ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

# Security Issues in Cloud Computing

Binto George

School of Computer Sciences, Western Illinois University, Macomb, IL 61455, United States

**Abstract**: Cloud computing allows on-demand provisioning of computing services. Despite the many advantages, the cloud computing environment faces many security challenges. This paper reviews major security issues arising in the cloud computing environment owing to computation outsourcing, multi-tenancy and broad network access. Notable research in the area is summarized. A set of recommendations for secure deployment on the cloud is also included.

**Keywords**: Cloud Computing, Security, Cloud Security, Data Security

## I. INTRODUCTION

Small electric generators were sold to customers around the world in 1870s. Later came the idea of setting up a central plant and a network to deliver electric energy to customers who pay utility charges on a monthly basis. Such transmission systems were then interconnected to reduce operational costs, to provide fault tolerance and to balance load. In many ways, cloud computing resembles power grids -- instead of deploying powerful computing devices on site, using a high speed data network an organization can tap into the computing resources of the cloud.

Cloud computing is characterised by on demand service provisioning, elasticity and standardized Application Programming Interfaces (API). Many types of cloud computing services have evolved over time. (i) Infrastructure as a Service (IaaS) provides the ability to provision basic computing resources such as processors, storage and networking. (ii) Platform as a Service (PaaS) model provides operating systems and tools required for applications development (e.g., compilers) in addition to the basic cloud infrastructure. (iii) Software as a Service (SaaS) model lets consumers to rent applications software instead of owing and maintaining them on their own.

Based on the ownership, clouds can be categorized into private clouds, public clouds and hybrid clouds. Private cloud is usually owned and operated by an organization. Public clouds can be availed by the general public. A hybrid cloud is a combination of different clouds: e.g., a private cloud and a public cloud. More information on cloud computing is available at [1].

An organization's computing needs may vary over time. For instance, the computing requirement may be the highest during peak sales seasons. Traditional computing will require businesses to procure and install additional computers (servers) for handling the peak load or risk losing sales due to the lack of resources. And the additional computers sit idle during off peak times. Further, it is also difficult for an organization to quickly scale their computing capability based on increase in demand as it generally needs significant lead time in procuring and setting up additional computing nodes. Cloud computing solves this problem by enabling customers to dynamically provision computing resources on a demand basis and pay for the computing resources they use. Cloud computing can also offer ubiquitous access to data, which is a considerable advantage for maintaining a global presence. Despite all the advantages, cloud computing also introduces additional security threats as you will discover in this paper.

## II. SECURITY ISSUES

Since cloud computing builds on technologies such as networking, databases, operating systems, virtualization, etc., cloud systems are subject to vulnerabilities of the underlying technologies [2]. Cloud computing also brings additional security challenges of its own. In this paper, we focus on security issues specific to cloud computing arising from computation outsourcing, multi-tenancy, remote network access, cloud architecture, cost of service and legal aspects [3] .

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

*A. Computation Outsourcing*

Using a third party cloud provider may require a tenant (cloud user) to relinquish the control of its data and programs (including proprietary algorithms). Cloud services may provide vulnerable Application Programming Interfaces (API) and use heterogeneous hardware making security even more challenging. In addition, cloud computing providers may access sensitive data or retain tenants' data beyond the desired data lifetime. Deleting data from the cloud providers is no assurance that the data is indeed destroyed. Cloud providers may also collect tenants' usage data and other information that they may retain for long time. Data may be also sold to third parties. The hidden cloud infrastructure and little known operations mean the tenant has to deal with an unknown risk profile.

Tenants' data may also be locked in with the cloud provider. This is especially true, if tenants are using the cloud provider's non-standard software applications or resources. For instance, an online store decides to host with a cloud hosting provider. The store uses the free shopping cart provided. In this scenario, at a later point of time, if the online store wants to use a different cloud provider due to service issues or cost reasons, significant reworking of their web application would be needed. Also, in some scenarios, the data may be held hostage by the cloud provider. A cloud provider closing its business will need all tenants to be relocated to other clouds, unexpectedly causing significant overhead. In some cases, the data stored at remote cloud providers may not be restored at all or a cloud service cannot be restarted with minimal user impact.

It is often difficult to know the hiring practices of the third party cloud provider. Malicious insiders can be a security threat to the tenants. Cloud service providers may also outsource their work to other contractors. Since multiple organizations are involved, probability of social engineering (attacks exploiting human psychology) is high.

Because of the reasons described above, many companies build their own private clouds rather than depending on third party providers. This choice, however, severely limits many of the benefits of cloud computing such as economy of scale and elasticity.

*B. Multi-Tenancy*

A cloud provider often hosts multiple tenants. This introduces some performance issues when other tenants procure resources. In addition, some tenants may snoop on other tenants or may pick up the data accidently left behind by another tenant. Cloud providers limit the possibility of data leakage by isolating each tenant using technology such as virtualization. Any isolation failure can result in data breaches.

Malicious activities of one tenant may tarnish the reputation of others. For example, a shared IP address may be blacklisted if one of the tenants send unsolicited emails.

*C. Remote Network Access*

Typically tenants manage cloud computing resources over the Internet using a web browser or using web services. Because of this broad network access, an attacker may tamper with the messages exchanged between the tenant and the cloud service provider. Malware such as viruses from Internet may find its way into the cloud computing infrastructure. An attacker may be able to create a malicious virtual machine within the cloud. A denial of service attack may cause the cloud system to provision more and more resources in the end causing shortage of resources, resulting in availability problems. The cloud APIs may also be vulnerable to many attacks from the Internet.

The current trend of Bring Your Own Devices (BYOD) means more and more users are accessing cloud infrastructure from personal devices. For instance, an employee may install apps including malware on a personal device. The same device may be used to access the cloud making it susceptible to key logging attacks. This may compromise cloud passwords.

*D. Cloud Architecture*

The cloud computing deploys many underlying technologies. Therefore, the cloud is susceptible to the inherent vulnerabilities of these technologies. It is also vulnerable to data leakage because virtual machines are moved around and data is replicated in multiple places.

Cloud architecture may be also subject to failure. Here is an example: Amazon's EC2 failed on April 21, 2011 when an Amazon technology team tried to upgrade the capacity of a primary network and wanted to shift the traffic to a backup router on the primary network. Instead of doings so, they shifted the traffic to a low capacity backup network.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

This overwhelmed the low capacity network and affected the data communications in the network. Heavy traffic prevented many nodes from syncing with their replicas causing massive build up of queues. Nodes failing to sync with replicas assumed that the replicas failed and tried aggressively to find new nodes for creating replicas [15]. Eventually much wider portions of the cloud were affected. As the result, many tenants suffered availability issues. Amazon's architecture assumes the responsibility to maintain availability with the tenants. Tenants are supposed to "design for failure" by deploying virtual machines or replicating the computing resources using the tools provided. Apparently, the tenants skipped this vital process were affected by the failure.

Cloud providers employ various types of redundancies to avoid failures. The physical redundancy means having multiple redundant infrastructural hardware systems. For example, having a RAID-6 configuration will help the system be tolerant of up to two disk failures. Virtual redundancy protects tenants from infrastructural failures - for example, two instances of virtual machines running in two different cloud infrastructures in the same location can let one instantly take over if the other fails. Further, even better protection is available by spreading out virtual machines across multiple geographical locations. Finally, organizations can deploy their applications with multiple cloud service providers.

### *E. Cost of Service*

The cloud Service Level Agreement (SLA) specifies the relationship between the tenant and cloud provider. Cloud providers usually charge an instance price based on the size of the virtual machine. There is also a hourly charge for the use. They also often charge for persistent data storage and database transactions. With this fee structure, Denial of Service (DoS) in the cloud environment has interesting implications. It is generally hard for Denial of Service attacks to affect the performance of cloud services. However, a tenant may be charged for additional computing resources as the result of Denial of Service attacks thereby resulting in considerably larger monthly bills.

### *F. Legal Aspects*

There are often legal restrictions on where the data can be hosted. Certain types of data are illegal in some jurisdictions. For instance, some countries prohibit strong encryptions. Some programs or data being export controlled are prohibited from leaving the national borders. Even the data flow across state boundaries can cause problems - gambling is legal in some states and is illegal in others.

Since data from multiple tenants is accumulated with a cloud provider, there can be increased political pressures and attempts from government for the control of data. Recently, Amazon evicted Wikileaks from its cloud. Cloud providers may also be targeted by subpoenas. In general, cloud providers' self-interest may affect tenants' opportunity for a proper defence. Swing of public opinion may also influence cloud providers.

Software licences are generally geared towards traditional computing. For instance, a license may specify that the software may be used at a particular location of a company. Deploying applications on the cloud may violate many license agreements.

Cloud computing providers may not provide enough transparency or reliable audit to meet compliance requirements such as Sarbanes-Oxley Act (SOX) or Health Insurance Portability and Accountability Act (HIPPA).

## III. RELATED RESEARCH

Chow et. al. [4] envision a few research directions by categorizing cloud security concerns into traditional security concerns, availability concerns and security concerns arising from third-party data control. Security issues of cloud including storage security, data security, network security and application security are discussed in [2]. They also explore how secure co-processors may be used to enhance security in a cloud environment.

A combination of Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP) and Single Sign-on (SSO) can address many threats faced by cloud computing systems. A third party, mutually trusted by cloud service provider and tenant, can verify security characteristics within a cloud system [5]. Systems such as Advanced Cloud Protection System (ACPS) [6] may be used to monitor the integrity of cloud infrastructure components without significant performance penalty.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

A set of protocols for ensuring privacy and legal compliance has been described in [10]. They use cryptographic coprocessors for providing isolation and establishing trust. The sensitive data processing is performed in isolated containers that are set up and maintained by a trusted third party.

Distributed Access Control in Clouds (DACC) algorithm [7] suggests a mechanism to enforce access control on the cloud, but assumes that the cloud is honest. DACC also needs the access control matrix to be transmitted within messages, exposing sensitive security information to the cloud.

Another approach to support access control in the cloud is Permission as a Service (PaaS) [11] which separates the access control from other services in the cloud. This provides a single point access control to all data, which is to be followed by all cloud services. It also helps logging. A PaaS prototype was also implemented using Attribute Based Encryption (ABE) [12].

Simplest and most common access control policy is to isolate tenant data traffic from one another. This puts a limit on collaboration between tenants within the same cloud infrastructure. Cloud Police [8] is an interesting work that can support inter-tenant communications, fair sharing of services and rate limiting capability. It also allows a tenant to initiate network connections to other tenants. This is possible because their Distributed Access Control mechanism is implemented within hypervisors rather than in the network.

A scheme for performing integrity measurements and remote attestations has been described in [13]. The system can thus detect any change in customers' data modified by the cloud provider itself or as a result of an attack from outside. An integrity measurement engine monitors and reports all changes to monitored files.

SLAs have been analysed in [9]. In general, SLAs only detail the services provided and waivers given if the cloud service provider fails to deliver those services. Ideally SLAs should address other issues such as security policies to help tenants to make informed decisions of security risks, performance impacts and liability.

## IV. RECOMMENDATIONS

Anyone considering cloud deployment should study the regulatory implications and their organization's internal policies of protecting trade secrets and intellectual property. Review the SLA carefully. There should be agreement of policies and procedures between the tenant and cloud provider for all security requirements. Tenants may also consider onsite inspections of cloud provider facilities. Make cloud providers responsible for the costs for data breaches or consider insurance policies to shift the risk.

Choose the right type of cloud for the application: public cloud, private cloud or hybrid cloud. Know how data integrity is maintained by the cloud service provider and how the integrity violations are detected and reported to the tenant. Tenant should always be able to know where the data is housed. Make sure the location of the data meets the compliance requirements. Tenants should be able to specify the access control and identities of authorized users. Tenants should ensure that the access control is allowed only on a need-to-know basis. Follow the principle of least privilege when assigning privileges. The cloud service provider should assume by default "deny all" for all data access controls. Secure federated identity management must be deployed across cloud systems. All stored data, by default, must be encrypted using strong cryptography.

Examine what isolation mechanisms are used to protect a tenant's data from other tenants. Understand how data destruction is performed by the cloud provider; especially study the destruction of cryptographic keys.

Identify trust boundaries and establish necessary safeguards along the trust boundaries. Consider setting up a firewall at the external interface and within each security zones within the cloud. Use strong encryption to protect data in transit. Make sure all passwords are changed from their defaults and use secure password protocols for authentication. Enforce a strong password security policy. Protect all encryption keys from accidental disclosures. There should be a reliable audit program to see if the security requirements are being continuously met. Also, develop a vulnerability and intrusion management program.

## V. CONCLUSIONS

Cloud computing presents immense opportunities for increasing productivity, fostering collaboration and reducing costs. However, cloud computing also brings additional security challenges. While there is some research in this area, more work needs to be done to protect data, establish trust, eliminate single point cloud failures and avoid lock-ins by ensuring portability across cloud service providers. Anyone considering cloud deployment should carefully weigh the risks and benefits. In closing, we hope that the above recommendations will serve as a good starting point.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Special Issue 1, December 2013**

**ACKNOWLEDGMENT**

The author acknowledges Susan S. Mathai and Jacob Soto for their suggestions and constructive feedback.

**REFERENCES**

[1] http://www.cstrends.com/cloud (Accessed on Nov 2, 2013).
[2] K. Hamlen, et. al., *Security issues for Cloud Computing*, IGI Global, 2010.
[3] H. Takabi, et. al., *Security and Privacy Challenges in Cloud Computing Environment*, IEEE, November/December 2010.
[4] R. Chow et. al. *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control*, CCSW'09, November 13, 2009, Chicago, Illinois, USA.
[5] D. Zissis and D. Lekkas, *Addressing Cloud Computing Security Issues*, Jl. of Future Generation Computer Systems. Elsevier, 2010.
[6] F. Lombardi and R. D. Pietro, *Secure Virtualization for Cloud Computing*, Jl. of Network and Computer Applications, Elsevier, 2010.
[7] S. Ruj, A. Nayak and I. Stojmenovic, *DACC: Distributed Access Control in Clouds*, Intl. Joint Conf. of IEEE TrustCom, 2011.
[8] L. Popa, et. al., *Cloud Police: Taking Access Control out of the Network*, Hotnets 2010.
[9] B. R. Kandukuri, et. al., *Cloud Security Issues*. IEEE SCC 2009.
[10] W. Itani, A. Kayssi, and A. Chehab, *Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures*, IEEE Intl. Conf. on Dependable, Automatic and Secure Computing, 2009.
[11] V. Echeverría, L. M. Liebrock, and D. Shin, *Permission Management System: Permission as a Service in Cloud Computing*, IEEE Computer Software and Applications Conf., 2010.
[12] A. Sahai and B. Waters, *Fuzzy Identity Based Encryption*, Eurocrypt, LNCS, Springer 2005.
[13] R. Neisse, D. Holling, and A. Pretshner, *Implementing Trust in Cloud Infrastructures*, CCGrid 2011.
[14] S. Pearson, *Toward Accountability in the Cloud*, IEEE Internet Computing, 2011.
[15] http://aws.amazon.com/message/65648/ (Accessed on Nov 2, 2013)

## BIOGRAPHY

Dr Binto George is a Professor in School of Computer Sciences at Western Illinois University, USA. He is also the founder and president of CSTRNEDS LLP. Dr George completed his Ph.D. from Indian Institute of Science, Bangalore. He has also worked as an Assistant Research Professor at Rutgers University.

Dr George has several publications in the area of secure real-time transaction processing, secure buffer management, database security and usable security. He was the principal investigator of National Science Foundation (NSF) funded project on incorporating Usable Security into Computer Science curriculum. Dr. George has been working closely with many organizations that promote cyber security and national infrastructure security. Dr. George is a member of the IEEE Computer Science Society and a professional member of the Association for Computing Machinery (ACM).