A Security Policy for Cloud Providers

The Software-as-a-Service Model

Dimitra Georgiou
Secure Systems Laboratory
Department of Digital Systems
School of Information & Communication Technologies
University of Piraeus, Piraeus, Greece
dimitrageorgiou@ssl-unipi.gr

Costas Lambrinoudakis
Secure Systems Laboratory
Department of Digital Systems
School of Information & Communication Technologies
University of Piraeus, Piraeus, Greece
clam@unipi.gr

***Abstract*—Cloud Computing is a new computing paradigm originating and combining characteristics from grid computing, distributed computing, parallel computing, virtualization and other computer technologies. Trust and security in Cloud Computing are more complex than in traditional IT systems. Conventional security policies designed for other technologies do not map well to the cloud environment, which, on top of that, may exhibit additional security requirements. In an attempt to assist cloud providers to secure their environment, and specifically for the Software-as-a-Service Model (SaaS), this paper starts with the presentation of the already reported threats. Because of these security threats, there are specific requirements that we claim must be clearly addressed in the Security Policy for the Cloud Environment. Our work focuses on the required structure and contents of such a security policy. In this respect, this paper proposes a model to describe the relationship between threats, measures, and security policies applicable to the SaaS model. It is worth stressing that in the SaaS service model, the client depends on the provider for the proper security measures.**

Keywords-Cloud Computing Security; Security Policies; Security Requirements; Software-as-a-Service (SaaS)

I. INTRODUCTION

Nowadays, in an interconnected world, every corporation needs a very well thought security policy. The rapid growth of the information age has significantly changed the nature of computing, and gives rise to a new set of security concerns and issues. According to the National Institute of Standards and Technology (NIST), the Security Policy is defined as an "Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects and distributes information"[1].

For the new era of Cloud Computing**,** the purpose of a security policy is to protect people and information, set rules for expected behavior by users, minimize risks and help to track compliances with regulation[2].Considering the fact that in recent times anyone with an interest in information technology has come across the term Cloud Computing [3], it is really important to seriously consider the security issues in Cloud Computing: Are there any Security threats in Cloud Computing, that do not appear in non- Cloud Systems? Is the Cloud secure and safe for the users? As Cloud Computing is achieving popularity, we attempt to demystify the security and privacy risks that are introduced, because of its transformational nature [4].The success of a Cloud Policy really depends on the way the security contents are addressed in the policy document and how the content is communicated to users [5]. But, before we analyze all these risks, we need to have a clear understanding of what "Cloud Computing" is.

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [6].Cloud is a recent trend in Information Technology that moves computing and data away from desktop and portable PCs into large data centers. It refers to applications delivered as services over the Internet, as well as to the actual cloud infrastructure, namely, the hardware and systems software in data centers that provide these services [7] (see Figure 1).

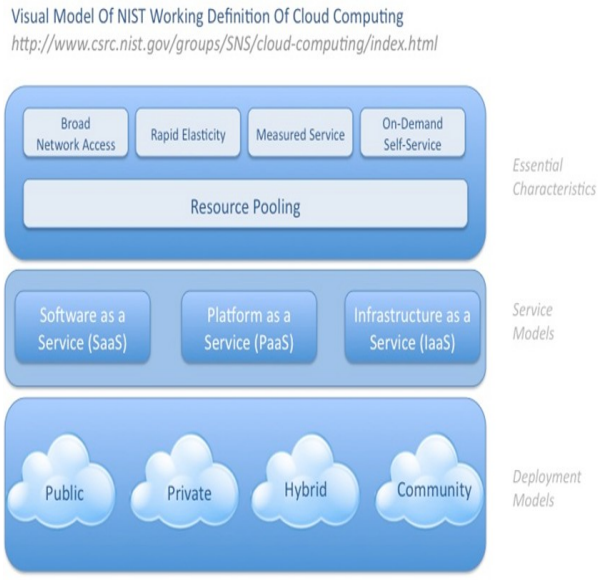

Figure 1. Visual Model of NIST Working Definition of Cloud Computing [7]

The advantages of Cloud Computing and specifically its ability to scale rapidly (through subcontractors), store data remotely (in unknown places) and share services in a dynamic environment, can become a major flow in maintaining a level of privacy assurance sufficient to sustain confidence in potential customers. Cloud has exacerbated the strain on traditional frameworks for privacy that globalization has already started. To understand the importance of Cloud

 ISBN: 978-1-61208-362-9

Computing and its adoption, we must understand its principal characteristics, its delivery and deployment models, how customers use these services, and how to safeguard them.

There are three service models of Cloud Computing: Software-as-a-Service **(SaaS)**, Platform-as-a-Service **(PaaS),** Infrastructure-as-a-Service **(IaaS)** and three main deployment models which are: Private cloud, Public cloud and Hybric cloud [8][9][10][11][12][13] (see Figure 2). These service models also place a different level of security requirements in the cloud environment. IaaS is the foundation of all cloud services, with PaaS built up on it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks.

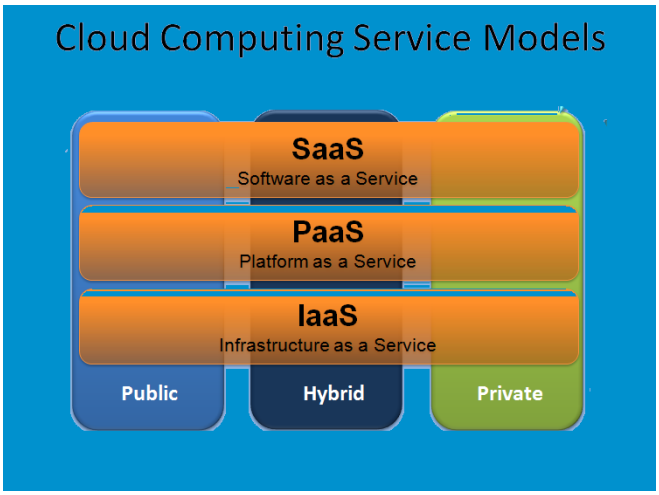

Figure 2. Cloud Computing Service Models

This paper proposes a methodology that may be adopted for the development of a Cloud Security Policy. It assesses how security, trust and privacy issues can be addressed in the context of a Cloud Computing Policy and is organized as follows: Section II presents an overview of related work on security issues and security Policies for Cloud Computing. Then, Section III, analyses the policy issues related to Cloud Computing, while Section IV depicts the proposed methodology for a Cloud Security Policy, for Cloud Providers in the SaaS service model. Section V presents the linking of threats, security measures and security policy rules for Threat 5 (Introduction of damaging or disruptive software) and finally, Section VI concludes the paper and provides some pointers for future work.

II. RELATED WORK

Cloud Computing is a new computing model originating from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies. It exhibits many advantages such as large scale computation and data storage, virtualization, high expandability, high reliability and low price service. Trust and security in Cloud Computing are more complex than in a traditional IT systems. But, what exactly is the problem?

In order to have a secure Cloud Computing deployment, it is necessary to consider the following areas: the Cloud Computing architecture, governance, portability and interoperability, traditional security, business continuity and disaster recovery, data center operations, incident response, notification and remediation, application security, encryption and key management, identity and access management [14][15][16]. Many of the security issues arising from the aforementioned areas, have been already addressed in other systems. However, the specific characteristics of cloud environments result into new security concerns; Cloud architecture is fundamentally different from other systems, the cloud environment is by nature multitenant with shared resources, and the location of the data and the local privacy requirements will not be controlled by the user. Another major problem is the lack of standardization. Since no proper standards for Cloud Computing exist, it becomes extremely difficult for a company to secure the services that it offers or uses through a cloud.

Cloud Computing security challenges and issues have been addressed by various researchers. The National Institute of Standards and Technology contends that security, interoperability, and portability are the major barriers to a broader cloud adoption [17]. Data confidentiality and service availability in Cloud Computing are also key security issues. A single security method cannot solve the Cloud Computing security problem and many conventional and new technologies and strategies must be employed together for protecting the entire Cloud environment.

Robert Gellman's report at the World Privacy Forum [18] focuses on privacy issues and legal compliance of sharing data in the cloud. He mentions various legal issues such as the possibility of the cloud being in more than one legal location at the same time with different legal consequences and such uncertainty making it very difficult to assess the privacy protection level offered to the users [19]. Also, ENISA investigated the different security risks related to adopting Cloud Computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in Cloud Computing that may lead to such risks [20].

According to Al Morsy et al. [21] the Cloud Computing model has different stakeholders involved, namely: cloud provider, service provider and service consumer. Each stakeholder has its own security management systems/processes and each one has its own expectations (requirements) from the other stakeholders.

Cloud environments exhibit different architectures based on the services they provide, thus making it even harder to find 'global' security measures .Louay Karadsheh [22] examines the risks encountered by implementing the Infrastructure-as-a-Service (IaaS) model and discusses the role of security policies, Service Level Agreement (SLA) and compliance for enhancing the security of the IaaS service model. Subashini and Kavitha [13] describe the various security issues of Cloud Computing in relation to its service delivery model and they list some of the existing solutions that partly address the security challenges posed by the cloud. Cheng and Lai [23] introduce the characteristics of the newly developed Cloud Computing technology first, and then they highlight the reasons for emphasizing the issue of information privacy in relation to new cloud applications. Vaquero et al. [24] analyze the security risks that multitenancy induces the Infrastructure-as-a-Service clouds and present the most relevant threats and relevant state of the art of solutions. Also, in the same paper they continue analyzing the open security issues and challenges that should be addressed. Even though the majority of the research work published focuses on security issues, legal and jurisdictional

 ISBN: 978-1-61208-362-9

risks [25][26][27], none addresses the need for a Cloud Security Policy. For instance, Karadsheh [22] discusses the role of security policies, SLA and compliance for enhancing the security of the IaaS service model, by presenting several applicable policies. Furthermore, this paper discusses the possibilities of applying different types of security policies to enhance security of IaaS to acceptable level, but they do not propose a security policy. Similar is the approach by Subashini and Kavitha [13], who describe the common security issues posed by the cloud service delivery models and the security threats posed by the IaaS delivery model, but they do not provide a comprehensive analysis of the specific threats to be addressed by cloud providers.

In an attempt to assist cloud providers to secure the environment that they offer, and specifically for the Software-as-a-Service Model (SaaS), this paper presents the already reported threats to ease their comprehension. Because of these security threats, there are specific requirements that we claim must be clearly addressed in the Security Policy for the Cloud Environment. Our work focuses on the required structure and contents of such a security policy.

III. AN ANALYSIS OF THE SECURITY POLICY ISSUES RELATED TO CLOUD COMPUTING

The Cloud Computing model involves different stakeholders: the Cloud Provider (an entity that offers the cloud infrastructure or /and services to the cloud consumers), the Service Provider (an entity that utilizes the cloud infrastructure to deliver applications/services to the end users) and the Service Consumer (End user; an entity that uses services hosted on the cloud infrastructure). Each stakeholder has its own expectations (requirements) and security management systems/processes [21]. For instance, if we consider user expectations they would expect that the cloud provides: reliability and liability, security, privacy, anonymity, access and usage restrictions [28].

The decision of whether the Cloud Customer or the Cloud Provider (Service Provider) is responsible for a given control and for security and privacy depends on three factors:

a) The cloud model (SaaS, IaaS, or PaaS) chosen.
b) The extent to which the Cloud Customer is allowed to configure the CP's controls.
c) Legislations, which may dictate the assignment of responsibilities and thereby overrides the previous two factors.

Next, we highlight the possible threats for a Cloud Provider who adopts the Software-as-a-Service (SaaS) model:

Threat 1: **Masquerading of user identity by insiders:** The threat of masquerading of user identity by insiders covers attempts by authorized users to gain access to information to which they have not been granted access. These users may attempt to gain access to that information by using another user's account.

Threat 2: **Masquerading of user identity by contracted service Providers:** The threat of masquerading of a user identity by contracted service providers covers attempts by people working for a contracted service provider to obtain unauthorized access to information by using an authorized person.

Threat 3: **Masquerading of user identity by outsiders:** The threat of masquerading of a user identity by outsiders covers attempts by outsiders to obtain unauthorized access to information by posing as an authorized user.

Threat 4: **Unauthorized use of an application:** It covers various cases of unauthorized use of an application.

Threat 5: **Introduction of damaging or disruptive software:** This threat covers Viruses, Worms, Trojan Horses, logic bombs, any other form of malicious software.

Threat 6: **Misuse of system resources:** Identifies factors that increase the threat of misuse of system resources; covers People playing games on business systems, People using business systems for personal work, People downloading non-work related information from the internet, People setting up databases or other packages for non-work related matters.

Threat 7: **Communications infiltration:** This threat covers the following types of event: Hacking into a system using, for example, buffer overflow attacks, Masquerading as a server, Masquerading as an existing user of an e-commerce application, Masquerading as a new user of an e-commerce application, Denial of service (deliberate), Flaming attacks, and Spamming.

Threat 8: **Communications interception:** This threat covers Passive interception and Traffic monitoring. The ease of interception is determined by two basic-factors: The medium of transmission and the type of protocols being used. Interception of some types of traffic on the internet is relatively easy. It can be achieved by attackers sending messages to target systems instructing them to send traffic via specific (hostile) machines.

Threat 9: **Communications manipulation:** Active interception, Insertion of false messages, Deliberate delivery out of sequence, Deliberate delay of delivery, Deliberate misrouting. If an attacker can force a message to be sent via a hostile host, the attacker may be in a position to intercept, alter and the forward the message.

Threat 10: **Repudiation:** This threat addresses cases of people denying that they sent a message (repudiation of origin), or that they received a message (repudiation of receipt).

 ISBN: 978-1-61208-362-9

Threat 11: **Communications failure:** Unavailability of Service Provider, Failure of data link, Non – delivery of message, Accidental delivery out of sequence, Accidental delay in delivery, Accidental denial of service. The Internet does not provide a service level agreement. There are no guarantees on how long it will take for a message to get to a recipient, or even that it will get there, eventually.

Threat 12: **Embedding of malicious code:** Includes email viruses and hostile mobile code (for example hostile Active X applets). Once on a network, they can quickly infect many machines causing significant disruption. Java and Active X raise a range of new security concerns. Users are now running code written by people from outside of the organization, sometimes from unknown sources. This code has often not been tested by the organization. There are concerns that hostile code written using these types of techniques could inflict damage on systems and networks.

Threat 13: **Accidental misrouting:** The threat of accidental misrouting covers the possibility that information might be delivered to an incorrect address when it is being sent over a network.

Threat 14: **Technical failure of host:** This threat covers failures of the CPU or other hardware items.

Threat 15: **Technical failure of storage facility**: This threat covers disk crashes and disk failures.

Threat16: **Technical failure of Print facility:** This questionnaire identifies the factors that increase the threat for a technical failure of the print facility.

Threat 17: **Technical failure of network Distribution Component:** This threat addresses cases of network distribution components, such as bridges and routers, failure.

Threat 18: **Technical failure of Network Management or Operational Host:** This questionnaire identifies the factors that increase the threat of technical failure of a network management or operation host.

Threat 19 : **Technical Failure of Network Interface:** Here, the factors that increase the threat of failure of the network interface are identified.

Threat 20: **Technical failure of Network service:** Here, the factors that increase the threat of failure of the network service are identified.

Threat 21: **Power failure:** This threat covers the possibility that the power supply to the building may fail. The types o power failure covered include: spikes, surges, brown outs, black outs.

Threat 22: **Air conditioning failure:** This threat covers the possibility that operation may have to be suspended because temperatures in the location fall outside of acceptable parameters.

These threats are being used for illustrating where the dangerous points lurk at every level of the typical SaaS model in a Cloud Provider's environment.

In all three cloud models, the Cloud Provider manages and controls the infrastructure, which comprises the servers, networks, electricity, human resources, and site services. As such, the Cloud Provider is responsible to implement and operate suitable infrastructure controls such as employee training, physical site security, network firewalls, and others. Infrastructure controls are of fundamental importance. It is evident, from the complexity of Cloud Computing and the threats that the cloud is facing, that the development and adoption of a Security Policy is necessary. Understanding the threats relevant to the SaaS service model will assist in formulating a well-established security policy.

Although much research into cloud services security engineering has been undertaken and almost everybody accepts that there are a lot of security and privacy issues for Cloud Computing, no one has raised the need for a Security Policy for Cloud Computing.

IV. A SECURITY POLICY STRUCTURE FOR CLOUD COMPUTING

Existing research analysis methodologies are not appropriate for Cloud Computing since threats in Cloud are different. The appropriate Security policies designed for conventional architectures do not map well to the cloud environment. Cloud architectures must have well-defined security policies and procedures in place. As companies move to Cloud Computing, the traditional methods of securing data are being challenged. For instance, it may be difficult for the cloud customer to effectively control the data processing that the cloud provider carries out and thus to be sure that the data is handled in a lawful way. Failure to comply with data protection law may lead to administrative, civil and also criminal sanctions, which vary from country to country, for the data controller. It is therefore important all security requirements, including the ones that are only applicable to the cloud environments, to be covered by a security policy. Therefore in this paper we indeed provide a new methodology for assessing the threats/risks in Cloud, in order to identify new rules that must be incorporated in the Cloud Security Policy. The work, in this paper, does not result in a Cloud Security Policy. Instead, it proposes a methodology that may be used for the development of the appropriate Cloud Security Policy.

The proposed methodology for the development of a cloud Security Policy exhibits three distinct levels:

 ISBN: 978-1-61208-362-9

1) The Cloud Provider level,
2) The Service Provider level and
3) The User level.

Even though there are parts of the security policy that are common to all levels, each level will also exhibit dedicated security policy parts/rules. This three-layered classification of security requirements of cloud systems and the common parts of the Policy (colored) is illustrated in Figure 3. As already mentioned earlier, the focus will be on SaaS (Software-as-a-Service) models.

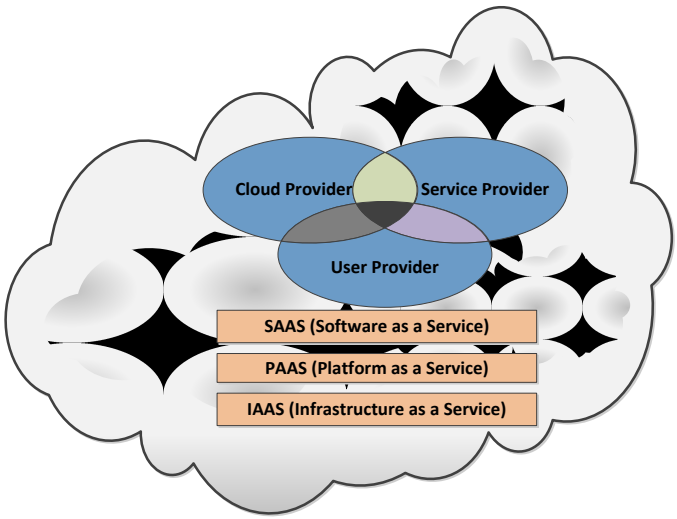

Figure 3. Security Policy Structure for Cloud Providers

The threats that we referred to in the previous section can be employed for deducing the security requirements that must be satisfied by the cloud provider.

To demonstrate this, a specific threat (Threat 5 - Introduction of damaging or disruptive software) has been chosen to depict the correlation between Threat -Requirement – Security Measures – Policy for a Cloud Provider (see Section V and Figure 4).

More specifically, in Figure 4, each security measure that can be employed for eliminating Threat 5 is associated with the necessary set of rules that make up the security policy of the cloud provider. The same information is provided in more detail with more analysis in Section V below. Doing this type of analysis for each Threat that the SaaS service model is facing will help in formulating a well-established security policy.

V. LINKING THREATS , SECURITY MEASURES AND SECURITY POLICY RULES

A. Threats

Next, Threat 5: *Introduction of damaging or disruptive software*, will be analyzed as an example. In parallel the security measures and policy rules linked to that threat will also be examined.

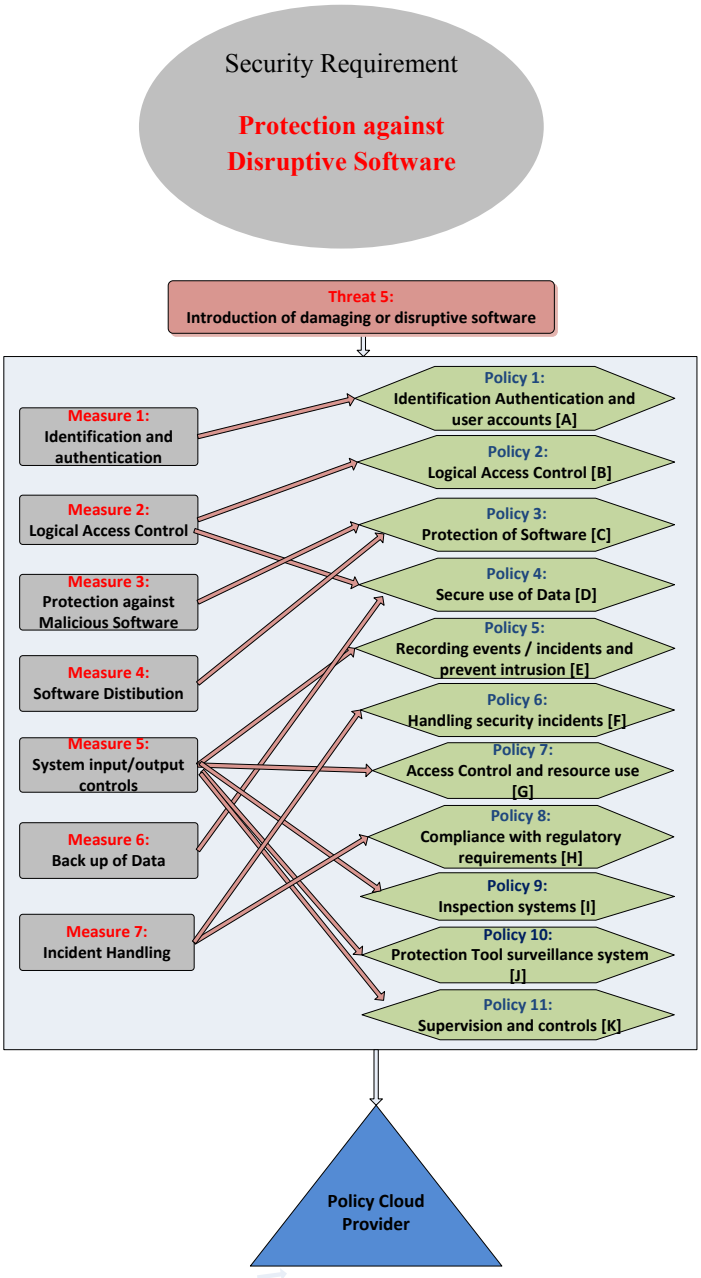

Figure 4. Security Policy rules covering Threat 5

B. Measures

The security measures associated with the aforementioned threat follow.

- Identification and authentication (Security Policy Rules A)
- Logical access control (Security Policy Rules B & D)
- Protection against malicious Software (Security Policy Rules C)
- Software Distribution (Security Policy Rules C)
- System input /output controls (Security Policy Rules E & G & I & J & K)
- Back-up of Data (Security Policy Rules D)
- Incident Handling (Security Policy Rules F & H)

 ISBN: 978-1-61208-362-9

C. Security Policy Rules

The security policy rules associated with the aforementioned threat and security measures follow.

1) Identification and authentication

Users are identified uniquely ensuring that any action can be attributed to a specific user. This rule applies to the operating system level and to the application level, while the following minimum requirements should be satisfied.

- Each user has a unique identity (user ID).
- A list of users and their unique identities is maintained.
- Each authentication identifier is assigned to a user and is used by a single user.
- The system administrators have identities that correspond to accounts with elevated privileges.

2) Logical access control

There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. Specifically:

- Registered user accounts shall be reviewed for applicability at specific periods.
- Privileges shall be defined for specific business purposes.
- The allocation and use of privileges shall be restricted and controlled.
- Privileges and privilege allocation shall be reviewed for applicability at specified periods.
- The allocation and establishment of user passwords shall be controlled through a formal management process.
- Management shall review user rights at regular intervals using a formal process.
- Users shall be required to follow good security practices in the selection use of passwords.

3) Protection software

Special care should be taken to control the development and maintenance of software applications. Specifically:

- Application development should be conducted with specific, scientifically accepted methodologies.
- Each new application must be accompanied by sufficient documentation in accordance with international standards.
- The risk analysis must fit into the requirements analysis.
- Systems utilized for the development and testing of software must be separate from the operational systems.

Software changes should be authorized prior to their implementation:

- Application software changes require approval by their respective makers.
- Any proposed change should be examined whether it affects the security of the information system.

Changes that affect - directly or indirectly - security requirements must be approved by the Security Officer. Specifically:

- The amendments must be made in the development/testing environment and should be tested prior to their application to the operational system.
- All changes must be characterized by a unique serial number.
- At each change request it is necessary to record the corresponding date and the name of the applicant.
- All software changes must be accompanied by documentation updates.

In case where urgent changes are required, it is necessary to ensure the following:

- Keep to a minimum the changes that will be performed.
- The modified files must be monitored.
- The Security Officer must be informed.
- Irrespectively of how urgent are the modifications, they must be tested before they are incorporated in the live system.

After any kind of modifications on the live system it is necessary to re-test system security. To this end the security officer must monitor the effectiveness of the security mechanisms after the modification took place.

4) Secure Data Management

Data should be categorized according to the protection they need, as derived from the risk analysis or assessment of the head of Information System. The following categories have been identified:

- Top secret: information and critical data of the Information System that any disclosure or unauthorized modification will have direct impacts on the operation.
- Confidential: information and data that is important for seamless operation and should be subject to strict controls and protected.
- Sensitive: information and data that is subject to legislation on protection of personal data. Disclosure of this data requires specific permission / license.
- Reportable: information and data that can be disclosed.

The requirements of information security and the way data is processed vary according to the category of information. It is necessary to specify the authorized data recipients, according to the above classification. Data processing must ensure procedural and technical resources that can be attributed to a specific individual. Therefore, all critical operations will be accessed in a strictly personalized way.

5) Recording actions / events and intrusion prevention

Incidents of failure or non-routine functions of hardware or/and software, should be recorded and evaluated in relation to the operation that they support. Critical application systems should exhibit real time alarm systems. If there is a risk of invasion by external systems, intrusion detection and prevention systems should be in place. Systems will record the suspicious actions for the invasion and react automatically if this is dangerous for the security of the Cloud Provider. Proven invasions activate alarm system in real-time. The log files should be protected from loss or intentional corruption. The logs will be inspected by authorized personnel from time to time to highlight events / actions that endangered the Service Provider.

 ISBN: 978-1-61208-362-9

6) Handling security incidents

A procedure for reporting faults and general security incidents is mandatory. There should be documented procedures that will ensure the timely and effective response to the occurrence of a security incident. This framework should include:

- The roles and responsibilities to be undertaken.
- Recorded evidence of what happened.
- Rescuing electronic material proving the breach (e.g., unchanged medium).
- The process of identifying the cause of the break up.
- The process of recovery.

7) Access control and resource use

A strict registration process should be in place. As a minimum it should support the following:

- The access rights are determined through a rigorous registration process.
- The new system users are required to submit an application in order to obtain an account.
- The application contains the elements of the applicant's position and the department to which she belongs.
- The application is signed by the user and her supervisor and is forwarded to the IT director.
- The rights granted are always appropriate for the purpose that they serve.
- Inspections must be conducted by the Security Officer.
- If a user changes responsibilities and requires a new set of usage rights, she should request it through a new application.
- When a user is given a new set of usage rights, old rights he should be removed.
- Users should take care of the safe use of their accounts.
- The idle time of a workstation should be limited. After some time of inactivity, workstations should lock (e.g., password protected screen saver).

Regarding the use of system resources it is necessary to keep a list of all IT resources (hardware, software and documentation) and to record the classification level of each resource.

Furthermore an Access Control Policy is necessary for controlling access to the resources of the Information System. The access control policy should exhibit the following:

- The access policy setting takes into account the principle of « need to know» (need-to-know).
- Users can use only the applications and the resources needed to perform the tasks associated with their position.
- The use rights assigned to each user category are inspected at least once every six months, with the responsibility of IS Security Officer to ensure that it is not given more rights than necessary.
- A copy of the password of the system administrator account must be kept in a safe place. The access to stored passwords should be controlled.
- System administrators should use different passwords for administrative accounts and the accounts they use as ordinary users.
- The exercise of rights of access users will be monitored and controlled in order to avoid the abuse of rights.

8) Compliance with regulatory requirements

It is necessary to comply with existing legal and regulatory framework. Specifically:

- Monitor all legal and regulatory requirements and examine how they can be satisfied.
- Notification of the Data Protection Authority for keeping personal data.
- If records of sensitive data are kept, permission from the Data Protection Authority is necessary.
- Description of procedures to ensure the fulfillment of legal obligations for use hardware / software, ie the necessary licenses.
- Employ the necessary measures for protecting critical data from loss, destruction and unauthorized amendment in accordance with legislative requirements.
- Employ the necessary measures to ensure data protection and privacy as required by laws and regulations.
- Monitor and comply with all existing technical standards.

9) Inspection systems

Determine all audit requirements in accordance to the existing legal and regulatory framework, as well as the procedures for controlled access to inspection tools in order to avoid damage, loss or misuse.

10) Protection of surveillance system

Access to the tools of IS surveillance shall be controlled. Specifically:

- Access to the monitoring tools should be restricted to authorized persons.
- Ensure that maintenance contractors will not have access to surveillance tools. If they need some data they should be provided by the system administrators according to the need-to-know principle.
- Restrict the access rights of the administrators in order to ensure that they will not be able to remove or change registration details of their own actions.
- In order to facilitate correct monitoring, the clocks of different systems must be synchronized.

11) Supervision and control

Audit trails and event logs must be recorded in order to support the identification of violations or attempted violations and scrutinizing every suspicious incident. To this end the following are necessary:

- To maintain monitoring data for all systems supporting multi-user access.
- To use special software for managing these files.
- To record the use of privileged functions.
- To record system startup.

 ISBN: 978-1-61208-362-9

- To record failed attempts.
- To record binding energy (log-on).
- To record disconnect actions (log-off).
- To record changes in access rights and use.
- To record the basic data for each suspected case.
- To record the user identifiers (User IDs).
- To record the time and the time of the event.
- To record the type of the event.
- To record the files accessed.
- To record the identity of the station.
- To record the state of the data before and after the changes.
- A copy of the audit data files must be kept in back up media (back-up).
- Data must be kept at least for a period of three months. In systems that manage classified information, data must be retained for the period specified by the national safety regulations.
- Copies are kept in a safe place, so to prevent any theft or sabotage.
- Access to log files is prohibited in those that do not have privileges (administrative rights).
- Log files should be protected from potential disaster.
- There should be integrity checks in place.
- Log files should be tested at least once a year.
- If the space available for log files reaches 75% of its storage capacity, an alarm must be produced.
- Inform users which of their activities are recorded by the system.
- Analyze logs of actions and events.
- Monitor the creation of accounts with elevated permissions.
- Identify deviations from normal use of system resources (e.g. unusually large number of prints from a user).
- The system automatically notifies the Security Officer when it detects certain suspicious events.

VI. CONCLUSION

Cloud Computing is a very promising technology that helps companies reduce operating costs while increasing efficiency. Even though Cloud Computing has been deployed and used in production environments, security in Cloud Computing is still in its infancy and needs more research attention. This paper reviews the potential threats for the Software-as-a-Service Model (SaaS), in an attempt to assist cloud providers identifying the security requirements and securing the environment that they offer.

We claim that by linking each threat to the security measures that can be utilized for eliminating it, and in turn, with the security rules that are necessary for the implementation of the security measures, a Security Policy for cloud providers that clearly addresses the specific threats can be defined. The aforementioned correlation / linking is provided indicatively, for only one of the identified threats.

REFERENCES

[1] National Institute of Standards and Technology, systems, “Guide for developing security plans for federal information systems”, vol. 800-18, February 2006, [Online]. Available from:http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf/, [accessed December 2013].

[2] Divers S. - SANS Institute, "Information Security Policy A development Guide for large and small companies", November 2007, pp. 43-44.

[3] Svantesson D. and Clarke R., “Privacy and consumer risks in Cloud Computing", Computer Law and Security Review, vol. 26, 2010, pp. 391-397.

[4] Kshetri, N., “Privacy and security issues in Cloud Computing: The role of institutions and institutional evolution”. 2012, Bryan School of Business and Economics, The Univ. of North Carolina at Greensboro, NC27402-6165,USA.

[5] Hone K., Eloff J. H., “Information security policy: what do international information security standards say?”, Proc. of the 8th European Conference on Information Warfare and Security, Computers and Security, vol. 21, Issue 5, 2002, pp. 402- 409.

[6] Mellet P.and Grance T., “The NIST Definition of Cloud Computing”, NIST, 2011, Special Publications 800-145.

[7] Dikaiakos, Katsaros M.D., Mehra D., Pallis P. and Vakali G, “Cloud Computing Distributed Internet Computing for IT and Scientific Research”, IEEE Press 2009, vol. 13, Issue: 5, pp. 10-13.

[8] European Network and Information Security Agency (Enisa), “Cloud Computing Benefits, risks and recommendations for information security”, November 2009.

[9] Arnold S., “Cloud Computing and the issues of privacy”, July 2009, KM World, pp.14-22

[10] Whitepaper, A, “Enterprise Cloud Computing: Transforming IT”, Platform Computing, viewed 13 March 2010, pp.6.

[11] Global Netoptex Incorporated, “Demystifying the cloud. Important opportunities, crucial choices”. 13 December, 2009, pp. 4-14., [Online]. Available from: http://www.gni.

[12] Kuyoro S.O., "Cloud Computing Security Issues and Challenges", Proc. International Journal of Computer Networks (IJCN), 2011, vol. 3, Issue: 5.

[13] KavithaV. and Subashini S.,“A survey on security issues in service delivery models of cloud”, International Journal of Network and Computer Applications, January 2011, vol. 34 Issue 1, pp.1-11

[14] Brodkin J., “Gartner: Seven cloud- computing security risks”, NetworkWorld, April 2013, [Online]. Available from: http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf

[15] Okuhara M. et al- FUJITSU, “Security Architecture for Cloud Computing”, vol. 46, no 4, October 2010, Sci.Tecch.J., pp.397- 402].

[16] Min Y., Shin H., Bang Y., “Cloud Computing Security Issues and Access Control Solutions”, Journal of Security Engineering, February 2012, vol. 9, no2.

[17] National Institute of Standards and Technology, “Cloud Computing Synopsis and Recommendations”, May 2012, Special Publication 800-146.

[18] Gellman R., “Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing”, World Privacy Forum February 2009, [Online]. Available from: http://www.scribd.com/doc/12805751/ Privacy-in-Cloud-Computing-World-Privacy-Council-Feb-2009, [accessed November 2013].

[19] Chadwick W.D. and Fatema K., "A privacy preserving authorisation system for the cloud", November 2012.

[20] European Network and Information Security Agency, “Cloud Computing benefits, risks and recommendations for information security”, 2009.

 ISBN: 978-1-61208-362-9

[21] Morsy M. Al., Grundy J. and Müller I., "An Analysis of the Cloud Computing Security Problem", Proc. APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.

[22] Karadsheh L. "Applying security policies and service level agreement to IaaS service model to enhance security and transition "Computers & Security, vol. 31, Issue 3, May 2012, pp. 315-326.

[23] Cheng F., and Lai W., "The impact of Cloud Computing Technology on Legal Infrastructure within Internet-Focusing on the Protection of Information Privacy", Proc International Workshop on Information and Electronics Engineering, Elsevier Ltd Press 2012, vol.29, pp.241-251, doi: 10.1016/j.proeng.2011.12.701

[24] Vaquero M., Rodero-Merino L., and Moran D., " Locking *the* Sky*:* A Survey on IaaS Cloud Security Computing", Springer, Press, January 2011, vol. 91*,* Number 1*,* pp. 93-118*.* doi: 10.1007/s00607-010-0140-x

[25] European Commission. "Official Journal of the European Union On Data protection guidelines for the Early Warning and Response System", 9 February 2012 L 36/31.

[26] Pearson S. and Charlesworth A., "Accountability as a Way Forward for Privacy Protection in the Cloud", HP Laboratories HPL-2009-178, Proc. 1st CloudCom, Beijing, Springer LNCS Press, December 2009.

[27] European Commission, "Safequarding Privacy in a Connected World: A European Data Protection Framework for the 21th Century" COM (2012), 25 January 2012, article 9 final Brussels.

[28] Jaeger P.T., Lin J. and Grimes J.M., "Cloud Computing and Information Policy: Computing in a Policy Cloud?", Forthcoming in the Journal of Information Technology and Politics (ITI 2008), vol. 5, no. 3, pp. 269-283.

 ISBN: 978-1-61208-362-9