the web browsers do not allow automatic updates which will append to the security concerns. To ensure secure cloud end-users should work on the existing internal policies, incorporate automatic update features to the web browsers and improvise its security strategies if necessary.

3. **Cloud Service Providers Side Security**
There exist many security concerns in server side. To adopt cloud computing it is necessary to ensure providers security measures. To enhance the trust factor, providers can get their system verified by external organizations or by security auditors.
Aside from the security factor other issues that needs attention is about the data in the cloud, if at the provider goes bankrupt or being acquired by another business. Traditional data centers used to have regular security audit and mandatory security certifications which ensure the data security. Cloud providers should also incorporate these measures to assure secure transaction among its customers. A secure infrastructure ensures and builds confidence that the data stored is secure in providers'side. Proper implementation of security measures is mandatory in cloud computing [Asha, 2012]. Cloud providers should also think beyond the customary security practices like restricted user access, password protection etc. Physical location of stored data is also vital and it's the responsibility of the provider to choose the right location of storage.

Restricted user access can vary from simple user name/password protection to Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) log in forms. When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked. Cloud Providers can also consider one time password authentication where the clients will get one time temporary password from SSN/mobile device which helps in data security even if password is compromised.

4. **Installation And Maintenance Of Firewall**
Installation of firewall and its maintenance is mandatory to ensure the protection. A firewall should be present in all external interfaces. A list of necessary port and services should be maintained. Assessment of firewall policies and rule sets and reconfiguration of router should be done in regular intervals. Build and deploy a firewall that denies access from ―untrusted‖ sources or applications, and adequately logs these events. Build and deploy a firewall that restricts access from systems that have direct external connection and those which contain confidential data or configuration data. [Wayne & Grance, 2011].

5. **Data Encryption**
Data encryption is one common approach the providers follow to safe guard their clients data but the question is whether the data is getting stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store crucial data, end-users can think of private or hybrid cloud where the data will be in secure corporate firewall. Encryption /decryption key should be kept secured.

6. **Certification and Auditing**
Providers should allow the customers to determine the security measures followed data storage details so that the customers can ensure the data security policies of the providers.
Data access to the cloud by the employees should be monitored and recorded so that the providers will be able to furnish the detailed report of who has accessed what data at a given point of time. Before moving any sensitive data to the cloud; consumers should ensure that the providers are certified by external agencies and they follow the expected security standards and practices [Asha, 2012]. Regular auditing should be conducted

7. **Data Sanitization**
Data sanitization is essential for cloud security especially since the data is stored in a common platform. Sensitive data should be removed from storage devices when the particular device is moved to different location or when it‘s removed from a particular service. Data refinement is valid in case of backed up data also. Data sanitizations should be done at the right time

8. **Back Up and Recovery**
The cloud end- users will never be able to make out the exact storage location of their records because data is stored in distributed location. Hence, data backup and recovery is essential.
Backup software should include public cloud APIs, enabling simple backup and recovery across major cloud storage vendors, such as Amazon S3, Nirvanix Storage Delivery Network, Rackspace and others, and giving end- users flexibility in choosing a cloud storage vendor to host their data vault.
One debatable question is whether to back up the entire data or to backup critical and vital data. If provider agrees to backup crucial data then the question arises on how to determine the priority of data. The easiest, least complicated and the best way is to protect the entire workstation or the server. It is critical for the backup application to encrypt confidential data before sending it offsite to the cloud, protecting both data-in-transit over a WAN to a cloud storage vault and data-at-rest at the cloud storage site. However, frequent data backup policy should be in place

9. **Identity and Access Management**
Identity and Access management eliminates the need for sharing the passwords and also allows the implementation of security best practices To ensure secure transaction, business employ two levels of security system; one in client side and another in the server side which is tiresome and may not be feasible always. Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard or the OpenID standard.

A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information, such as assertions related to a subject or authentication information, between cooperating domains. SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the eXtensible Markup Language (XML) for its format. SOAP messages are digitally signed. For example, once a user has established a public key certificate for a public cloud, the private key can be used to sign SOAP requests. SOAP message security validation is complicated and must be carried out carefully to prevent attacks. For example, XML wrapping attacks have been successfully demonstrated against a public IaaS cloud [Gruschka, 2009]. XML wrapping involves manipulation of SOAP messages. A new element (i.e., the wrapper) is introduced 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]. The original body can still be referenced and its signature verified, but the operation in the replacement body is executed instead. SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud subscriber privileges and maintain control over access to resources is also needed. As part of identity management, standards like the eXtensible Access Control Markup Language (XACML) can be used by a cloud provider to control access to cloud resources, instead of using a proprietary interface. 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. XACML is capable of controlling the proprietary service interfaces of most providers, and some cloud providers already have it in place. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, making it important to have safeguards in place to protect decision requests and authorization decisions from possible attacks, including unauthorized disclosure, replay, deletion and modification [keleta et al., 2005].

4. CONCLUSION

Despite the mouth –watering benefits and importance of cloud computing, it has some disadvantages over privacy and security issues. This research has comprehensive discussed the issues and the mitigating strategies. Though the paper does not specify any cloud computing service, service arrangement, service agreement, service provider, or deployment model, it would channel end-users (individuals and enterprises) towards the path that can best fulfill their needs.

REFERENCES

1) *Andy Greenberg*, IBM's Blindfolded Calculator, Forbes Magazine, July 13, 2009,
2) *B. Schneier.* Why cryptography is harder than it looks. 1997
3) *Bee Leng*, A Security Guide for Acquiring Outsourced Service, GIAC GSEC Practical (v1.4b), SANS Institute, August 19, 2003
4) *Bernd Grobauer, Thomas Schreck,* Towards Incident Handling in the Cloud: Challenges and Approaches, ACM Cloud Computing Security Workshop, Chicago, Illinois, October 8, 2010.
5) *Daniel Adkins Karthik Lakshminarayanan Adrian Perrig Ion Stoica,* Towards a more functional and secure network infrastructure
6) *Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall*, Common Sense Guide to Prevention and Detection of Insider Threats, Third Edition, Version 3.1, CERT, January 2009,
7) *Eileen Kowalski et al.,* Insider Threat Study: Illicit Cyber Activity in the Government Sector, U.S. Secret Service and Carnegie Mellon University, Software Engineering Institute, January 2008,
8) *Erika McCallister, Tim Grance, Karen Scarfone*, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), SP 800-122, National Institute of Standards and Technology, April 2010,
9) *Geoffrey Fowler, Ben Worthen*, The Internet Industry Is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009
10) *Haroon Meer, Nick Arvanitis, Marco Slaviero*, Clobbering the Cloud, Part 4 of 5, Black Hat USA Talk Write-up, SensePost SDH Labs, 2009,
11) *john W. Rittinghouse and james F. Ransome, Cloud computing: implantation, management and security 2009*
12) *Julia Allen et al.,* Security for Information Technology Service Contracts, CMU/SEI-SIM-003, Software Engineering Institute, Carnegie Mellon University, January 1988,
13) *Kim Zetter*, Bank Sends Sensitive E-mail to Wrong Gmail Address, Sues Google, Wired Magazine, September 21, 2009,
14) *Kui Ren, Cong Wang and Qian Wang*, ?Security Challenges for the Public Cloud?, Internet Computing, IEEE, Vol. 16, No. 1. (January 2012),
15) *Marco Slaviero*, BlackHat Presentation Demo Vids: Amazon, part 4 of 5, AMIBomb, August 8, 2009.

16) *Michael Armbrust et al.,* A View of Cloud Computing, Communications of the ACM, Association for Computing Machinery, Vol. 53, No. 4, April 2010.
17) *Nils Gruschka, Luigi Lo Iacono*, Vulnerable Cloud: SOAP Message SecurityValidation Revisited, IEEE International Conference on Web Services, Los Angeles, California, July 2009.
18) *Peter Mell, Tim Grance*, The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, August 2011
19) *Richard Chow et al*., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security, Chicago, Illinois, November 2009
20) *Sebastian Gajek, Meiko Jensen, Lijun Liao, and Jörg Schwenk*, Analysis of Signature Wrapping Attacks and Countermeasures, IEEE International Conference on Web Services, Los Angeles, California, July 2009.
21) *Simon Bradshaw, Christopher Millard, Ian Walden*, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary School of Law Legal Studies, Research Paper No. 63/2010, September 2, 2010
22) *Stephanie Overby,* How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010,
23) *Tim Grance et al.,* Guide to Information Technology Security Services, Special Publication 800-35, National Institute of Standards and Technology, October 2003
24) *Warwick Ashford*, Google Confirms Dismissal of Engineer for Breaching Privacy Rules, Computer Weekly, September 16, 2010,
25) Wayne Jansen, Timothy Grance, Guidelines onSecurity andPrivacyin Public Cloud Computing, 2011
26) *Wik, Philip* (2011-10) "thunder clouds; managing SOA- Cloud risk" – service technology magazine
27) *Winkler, vic* " cloud computing: virtual cloud security concerns"telnet magazine, Microsoft. 12 – 02 - 2012
28) *Yared Keleta, J.H.P. Eloff, H.S. Venter*, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005,