On Current Trends in Security and Privacy of Cloud Computing

Asst. Prof. Dr. Serap Şahin
Department of Computer Engineering
Izmir Institute of Technology
Izmir, Turkey
serapsahin@iyte.edu.tr

Abstract: **One of the major components of the Cloud Computing is "Security and Privacy". These concerns about security and privacy directly address the trustworthy and reliability levels of a system. The researches and studies about security and privacy on cloud computing are continuing. The aim of this paper is to analyze the privacy and security requirements and highlight new tools and open research topics for cloud computing systems.**

Index Terms **Cloud Computing; Computer Security and Privacy; Information Technology Outsourcing; Homomorphic Encryption; Public Key management systems.**

1. INTRODUCTION

Cloud computing may have different meaning for different participants of the cloud. But, the common characteristics are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere and, displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. But, the security and privacy challenges persistent for the cloud computing and organizations or persons should take when outsourcing data, applications, and infrastructure to a cloud environment.

To analyze the security and privacy issues, first the architecture and security risks should be defined hence well known. Therefore the article will start to provide some main concepts and architectural definitions of cloud computing in section 2.Then the article will continue by analyzing the security and privacy requirement in section 3. The section 4 includes the description of existent and new cryptographic tool to satisfy the specifically defined privacy requirements. Conclusion is presented as section 5.

2. THE CLOUD DEFINITIONS AND ARCHITECTURE

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four deployment models [1]. The essential characteristics are rapid elasticity, on demand self-service, broad network access and resource pooling. The cloud has four different deployment models according to users' needs. These are; public cloud, private cloud, hybrid cloud and community cloud [3].

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. The physical location of the infrastructure is determined by the cloud provider as is the design and implementation of the reliability, resource pooling, scalability, and other logic needed in the support framework. Applications are built on the programming interfaces of Internet-accessible services, which typically involve multiple cloud components communicating with each other over application programming interfaces [4].

2.1 Multi-Tenancy Structure

Multi-tenancy defines the simplest form that implies use of same resources or applications by multiple entities (users or machines). The impact of this specification is the visibility of residual data or trace of operations by other entities. This specification of cloud service models requires the existence of policy-driven processing, segmentation, isolation, governance, service level separation and billing models. Multi-tenancy should be separately defined for each service model as:

- Infrastructure as a Service (IaaS); delivers computer infrastructure by a platform virtualization environment.
- Platform as a Service (PaaS); The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly

application hosting environment configurations.

- Software as a Service (SaaS); also called as "on demand software". In this model software and its associated data are kept centrally, generally on the internet based cloud. Generally, entities can access them by using a thin client and its web browser which is connected to the internet.

There are important relationships and dependencies between cloud computing models and security risks. The platforms are built on as a stack on each other.

Before to start analyzing of security and privacy problems of Cloud computing, some of the major players should also be defined with their roles and boundaries therein:

- Cloud Provider: Person, organization or entity responsible for making a service available to service consumers. Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) in the cloud [6]. A Cloud Provider's activities can be described in five major areas as service deployment, service orchestration, cloud service management, security, and privacy.
- Cloud Auditor: A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation. A cloud auditor can independently evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. The auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

3. Analyzing Cloud Security Risks and Requirements

The information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification and/or destruction. To provide these requirements the necessary security functions are integrity, confidentiality and, availability. Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of disposition of personal information (PI) and personally-identifiable information (PII) throughout its life cycle. And, some aspects of privacy are closely related to the aforementioned objectives of security.

3.1 Security and Privacy Analysis of Cloud

The sections below highlight five main privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models [4].

#1: 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. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems [5]. To solve it; audit mechanisms and tools should ensure organizational practices.

#2: Compliance refers to an organizations' responsibility to operate. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

- ***Data Location*** is one of the most common compliance issues facing an organization is data location [6, 7,8]. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer.
- ***Electronic Discovery***; involves the identification, collection, processing, analysis, and production of Electronically Stored Information (ESI) in the discovery phase of litigation [9]. ESI includes not only electronic mail, attachments, and other data objects stored on a computer system or storage media, but also any associated metadata, such as dates of object creation or modification, and non-rendered file content. The cloud provider's electronic discovery capabilities and processes must not compromise the privacy or security of the data and applications of the organization in satisfying the discovery obligations of other cloud consumers, and vice versa.

#3: Trust- By the using of cloud computing, organizations lost their direct control over many aspects of security and privacy, and should have a high level of trust to the cloud provider.

- ***Insider Access*** This can be done by cloud provider and additionally by sub constructors, and also potentially to other customers using the service, thereby increasing the risk.

- ***Data Ownership:*** 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. [4] Ideally, the cloud provider acquires no rights or licenses to use the organization's data for its own purposes or due to security of data [10].
- ***Visibility:*** Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions [11]. To fulfill the obligations of continuous monitoring, the organization is dependent on the cloud provider. Ideally, the consumer would have control over aspects of the means of visibility to accommodate its needs, such as the threshold for alerts and notifications, and the level of detail and schedule of reports [4].
- ***Ancillary Data:*** While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

#4-Identity and Access Management: Data sensitivity and privacy of information have become increasingly an area of concern for organizations. Today, Identity Federation [4] allows the organization and cloud provider to trust and share digital identities and attributes across both domains, and to provide a means for single sign-on (SSO). Clear separation of the managed identities of the cloud consumer from those of the cloud provider must also be ensured to protect the consumer's resources from provider-authenticated entities and vice versa. Identity Federation can be accomplished by Security Assertion Markup Language (SAML) [13] and OpenID [14].

Their workflows involve a web user interacting through a browser with two web based service providers, one of which acts as the identity provider. A user requesting service S at service provider (SP) site is redirected to identity provider (IdP) with an authentication request. The request also includes a callback URL to be used by IdP to redirect the user back to SP. After authenticating the user as Q, IdP redirects user back to SP site with an authentication response containing a signed token asserting the identity Q. SP then validates the token and identifies the user as Q. Identification process continues on a secure SSL/TLS channels with server authentication. This generic workflow can be used to describe both OpenID SSO protocol as well the "SP initiated SSO" of SAML 2.0.

- ***Authentication:*** 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.
- ***Access Control:*** SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud consumer 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. The XACML standard defines an XML-based language for stating policy and forming access control decisions. 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 [15].

#5 Data Protection: Organizations have already been placing sensitive and regulated data into a public cloud, therefore, they must account the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds. Data must be secured while at rest, in transit, and in use, and access to the data must be controlled. While access controls are one of the means to keep data away from unauthorized users; encryption is another. Access controls are typically identity-based, which makes authentication of the user's identity an important issue in cloud computing. Lacking physical control over the storage of information, the encryption is the only way to ensure that it is truly protected.

Standards for communications 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 [16]. Protecting data while in use is an emerging area of cryptography with little practical results to offer, leaving trust mechanisms as the main safeguard.

The security of a system employing cryptography depends on the proper control of central keys and key management components. 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. NIST's Cryptographic Key Management Project is identifying scalable and usable cryptographic key management and exchange strategies for use by governments, which could help to alleviate the problem eventually [2].

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 [12]. Cryptographic operations performed in the cloud become part of the key management process and, therefore, should be managed and audited by the organization.

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service [4].

4. Cloud Computing Privacy Solution

Homomorphic encryption is one of the most exciting new research topics in cryptography, which promises to make cloud computing perfectly secure. With it, a Web user would send encrypted data to a server in the cloud, which would process it without decrypting it and send it back a still-encrypted result.

Suppose, for instance, that the task you've outsourced to the cloud is to search a huge encrypted database for the handful of records that match an encrypted search term. Homomorphic encryption ensures that the server has no idea what the search term is or which records match it. As a consequence, however, it has no choice but to send back information on every record in the database. The user's computer can decrypt that information to see which records matched and which didn't, but then it's assuming much of the computational burden that it was trying to offload to the cloud in the first place.

For example, some specific data would like to be searched on an encrypted data base and no one should know that which data is questioned. Give Homomorphic encryption a chance such as like this:

- You should have an authorized person to access the data base, therefore you should have correct keys to encrypt/decrypt the data.
- Encrypt the searching data terms and upload them to search engine of cloud service provider-SP.
- SP leaves them encrypted,
- SP searches for them directly in the still-encrypted database, and
- Get the same encrypted results thus.

If SP perform calculations directly on encrypted data, yet get the same results that consumer get from the unencrypted data, so both parties win enormously from a security and privacy point of view.

In this process, SP doesn't need any decryption keys, so the consumer no longer has to trust Cloud Providers as not to lose, not steal or not to sell customer data. In this solution, customer still has to trust cloud provider to give the correct results, but that is a completely different issue from privacy. This is related to correctness and completeness issue. The relevant references concerning Homomorphic encryption have been provided in References.

5. Conclusion

Threats to network and computing infrastructures continue to increase each year and have a tendency of becoming more sophisticated than ever. Having to share an infrastructure with unknown outside parties can be a major drawback for some applications and require a high level of assurance pertaining to the strength of the security mechanisms used for logical separation.

The main solution; which outlines of security and privacy problems, can be summarized as follows:

- The underlying architecture along with the technologies on each and every level of cloud should be understood well to create a sufficient solution for the problems defined above.
- Trust, as one of the main participant, ensures that (i) the service arrangements have sufficient means to allow visibility into the security and privacy controls, (ii) processes employed by the cloud provider are the ones that were promised to be and, (iii) positive performance of the processes against time.
- Solution systems should establish clear & mutually exclusive ownership rights over data.
- Identity and Access Management should ensure secure authentication, authorization, and other identity and access management functions, and thus are suitable for the organization.
- To satisfy Data Protection requirements; as mentioned in section 3 #5 and section 4 about new developments on cryptography, should be evaluated. But there are already open problems about data while at rest, in transit, and in use, and in sanitization of it.
- Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment.

Cryptography, key management, identity and access managements are the main tools for the security

and privacy requirements of the cloud and, there are already many problems persistent at the moment.

6. REFERENCES

[1] The National Institute of Standards and Technology definition of cloud computing at http://csrc.nist.gov/groups/SNS/cloud-computing/

[2] Cloud Security Alliance, "Security Guidance for critical areas focus in Cloud Computing V3.0", 2011 https://cloudsecurityalliance.org/research/security-guidance/

[3] NIST, "Cloud Computing Reference Architecture, 09-2011", http://www.cloudcredential.org/images/pdf_files/nist%20reference%20architecture.pdf

[4] NIST, "Guidelines on Security and Privacy in Public Cloud Computing", 12-2011,

http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[5] Larry Ponemon, Security of Cloud Computing Users, Ponemon Institute, May 12, 2010, http://www.ca.com/files/IndustryResearch/security-cloud-computing-users_235659.pdf

[6] David Binning, Top Five Cloud Computing Security Issues, Computer Weekly, April 24, 2009, http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm

[7] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Atanu Rakshit, Cloud Security Issues, IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009

[8] Stephanie Overby, How to Negotiate a Better Cloud Computing Contract, CIO, April 21, 2010, http://www.cio.com/article/591629/How_to_Negotiate_a_Better_Cloud_Computing_Contract

[9] Alistair B. Dawson, Understanding Electronic Discovery and Solving Its Problems, 56th Annual Program on Oil and Gas Law, The Center for American and International Law, February 17-18, 2005, Houston, Texas.

[10] Steve McDonald, Legal and Quasi-Legal Issues in Cloud Computing Contracts, Workshop Document, EDUCAUSE and NACUBO Workshop on Cloud Computing and Shared Services, Tempe, Arizona, Feb. 8–10, 2010

[11] Kelley Dempsey et al., Information Security Continuous Monitoring for Federal Information Systems and Organizations, Initial Public Draft, SP 800-137, NIST, Sept. 2011, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

[12] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, Guide to Security for Full Virtualization Technologies, Special Publication 800-125, National Institute of Standards and Technology, January 2011, http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

[13] S. Cantor, I. Kemp, N. Philpott, and E. Maler. Assertions and protocols for the OASIS Security Assertion Markup Language V2.0. OASIS Standard (March 2005), 2005

[14] OpenID Standards http://openid.net/specs/openid-authentication-2_0.html

[15] 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, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf

[16] Encryption and Key Management, Cloud Security Alliance, January 12, 2011, https://wiki.cloudsecurityalliance.org/guidance/index.php/Encryption_and_Key_Management

[17] For more information about Homomorphic Encryption

http://phys.org/news/2013-06-cloud-algorithm-major-problem-homomorphic.html

http://www2.technologyreview.com/article/423683/homomorphic-encryption/

http://crypto.stanford.edu/craig/

https://github.com/shaih/HElib