ICIBA 2014, the Third International Conference on
Information Technology and Business Aplication
Palembang-Indonesia, 20-21 February 2014

A Review : Security Framework Information Technology for University Based on Cloud Computing

E.S. Negara, R. Andryani

Bina Darma University, Computer Science
e-mail: E.S.Negara@mail.binadarma.ac.id
e-mail: ria@mail.binadarma.ac.id

Abstract

Information technology architecture based cloud computing become one of the architectural model for the university's information technology development. cloud computing security on the network and system architecture has become an important issue recently due to the increasing dependence of organizations and the people in the system. So with the standardization of information security technologies will have a significant impact in improving the safe use of the system. A review of the security framework of information technology will be presented in this paper. This paper will review some of the recommended framework for the security of information technology development based on cloud computing such as: European Network and Information Security Agency (ENISA), Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST.

Keywords : *Security Framework, ENISA, CSA, NIST*

1 INTRODUCTION

Information technology architecture within an organization becomes a blueprint (blue print) that explains how the elements of information technology and management work together as a single unit. Thus the application of appropriate information technology architecture will greatly assist the achievement of organizational objectives, including educational organizations.

In educational institutions, information technology architecture perancanaan be one important thing to do so as technology strategy aligned with the business strategy of the institution. But now there are a lot of available information technology architecture models appropriate for application in educational institutions in South Sumatra. utilization of information technology in higher education, among others, for the development of the education system, e-learning, e-journals and search as a bridge to get the other information in the world.

The presence of the latest technology in the world of Cloud Computing information technology provide a huge benefit in the design of modern information technology architecture. Architecture that will be able to adjust to the needs and kedaan educational institutions

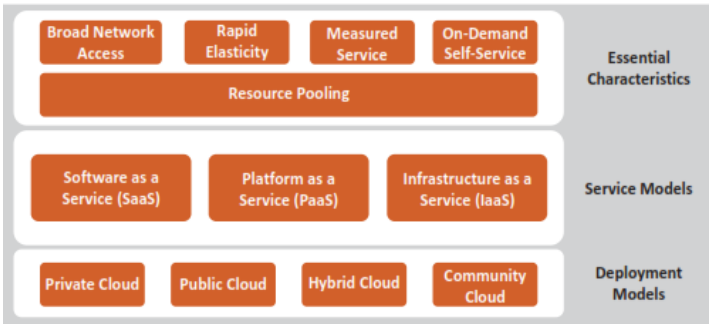

Figure 1: NIST Architecture for Cloud Computing

today. Carl Hewitt [1] states that cloud computing is a technology where most of the computational process and is dijaringan the internet, allowing users to access necessary services from anywhere. Another expressed the opinion cloud computing is a way of delivering IT-enabled capabilities to users in the form of 'services' with elasticity and scalability, where users can use of resources as the make, platform, or software without having to possess and manage the underlying complexity of the technology. According to the National Institute of Standards and Technology (NIST), Cloud computing is a model for enabling a convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be provisioned and released Rapidly with minimal management effort or service provider interaction.

2 SECURITY ISSUES CLOUD COMPUTING

There are a number of security issues/concerns associated with Cloud computing. Gartner report specifies the following seven security issues in Cloud computing :

1. **Privileged User Access Data Location :**

   Cloud computing allows the processing of the confidential data of user by personnel outside the organization, so non-employees could possibly have full access to it. Consumer should ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

2. **Regulatory Compliance:**

   Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications.

3. **Data Location:**

   When a customer uses the Cloud, customer probably would not know exactly where his data is hosted. It is required to ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. **Data Segregation :**

Data in the Cloud is typically in a shared environment alongside data from other customers. Encryption is effective but is not a cure-all. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability

5. **Recovery:**

   Even if the consumer does not know where his data is, a Cloud provider should tell to his consumer what will happen to data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.

6. **Investigative Support:**

   Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

7. **Long-term Viability:**

   Ideally, Cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But the consumer must ensure that his data will remain available even after such an event. It is essential to know fromproviders howhe would get his data back and if it would be in a format that could import into a replacement application.

Other related Concerns in Cloud are as follows :

1. **Virtualization:**

   One potential new risk has to do with the potential to compromise a virtual machine (VM) hypervisor. If the hypervisor is vulnerable to exploit, it will becomea primary target. Identity and Access Control Management: system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.

2. **Legal Issues:**

   Providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

3. **Isolation of Roles:**

   Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the Cloud providers and Cloud consumers information security policy.

4. **Encryption and Key Management:** Organizations' confidential or sensitive data must be appropriately protected while at rest and in transmit. Keys used for appropriate encryption adopted by organizations should be managed securely throughout its life cycle.

5. **Browser Vulnerabilities:**

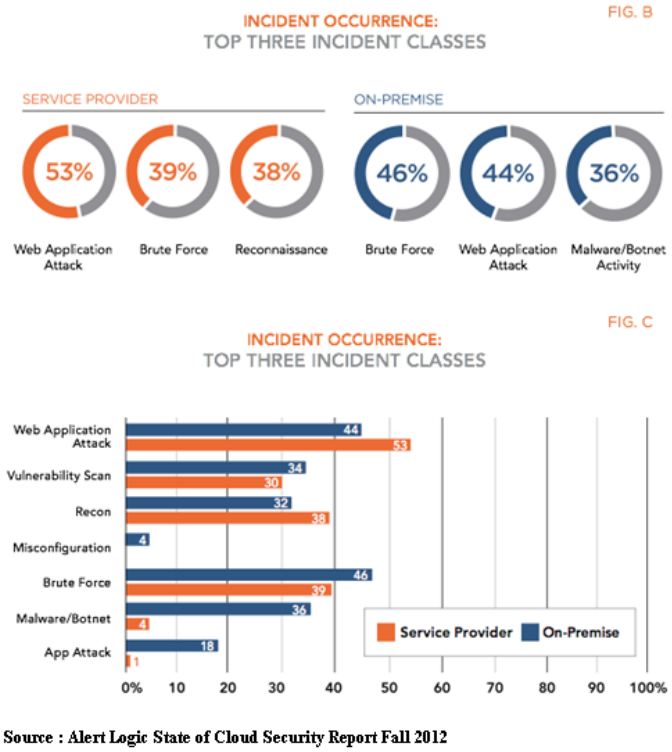

Figure 2: Top Three Incident Classes

Consumers access their applications or services offered by providers using secure communication through a web browser. Web browsers are a common target for malware and attacks. If the consumer's browser becomesinfected, the access to the services can be compromised as well.

in February 2012, Alert Logic launched the first in a series of semi-annual reports on cloud security, based on analysis of threat data from its customers production environments. Reviewing 12 months of operational data, including more than two billion events and over 60,000 security incidents. Show in Figure 2 and Figure 3.

3 CLOUD SECURITY FRAMEWORK

Security frameworks concentrate information on security and privacy aiming to provide a compilation of risks, vulnerabilities and best practices to avoid or mitigate them. There are several entities that are constantly publishing material related to cloud computing security, including the European Network and Information Security Agency (ENISA), Cloud Security Alliance (CSA), the National Institute of Standards and Technology (NIST), CPNI (Centre for the Protection of National Infrastructure fromUK government) and ISACA (the Information Systems Audit and Control Association). In this paper we focus on the rst three entities, which by themselves provide a quite comprehensive overview of issues and solutions and, thus, allowing a broad understanding of the current status of cloud security.

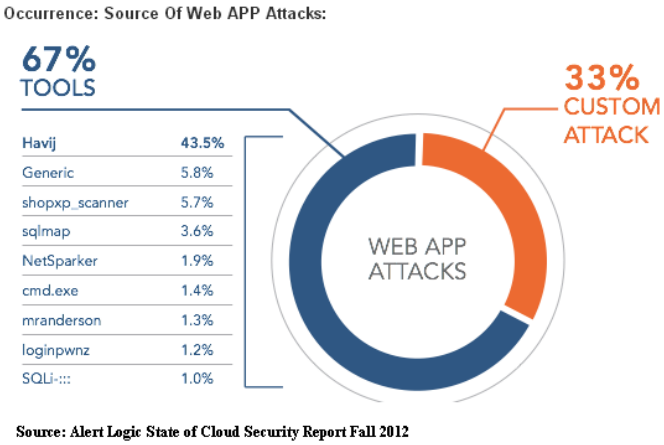

Figure 3: Source if Web APP Attacks

3.1 European Network and Information Security Agency (ENISA)

ENISA is an agency responsible for achieving high and eective level of network and information security within the European Union. In the context of cloud computing, they published an extensive study covering benets and risks related to its use. In this study, the security risks are divided in four categories:

1. Policy and organizational: issues related to governance, compliance and reputation;
2. Technical: issues derived from technologies used to implement cloud services and infrastructures, such as isolation, data leakage and interception, denial of service attacks, encryption and disposal;
3. Legal: risks regarding jurisdictions, subpoena and e-discovery; Not cloud specic: other risks that are not unique to cloud environments, such as network management, privilege escalation and logging;

As a top recommendation for security in cloud computing, ENISA suggests that providers must ensure some security practices to customers and also a clear contract to avoid legal problems. Key points to be developed include breach reporting, better logging mechanisms and engineering of large scale computer systems, which encompass the isolation of virtual machines, resources and information. Their analysis is based not only on what is currently observed, but also on what can be improved through the adoption of existing best practices or by means of solutions that are already used in non-cloud environments. This article aims at taking one step further by transforming these observations into numbers a quantitative approach.

3.2 Cloud Security Alliance (CSA)

The CSA alliance covers key issues and provides advice for both Cloud computing customers and providers within various strategic domains.

CSA is an organization led by a coalition of industry practitioners, corporations, associations and other stakeholders, such as Dell, HP and eBay. One of its main goals is to promote the adoption of best practices for providing security within cloud computing environments.

Three CSA documents are analyzed in this paper the security guidance, the top threats in cloud computing and the Trusted Cloud Initiative (TCI) architecture as they comprise most of the concepts and guidelines researched and published by CSA.

The latest CSA security guidance (version 3.0) denotes multi-tenancy as the essential cloud characteristic while virtualization can be avoided when implementing cloud infrastructures multi-tenancy only implies the use of shared resources by multiple consumers, possibly from dierent organizations or with dierent objectives. They discuss that, even if virtualization-related issues can be circumvented, segmentation and isolated policies for addressing proper management and privacy are still required. The document also establishes thirteen security domains:

1. Governance and risk management: ability to measure the risk introduced by adopting cloud computing solutions, such as legal issues, protection of sensitive data and their relation to international boundaries;

2. Legal issues: disclosure laws, shared infrastructures and interference between dierent users;

3. Compliance and audit: the relationship between cloud computing and internal security policies;

4. Information management and data security: identication and control of stored data, loss of physical control of data and related policies to minimize risks and possible damages;

5. Portability and interoperability: ability to change providers, services or bringing back data to local premises without major impacts;

6. Traditional security, business continuity and disaster recovery: the inuence of cloud solutions on traditional processes applied for addressing security needs;

7. Data center operations: analyzing architecture and operations from data centers and identifying essential characteristics for ensuring stability;

8. Incident response, notication and remediation: policies for handling incidents;

9. Application security: aims to identify the possible security issues raised from migrating a specic solution to the cloud and which platform (among SPI model) is more adequate;

10. Encryption and key management: how higher scalability via infrastructure sharing aects encryption and other mechanisms used for protecting resources and data;

11. Identity and access management: enabling authentication for cloud solutions while maintaining security levels and availability for customers and organizations;

12. Virtualization: risks related to multi-tenancy, isolation, virtual machine co-residence and hypervisor vulnerabilities, all introduced by virtualization technologies;

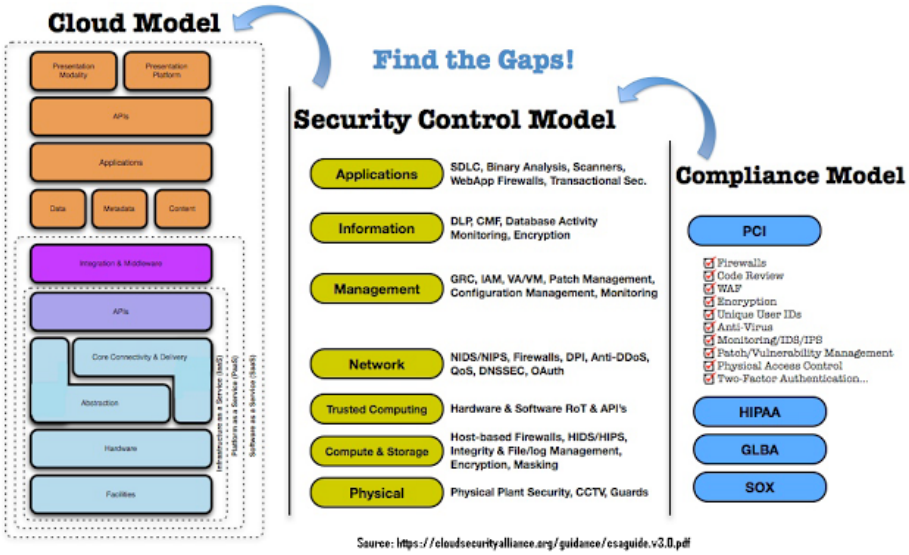

Figure 4: Mapping the Cloud Model to Security Control and Compliance

13. Security as a service: third party security mechanisms, delegating security responsibilities to a trusted third party provider

CSA also published a document focusing on identifying top threats, aiming to aid risk management strategies when cloud solutions are adopted. As a complete list of threats and pertinent issues is countless, the document targets those that are specic or intensied by fundamental characteristics of the cloud, such as shared infrastructures and greater exibility. As a result, seven threats were selected:

1. Abuse and nefarious used of cloud computing: while providing exible and powerful resources and tools, IaaS and PaaS solutions also unveil critical exploitation possibilities built on anonymity. This leads to abuse and misuse of the provided infrastructure for conducting distributed denial of service attacks, hosting malicious data, controlling botnets or sending spam;

2. Insecure application programming interfaces: cloud services provide APIs for management, storage, virtual machine allocation and other service-specic operations. The interfaces provided must implement security methods to identify, authenticate and protect against accidental or malicious use, which can introduce additional complexities to the system such as the need for third-party authorities and services; Malicious insiders: although not specic to cloud computing, its eects are amplied by the concentration and interaction of services and management domains;

3. Shared technology vulnerabilities: scalability provided by cloud solutions are based on hardware and software components which are not originally designed to provide isolation. Even though hypervisors oer an extra granularity layer, they still exhibit aws which are exploited for privilege escalation;

Table 1: Summary of CSA security frameworks

Framework	Objectives	Structure and comments
CSA Guidance		
	• Recommendations for reducing risks • No restrictions regarding specic solutions or service types • Guidelines not necessarily applicable for all deployment models • Provide initial structure to divide eorts for researches	• One architectural domain • Governance domains: risk management, legal concerns, compliance, auditing, information management, interoperability and portability • Operational domains: traditional and business security, disaster recovery, data center operations, encryption, application security, identication, authorization, virtualization, security outsourcing • Emphasis on the fact that cloud is not bound to virtualization technologies, though cloud services heavily depend on virtualized infrastructures to provide exibility and scalability
CSA Top Threats		
	1. Provide context for risk management decisions and strategies 2. Focus on issues which are unique or highly inuenced by cloud computing characteristics	• Seven main threats: – Abuse and malicious use of cloud resources – Insecure APIs – Malicious insiders – Shared technology vulnerabilities – Data loss and leakage – Hijacking of accounts, services and trac – Unknown risk prole (security obscurity) • Summarizes information on top threats and provide examples, remediation guidelines, impact caused and which service types (based on SPI model) are aected
CSA Architecture		
	• Enable trust in the cloud based on well-known standards and certications allied to security frameworks and other open references • Use widely adopted frameworks in order to achieve standardization of policies and best practices based on already accepted security principles	• Four sets of frameworks (security, NIST SPI, IT audit and legislative) and four architectural domains (SABSA business architecture, ITIL for services management, Jericho for security and TOGAF for IT reference) • Tridimensional structure based on premises of cloud delivery, trust and operations • Concentrates a plethora of concepts and information related to services operation and security

4. Data loss and leakage: insucient controls concerning user access and data security (including privacy and integrity), as well as disposal and even legal issues;

5. Account, service and trac hijacking: phishing and related frauds are not a novelty to computing security. However, not only an attacker is able to manipulate data and transactions, but also to use stolen credentials to perform other attacks that compromise customer and provider reputation.

6. Unknown risk prole: delegation of control over data and infrastructure allows companies to better concentrate on their core business, possibly maximizing prot and eciency. On the other hand, the consequent loss of governance leads to obscurity: information about other customers sharing the same infrastructure or regarding patching and updating policies is limited. This situation creates uncertainty concerning the exact risk levels that are inherent to the cloud solution;

It is interesting to notice the choice for cloud-specic issues as it allows the identication of central points for further development. Moreover, this compilation of threats is closely related to CSA security guidance, composing a solid framework for security and risk analysis assessments while providing recommendations and best practices to achieve acceptable security levels.

Another approach adopted by CSA for organizing information related to cloud security and governance is the TCI Reference Architecture Model [64]. This document focuses on dening guidelines for enabling trust in the cloud while establishing open standards and capabilities for all cloud-based operations. The architecture denes dierent organization levels by combining frameworks like the SPI model, ISO 27002, COBIT, PCI, SOX and architectures such as SABSA, TOGAF, ITIL and Jericho. A wide range of aspects are then covered: SABSA denes business operation support services, such as compliance, data governance, operational risk management,human resources security, security monitoring services, legal services and internal investigations; TOGAF denes the types of services covered (presentation, application, information and infrastructure; ITIL is used for information technology operation and support, from IT operation to service delivery, support and management of incidents, changes and resources; nally, Jericho covers security and risk management, including information security management, authorization, threat and vulnerability management, policies and standards. The result is a tri-dimensional relationship between cloud delivery, trust and operation that aims to be easily consumed and applied in a security-oriented design.

3.3 National Institute of Standards and Technology (NIST)

NIST discusses the threats, technology risks, and safeguards surrounding public Cloud environments, andtheir suitable defense mechanisms. NIST has recently published a taxonomy for security in cloud computing that is comparable to the taxonomy introduced in section Cloud computing security taxonomy. This taxonomys rst level encompass typical roles in the cloud environment: cloud service provider, responsible for making the service itself available; cloud service consumer, who uses the service and maintains a business relationship with the provider; cloud carrier, which provides communication interfaces between providers and consumers; cloud broker, that manages use, performance and delivery of services and intermediates negotiations between providers and consumers; and cloud auditor, which performs assessment of services, operations and security. Each role is associated to their respective

Table 2: Summary of ENISA and NIST security frameworks

Framework	Objectives	Structure and comments
ENISA Report		
	• Study on benets and risks when adopting cloud solutions for business operations • Provide information for security assessments and decision making	• Three main categories of cloud specic risks (policy and organizational, technical, legal) plus one extra category for not specic ones • Oers basic guidelines and best practices for avoiding or mitigating their eects • Presents recommendations for further studies related to trust building (certications, metrics and transparency), large scale data protection (privacy, integrity, incident handling and regulations) and technical aspects (isolation, portability and resilience) • Highlights the duality of scalability (fast, exible and accessible resources versus concentrations of data attracting attackers and also providing infrastructure for aiding their operations) • Extensive study on risks considering their impact and probability
NIST Taxonomy	1. Dene what cloud services should provide rather than how to design and implement solutions 2. Ease the understanding of cloud internal operations and mechanisms	• Taxonomy levels: – First level: cloud roles (service provider, consumer, cloud broker,cloud carrier and cloud auditor) – Second level: activities performed by each role (cloud management, service deployment, cloud access and service consumption) – Third and following levels: elements which compose each activity (deployment models, service types and auditing elements) • Based on publication SP 500-292, highlighting the importance of security,privacy and levels of condence and trust to increase technology acceptance • Concentrates many useful concepts, such as models for deploying or classifying services

activities and decomposed on their components and subcomponents. The clearest dierence from our taxonomy is the hierarchy adopted, as our proposal primarily focuses on security principles in its higher level perspective, while the cloud roles are explored in deeper levels. The concepts presented here extend NISTs initial denition for cloud computing, incorporating a division of roles and responsibilities that can be directly applied to security assessments. On the other hand, NISTs taxonomy incorporatesconceptssuchasdeploymentmodels,service types and activities related to cloud management (portability, interoperability, provisioning), most of them largely employed in publications related to cloud computing including this one.

4 CONCLUSION

Security is one of the factors that must be designed with good build information technology. Development of information technology-based secure cloud computing in the university may be some framework uses, among others: the European Network and Information Security Agency (ENISA), Cloud Security Alliance (CSA), the National Institute of Standards and Technology (NIST).

References

ENISA,(2011) About ENISA. *http://www.enisa.europa.eu/about-enisa*

Catteddu, D., Hogben, G.,(2009), *Benefits, risks and recommendations for information security.* Tech. rep., European Network and Information

ENISA, (2011), *Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment*

CSA,(2011) About. *https://cloudsecurityalliance.org/about/*

CSA, (2009) *Security Guidance for Critical Areas of Focus in Cloud Computing.* Tech. rep., Cloud Security Alliance

Hubbard, D., Jr LJH, Sutton, M., (2010), *Top Threats to Cloud Computing.* Tech. rep., Cloud Security Alliance.*cloudsecurityalliance.org/research/ projects/top-threats-to-cloud-computing*

CSA,(2011), CSA TCI Reference Architecture. *https://cloudsecurityalliance. org/wp-content/uploads/2011/11/TCI-Reference-Architecture-1.1.pdf*

CSA, (2011) Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Tech. rep., Cloud Security Alliance. *[Http://www. cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf]*

Ramireddy, S., Chakraborthy, R., Raghu, TS., Rao HR, (2010), Privacy and Security Practices in the Arena of Cloud Computing - A Research in Progress. *In: AMCIS 2010 Proceedings, AMCIS 10. http://aisel.aisnet.org/ amcis2010/574*

NIST, (2011), NIST Cloud Computing Reference Architecture: SP 500-292. *http://collaborate.nist.gov/twiki-cloud-computing/pub/ CloudComputing/ReferenceArchitectureTaxonomy/NIST SP 500-292 - 090611.pdf*

Mell P, Grance, T., (2009), The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, *www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf http://www.rackspace.com/knowledge_center/whitepaper/alert-logic-state-of-cloud-security-report-fall-2012*