O 28. CLOUD COMPUTING MANAGEMENT AND NETWORK SECURITY. CASE STUDY, E-ALBANIA PORTAL

Valma Prifti*[1]

[1]*Department of Production and Management, Faculty of Mechanical Engineering, Polytechnic University of Tirana, Tirana, Albania*

E-mail: *vprifti@fim.edu.al*

ABSTRACT: This paper studies the security of applications in Cloud Computing, and belongs to the discipline of information systems, governance of information systems. As a case study in Albania, it was analysed the cloud computer used in the e-Albania portal. Cloud Computing is today a trend in the information and communication technology (ICT) industry, for which there is a growing interest both in technology and economics. Cloud computing has found wide use in various fields, from individuals to governments or large enterprises. The facilities that this use brings are numerous, ranging from easy access of data by customers to monitoring of every transaction by those responsible. The paper presents and analyses the basic concepts of Cloud computing, construction and use of the Albanian e-Government Cloud, its development model and service. The paper addresses the threats in the cloud, especially network security. It elaborates on the security problem by taking the source of the problem and also the possible solution. It addresses the privacy, data protection and identity management. The paper talks about the e-Albania portal, where it is based to guarantee security in the networks it uses. It presents the strategies taken by the Albanian government to encrypt and code data on networks. The paper analyses any security risks in order to be able to suggest an efficient and economical solution for network security.

Keywords: *Cloud Computing, Network Management, Cloud Security, Government Cloud, Cloud Usage, Cloud Framework, Computer Networking*

INTRODUCTION

Cloud Computing is today a trend in the information and communication technology (ICT) industry, and there is a growing interest in technology and economics.

A cloud infrastructure can be built according to several development models: Public Cloud, Private Cloud, Community Cloud, or Hybrid Cloud [1] The differences between these models are based on how resources are provided to the customer of Cloud services. A Public Cloud is a model in which resource utilization and infrastructure are generally enabled by a public network. A private Cloud is owned by an organization, which sells services and serves a diverse number of clients.

Cloud computing is a platform by which are shared the resources and data used among various enterprises, but there is always a security threat. An important aspect of cloud computing is security. Cloud service providers have the responsibility for providing security as one aspects of quality of service. Many challenges related with security in Cloud computing have not been addressed well yet. [2]

Pecchia et al. 2020, stated that "security alerts collected under real workload conditions represent a goldmine of information to protect integrity and confidentiality of a production Cloud". Their paper investigated the use of different text weighting schemes to filter an average volume of many alerts produced in a day by a security information and event management tool in a production SaaS Cloud.

The data shared and accessed through many devices from the cloud are not safe. They are likely to have various attacks like Identity Access Management, by internal or external intruders, hijacking a service. Ethelbert et al. 2020 stated that "a major role to secure the data within the cloud environment is done from the cryptography". The mandatory element is to protect the data stored in the cloud by using standard encryption and decryption mechanisms. Every cloud provider has its own security mechanisms to protect the key. The client cannot trust the service provider completely in spite of the fact that, at any instant, the provider has full access to both data and key. In their paper, they defined a new system which can prevent the exposure of the key as well as a framework for sharing a file that will ensure security using asymmetric key and distributing it within the cloud environment using a trusted third party.

Rathore and Chouradage, 2017 have defined that "compromise in terms of security is one of the flaws that proves to be a big threat for the user". In the paper they explained cloud computing and its threats faced by the users and introduce the existing systems which have been previously deployed to rectify the mentioned problems. They tried to rectify this flaw by proposing a system which provided both encryption and also an access control system for the users.

Liu et al. 2015 have proposed a two-factor data security protection mechanism with factor revocability for cloud storage system. Their system allowed a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needed to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needed to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the ciphertext without either piece. Once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext. The cloud server cannot decrypt any ciphertext at any time. It will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device. This process is completely transparent to the sender. Security and efficiency analysis show that their system was secure and also practical. [3]

MATERIAL AND METHOD

In the architecture of Cloud computing, five main actors are identified: the customer of cloud services, the cloud service provider, the carrier of services in the cloud, the cloud services auditor and the cloud services broker. Each actor is an entity in the Cloud and can be a person or an organization that participates in a transaction or process and performs certain tasks.

Cloud Consumer is a person or organization that maintains a business relationship with, and uses service from, Cloud Providers. Cloud Provider is a person, organization, or entity responsible for making a service available to interested parties. Cloud Auditor is party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

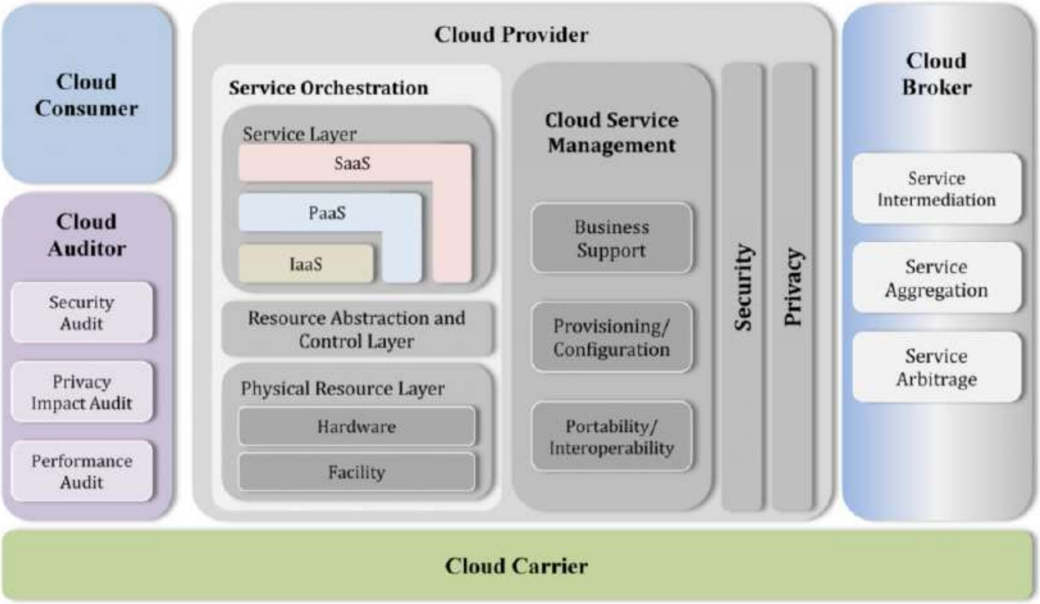

Figure 6. Cloud computing conceptual model (Source NIST,2020)

Cloud Broker is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers. Cloud Carrier is an intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Security Threats in the Computer Cloud System

We highlight in this section the main security risks which can be classified into three categories. Each of these types of attacks is examined in more detail below:
- Security threats originating from the host (hypervisor).
- Security threats originating from VM, Virtual Machines.
- Security threats coming from the client and the data center.

Security problems faced by businesses and governments

Businesses and governments are shifting more and more workloads into the cloud. However, some organizations remain resistant to significant cloud pulls due to prolonged concerns about data security in Cloud Computing.
The main security risks of cloud services are:
-Compliance violations
-Identity theft
-Malware infections and data breaches
-Decreased consumer confidence and potential loss of revenue

A good cloud security provider will provide a scalable solution that detects threats before they reach the data center, helping to alleviate the following security concerns:
-Data loss
-Malware infections
-Legal / compliance issues

Security issues in service models

Security is based on a wide range of policies and technologies, which are used to protect the data, applications and various infrastructures of Cloud Computing. Security risks are shared between Cloud providers and customers in the Cloud, based on Cloud delivery and service model. [4] The most security risks in the Cloud are related to weak policies, integrity, data control, privacy, availability of respective services and data, physical network security, encryption complexity, logistics security, and physical security. Each service model has its own specific problems regarding security. [5]

Table 4. Security issues according to the service model

Service Model	Service provider	Customer of the service
IaaS	-Virtual instances in IaaS often do not have continuous storage methods (incoming data must be stored in the long-term storage location) and volatile (volatile) data can be lost. -Providers in many cases do not want to provide final disk images because they may infringe on privacy rights. Problems may arise with the unclear situation regarding how the provider manages the termination of clients' contracts. Clients find it impossible to verify whether sensitive data stored on virtual machines has been deleted or not.	-IaaS instances provide more information for analyzing various attacks or incidents occurring in the Computer Cloud. -RFC 3227 contains some practices of good applicable to the IaaS in the event of security incidents.
PaaS	- Some cloud service providers offer the ability to collect and store a variety of incident diagnostic data.	-The main applications are under the control of consumers. -Customers do not have direct control over the execution environment

		-Login and encryption mechanisms can be applied.
SaaS	-Logging tools must be executed on the service provider infrastructure -Providers may not give access to clients' IP logs that access content or metadata of all devices	- The client does not have an in-depth view of the system and infrastructure that enables the service. - SSO (Single sign-on) checks must be requested -The client should contribute to the process of identifying past incidents by implementing rules to enable data retrieval.

Disadvantages of cloud computing

Despite the huge benefits that come from using of Cloud Computing, the downsides and disadvantages that come with centralization and distributed resources are growing so much that the benefits gained from these platforms can be overstated. Data in the Cloud are not under the control and management of the institution that owns them, and this fact carries in itself risks and threats which may pose a risk to the security of the system and data of the organization. [6] Risk identification and analysis is important to prioritize the implementation of governance and data control implementation, as well as to deploy an auditor or controller of the virtualized and cloud environment. Based on the identification and analysis of risks, appropriate controls should be built and implemented to ensure that the necessary measures are taken to address the risks and achieve the IT objectives.

Safety represents the measures taken to avoid the impact that the occurrence of an incident has as a result of vulnerabilities associated with Computer Cloud. The latter can cause damage to the system or organization. The cloud is evolving and the risks associated with its use are not fully understood. Effective security management is essential to establish a balance between benefits and risk reduction.

RESEARCH AND FINDINGS

In public administration, it is necessary to use new technologies which can lead to a reduction in costs. Some of the more developed countries view Cloud computing as a partial or complete solution to existing problems, where CC allows it to focus its resources where it is most needed, enables better organization of government structures and allows easier and faster exchange of information between different government organizations.

Use of Computer Cloud in Albania

If before most of the applications in the Albanian government and programs were executed by software loaded on physical machines or servers in the same building, now Computer Cloud allows access to the same applications through the Internet. Many businesses and governments, including the Albanian government, are moving their services to the Cloud. This comes as a result of the positive effects that Cloud has in improving efficiency, helping to reduce costs, good use of resources, etc.

The following are some of the most important reasons that the paper found from the research of the transition of Albanian e-government services to Cloud Computing platforms.

1. Cost savings. One of the main benefits of moving to the Cloud is the reduction of financial costs.
2. Speed of adaptation. Cloud is designed to provide services with unlimited scalability, which is considered as one of its main features.
3. Ease of use. Cloud computing is also easy to use. All employees of an institution or organization can access data in the Cloud very easily, wherever there is an Internet connection.
4. Increasing storage capacity. The cloud offers unlimited storage capacity compared to typical hard drives or server limits.
5. Flexibility and scalability. Cloud based services are very suitable for institutions or organizations and their increasing bandwidth requirements. Through the use of the Cloud, scaling up or down capacity is much easier than before and institutions can always pay depending on the capacity they use. [7]

6. Facilitate the work of IT staff. The IT departments of the respective institutions will spend less time on maintenance and will be freer to focus on strategic initiatives, which would increase the performance of the respective institution.
7. Recovery from injuries. The backup and recovery solutions provided by the use of the Cloud enable time savings as well as eliminate the need for large investments made by government institutions for error recovery.
8. Security. Since our data is stored in the Cloud, any institution can access it, regardless of any type of accident that may occur. It also offers the ability to delete all data from lost laptops so that they do not fall into the wrong hands.
9. Auditing and Logging. The audit process as well as the security audit should be performed periodically to ensure the security of the system. The cloud can help analyze large volumes of data and detect fraud. This data analysis would help build protection and security enhancement mechanisms, thus making applications more accessible and reliable. [8]
10. Environmentally friendly. The environment also benefits from the movement on the platforms in the Cloud. The use of hardware resources makes it possible to use only the necessary energy, ensuring a smaller impact on the environment.
11. Reporting and intelligence. Data submission makes many reporting services provided by the government more transparent. Applications can get a large amount of reliable real-time data, which helps in making decisions about providing the best services.
12. Policy management. Cloud architecture helps implement policies in data centers. Security-related policies can be designed and implemented in the data center.

Cloud Infrastructure in Albania

The Albanian government is focused and investing in a data digitization program, which includes the process of digital data transfer, indexing, integration into ICT systems, and interoperability. [9]
Some of the concrete and most important steps in building digital infrastructure are 3:
• Back-end systems (`basic registers´) in the IT departments of organizations, where the main applications are executed, which provide services and where the data are stored (civil registry data, property register data, addresses, asset information, pension data, etc.);
• The central component is the connecting layer for each civic service application. Further, it serves as a layer of interaction for any data exchange between government institutions.
Its basic components are:
• Government Portal (GG - which is primarily an Enterprise Service Bus application)
• Department Integration Servers (DIS), which is a connecting component located in the back-end institution building. Enables mediation / interpreter between GG and back-end institution.
• Payment Gateway to provide payment services for citizens who use services published through the e-Albania portal.
• e-Albania portal. Currently services for citizens / businesses (Front Office) are exposed through a public portal called e-Albania. The portal enables the exposure of electronic services published through GG to the user interface. This means: citizens are using 'network services' in a self-serving way.

Enforcing security in the Albanian e-government cloud and the risks imposed

Private Cloud in Albania offers dedicated services and a dedicated (single-tenant) operating environment, with all the benefits and functionality of resilience and a support model suitable for many public institutions. This is the most convenient way for applications that require full control and configuration of infrastructure and security. The main reasons why the combination of public and private cloud was chosen in Albania are:
1. The hybrid cloud enables the creation of a cloud covering the entire building, which is used in conjunction with the public cloud (Microsoft solution in this case) to reduce maintenance costs;
2. Hybrid cloud enables greater security of data and processes.

This mix of Cloud models has brought several advantages:
• Infrastructure in the data storage center;

• Elimination of delays due to internet traffic; each user in the perspective of the public body benefits from access to the data center infrastructure using a VPN;
• Faster processing time as some data is processed locally.

The hybrid model used may provide effective management of distributed resources, but it risks becoming complex due to security issues that may arise. It also carries problems with logging data logging and actions taken to obtain logs / logs in a single location in a common format. On the Government Cloud platform in Albania, Hyper-V servers are exposed to malware and viruses just like any other operating system and therefore adequate protection must be provided. The potential complexity of this model underscores the need to use virtualization tools to develop, maintain, and audit the translation of rules and rights into access controls. [56]

Some concrete examples to be addressed in the full protection of the Government Cloud are listed as follows:

o Anti-virus, anti-spyware for HTTP;
o Anti-phishing;
o Firewall and firewall application should detect VoIP and p2p applications;
o Incident reporting;
o An Antivirus service for HTTP, HTTPS 2.3.1 and FTP applications;
o Antivirus that enables the blocking of Viruses, spyware, Trojans, scams, worms, etc .;
o Advanced firewall functionality;
o Services blocking should be possible for protocols such as: http, ftp, smtp, pop3, p2p, etc .;
o Protocol-based blocking or application should be specifically possible: p2p, instant messaging, chat, etc .;
o All actions should be listed in logs, according to a well-defined configuration;
o Domain Keys (DKIM): use of Public / Private pair keys in order to be controlled against those published in the DNS;
o Tar pitting: a technique consisting of inserting a delay when negotiating an SMTP connection so that the email server or SMTP Gateway is protected from connections initiated by systems that send spam automatically;
o Antiphising Services;
o Bandwidth Management must be provided. This functionality should allow administrators to restrict traffic to IP addresses or an institution which is managed and provisioned independently.

CONCLUSIONS AND DISCUSSION

The portal enables the exposure. Security is one of the major issues on New platforms worldwide. The portal enables the exposure. Security problems can be of different types such as: security of resources, unauthorized access, data loss, potential malware, etc. The Albanian e-government cloud with the use of the Hybrid Cloud model, may encounter many problems in terms of security. It is imperative to enable proper security controls in the Government Cloud environment based on a predefined security model or architecture. In order to enable proper security controls in government cloud, the computing environment, security architecture / model, and regulatory framework must be interconnected between all actors and roles in cloud.

Citizens and businesses need to rely heavily on government-enabled cloud services, which must do all they can to ensure that service users data is properly stored.

Risk forecasting is one of the most important points in cloud computing platforms both in its use and in the governance framework. Risks are closely related to the new service model.

The service level agreement is one of the key elements of using Cloud Computing whatever the service model it offers. SLA carefully address the use, monitoring, obligations and responsibilities between the parties in consuming or providing services.

Some of the key recommendations of the paper are related to the drafting of strategic documents by the Albanian state regarding the security of the Cloud. Development of SLA models, which defines the relationship between all New actors. Draft a framework document for the governance of the Government Cloud, which addresses issues of risks and controls.

What is of great interest is the fact that cloud computing platforms are finding such widespread use and are becoming increasingly essential to the future of human society.

REFERENCES

[1] Liu, F., Tong, J., Bohn. R., Messina, J., Badger, L. and Leaf, D., 2011, NIST Cloud Computing Reference Architecture, *IEEE World Congress on Services. IEEE Computer Society*, Washington, DC, USA.

[2] Ethelbert, O., Moghaddam, F. F., WIeder, P. and Yahyapour, R., 2017, A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications, *IEEE 5th International Conference on Future Internet of Things on Cloud (FiCloud)*.

[3] Liu, J. K., Liang, K., Susilo, W., Liu, J. and Xiang, Y., 2016, Two-Factor Data Security Protection Mechanism for Cloud Storage System, *IEEE Transactions on Computers*, vol. 65, no. 6.

[4] Tran, H. V., 2017, Data Managment Challenges in Cloud Computing, *13th International Conference on Computational Science and its Applications*.

[5] Anonim, 2021, Implementing the Cloud Security Principles, *National Cyber Security Centre* (a part of GCHQ), [Online]. Available: https://www.ncsc.gov.uk/ . UK.

[6] Hogan, M., Liu, F., Sokol, A. and Tong, J., 2011, NIST Cloud Computing Standards Roadmap, *NIST Special Publication*, 500-291.

[7] (Haeberlen, T., Liveri, D. and Lakka, M., 2015, Good Practice Guide for securely deploying Governmental Clouds.

[8] Aymerich, F., 2009, A real time financial system based on grid and cloud computing, *ACM symposioum on Applied Computing*, Honolulu, Hawaii, USA.

[9] AKSHI., 2021, Technical Proposal on the Improvements of the e-Albania Government Portal.

[10] Sabahi, F., 2012, Secure Virtualization for Cloud Environment Using Hpervisor-based Technology, *International Journal of Machine Learning and Computng*, vol. 2.

[11] Hashemi, S., Monfaredi, K. and Masdari, M., 2013, Using Cloud Computing for E-Government: Challenges and Benefits, *International Journal of Computer and Information Engineering*, vol. 7, no. 9.

[12] Pathare, K. G. and Chouragade, P. M., 2017, Reliable Data Sharing Using Revocable-Storage Identity-Based Encryption in Cloud Storage*, International Conference on Recent Trends in Electrical, Electronics and Computing Technologies, IRTEECT*.

[13] Anonim, 2020, Good Practice Guide for Securely deploying Governmental Clouds, *Europian Union Agency for Network and Information Security, ENISA*, 5-10.

[14] Sharma, D. H., Dhote, C. A. and Potey, M. M., 2013, Security as a service from Clouds: A comprehensive analysis, *International Journal of Computers and Applications*, 67(3), 15-18.

[15] Yang, K. and Jia, X., 2014, Expressive, efficient and revocable data access control for multi-authority cloud storage, *Parallel and distributed systems, IEEE Transactions*, 25(7), 1735-1744.