Journal of Theoretical and Applied Information Technology
31st December 2013. Vol. 58 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DATA INTEGRITY IN CLOUD COMPUTING SECURITY

[1]Dr. NEDHAL A. AL-SAIYD, [2]NADA SAIL

[1]Assoc. Prof., Faculty of Information Technology, Computer Science Dept., Applied Science University, Amman-Jordan

[2]MSc. Student, Faculty of Information Technology, Computer Science Dept., Applied Science University, Amman-Jordan

E-mail: [1]nedhal_alsaiyd@asu.edu.jo, [2]nadasail@yahoo.com

ABSTRACT

Cloud computing requires comprehensive security solutions based upon many aspects of a large and loosely integrated system. The application software and databases in cloud computing are moved to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Threats, vulnerabilities and risks for cloud computing are explained, and then, we have designed a cloud computing security development lifecycle model to achieve safety and enable the user to take advantage of this technology as much as possible of security and face the risks that may be exposed to data. A data integrity checking algorithm; which eliminates the third party auditing, is explained to protect static and dynamic data from unauthorized observation, modification, or interference.

Keyword: *Cloud Computing, Cloud Computing Security, Data Integrity, Cloud Threads, Cloud Risks*

1. INTRODUCTION:

There are several different definitions of cloud computing, but all of them agree on how to provide services to users of the network. Cloud computing is an Internet-based development and use of computer technology. It refers to the use of computing resources; hardware and software, available on demand as a service over the Internet. It offers a range of services for users of the network, which include applications, storage, and various operations and remote printing, etc. [1]. It typically involves over the Internet provision of dynamically scalable and often virtualized resources [2]. Businesses are running all kinds of apps in the cloud. Cloud computing can be considered as the technology that keeps the data, uses in different applications and is remotely controlled without the need to download certain applications on computers.

Some of the potential benefits that apply to almost all types of cloud computing includes the following:

1. Cost Savings: Companies can reduce their capital expenses and use operational expenses for increasing their computing capabilities.
2. Flexibility: The flexibility of cloud computing allows companies to use additional resources in peak times, to enable them to satisfy consumer demands.
3. Reliability: Services using multi-redundant sites can support business continuity and disaster recovery.
4. Reduce Maintenance: Cloud service providers do the system maintenance that does not require application installations onto PCs.
5. Mobile Accessible: Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.
6. Transparency: Additional servers to be added to the provisioned service without interrupting the service or requiring reconfiguration of the application delivery solution. If the application delivery solution is integrated via a management API, then transparency is also achieved through the automated provisioning and de-provisioning of resources.

Information security can be viewed as including three functions: Access control, secure communications, and protection of private data [3]. Information security is also defined as the protection of private data and processing from unauthorized observation, modification, or interference.

This paper describes several information security concepts that apply to all information security research specific to cloud computing. Cloud computing requires comprehensive security

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

solutions based upon many aspects of a large and loosely integrated system**.**

Cloud Computing has been considered as the next-generation architecture of IT Enterprise, and this new paradigm makes many new security challenges. Therefore, the security issues that are related to static and dynamic data in cloud computing are investigated. Security on the cloud will be a major research topic in itself. Cloud computing increases some of security risks to the cloud users and businesses. It might be difficult for the user to effectively verify the data managing of the cloud provider and therefore to make sure that the data is being handled in a valid way. The greater damages in the cloud will often caused by malicious insider. The cloud architectures, which involve system administrators and security service providers, are extremely high-risk by their nature.

Data breaches is the most important concerns facing the cloud computing users whether from inside or outside the cloud.

The rest of paper is organized as follows: section 2 describes the related works. Section 3 addresses a general description of cloud computing, types, service models, and deployment models. Section 4 is a description of threads and attacks on cloud computing. Section 5 presents the security risks. The description of the proposed model is discussed in section 6. And finally, the conclusions are summarized in section 7.

2. RELATED WORK

Recently the cloud computing technology became widely used by most of the business companies to increase their productivity and with that there are still some concerns about the security provided by cloud computing [4]. In 2013, cloud computing is still in high demand where the organizations are either already using or intending to use cloud computing infrastructure services, and the share of cloud service will continue to increase as a percentage of total revenue [*5*]. One of the biggest concerns with cloud data storage is the verification of data integrity at untrusted servers, and how to deal with sensitive data. It is not an easy task to maintain customer's most sensitive cloud data securely, which is needed in many applications for clients.

This makes some companies wary of switching to cloud computing because the user does not know on which server the data is stored and is this server provides secure data or not.

The first proposed a solution to remote data integrity is proposed by Deswarte et al [6], use RSA-based functions to hash the whole data file for every verification challenge. It is inefficient for the large data files, which need more time to compute and transfer their hash values. Caronni proposed another protocol [7], where the server has to send Message Authentication Code (MAC) of data as the response to the message instead of storing the hash of all data. The verifier sends a unique random key for the message authentication code to achieve integrity on data from any modification or deletion. Instead of storing the whole data at server specific portions of data is stored; a deterministic verification approach is used. Ateniese et al proposed a model for using homomorphic verifiable tag that is calculated as a number that is equal to two times of number of data chunks, and stores the data file and it tags on the server. Then, the client can verify that data integrity of the file Using the queried blocks and their corresponding tags and the server generates a proof of integrity [8] [9]. For the dynamic data integrity verification, Wang et al.[9] discussed the problem of ensuring the availability and integrity of data storage in cloud computing. They utilized the homomorphic token and error correcting codes to achieve the integration of storage correctness insurance and data error localization.

3. CLOUD COMPUTING COMPONENTS:

Cloud Computing has been considered as the next-generation architecture of IT Enterprise. Cloud computing moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This new paradigm makes many new security challenges.

Figure (1) depicts Cloud Data Storage Model [10]. A cloud computing is made up of several elements: Cloud users, cloud service providers, third parity auditors [11]. Each element plays a specific role in delivering functional cloud-based application.

a. Cloud Users:

The users can be an individual or an organization storing their data in cloud and accessing the data. He can use:

- Mobile including PDAs and smart phones
- Thin, where the client's computer does not have hard drive and the work is done by the server. Thin client becomes popular because of low hardware cost and since data is stored on servers there is less chance for data to be lost or stolen
- Thick, uses regular computer that uses a web browser to connect to the cloud.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

b. Cloud Service Providers (CSP):

The CSP, who manages cloud servers (CSs) and provides a paid storage space on its infrastructure to users,. Servers are geographically housed on different locations. The servers on cloud computing is based on the principle of virtual servers because the user does not know which server will give him the required service. This is the main difference between cloud computing and distributed computing.

c. Datacenters:

A collection of servers form the data center, where the application is housed. Cloud data centers are known as cloud data storages (CDSs). The software can be installed on one physical server and allowing multiple instances of virtual servers to be used. The number of virtual servers depends on the size and speed of physical server and what application will be running on the virtual server. The data on the cloud computing can be either static or dynamic

i. **Static data:** It is data that cannot be altered or edited them and any amendment thereto will become the new data and this data can be read and re-write them again but without modification. Example: Data Centers.

ii. **Dynamic data:** It is the data obtained by the modification or change continuously which are used in transfer between users on cloud computing. Example: E-mail.

d. Third Party Auditor (TPA) or Verifier:

The TPA or Verifier has expertise and capabilities (that users may not have) and verifies the integrity of outsourced data in cloud on behalf of users. The TPA could release an audit report to user.

3.1 Cloud Computing Service Models

The cloud service provider (CSP) offered its customers with kind of services and tools, which are:

a. Software as a Service (SaaS): involves using their cloud infrastructure and cloud platforms to provide customers with software applications. In this service, the user can take advantage of all applications. The end user applications are accessed by users through a web browser, such as Microsoft SharePoint Online. The need for the user to install or maintain additional software is eliminated [12].

b. Platform as a Service (PasS): enables customers to use the cloud infrastructure; as a service plus operating systems and server applications such as web servers. The user can control the development of web applications and other software and which use a range of programming languages and tools that are supported by the service provider [12].

c. Infrastructure as a Service (IaaS): the registered user may access to physical computing hardware; including CPU, memory, data storage and network connectivity of the service provider. IaaS enables multiple customers referred to as "multiple tenants" using virtualization software. The user gains greater flexibility in access to basic infrastructure [12].

d. Security as a service (SecaaS): categorize the different types of Security as a Service and to provide guidance to organizations on reasonable implementation practices [13].

3.2 Deployment Models of Cloud Computing

Cloud Computing can be run on different deployment models. The deployment model is selected depending on the user requirements and market availability:

a. Private Cloud: a cloud that is used exclusively by one organization. The cloud may be operated by the organization itself or a third party. If the private cloud is properly implemented and operated, it has reduced potential security concerns. The St Andrews Cloud Computing Co-laboratory and Concur Technologies are example organizations that have private clouds [14].

b. Public Cloud: a cloud that can be used (for a fee) by the general public, and involves an organization using a cloud infrastructure which is shared via the Internet with many other organizations and other members of the public; such as Microsoft, Google and Amazon [14]. Public cloud has variety of inherent security risks that need to be considered.

c. Community Cloud: is shared by several organizations and is usually setup for their similar security requirements and a need to store or process data of similar sensitivity; such as several agencies of the same government [14].

d. Hybrid Cloud: is a combination of cloud deployment models. Each cloud could be independently managed while applications and data would be allowed to move across the hybrid cloud. A private cloud can burst-out to a public cloud when it requires more resources [14]. A specific business and technology requirements are used in designing hybrids, which helps to optimize

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security and privacy with a minimum IT costs [15].

4. CLOUD COMPUTING SECURITY THREATS:

Although cloud computing certainly gives organizations with significant cost savings and operational efficiencies, it also brings new security risks and uncertainties. The increased attack surface in a Cloud environment allows for other vulnerabilities to be exploited, thereby increasing the organization's risk [An Introduction To Securing a Cloud Environment]. The risk is defined as a given threat that exploits vulnerabilities of an asset or group of assets and thereby cause harm to the organization [16]. The increased attacks in cloud environment; virtual switches and hypervisor that are not present in the traditional data center, allows for other vulnerabilities to be exploited, thereby increasing the organization's risk [17].

The most important threats facing cloud computing are identified as follows [18], [19] [20]:

a. *Data breaches*: The most important thing is to prevent any data violation. The challenge addressing the threats of data loss and data leakage is that "the measures you put in place to improve one can worsen the other". Data is encrypted to reduce the impact of a violation, but if the encryption key is lost, then data will be lost. However, if offline backups of data are chosen to reduce data loss, exposure data breaches are increased.

b. *Data Loss*/Leakage: There are many ways to compromise data because of insufficient authentication, authorization, and audit (AAA) controls, such as deletion or alteration of records without a backup of the original content. Loss of an encoding key may result in effective destruction. Unauthorized parties may gain access to sensitive data. A malicious hacker might delete a target's data.

c. *Account or Service hijacking*: Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. If an attacker gains access to credentials, he can eavesdrop on user activities and transactions, manipulate data, falsify information, and redirect your clients to illegal sites.

d. *Insecure Application Programming Interfaces APIs*: APIs are integral to security and availability of general cloud services. These interfaces must be designed to protect against both accidental and malicious attempts. Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities; are examples of this type of threats.

e. *Malicious insiders*: a provider may not reveal how it allows employee's access to physical and virtual assets, how it monitors these employees, or how it analyzes. In cloud computing, the organization doesn't need to know the technical details of how the services are delivered. In situations, the risk is great. Without full knowledge and control, your organization may be at risk. In situations, the risk is great. Without full knowledge and control, your organization may be at risk.

f. *Unknown risk Profile:* Versions of software, code modifications, security policies and applications, vulnerability reports, interference attempts, and security design, are all important factors for estimating company's security status. Information about who is sharing your infrastructure may be relevant.

g. *Cloud abuse*: Some providers offer free limited trial periods. By abusing the relative secrecy behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative invulnerability, such as password and key cracking. A malicious hacker uses cloud servers to launch a Distributed Denial of Service (DDoS) attack, propagate malware, or share illegally copied software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.

h. *Shared Technology Issues*: (IaaS) is based on shared infrastructure (e.g. disk partitions, CPU caches, GPUs, etc.), were not designed to offer strong isolation properties for a multi-tenant architecture. A virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Overlooked flaws have allowed guest operating systems to gain unauthorized levels of control and/or influence on the platform.

i. *Changes the business model.* Cloud computing changes the way IT services are delivered. No longer delivered from an on-site location, servers, storage, and applications are provided by external service

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

providers. Organizations need to evaluate the risks associated with the loss of control of the infrastructure.

j. Exploiting browser vulnerabilities: Several years ago, hackers used to attack software operating systems. More recently, hackers have shifted their attacks to target user browsers.

5. CLOUD COMPUTING SECURITY RISKS:

Virtualized servers will be less secure than the physical servers. However, all risks are not reduced by moving operations to a cloud environment. While some risks are reduced, other risks may increase. With the addition of virtual network switches, hypervisors and virtual images, the attack surface increases. A single host with multiple virtual machines may be attacked by one of the guest operating systems,or a guest operating system may be used to attack other guest operating systems.

- vulnerabilities are particularly risky because other virtual machines residing on the host and the data files stored out sides the owner's trusted domain
- Movement from one provider to while unencrypted or logged access. Anyone sniffing the network has an opportunity to extract sensitive data such as passwords or logins.
- With virtualization, a customer's sensitive data is stored over a shared infrastructure that may be distributed on multiple sharing of servers and data centers.
- Organizations should consider their risks due to anonymous signup, lack of validation, service fraud, and ad-hoc services**.**

Virtualized platforms Risks are:

- Management console vulnerabilities
- Management server vulnerabilities
- Administrative VM vulnerabilities
- VM vulnerabilities
- Hypervisor vulnerabilities
- Hypervisor escape

6. PROPOSAL CLOUD DATA SECURITY MODEL

From a business point of view, cloud Security is a set of organization safe policies, layered technologies and controls which are designed to protect data and infrastructure from attacks. In order to deliver reliable, well-managed, secure, and patched services, a cloud computing system development model is proposed, as it is well-described in figure 2. It aims to be the standard that defines all the tasks required for developing and maintaining the cloud security, where the cloud training staff needs to follow the following phases in order:

a. Identifying Cloud Security Domains and Their Subcategories: including physical and logical infrastructure as well as the hosted applications and platform services with different risk classes. The physical infrastructure includes the data center facilities themselves, as well as the hardware and components that support the services and networks. The logical infrastructure consists of operating system instances, routed networks, and unstructured data storage, whether running on virtual or physical objects. Platform services include compute runtimes, name services (DNS), and other advanced functions consumed by online services. Infrastructure services may be virtualized or actual.

- **Physical Infrastructure Security:** including servers, routers, storage devices, power supplies and other components that support operations—should be physically secure. Security includes managing, controlling and monitoring of physical access, protection from fire, natural disasters, burglary, theft, vandalism, and terrorism
- **Network, servers and End Points Security:** applies many security layers of security appropriately to data center devices and network connections.
- **Data Security:** Data can be classified as high, moderate or low- sensitive data. It may be stored virtually and distributed across many locations; static or dynamic data. The data may reside on removable data storage or include in external network transfers. The encryption for storage, internal system and network transfers are required
- **Security of personal information:** to help protect personal information from unauthorized access, use, or disclosure.
- **Identity and Access Management:** role-based access controls are used to allocate logical access to specific job functions or areas of responsibility. They are based on an identified business requirements and authentic and authorized for the requested access. It uses technical systems to automate authorization for access and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

authentication for certain safeguards to access to the cloud resources

- **Application and Process Security:** to secure its cloud computing environment

b. Identify Data and Information Assets to Categorize Sensitive Data: which determine exactly what information assets and their value that the organization has and the potential damages if the information was lost or accessed inappropriately. The advantage of cloud technologies result in a decoupling of information assets from a common physical infrastructure for many types of customer objects.

The assets are classified to determine the strength of security controls that are needed to apply. Once classified, a defense approach is taken to determine what protections are needed. The six issues that must be addressed are [21]:

- Breach notification and data residency
- Data management at rest (being stored).
- Data protection in motion (being processed)
- Encryption key management
- Access controls
- Long-term resiliency of the encryption system

c. Threat Analysis & Vulnerability Analysis: the threat models are analyzed and vulnerabilities analyses are produced to verify they are complete and current, and documenting the potential attacks and conducting threat modeling**.**

- **Threats:** (Disclosure, Integrity, Denial of service).
- **Vulnerabilities:** (Personnel view, Physical view, Operational view, Communications view, Network view, Computing view, Information view).

d. Risk Identification/Resources: addresses all identified risks. Risk assessments occur at a variety of levels. A set of common risks and requirements can be affected by the type of cloud being used (private clouds versus non-private clouds). All of the resources of a private cloud are inside an organization's firewall; all other types of clouds (the public, hybrid and community) have at least part of their resources on a shared network.

Risk is managed depending on the requirements of three top-level security domains. The three categories of information security [22]:

i. Logical security: protects data using software such as password access, authentication, and authorization,
ii. Physical security: protects the infrastructure, building and physical access to the data center, and
iii. Administrative or Premises security: protects the people who may have access to data and the property within the data center**.**

e. Risk Impact Analysis: is a risk calculation-based on impact assessment and the associated business, focusing on those threats that could be highly disruptive. The magnitude of a threat 'T', the vulnerabilities 'V' to that threat, and the consequences 'C' that could result; are the factors that affect the risk R. Therefore, risk is considered as a *function* of *C*, *V*, and *T* [23].

$$\mathbf{R = f\ (C, V, T)} \qquad \mathbf{(1)}$$

Risk formula can be expressed as a multiplicative formula that may be written as follows:

$$\mathbf{R = C\ x\ V\ x\ T\ x\ } l_k \qquad \mathbf{(2)}$$

Where k is a constant introduced to scale *R* from 0 to 100. When *T* and *V* are treated as probabilities, the unit of measure for *C* becomes the unit of measure for *R*. The value of each factor is 1to 10 or 0 to 1 depending on the type of statistical method used. The multiplicative formula, Risk = T *x* V *x* C, is not an adequate calculation tool for estimating risk**.** Therefore, an additive formula at one time was used

$$\mathbf{R = aC + bV + cT} \qquad \mathbf{(3)}$$

Where parameters *a*, *b*, and *c* are constants. The additive formula involves assumptions about the way the components aggregate to risk.

The calculation of risk depends on the policy of each organization and what are the other issues that depend on them when it is applied in a security system.

f. Risk-Based Prioritization: Determine Prioritization per resource (Is it Critical or Not). It is to see how useful, reliable and cost-efficient they can be. It guides development of security controls and related activities.

g. Decision Making Depending on Selecting Cloud Data Protection Techniques: The appropriate decision need to be taken to mitigate the security vulnerabilities. Solution that do not provide the appropriate balance between protection and usability need to be discarded, and effectively minimize the risks of data theft, loss or accessed inappropriately

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

achieve compliance with existing regulation and equip personnel with tools that help them work productively and securely.

Cloud Security depends on significant constraints depending on the type of data it handles, the organization's location and the nature of its business. Security issues are classified into sensitive data access, data segregation, privacy, error exploitation, data recovery, cloud user authorization, malicious insiders, management console security, and account control, encrypting and managing encryption keys of data and multi-tenancy issues.

In cloud computing, anyone has access to the cloud service provider and has access to the data. Therefore, to reduce the threads and risks on data the following techniques are needed to implement:

- *Using Secure Hash Function to Check Data Integrity:*

  Cloud data integrity checking, as shown in figure 3; uses a one-way mathematical function, which takes a stream of data and reduces it to a fixed size data. The result is called a digest and can be thought of as a fingerprint of the data. The data digest can be reproduced with the same stream of data, but it is virtually impossible to produce a different stream of data that produces the same data digest. A data digest can be used to provide integrity in electronic communications [24]. However, this does not protect receiver from an attacker if third party can intercept sender's message and replace it with a new message and the digest of the new message.

  A secure hash can be used to generate a Hash-based Message Authentication Code, or HMAC, if the data owner and cloud user (receiver) share the same secret key. The resultant hash value is stored along with its corresponding data file in the cloud.

  If the user requests a data from cloud, a data and its HMAC are sent to the user. He can re-generate the HMAC to protect against changes in the data from any source. Third party can intercept sender's message and replace it with a new message, but he cannot generate an acceptable HMAC without knowing the secret key [25]. HMAC can be used in combination with any iterated cryptographic hash, such as Message Digest 5 (MD5) and Secure Hash Function SHA-1. It also provides for use of a secret key to calculate and verify the message authentication values.

- *Using a Digital Signature*

  A digital signature also verifies the integrity of the data. If the data has been changed since the signature was applied, a different digest would be produced. This would result in a different signature. Therefore, if the data does not have integrity, the validation will fail.

  Digital signatures are also used for authentication to systems or applications. Authentication is also useful for remote access to information on a server, protecting network management from masqueraders, or for gaining physical access to a restricted area.

- *Using Security for Infrastructures*

  To achieve the wide domain of security services, sender and receiver will need to use several types of cryptographic security mechanisms. In particular, they will need to distribute symmetric encryption keys, to achieve confidentiality. Distributing symmetric keys can be done effectively using public key based key management with a trusted third party (TTP). To achieve security services across organizational boundaries, many inter-linked TTPs will be required. It provides a comprehensive solution.

  Sender and receiver must be able to obtain each other's public keys and authenticate the other party's identity. They must depend on a trusted third party to distribute the public keys and authenticate the identity of the party associated with the corresponding key pair.

- *Using Cloud Data Tokenization at the field-level*

  It can be used to keep sensitive data local (resident) while tokens are stored and processed in the cloud. Tokens can reversed back to their original values using "look-up" table that matches them up to their original values. These tables are typically kept in a secure database located inside a company's firewall to prevent Denial of service (DoS). Tokens are used as the same structure and data type as their original values.

- *Using Decrypting inside a Processor*

  A sensitive data needs to be decrypted inside a processor that is based on the authenticated computing technology. The

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

technology will allow companies to have confidence in the security of the virtual machine running in the cloud, as long as it is running on the trusted platform

- Data links need to be inspected and access ports are required in order to ensure that the data links are not compromised.
- *Using API Standards*
  A standardization of APIs is needed to tight integration with virtualization management machines.
- *Apply Restrict access to sensitive information*
  Adequate security measures must be put in suitable place to ensure that unauthorized users cannot access data either intentionally or accidently.
- *Apply Monitoring Tools*
  Integrity monitoring software must be applied at the virtual machine level that makes extensive file property checking, including attributes, Directory-level monitoring, and auditable reports
- *Data Backup*
  It is the most important means to keep the data from being lost due to intentional or unintentional. It is also important to encrypt the up-to-date backups.
- *Apply tiered access control lists (ACLs)*
  It is to segmented virtual local area networks (VLANs) and applications as needed, and using a globally redundant internal and external DNS infrastructure through clustering of DNS servers.

h. Implement Security Controls (Risk Reduction or Avoidance): where the appropriate solution will be implemented in order to protect data in motion, in process and a rest.

i. Operational Security Evaluation (OSE): consists of reviewing associated network communications, platform, system configuration, and monitoring capabilities against established security standards and baselines. OSR process ensures appropriate and acceptable security controls levels.

j. Evaluate Effectiveness by periodically review the Information Security: The review of information security will lead to periodically assess the effectiveness of the security system, the extent of its success, the level of performance of the system and what are the things that will be modified in the future to improve the level of effectiveness of the system.

7. CONCLUSION:

In order to provide a secure environment and to protect sensitive static and dynamic data on cloud computing, firstly, different threats, vulnerabilities and risks are explained. Then, we have proposed a cloud computing security development lifecycle model to achieve safety and enable the user to take advantage of this technology as much as possible of security and face the risks that may be exposed to data. The data integrity checking algorithm that eliminates the third party auditing is explained. The cloud user has to deal with the cloud provider as the third party through managing the data integrity checking and evaluation in efficient way using set of hash functions. The data and its corresponding hash value are retrieved back when the cloud user needs cloud data, and checked for any data altercation by re-generating and comparing the hash result with the pre-generated hash value. Cloud computing security approach provides better protection in terms of filtering, risk management, deployment of standard information security policies.

ACKNOWLEDGMENT

The authors are grateful to the applied science private university, Amman-Jordan, for the financial support granted to this research article (GRANT No. DRGS-2012-2013-41).

REFERENCES:

[1] Brian O. and others, Cloud Computing, authors:, 2012-11- 06, page 6, publish Swiss.
[2] http://www.kalyxinfotech.com/cloud.php
[3] Sehgal NK, et al.: Information Security and Cloud Computing, Iete Technical Review, Vol 28, Issue 4, Jul-Aug 2011.
[4] Rajiv R.Bhandari, Mishra N., Encrypted IT Auditing and Log Management on Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, pp. (302), September 2011.
[5] Cloud Computing Evolution in the Cloud. Available at: http://www.pwc.de/de_DE/de/prozessoptimierung/assets/cloud_computing_2013.pdf.
[6] Deswarte Y., Quisquater J.-J., and Saidane A.. Remote Integrity Checking, Proc. of Conference on Integrity and Internal Control in Information Systems (IICIS'03), November 2003, Switzerland.
[7] Caronni G. and Waldvogel M., "Establishing Trust in Distributed Storage Providers", In

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Third IEEE P2P Conference, Linkoping 03, 2003.

[8] Golle P., Jarecki S. and Mironov I., "Cryptographic Primitives Enforcing Communication and Storage Complexity", In proc. of Financial Crypto 2002. Southampton, Bermuda.

[9] Syam Kumar P., Subramanian R., An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[10] http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=6&sid=5db89225-077d-4576-b4fc-7a7e0ebf9359%40sessionmgr112&hid=128.

[11] Velte T. A., Velte J. T. and Elsenperter R., Cloud Computing A Practical Approach, Chapter 1: Cloud Computing Basics, McGrawHill, USA, 2010. Available at: .http://www.south.cattelecom.com/Technologies/CloudComputing/0071626948_chap01.pdf.

[12] Sriram L., Khajeh-Hosseini A., Research Agenda in Cloud Technologies, 2010.

[13] https://cloudsecurityalliance.org/research/secaas/.

[14] Sriram L., Khajeh-Hosseini A., Research Agenda in Cloud Technologies, 2010.

[15] IBM Point of View: Security and Cloud Computing, Nov., 2009. Available at: http://www.ibm.com/ibm/files/X869751J69908G27/1securityandCloudIBM_382KB.PDF.

[16] Katiskas, S., Risk Management, In J. Vacca (Ed.), Computer And Information Security Handbook. Bedford, MA: Morgan Kaufmann Publishers, 2009.

[17] Northcutt, S. (2011). The Attack Surface Problem. Available at: http://www.sans.edu/research/security-laboratory/article/did-attack-surface.

[18] http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428?page=0,1.

[19] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[20] http://www.altiusit.com/files/blog/Top10CloudComputingThreats.htm.

[21] http://www.computerweekly.com/news/2240180087/Six-security-issues-to-tackle-before-encrypting-cloud-data.

[22] http://www.sans.org/reading-room/whitepapers/cloud/introduction-securing-cloud-environment-34052.

[23] GRiP – A Flexible Approach for Calculating Risk as a Function of Consequence, Vulnerability, and Threat. Available at: http://www.dis.anl.gov/pubs/69700.pdf.

[24] Kuhn R. D. and others, (2001), "Introduction to Public Key Technology and the Federal PKI Infrastructure", U.S. Government publication. http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.

[25] Kuhn R. D. and others, (2001), "Introduction to Public Key Technology and the Federal PKI Infrastructure", U.S. Government publication. Available at: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.

Journal of Theoretical and Applied Information Technology
31st December 2013. Vol. 58 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

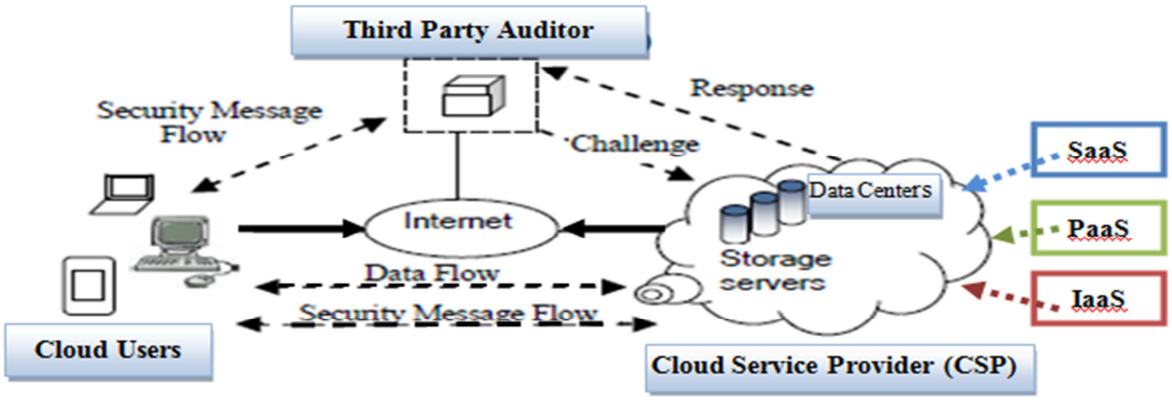

Figure1: Cloud Data Storage Model

Journal of Theoretical and Applied Information Technology
31st December 2013. Vol. 58 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

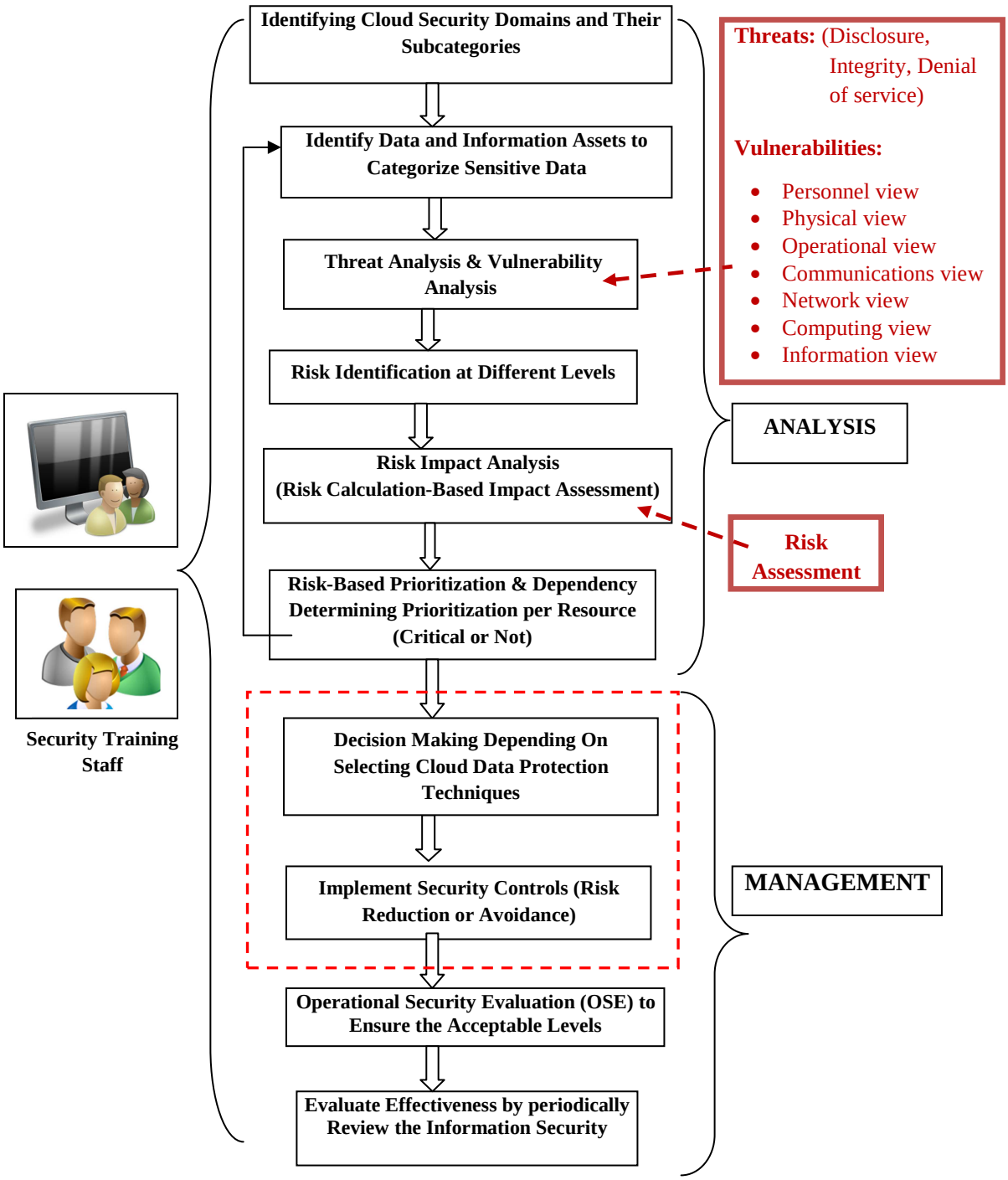

Figure2: Proposed Cloud Computing Security System Development Model

Journal of Theoretical and Applied Information Technology
31st December 2013. Vol. 58 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

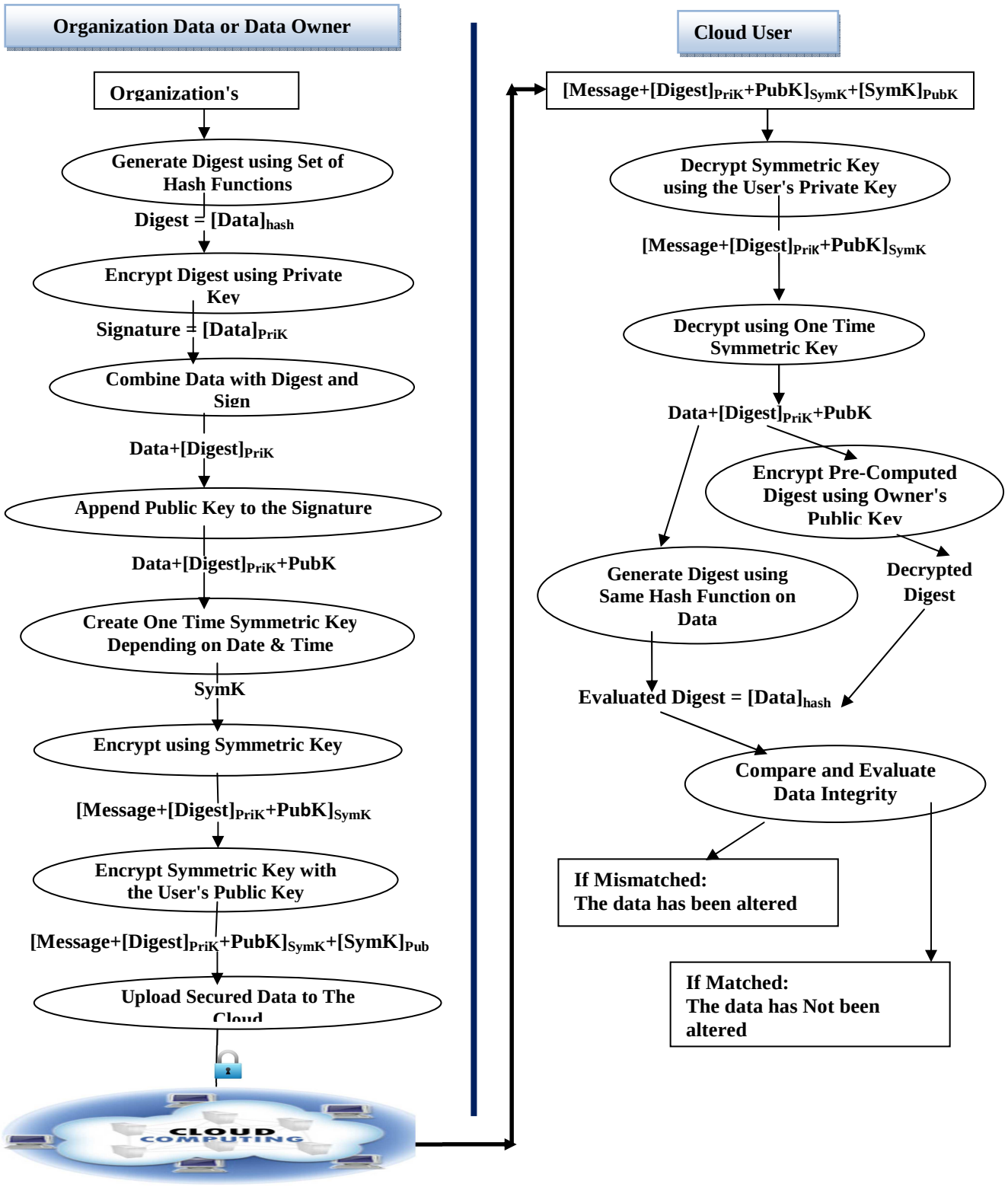

Figure 3: Data Integrity Checking Algorithm