ISSN:2249-5789
K Suriya et al , International Journal of Computer Science & Communication Networks,Vol 5(2),136-144

SECURITY CONCERNS AND SOLUTIONS FOR CLOUD COMPUTING

1. K.SURIYA
Assistant professor
Department of Computer Applications
Dhanalakshmi Srinivasan College of Arts and Science for Womren
Perambalur
Mail: Surik.mca@gmail.com

2. R.JOTHI
Assistant professor
Department of Computer Applications
Dhanalakshmi Srinivasan College of Arts and Science for Womren
Perambalur
Mail: jothi1981.ramadoss@gmail.com

ABSTRACT

The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, this paper gives classification of main security concerns and solutions in cloud computing.

I.INTRODUCTION

Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution. This view point is shared by many distinct groups, including academia researchers business decision makers and government organizations. Due to the ever growing interest in cloud computing, there is an explicit and constant effort to evaluate the current trends in security for such technology, considering both problems already identified and possible solutions .An authoritative reference in the area is the risk assessment developed by ENISA (European Network and Information Security Agency). Not only does it list risks and vulnerabilities, but it also offers a survey of related works and research recommendations. A similarly work is the security guidance provided by the Cloud Security Alliance (CSA) , which defines security domains congregating specific functional aspects, from governance and compliance to virtualization and identity management. Both documents present a plethora of security concerns, best practices

and recommendations regarding all types of services in NIST's SPI model, as well as possible problems related to cloud computing, encompassing from data privacy to infrastructural configuration.

The main goal of this paper is to identify, classify, organize and quantify the main security concerns and solutions associated to cloud computing, helping in the task of pinpointing the concerns that remain unanswered. Aiming to organize this information into a useful tool for classifying already identified concerns and solutions for cloud computing security. Focus is made to specific cloud computing, without losing sight of important issues that also exist in other distributed systems. This paper provides an enhanced review of the cloud computing security concern and solution to it.

II.CLOUD COMPUTING SECURITY

Key references such as CSA's security guidance and top threats analysis ENISA's security assessment and the cloud computing definitions from NIST highlight different security issues related to cloud computing that require further studies for being appropriately handled and, consequently, for enhancing technology acceptance and adoption Aiming to concentrate and organize information related to cloud security and to facilitate future studies, in this section we identify the main problems in the area and group them into a model composed of seven categories, based on the aforementioned references . Namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues[1]. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references:

1. **Network security**: Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solution is to have cloud services as an extension of customers' existing internal networks adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process .

(a) Transfer security: Distributed architectures, massive resource sharing and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing,

spoofing, man-in-the-middle and side-channel attacks.

(b) Firewalling: Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders . They also enable VM isolation, fine-grained filtering for addresses and ports, prevention of Denial-of Service (DoS) and detection of external security assessment procedures. Efforts for developing consistent firewall and similar security measures specific for cloud environments reveal the urge for adapting existing solutions for this new computing paradigm.

(c) Security configuration: Configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency .

2. **Interfaces:** Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.

(a) API: Programming interfaces (essential to IaaS and PaaS) for accessing virtualized resources and systems must be protected in order to prevent malicious use

(b) Administrative interface: Enables remote control of resources in an IaaS (VM management), development for PaaS (coding, deploying, testing) and application tools for SaaS (user access control, configurations).

(c) User interface: End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment.

(d) Authentication: Mechanisms required to enable access to the cloud . Most services rely on regular accounts consequently being susceptible to a plethora of attacks whose consequences are boosted by multi-tenancy and resource sharing.

3. **Data security**: Protection of data in terms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution requiring basic security levels) .

(a) Cryptography: Most employed practice to secure sensitive data , thoroughly required by industry, state and federal regulations .

(b) Redundancy: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes and, thus, mission-critical data integrity and availability must be ensured.

(c) Disposal: Elementary data disposal techniques are insufficient and commonly referred as deletion .In the cloud, the complete destruction of data, including log

references and hidden backup registries, is an important requirement .

4. **Virtualization:** Isolation between VMs, hypervisor vulnerabilities and other problems associated to the use of virtualization technologies . (a) Isolation: Although logically isolated, all VMs share the same hardware and consequently the same resources, allowing malicious entities to exploit data leaks and cross-VM attacks[3] . The concept of isolation can also be applied to more fine-grained assets, such as computational resources, storage and memory.

(b) Hypervisor vulnerabilities: The hypervisor is the main software component of virtualization. Even though there are known security vulnerabilities for hypervisors, solutions are still scarce and often proprietary, demanding further studies to harden these security aspects.

(c) Data leakage: Exploit hypervisor vulnerabilities and lack of isolation controls in order to leak data from virtualized infrastructures, obtaining sensitive customer data and affecting confidentiality and integrity.

(d) VM identification: Lack of controls for identifying virtual machines that are being used for executing a specific process or for storing files.

(e) Cross-VM attacks: Includes attempts to estimate provider traffic rates in order to steal cryptographic keys and increase chances of VM placement attacks. One example consists in overlapping memory and storage regions initially dedicated to a single virtual machine, which also enables other isolation-related attacks.

5. **Governance:** Issues related to (losing) administrative and security controls in cloud computing solutions,.

(a) Data control: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.

(b) Security control: Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps.

(c) Lock-in: User potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats), consequently becoming particularly vulnerable to migrations and service termination.

6. **Compliance:** Includes requirements related to service availability and audit capabilities .

(a) Service Level Agreements (SLA): Mechanisms to ensure the required service availability and the basic security procedures to be adopted .

(b) Loss of service: Service outages are not exclusive to cloud environments but are more serious in this context due to the interconnections between services (e.g., a SaaS using virtualized infrastructures provided by an IaaS), as shown in many examples . This leads to the need of strong disaster recovery policies and provider recommendations to implement customer-side redundancy if applicable.

(c) Audit: Allows security and availability assessments to be performed by customers, providers and third-party participants. Transparent and efficient methodologies are necessary for continuously analyzing service conditions and are usually required by contracts or legal regulations. There are solutions being developed to address this problem by offering a transparent API for automated auditing and other useful functionalities .

(d) Service conformity: Related to howcontractual obligations and overall service requirements are respected and offered based on the SLAs predefined and basic service and customer needs.

7. **Legal issues:** Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

(a) Data location: Customer data held in multiple jurisdictions depending on geographic location are affected, directly or indirectly, by subpoena law-enforcement measures.

(b) E-discovery: As a result of a law-enforcement measures, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware . Data disclosure is critical in this case.

(c) Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information.

.

(d) Legislation: Juridical concerns related to new concepts introduced by cloud computing.

III.SECURITY CONCERNS

The results obtained for the number of citations on security issues is shown in Fig:1 The three major problems identified in these references are legal issues, compliance and loss of control over data. These legal- and governance related concerns are followed by

the first technical issue, isolation, with 7% of citations. The least cited problems are related to security configuration concerns, loss of service (albeit this is also related to compliance, which is a major problem), firewalling and interfaces. Grouping the concerns using the categories presented in section "Cloud computing security" leads to the construction of Fig:2. This figure shows that legal and governance issues represent a clear majority with 73% of concern citations, showing a deep consideration of legal issues such as data location and e-discovery, or governance ones like loss of control over security and data. The technical issue more intensively evaluated (12%) is virtualization, followed by data security, interfaces and network security.

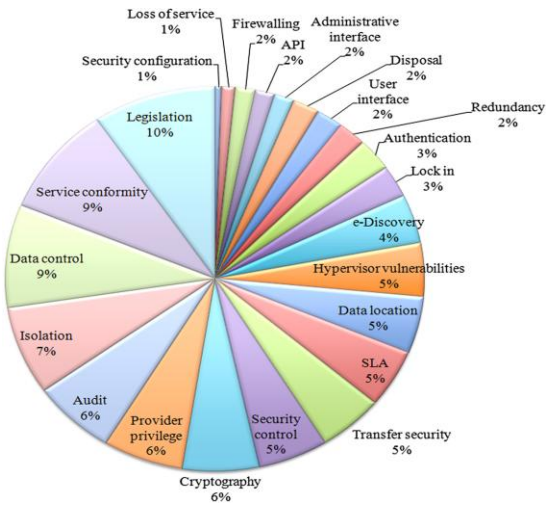

Fig:1 **Security problems.** Pie chart for security concerns.

Virtualization is one of the main novelties employed by cloud computing in terms of technologies employed, considering virtual infrastructures, scalability and resource sharing, and its related problems represent the first major technical concern.

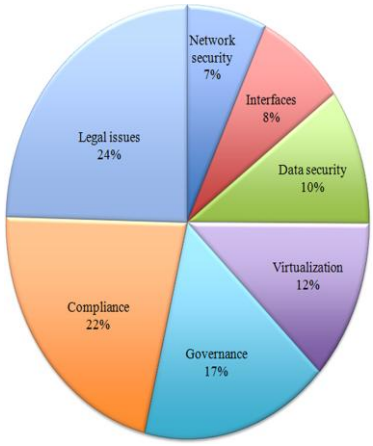

Fig: 2 Security problems with grouped categories.

IV.SECURITY SOLUTIONS

When analyzing citations for solutions, we used the same approach described in the beginning of this section. The results are presented in Fig:3, which shows the percentage of solutions in each category defined in section "Cloud computing security", and also in Fig:4, which highlights the contribution of each individual sub-category. When we compare Fig: 2 and 3, it is easy to observe that the number of citations covering security problems related to legal issues, compliance and governance is high (respectively 24%, 22%, and 17%);

however, the same also happens when we consider the number of references proposing solutions for those issues (which represent respectively 29%, 27%, and 14% of the total number of citations). In other words, these concerns are higly relevant but a large number solutions are already available for tackling them. The situation is completely different when we analyze technical aspects such as virtualization, isolation and data leakage.

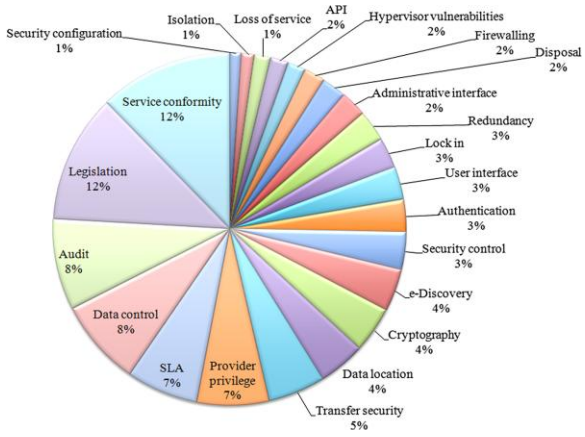

Fig: 3 Security solutions with grouped categories.

Indeed, virtualization amounts for 12% of problem references and only 3% for solutions. Isolation is a perfect example of such discrepancy as the number of citations for such problems represents 7% in Fig:1, while solutions correspond to only 1% of the graph from Fig:4. We note that, for this specific issue, special care has been taken when assessing the most popular virtual machine solution providers (e.g., XEN, VMWARE, and KVM) aiming to verify their concerns and available solutions.A conclusion that can be drawn from this situation is that such concerns are also significant but yet little is available in terms of solutions. This indicates the need of evaluating potential areas still to be developed in order to provide better security conditions when migrating data and processes in the cloud.

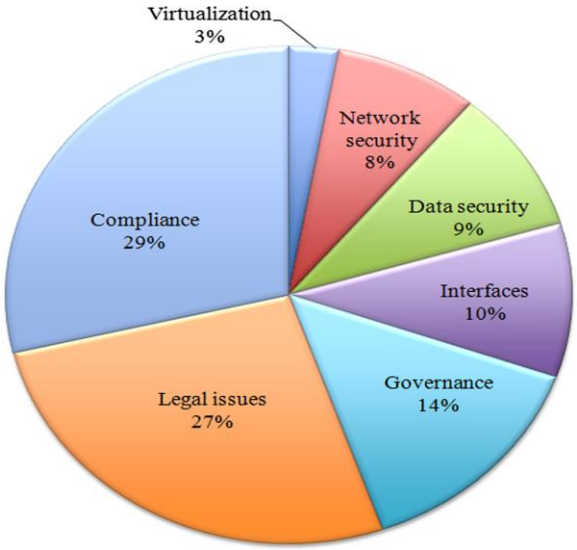

Fig: 4 Security solutions

V.SECURITY FRAMEWORKS

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 ENISA, CSA, NIST, CPNI (Centre for the Protection of National Infrastructure from UK government) and ISACA (the Information Systems Audit and Control Association).In this paper two entities are discussed.

ENISA

ENISA is an agency responsible for achieving high and effective level of network and information security within the European Union[6] . In cloud computing, they published an extensive study covering benefits and risks related to its use . In this study, the security risks are divided in four categories:

• Policy and organizational: issues related to governance, compliance and reputation;

• 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.

• Legal: risks regarding jurisdictions, subpoena and e-discovery. 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.

CSA

CSA is an organization led by a coalition of industry practitioners, corporations, associations and other stakeholders [7], 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. 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 different organizations or with different objectives.

VI.CONCLUSION

Conclusion can be drawn that cloud security includes old and well-known issues – such as network and other infrastructural vulnerabilities, user access, authentication and privacy – and also novel concerns derived from new technologies adopted to offer the adequate resources (mainly virtualized ones), services and auxiliary tools.

These problems are summarized by isolation and hypervisor vulnerabilities (the main technical concerns according to the studies and graphics presented), data location and e discovery (legal aspects), and loss of governance over data, security and even decision making (in which the cloud must be strategically and financially considered as a decisive factor). Finally, the analysis of current trends for cloud computing reveals that there is a considerable number of well studied security concerns, for which plenty solutions and best practices have been developed, such as those related to legal and administrative concerns.

REFERENCES

[1]. IDC (2009) Cloud Computing 2010 – An IDC Update.slideshare.net/JorFigOr/cloud computing-2010-an-idc-update

[2]I.brahim AS, Hamlyn-Harris J, Grundy J (2010) Emerging Security.Challenges of Cloud Virtual Infrastructure. In: Proceedings of APSEC 2010 Cloud Workshop, APSEC ’10.

[3]. TrendMicro (2010) Cloud Computing Security - Making Virtual Machines Cloud-Ready. Trend Micro White Paper.

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

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

[6].ENISA (2011) About ENISA. http://www.enisa.europa.eu/about-enisa.

[7]. CSA (2011) About. https://cloudsecurityalliance.org/about/

[8]. CSA (2011) CSA TCI ReferenceArchitecture.https://cloudsecurityalliance.org/wp-content/uploads/2011/11/TCI-Reference-Architecture-1.1.pdf