Privacy, Security and Trust Issues in Cloud Computing

Andrea Li

#Graduate Student& Departmentof Computer Science &Dartmouth
Hanover, NH,USA

Abstract

The use of technology has become an intrinsic part of our lives and most of the economic activities now takes place electronically. Emerging at a fast pace, new technologies allow businesses to be more innovative and competitive. Many of these new technologies foster collaboration, not without creating conflicting needs. Companies must ensure that they use technology safely while engaging more stakeholders to be more competitive. As the Cloud computing gaining popularity, it is also carrying some concerns to the implementors. This paper focuses on the topics such as issues in Cloud Computing, risks related to the privacy and how we can ensure the confidentiality of data.

Keywords — *Cloud, Cybersecurity, Issues, Trust Cloud, Privacy*

I. INTRODUCTION

For many years, security has been considered as a form of insurance, a reluctant purchase that many do not like to do. Security technology vendors often tell obscure stories and warn of the consequences if we do not buy specific solutions to solve problems. However, nurturing fear can paralyse innovation and make companies close hatches and take a reactive approach based on fear. The fear of security issues that is pushing some companies aside the opportunities offered by cloud computing [1] is a typical example. The collaboration and use of applications from external sources have led to the erosion of the perimeters of companies. While the proliferation of mobile devices in the economic environment makes these perimeters even more illusory than ever. Closing the hatches to protect as much as possible is no longer a solution. A new approach to security is needed, a strategy that migrates security in the network layer. For many companies, given the importance of the Internet for their business, the Net is the new network. Many of them are migrating their data, their applications or their security to the cloud. They begin to realize that, rather than being a security concern, the cloud can offer higher levels of security and is a trusted, reliable technology delivery mechanism which deploys hardened security controls within a trusted scope. In the cloud, granular access controls can be enforced, data encrypted to protect against unauthorized access during transport or storage, and higher levels of control depending on data criticality. Business continuity and disaster recovery are further guaranteed through cloud services, while mobile devices can be more easily managed to make employees productive wherever they are.

With the cloud's secure bubble, businesses can have confidence in the secure processing of their data, provided the service provider has the necessary security infrastructure. However, there are still security challenges that need to be resolved before trust is established. The biggest challenge is the security of the Internet itself. Web applications and websites have become the target of hackers and are the weak points of our digital world. We must put more effort into securing them and making them trustworthy. Services in the cloud offer a solution.

II. THE REAL ISSUES [2]

In the modern digital world, effective sharing of information between individuals and organizations has become a critical requirement. This increases the demand for data sharing and privacy. The presence of personal information (IPI) such as medical records, financial records and school records have been identified as a major barrier to data sharing. This limits the sharing of data for different purposes, such as academic or academic researchwhich are important to support various activities in society such as improving public health care and policy making. Sharing of data effectively and without any revelation of IPI is still a major challenge. Several approaches, such as anonymization and encryption, have emerged to solve this problem, but this is achieved with a significant loss of information. There is therefore a problem of sharing the micro data while protecting the data. The main challenge when disclosing information is to provide as much information as possible while ensuring the confidentiality of an individual. This means that limiting disclosure of shared [8] data requires careful consideration between data utility and individual privacy.

This research problem can be represented by asking the following main research questions:

- How can we ensure privacy in a cloud environment while reducing the loss of information?

- What approaches can be put in place to reduce the amount of information loss while striving to protect the privacy of the individual in a cloud environment?

- How to design, develop and implement anonymization approaches to improve data privacy and utility in a distributed environment and especially in a cloud mode?

III. WAYS TO ENSURE THE PRIVACY AND CONFIDENTIALITY OF DATA [3]

A. Trust is primary

Despite the significant advances that have occurred in recent years in the cloud industry, privacy and security of personal data are still among the barriers to adoption. Even if most companies use cloud technologies and consumers are increasingly adopting cloud-based products and services, it is still very difficult to know exactly if the data stored online is secure. In highly sensitive sectors such as health and finance, this uncertainty represents a major obstacle to the adoption and implementation of Cloud solutions.

Adherence to a set of standards may be insufficient in the face of the most advanced issues of confidentiality but will in fact stimulate longer-term adoption in the most vulnerable sectors would enjoy the benefits of the cloud.

B. Ensure confidentiality [4]

"You can have security and not have privacy, but you can never have privacywithout security." -Tim Mather.

Confidentiality ensures that customer data is accessible only by authorized entities. Different cloud computing solutions include privacy mechanisms such as identity and access management, encryption, and anonymization. The most secure access controls have no protection against an attacker gaining access to information, identification or keys. Thus, credentials or key management information are essential links in the design of security.[17]Majority of internal and external exchangers are encapsulated in SSL (Secure Sockets Layer) and authenticated with a certificate generated by the client. This certificate is not linked to any trusted root CA but rather self-signed by the client itself. If the latter controls his private key, the mechanism allows a high degree of assurance: only authorized clients with this key can access specific aspects of the service. Encryption is attractive in the first place, especially the traditional method where only the recipient of the information can decipher the data that is intended for him with his private key, known only to him, but not to the provider of the Cloud solution. This is a very secure method (depending on the size of the key) and selective because user can choose to encrypt only what requires it. However, the encryption imposes some reflections on its implementation, especially in the case where processing is necessary (calculation, indexing, backup), which can force the manipulation of decrypted data.Anonymization of the data is one of the techniques of confidentiality which result in the conservation of the information, which makes the data useless for everyone except the owners.

a) Life cycle of the data

Personal information of an individual, IPI must be managed within the framework of the data used by the organization. They must be managed from the moment the information is conceived until its final destruction. The cycle of data consists of generation, transfer, use, sharing, storage, archiving and destruction. Although this cycle is presented sequentially, the data can follow it in a non-sequential way. This approach can also be used in the case of a "classic" systemi.e “no cloud". In such a context the security controls will be different. The protection of personal information must consider the impact of the Cloud on each of the following phases as Figure 3.4 indicates:

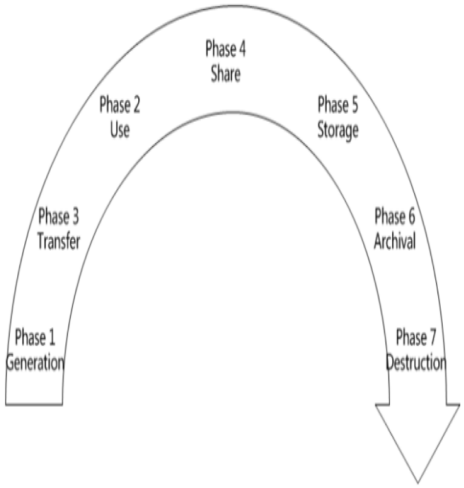

Figure 3.4The life cycle of a datum

[Chen and Zhao, 2012] [5]

b) Privacy risks in cloud

- Anonymous communications: A user may wish to send one or more messages to a given recipient, or hope to receive responses, [18]to his messages. Answers can arrive long after sending messages or almost immediately, and in some cases, responses can even be intertwined with requests. The difficulty to remain anonymous in each of these cases is growing, and unfortunately in the Cloud. Anonymous communication protocols are proposed to resolve this situation [Ardagna et al, 2010]. Specific solutions taking advantage of the peculiarities of cloud systems are also under study [Jones et al, 2011].
- Collaborative execution of requests:In the distribution of information and the cooperation of

the calculation of query results, the confidentiality of sensitive information must be taken into consideration. The need for one party to publish information and to cooperate with another can characterize several scenarios: ranging from traditional distributed database systems (where centralized database administration is distributed) to cloud systems (where the different cloud servers collaborate and integrate their data and services to provide users with applications available anywhere and anytime.) This situation calls for innovative solutions that support the selective sharing of information stored on multiple cloud servers.even beyond the boundaries of administrative and business [Benedikt et al, 2012] [Li, 2003].

c) ***Privacy risks for user -***

They focus on the issues of protecting the identities of users who have access to resources in the cloud. It allows users to interact with cloud servers and distribute their information without disclosing their identities. Traditional approaches to resource access are based on user authentication.

d) Privacy risks for stored data -

Since the data is stored in cloud servers (which are not under the control of the data owner) confidentiality can be an issue. In addition, access to the data must be regular (different parties may have different access privileges).

- Privacy and integrity:The problem of confidentiality preservation is addressed in DaaS (Database as a Service) scenario, the solution proposed by [Samarati et al, 2010] consists in encrypting the data before it is stored in the server. Sometimes the data is not sensitive, but what is sensitive is their associations with other information. So, the encryption seems like an "OverKill" (Ex: The list of names of patients and the list of diseases treated in a hospital can be made public while the association of the name of each patient to a specific disease must be protected).
- Selective access:In a Cloud scenario, neither the owner of the data nor the server that can apply the access control policy [11]. The server can not directly apply access control restrictions because it is not confident to apply them, and because the policy regulating access to data may depend on the content of the data (which must always be kept confidential by the server). [13] The owner needs to filter for each access request, which forfeits the benefits of the cloud. So, it is necessary to design a mechanism such that the data themselves apply restrictions on the set of users who can access them.

IV. LEGAL RESPONSIBILITY FOR DATA SECURITY AND PRIVACY IN THE CLOUD [6]

The Customer is legally responsible for its data and usage, including all that relates to their compliance with legal obligations. The provider is subject to technical and organizational obligations. [14] It undertakes to preserve the integrity and confidentiality of the data, by preventing any fraudulent access or use and by preventing any loss, alteration or destruction. His legal responsibility may be incurred if he transfers his client's data without warning him and without ensuring that the necessary declarations have been made.

In general, the more the infrastructure is outsourced to the cloud provider, [15] the greater the responsibility. In the case of PaaS and SaaS, the customer only controls the content of his data (and still partially in SaaS where the responsibility is shared with the supplier). Depending on the service provided to the customer, the provider may be responsible for (and therefore responsible for) the backup, a defined level of service availability, and data confidentiality. Even in this case, the end customer is not released from all responsibilities: he must for example, secure the passwords or certificates that are used to access his cloud environment, do not leave open access to the service via his own network. The consequences of proven negligence of the end customer cannot be attributed to the supplier. The service contract must address the area of responsibility of each party. If the customer must demand from his provider confidentiality commitments and the means of control to monitor that the provider meets its commitments, it is obvious that the latter cannot fully assume the confidentiality of the data entrusted to the storage system. Cloud. [12]It is necessary that the parties, each on their own, can control their own security, and on the other hand, control the third domain. In the absence of contracts formalizing these points of division of responsibilities, and control and registration tools, litigation procedures can be long and laborious, especially in a field where case law is rare.

V. CLOUD DATA ACCESSIBLE TO AUTHORITIES IN ANOTHER COUNTRY [7]

Every country has the legitimate right to have access, under the legal conditions peculiar to it, to data stored in its territory or transiting through it. [16]Thus, in France for example, in the context of a search and in accordance with Article 97 of the Code of Criminal Procedure, the host must be able to extract from the Cloud the requested elements or all the information concerning a client in particular, without having to deliver all the data of clients hosted in the Cloud. The good practice is to contractually ensure the country (or countries) where the infrastructure elements will be physically installed

and to know, before engaging in a cloud service contract with a provider, the relevant jurisdictions.

VI. CONCLUSION

The Cloud Computing model offers more choice, flexibility and operational efficiency, and enables businesses and individuals to realize greater savings. To take full advantage of all these benefits, users must have reliable guarantees regarding the confidentiality and security of their data [9]. The use and sharing of data collected in the Cloud is limited due to the presence of personally identifiable information whose confidentiality of individuals may be violated during such sharing. The difficulty in sharing data stems mainly from the fact that preserving the confidentiality of an individual with a loss of information, which makes the data less useful. The challenge of ensuring the privacy of an individual while providing useful information makes the preservation of confidentiality for published data difficult. He still has a long way to go before he reaches maturity. To facilitate this progress, providers can start by adopting international standards that guarantee the security, integrity and confidentiality of personal data.[10] On the other hand, this is not enough to solve the problem: transparency is a good start, but governments around the world should also define international laws on data privacy because cloud-related debates are far from over to be resolved. To ensure that this aspect remains a priority, it is up to cloud providers to make their voices heard.

REFERENCES

[1] Cloud Computing Security, Privacy and Forensics: Issues and Challenges Ahead. (2018). International Journal of Recent Trends in Engineering and Research, 4(3), 10–13. https://doi.org/10.23883/ijrter.2018.4083.xwpna

[2] Security and Privacy Challenges in Cloud Computing Environments - Hassan Takabi, James B.D. Joshi, Gail-Joon Ahn,

[3] Security and Privacy Issues in Cloud Computing Environment - ShaziaTabassamEng 2017

[4] View on Security, Privacy and Trust Issues in Cloud Computing Environment - Jitendra Kumar Verma, C.P. Katti

[5] Cloud-based Services Users and Trust Issues-A Comparative Study of Gender and National Culture Perspectives – Chetan, Sharma Kandel

[6] Cloud Computing: Legal and Security Issues - Hussam Hourani, Mohammad Abdallah

[7] Security threats and legal issues related to Cloud based solutions - EesaAlsolami

[8] Simanta Shekhar Sarmah. (2019). Cloud Migration- Risks and Solutions. Science and Technology, 9(1), 7–11. Retrieved from http://article.sapub.org/10.5923.j.scit.20190901.02.html

[9] Towards a Quantitative Model of Cloud Computing Risks and Benefits. (2016). Bulletin of the South Ural State University. Series "Computational Mathematics and Software Engineering," 5(2). https://doi.org/10.14529/cmse160206

[10] Controlling & Analyzing Risks in Cloud Computing Security. (2017). American Research Journal of Business Management. https://doi.org/10.21694/2379-1047.15004

[11] Chaves, S. (2011). The Risks Issue in Cloud Computing. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1991156

[12] Achara, S., &Rathi, R. (2014). Security Related Risks and their Monitoring in Cloud Computing. International Journal of Computer Applications, 86(13), 42–47. https://doi.org/10.5120/15049-3417

[13] A Study of Cloud Computing with its Risks Factors and Security Issues. (2017). International Journal of Innovations in Engineering and Technology, 9(2). https://doi.org/10.21172/ijiet.92.04

[14] IEEE Cloud Computing. (2013). IEEE Transactions on Cloud Computing, 1(2), 230–230. https://doi.org/10.1109/tcc.2013.24

[15] IEEE Cloud Computing Call for Papers. (2014). IEEE Cloud Computing, 1(2), 41–41. https://doi.org/10.1109/mcc.2014.35

[16] Garg, A., &Rathi, R. (2019). A Survey on Cloud Computing Risks and Remedies. International Journal of Computer Applications, 178(29), 35–37. https://doi.org/10.5120/ijca2019919139

[17] Measures in Cloud Computing. IMS Manthan (The Journal of Innovations), 9(1and2). https://doi.org/10.18701/imsmanthan.v9i1and2.5159

[18] Mathkunti, N. M. (2014). Cloud Computing: Security Issues. International Journal of Computer and Communication Engineering, 3(4), 259–263. https://doi.org/10.7763/ijcce.2014.v3.332