Journal of
Electrical & Electronic Systems

Beretas, J Electr Electron Syst 2017, 6:4
DOI: 10.4172/2332-0796.1000246

Perspective Open Access

Cloud Computing and Privacy

Christos Beretas*

Member of Alpha Beta Kappa Honor Society, Ohio, USA

Cloud computing is one of the most widespread architectures in recent years, services and applications that rely on it are rapidly deploying smart platforms for implementing information systems where resources can spread something that is extremely important but also quite different from the existing conventional computer systems. The difference is felt when one begins to think about the possibilities offered by modern environments and how they can be modified for every need. In this new philosophy, subscribers can offer services to other subscribers. Sharing computing resources globally is the main trick of a geographic limitation. For this reason, it has been and is the subject of many issues relating to the precaution, security and use of personal data. Both service providers and users should consider both existing data protection laws as well as security policies implemented by the service provider. So before a user goes to the cloud, they should first assess the following risks.

- The compatibility difficulties and loss of management of the remote system
- Loss of access passwords and keys to a remote system in combination or not with information leakage
- Software licenses per country, applicable laws and terms of use
- Non-coincidental risks from the customer side, such as information leakage, network problems, unauthorized access, etc.

In a modern work environments that the immediate provision of unchanged information must be taken for granted, it must always be in mind that the transition to cloud systems involves dangers and risks, which should first be analysed before a business decides moving to cloud, in particular, the following should be considered:

- The architectural implementation of a cloud system, security measures, and licensing
- Cost/dangers Analysis
- Compatibility with existing or future systems
- Ways to encrypt and isolate data
- The legal framework of each country where the cloud provider operates
- Dangers from internal role of abuse by network administrators
- The lack of information during transport
- Permanent or not data deletion
- Network quality
- External attacks on the network and ways to mitigate them

The integrity of the information should be ensured from creation to final disposal. So in a cloud system needs to clarify the following:

- Who is the real owner of the information
- What is personal data for the cloud provider
- Interlocking of personal data in accordance with the cloud provider policy
- Ensure from who and if third-parties will have access in data
- How does the cloud provider check if someone complies with their policy
- Checking whether the data is being encrypted, how, what level, and how it can be distributed without the owner's permission
- Ensure that personal data required to connect users to a cloud system in conjunction with the information stored in it will never be used to create a human virtual profile
- Ensure that when the data are deleted, their deletion is permanent and is not copied to a data warehouse

Based on the above, conclude that the security of information in a cloud system is very important and before anyone decides to transfer its services to it, it needs to evaluate it in detail. Currently offered cloud services at very affordable prices, if judging only on the economic benefits and excluding areas such as increased privacy and high security, then we can safely say that we are facing a new major technological revolution.

***Corresponding author:** Christos Beretas, Member of Alpha Beta Kappa Honor Society, Ohio, USA, Tel: (+30) 693-890-9477; E-mail: c_beretas@yahoo.com

Received November 13, 2017; **Accepted** December 05, 2017; **Published** December 12, 2017

Citation: Beretas C (2017) Cloud Computing and Privacy. J Electr Electron Syst 6: 246. doi: 10.4172/2332-0796.1000246