Security and privacy in cloud computing

Alma Hyra, Grigorina Boce

Abstract- Security and privacy are key issues on the Cloud platform worldwide. Problem and possible protection of different types such as security of resources, unauthorized access, data loss, etc. This article offers an introduction to cloud computing by describing the main features of this technology including the essential technical characteristics. Furthermore, the intention is to identify security and privacy issues in cloud computing and at the same time present the current solutions on these challenges. The main concerns to address in this article are lack of data control, lack of access trust, illegal usage of data and undefined authorities and responsibilities.

Index Terms- Security, Privacy, security risks, Cloud service models, security requirements, SaaS, PaaS, IaaS.

1 Introduction

The age of technology is changing the world and we are witness of its effects. With the invention of the internet, the world became smaller in terms of communication and cooperation between people. Furthermore, the services over the internet that enabled this connected world required technical resources.

As data transfer volume, applications, social media, business and other online services increased vastly in recent years, the need for cloud computing services became nearly inevitable. Moreover, the cloud computing technology emerged since it provided possibilities to utilize various online services such as cloud hosting, cloud storage, cloud servers by use of shared computer resources such as hardware and software.

To define the term "Cloud computing", most of the research papers refer to the NIST (National Institute of Standards and Technology) definition. This definition is cited from the book (Siani Pearson, George Yee, 2013) as follows: *"Cloud computing is a model for enabling 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's interaction"*. According to NIST, cloud-computing model consist of five essential characteristics (On demand self-service, broad network access, resource pooling, rapid elasticity and measured service), three service models (Software SaaS, Platform PaaS and Infrastructure IaaS) and three deployment models (Private, Public and Hybrid).

Today, many organizations and industry companies are moving towards this technology due to benefits offered by cloud computing model such as quick positioning, measured services, scalability, accelerated delivery, adaptability, universal network access, prominent elasticity, low-cost catastrophic restoration, data storage solutions, fast reconstruction of services, etc.

In 2018 (Fig. 1), 26% of European enterprises purchased cloud computing services and incorporated cloud technologies to improve their operations while reducing costs; this was an increase of 25% on 2016.

18% of companies use medium-highly sophisticated services (i.e. hosting of the enterprise's database, accounting software applications, CRM software and computing power). The ratio for large enterprises is 39%, well above that of SMEs (17%).

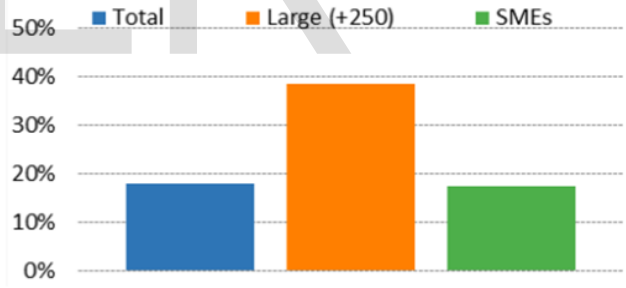

Fig. 1. Eurostat, Cloud computing services of medium-high sophistication (% of enterprises), 2018.

Beside many benefits, cloud computing also faces many challenges especially in privacy and security issues, which are the key elements of this article.

2 Privacy

In general, the term "privacy" defines the right of using your assets without being disturbed, observed, intercepted or interrupted. The users of cloud computing technology are concerned regarding their information and interactions in the cloud because they are aware of:

1. Who is behind that foreign and unknown online platform that has full control over their data?

2. Who manages their sensitive data?
3. What will happened with their stored data?
4. Does somebody else has access to his or her data?

On the other hand, cloud computing service providers are concerned on how to ensure the main principles such as confidentiality, availability, integrity, reliability and performance for their users. Furthermore, there exists many challenges and issues for cloud service providers in achieving these principles, notably in privacy and information control.

The main concerns to address in this article are lack of data control, lack of access trust, illegal usage of data and undefined authorities and responsibilities. Bellow, will define the main privacy challenges in the cloud computing arranged as follows according to article:

Protection of data – is a key concern in cloud computing, therefore many research are conducted that came up with the solution of using encryption techniques on stored data but also in transmission over the internet such as SSL encryption, but still protection must be enhanced.

Lack of user control – includes both legal issues and issues raised by users.

This means that users cannot always control their data on cloud because service providers host and manage their data, which sometimes raises the issue of data transparency and data exposure.

Illegal use of data - is another privacy concern for the users because the cloud service providers may sell user's data to third party companies without their approval. There must be defined the agreements between providers and users regarding unauthorized data usage.

Training of Employees – lack of trained staff could affect data management that usually leads to user's data privacy breach.

Legal protection – is another serious concern due to lack of uniformed legislation for cloud computing across different countries. Furthermore, data on cloud is not defined in terms of location hence data flow across borders can impose different privacy laws.

2.1 Data protection by means of encryption technique

Since data integrity and confidentiality are essential issues when deploying Cloud computing, modern systems use data encryption by allowing the sender to send an encrypted message to the recipient via a cloud storage server. The sender should not know any other information except the identity of the recipient (should not know the public key or the certificate of the recipient). The recipient must possess two things in order to be able to decrypt the text.

As a start, it is necessary his secret key stored on the computer. In addition to the secret key, he needs a unique personal security device which can be connected to the computer. It is impossible to decrypt the text without one of them.

Moreover, the moment a security device is lost, it is revoked and can no longer be used to decrypt any text.

This can be achieved through the Cloud server, which immediately executes an algorithm to change the existing encrypted text making it decrypted from the lost device. This process is completely transparent to the recipient.

The Cloud client generates an encryption key, through which data is encrypted and decrypted on the way to the Cloud provider.

1. Good encryption key management is required to ensure data privacy. For this reason, the following steps should be followed:
2. It should be determined whether the keys will be maintained by the Cloud customer or by trusted key management providers;
3. It must be determined whether the keys are stored in the Cloud;
4. Encryption keys should not be stored with encrypted data;
5. Encryption keys must be managed securely. Data encryption and the use of sophisticated encryption algorithms have the side effect of increasing CPU load on servers and users' computers. This load and processing delay becomes even more apparent in Big-Data situations. The solutions offered in such cases and the best options are those that encrypt the data before placing it in the Cloud and decrypting it after receiving it from it.

3 Security

The term, "security" means protection of your own assets. 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 Cloud customers, based on Cloud distribution and service model. Therefore, the same principle also applies to cloud computing privacy and security due to the possibilities of online data theft, violation, interception and alternation.

Even though security in cloud computing is more enhanced than privacy, there are some issues that need to be considered, as described below:

IJSER

Data breaches – data stored on the cloud may include financial statements, health information, trade secrets or personal information, therefore it is very attractive target for the hackers.

Network security – data needs to be secured not only at databases but also during transmission. It is required to use strong traffic encryption in order to secure network traffic.

Data access – data stored in the cloud must to be accessible from anywhere at any time from any system. There are some issues in the cloud regarding access from any device, such as information interruptions and different types of attacks occur in situations when there is weak client verification system

Multitenancy – cloud computing is a shared service with multiple users therefore they are not very isolated from each other. Furthermore, cloud service providers use virtualization to offer different services and separate users, which includes sharing virtual machines or allocating a virtual machine to a user. This means that one user might affect other users on the same service.

Deletion of data – data deletion may occur due to any attack or disaster so there is a need for backup. Cloud data destruction or loss can incur a permanent damage to the business.

Phishing – cloud computing suffers from phishing attacks as they target email platforms, websites and other services by inserting a malware on attached files which activates it by only a click, therefore the hackers can hijack user's accounts.

Data location – as cloud computing offers data mobility, the users usually keep their sensitive data in cloud, thus the data location must be a priority.

Attacks – the main attack that targets cloud-computing services include man-in-the-middle attack, wrapping attack, denial of service attack, malware injection attack, data stealing, side channel attack and authentication attack. It is crucial for cloud service providers to take measures in preventing and protecting from these attacks.

Malicious insiders – human mistake is evident and very often cause the loss or damage of data. Apart from human mistakes, there also exists malicious insiders who can damage, use or steal the data on purpose. An insider may be a present or previous employee, contractual employee, a company partner etc.

3.1 Security and service models in Cloud

In addition, (Fig. 2), to the common security issues related to Cloud in general, each service model has its own specific security issues.

In the IaaS model, the developer has greater control over security because applications run on virtual machines separate from each other but executed on the same physical machine. The only point to be careful in this model is the virtual machine operator who must own and provide a higher security. In the PaaS model, the provider can provide a certain level of control to the specialists who build applications on this platform. For example, developers can create their own data authentication or encryption systems. However, providers provide a security below the application level by making data inaccessible between applications.

In the SaaS model, the most problematic issues are the analysis and filtering of security alarms, loss of data control, data protection, and compliance with government regulations. Employees of the Cloud provider may accidentally or not lose important and confidential data about a company. In order to maintain confidentiality, Cloud clients must use encryption and sophisticated methods to manage access to SaaS services Encryption is an effective method of securing data before it is stored in the Cloud provider. However, encryption cannot be applied to services where data is to be used in computing. It is important that migration policies in the new SaaS model enable a well-defined security architecture for accessing SaaS services.

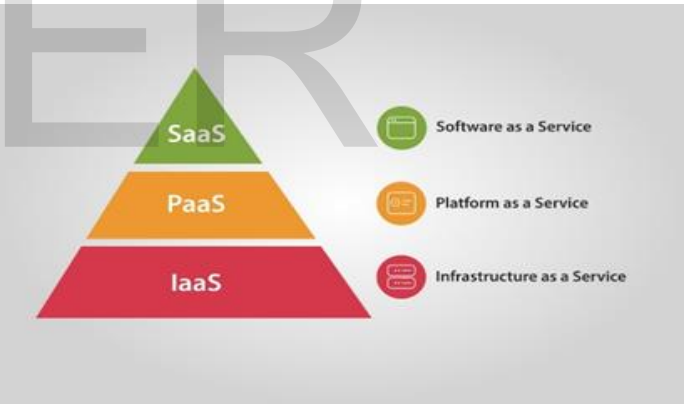

Fig. 2. Source, LISLINK, Startup laboratory.

In 2018, in the framework of the defense of a dissertation, a questionnaire was conducted through 22 representatives of Albanian government institutions, who use public and Cloud government services, as well as representatives of institutions which are trying to pass their applications and services in Government reindeer.

From the answers received (Fig1.eps), 82% of the institutions specified the time out of service as the biggest problem for security. Off-time time can lead to significant cost losses and impair important processes for the institution. Other major problems are identity theft (77%), denial of service attacks (73%), privacy (55%), etc.

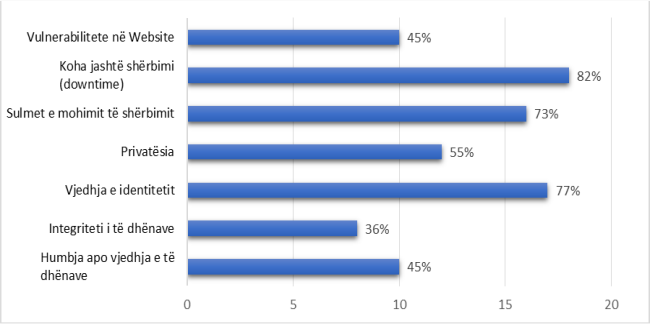

Fig.1.eps. Security problems.

Although they may have a security problem, according to INSTAT in 2020, cloud services (services used on the Internet to access software, storage capacity, etc.) are used by 18.2% of Albanian enterprises that have access to the Internet from 11.4% that resulted in 2019.

3.2 Identity Management in Cloud

Identity management enables the authorization of access only to persons with certain rights. To accomplish this, solutions like Single Sign On (SSO) must be implemented for existing users. In addition, identity management standards such as SAML, SPML, WS-Federation, etc. can be used as a way of authenticating and authorizing users.

Cloud applications in more sensitive areas such as in e-Government require more reliable and secure mechanisms. This gap for such cloud applications is solved by applying the STORK framework for secure cloud authentication using eIDs. The STORK framework supports various national eID solutions and will be the relevant eID framework across Europe in future.

Identity theft is considered one of the main security problems. Blocking access to unauthorized persons comes as a necessity to enable basic security criteria and to keep confidential data. Secure authentication options include electronic certificates, token use, biometric methods, etc., which maximize forceful interference with cloud systems. Compromise in terms of security is one of the weak points, which brings a great risk to the user. There are many systems that seek to fix this vulnerability, proposing a way that enables both encryption and access controls for users.

In addition to the protection methods, the appropriate password policies (such as minimum length, duration of use, history, complexity, etc.) as well as those for account protection (duration of blocking access after failed attempts) must be followed. Since most resource allocation is done through remote connections, unprotected API-s, the center of attacks are mainly management API-s and PaaS services.

Ways of attacks such as phishing, fraud and exploitation of software vulnerabilities continue to succeed. Credentials and passwords are often reused, increasing the impact of these attacks. But the solutions in Cloud add a new threat. If an attacker obtains credentials, he can view activities and transactions, manipulate data, return falsified information, and redirect customers to dangerous sites. The service instance can become a base for the attacker, from where he can use the user's reputation for further attacks. It is very important that the institutions that deal with the policies of Cloud and their implementation, take into account the above principles when transferring services to Cloud.

In this respect, some services in cloud meet the principles of security, while some others only a part of them.

3.3 Actors' responsibilities for security in Cloud

When applying for the use of cloud computing services, users usually have serious concerns about the lack of information or the way resources are managed by Cloud providers, e.g., location of sensitive data, lack of physical control of the data storage center, reliability of data backup, measures to be taken in case of damage, etc.

Also, Cloud users have concerns about exposing their data to foreign governments and their privacy laws. Different user roles, e.g., the Cloud service provider, the Cloud user and the IT administrator need to be defined, defined and used on its platform. Uncertainty in these roles and in defining the responsibilities of each role in relation to data ownership, access control, infrastructure maintenance, etc., can lead to legal or technical problems (especially when working with third parties).

Also, contractual uncertainties can lead to anomalies or incidents. Users of Cloud service usually consider the Cloud service provider as primarily responsible for security issues in Cloud, although each actor is responsible for specific security-related issues.

Among other things, the decision of a Cloud user to migrate part of its IT infrastructure to a Cloud infrastructure would result in the transfer of part of the data control to the service provider. This can pose a major threat to user data in terms of roles and privileges.

Along with the transparency associated with the Cloud provider's practices, a misconfiguration can occur which can trigger internal attacks. These weak points would damage the reputation of the provider and may result in a lower trust of the Cloud user.

The institutions surveyed in the above survey, which were considering switching their services to SaaS, face some technical challenges.

73% of institutions (Fig2.eps), rated 'Applications Security' as one of the main challenges, followed with difficulties of

integration with the existing system (68%) and system and network security.

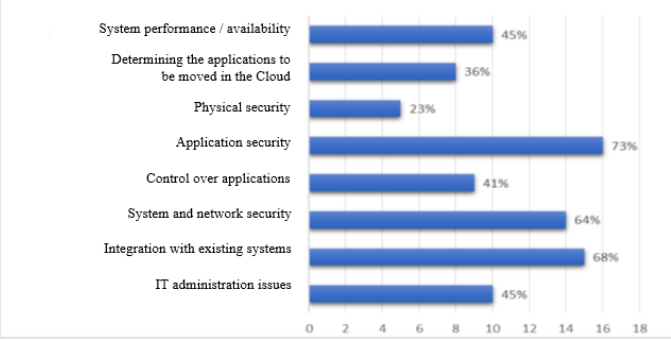

Fig.2.eps. Technical challenges of adaptation to Cloud environment.

From this survey (Fig3.eps), only 5% of the representatives of the institutions considered security as a responsibility of the user, 77% of the representatives of the institutions considered security as a responsibility of the Cloud service provider.

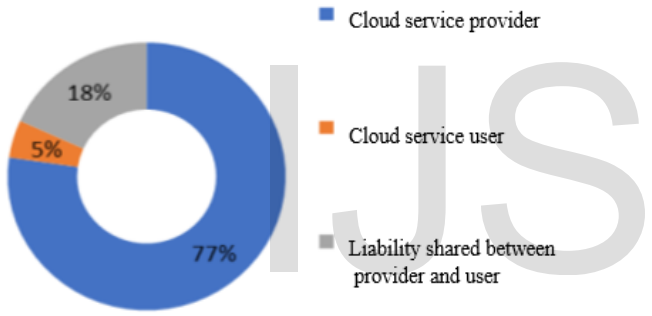

Fig.3.eps. Actors' responsibilities for security in Cloud

3.4 Threats associated with Cloud computing services

An important measure to be taken to secure the Cloud computing environments is proper encryption and key data management. Sensitive data is in transit over the network, increasing the risk of capture, hijacking, or loss, so it is very important to implement access control and data encryption systems, which are transferred between the parties. The best methods today, provide effective cryptographic schemes for controlling access to the cloud for data sharing. These systems provide temporary data encryption schemes, which are shared between parties based on the identity of the parties.

Also, it is quite important to determine the actor, who will control the encryption and decryption of the keys (customer or provider), and whether the encryption method used is appropriate. In Cloud environments, service providers have the privilege of accessing data, creating the risk of data loss or unauthorized access to the Cloud.

In Albania, the Authority of the Commissioner for the right to information and protection of personal data, suggests some of the rules that must be respected when using the Cloud computing service, so that the processing is in accordance with the rules for protection of personal data and guarantee security of personal data processed, as follows:

1. The Cloud client and the Cloud service provider enter into a written contract between themselves and each sub processor in case of delegation.
2. Transparency is essential for a fair and lawful processing of personal data.
3. The client determines the goals of the processing before the collection of data by the data subject and informs the latter
4. Personal data must be kept in a form which allows the identification of data subjects for no more than is necessary for the purpose for which the data were collected or for which they are further processed.
5. Defines the rights and obligations of the Cloud client.
6. Defines the rights and obligations of the Cloud service provider.
7. Audit. Given the possibility of collecting a large amount of personal data from the Cloud service provider, the latter should be subject to third party audits in addition to the audit performed by the Cloud client itself.

4 Summary of Solutions to security challenges and issues

Many security issues need to be considered in order to enhance cloud security. Presented below, there are summary of some solutions security challenges and issues mentioned in the article.

Encryption techniques: is a method that includes usage of cryptographic algorithms and techniques in order to establish secure transmission and storage of data in the cloud. This method also protects data processing and computation thus it is a great tool for privacy maintenance.

Identity and access management: usage of an identity management guidance that includes all main issues and recommendations such as access management, identity management, access control, user access certifications, identity and access reporting etc.

Intrusion management: include the method of pattern recognition for detecting unfamiliar and unpredicted events in order to react proportionally for preventing the intrusions.

Authentication and authorization management: used for detecting unauthorized access to cloud computing. In general, an authorized person must use a valid username and password

IJSER

to access the cloud services, including verification steps before using cloud services.

Digital signatures: used to identify the authenticity and integrity of the user. It is an asymmetric cryptographic technique.

5 Conclusion

Based on the literature review, it is depicted that cloud computing is an emerging technology that offers facility to share software and hardware resources over the internet. The advantages of this technology include lower IT infrastructure cost, increased computing power, unlimited storage capacity, easier group collaboration etc.

Beside advantages, it has also some disadvantages such as dependence on stable network connection bandwidth, no access of information in case of cloud data loss and the most important security and privacy of stored data. However, the issues that must be further enhanced include the innovation mostly on the side of cloud service providers.

Furthermore, specification of unauthorized service usage must be defined by agreements between users and cloud service providers. The other open issues that also need further research include uniformity of laws for stored data between countries and necessity of employees training at every level. As the demand for cloud computing is increasing, the security and privacy issues will be solved by the competition between cloud service providers.

IJSER

References

[1] Shankarwar M.U., Pawar A.V. (2015). *Security and Privacy in Cloud Computing:* A Survey. In: Satapathy S., Biswal B., Udgata S., Mandal J. (eds) *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)* 2014. Advances in Intelligent Systems and Computing, vol 328. Springer, Cham.

[2] Siani Pearson, George Yee. (2013). *Privacy and Security for Cloud Computing.* London: Springer.

[3] Singh, Harshpreet & Ahluwalia, Nisha. (2016). *Cloud Computing Security and Privacy Issues* – A Systematic Review. International Journal of Control Theory and Applications. 9. 4979-4992.

[4] Eesa Alsolam. (2018) *Security threats and legal issues related to Cloud based solutions.* International Journal of Computer Science and Network Security. VOL.18 No.5. pp. 156-163.

[5] Tabassam S. (2017). *Security and Privacy Issues in Cloud Computing Environment*. J Inform Tech Softw Eng 7: 216.

[6] R. Soni, S. Ambalkar and P. Bansal. (2016). *Security and privacy in cloud computing. Symposium on Colossal Data Analysis and Networking (CDAN*). Indore. pp. 1-6.

[7] G. Himanshu and K. Desire Afewou. (2017*). A trust model for security and privacy in cloud services.* 6th International Conference on Reliability Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). Noida. pp. 443-450.

[8] J. W. Rittinghouse and J. F. Ransome, "*Cloud Computing Implementation, Management, and Security*," 2010.

[9] B. Stanton, M. Theofanos and K. P. Joshi, "*Framework for Cloud Usability," National Institute of Standards and Technology*, 2015.

[10] M. Hogan, F. Liu, A. Sokol and J. Tong, "*NIST Cloud Computing Standards Roadmap," NIST Special Publication* 500-291, 2013.

[11] *World Economic Forum's IT Industry Partnership with Accenture, "Advancing Cloud Computing: What to Do Now?," World Economic Forum*, Geneva, Switzerland, 2011.

[12] K. McCabe, R. Nachbar, "*Survey by IEEE and Cloud Security Alliance details importance and urgency of cloud computing security standards,*" 2010.

[13] C. C. Rao, M. Leelarani and Y. R. Kumar, "*Cloud: Computing Services and Deployment Models," IJECS, vol. 2*, no. 12, pp. 3389-3392, 2013.

[14] B. Khasnabish, J. Chu, S. Ma, Y. Meng, N. So, P. Unbehagen, M. Hasan, "*Cloud Reference Framework*," 2010. http://alturl.com/6vhzs.

[15] P. Mell and T. Grance, "*The NIST Definition of Cloud Computing,*" Special Publication 800-145, 2011.

[16] 2012 IEEE 2nd *International Conference on Cloud Computing and Intelligence Systems*

[17] *Digital Economy and Society Index (DESI) 2020 Integration of digital technology*

[18] E. Kuka, "*Vlerësimi i përdorueshmërisë së aplikacioneve cloud computing"*, 2018

[19] INSTAT, "*Përdorimi i Teknologjisë së Informacionit dhe Komunikimit në Ndërmarrje"*, 2020, www.instat.gov.al

[20] IDP, "*Udhëzues për Cloud Computing"* https://www.idp.al/wp/content/uploads/2016/11/Udhezues_per_CLOUD_COMPUTING.pd

AUTHORS PROFILE:

MSc. Alma Hyra

Currently working as, a Lecturer in Mediterranean University of Albania, Faculty of Economic Sciences, Department of Informatics and Scientific Education.
Email: hyra.alma@gmail.com

IJSER

Msc. Grigorina Boce

Currently working as, a Lecturer in Mediterranean University of Albania, Faculty of Economic Sciences, Department of Informatics and Scientific Education.
Email: grigorinabo@gmail.com

IJSER