WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Privacy Regulations for Cloud Computing

Yashaswini C

VTU

INTRODUCTION

Michael Porter's value chain concept can be used to derive the mission-critical and enabling activities. Activities that directly result in the organization's output are considered mission critical. Activities that directly support the mission are known as enabling activities . Public-Private Collaboration (PPP) is a tool that the government can use to effectively use technology to enable such service activities for the general public. Communication, education, information sharing, teamwork, and management of the public IT management profession are the goals of PPP organizations . Since privacy is regarded as one of the fundamental human rights, it becomes a crucial topic of conversation in situations like this . Article 12 of the United Nations Declaration of Human Rights (UDHR 1948), Article 17 of the International Covenant on Civil and Political Rights (ICCPR 1976) , as well as numerous other international and regional treaties, acknowledge privacy as a fundamental human right. The courts have found that right in other provisions in many nations, including the US, Ireland, and India, where privacy is not expressly guaranteed by the constitution . The most recent EU Data Protection legislation (Council Directive 95/46/EC) is the most thorough translation of these rights into privacy protection laws. Many of the provisions found in the IT policy are also found in the Indian IT Act and Rules. Due to intricate legal concerns, no nation has yet to establish a true government cloud, according to Dr. Gulshan Rai, CERT, India . The reason for this is that the three elements—privacy, security, and the right to information—are comparable to the three vertices of a triangle. Compromises on security and the right to information are necessary if one desires privacy, and vice versa. Therefore, striking a balance is necessary, and doing so calls for a great deal of maturity and awareness.

2.DATA SECURITY LAWS AND REGULATIONS AND PRIVACY CONCERNS

The privacy concerns, data security issues, laws, regulations, and standards pertaining to cloud computing are compiled in the following table :

Sl. No.	**Cloud Computing Privacy and Data Security Concerns**	**Description of Issues**	**Related Laws, Regulations and Standards**	**Remarks**
1.	Required Disclosure to the Government	• Depending on the data stored in the cloud, different levels of security may apply.	The FTC's Fair Information Practices, the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA), and the USA Patriot Act.	National cryptography laws in the UK, India, Singapore, and Malaysia may allow lawful access to plaintext or cryptographic keys and data in accordance with the OECD's encryption guidelines.
2.	Data Security and Vulnerability Disclosure	• How does a cloud provider protect customer data?	The Family Educational Rights and Privacy Act (FERPA) and the Gramm-LeachBiley Act (GLBA) in the United States	The Joined together States' Cybersecurity Upgrade and Shopper Information Security Act (H.R. 5318)
3.	Where the Data Is	Legal ramifications could arise from the actual location of the server housing the data (such as jurisdiction issues).	The United States' NARA rules (Title 36 of the Code of Federal Regulations); the Sarbanes-Oxley Act's Payment Card Industry Security Standard (PCIDSS); and the FTC's Fair Information Practices	In the USA, it indicates Do the laws of the states where documents are physically located, the location of the company that owns them, or the laws of the state where an individual resides govern cloud computing? In the UK Traditional methods like model

				contracts or the Safe Harbor program, which are used to comply with the EU Data Protection Directive (EC/95/46) (the Directive), may not provide a practical solution and, at best, would be difficult to implement and maintain depending on where the vendor's servers are located.

The Clinger-Cohen Act of 1996, Office of the Management Budget (OMB) Circular No. The Federal Information Security Management Act (FISMA) of 2002, the E-Government Act of 2002 and its accompanying OMB guidance, the Privacy Act of 1994, A-130, particularly Appendix III, and the previously mentioned categorized listing of cloud computing concerns are additional U.S. laws and regulations that are related to (1) compliance. (2) NARA regulations (Title 36 of the Code of Federal Regulations) contain the information. (3) Electronic Discovery under the Freedom of Information Act In contrast, NIST special document 800-144 offers comprehensive security and privacy guidelines for public cloud computing in the United States. EU Directive 95/46/EC will be used in the UK to provide a basic standard for privacy protection and to harmonize the privacy laws that were previously in effect in the various EU member states. India may benefit from the Information Technology Act 2008, which includes cyber laws, in terms of data security and privacy.

2. Concerns about privacy in relation to third-party storage

Information stored with a third party, such as a cloud computing provider, might not be as protected by privacy laws as information that belongs to the original author. When they give up control of their resources to outside providers who have the authority to alter the underlying technology without the consent of their clients, IT managers are likely to experience anxiety. Performance and latency problems can therefore be considered problematic. Getting information from a third party instead of the original source may be simpler for government organizations and private litigants. Both people and businesses are impacted by the government's and others' growing capacity to gather information from third parties. In the United States, the Electronic Communications Privacy Act of 1986 (ECPA) offers some safeguards against government access to electronic mail and computer records stored by parties (such as Internet service providers) in an electronic environment. Losing notification of a government data request is a major restriction on rights for many users. However, the FBI has access to all corporate records under provisions of the USA Patriot Act, which was first passed in 2001 and revised in 2005. This is an extension of the ECPA, requiring cloud providers to disclose records. Under A private litigant or other party may request records from a cloud provider instead of a user directly under the Freedom of Information Act 2000 or the Right to Information Law. This is because the user would be more motivated to avoid a subpoena or other request than the cloud provider would be. Consequently, cloud providers' disclosures to third parties may be in violation of other laws, values, and interests. Requesting health information from cloud service providers raises concerns about confidentiality due to the Health Related Information Act, the Fair Credit Report Act, the Video Piracy Protection Act, bankruptcy, and trade secrets. The long list of publications that websites continue to publish on their terms and service in terms of privacy and confidentiality may be the most significant aspect of cloud computing for the typical user, who is not bound by any professional or legal obligations. Cloud providers typically offer their services to users without requiring individual contracts, subject to their published terms and conditions. Users are probably bound by the terms of service if they grant the cloud provider access to their data. This may have an impact on a user's ability to share information legally. The user may be at a lower risk of legality or a higher risk of protection failure, which would prevent them from bringing a claim from a particular jurisdiction, if the data is stored in multiple locations (on multiple platforms).

3. PRIVACY REGULATION UNDERSTANDINGS

With the possible exception of the USA-Patriot Act, which might have been included under a different name, the privacy laws covered in this paper are fairly similar. However, it's crucial to realize that these regulations are generally accepted as the norm for privacy. As a result, these guidelines offer a benchmark for evaluating privacy laws. With the possible exception of the USA-Patriot Act, which might have been included under a different name, the privacy laws covered in this paper are fairly similar. It's crucial to realize, though, that these rules are generally accepted as the industry standard for privacy. These guidelines can serve as a benchmark for comparing privacy laws, as illustrated in Figure 1. Cloud service provider (CSP) businesses are therefore legally bound to abide by the law and are held accountable for compliance. Organizations may be held accountable if a subcontractor violates the law. The legal status of a CSP as a subcontractor is unknown. As of right now, this issue has no precedent. Nonetheless, a CSP might be regarded by the law as a subcontractor. This implies that businesses should make sure a CSP conforms to all applicable privacy regulations. In other instances, jdiction is thought to have an impact on cloud computing privacy.

In summary, identity management, physical and personnel security, application security, cloud availability and customer accessibility, privacy, and legal issues are among the many concerns associated with cloud computing.

4. A FEW TECHNICAL CHANGES TO CLOUD SECURITY PROBLEMS

Initiated from within the cloud. Distributed Denial of Service (DDoS) and Click Fraud are two types of botcloud attacks. The planning and execution of these two attacks, which both succeeded in their objectives, cost about 100 euros and took less than a day. Furthermore, the Cloud Service Providers failed to detect or thwart either attack. Identity theft is most likely to be committed by criminals who are willing to use botnet attacks. Fraudulent names and stolen credit card information are used to create an account for Cloud services, which eliminates the need to pay for the service. A criminal could start a dozen botclouds, possibly on various CSPs, using a dozen credit cards that were stolen. An ongoing, massive attack results from the launch of the next Cloud after the first is finally located and shut down. At the moment, CSPs are not motivated to keep an eye on every client from the moment they sign up for cloud services. Until the victims have gotten in touch with the relevant CSP, nothing is being done to stop the attack. Unless CSPs establish a thorough policy and process for detecting and removing botclouds, botmasters will keep shifting their malicious operations into the cloud, and botclouds will keep expanding.

5.CONCLUSION

Cloud computing may offer the capacity to powerfully reconfigure computing assets in reaction to changes in request. A Client Service Provider (CSP) must be able to fulfill this requirement. If a CSP is forced to outsource organizational data to another CSP due to inability to comply with this requirement, the location-related privacy issues raised above might be made worse. Thus, the effect of privacy laws is most apparent when contrasting external cloud computing with traditional IT. As a result, there may be many concerns about cloud computing's compliance with privacy regulations. As a result, it is clear that the privacy laws in place today are inadequate to handle all privacy issues related to cloud computing. It seems that a more mature understanding of the issues and the existing regulations is required to address this. Security regulations may be more important when it comes to cloud computing adoption than privacy issues, which many organizations do not fully comprehend.

6.ADDITIONAL RESEARCH

Therefore, we think that more case studies that illustrate different scenarios using laws, policies, and regulations related to cloud computing and privacy legislation would be very helpful to future researchers. This could offer concrete examples of how a company's adherence to privacy laws is impacted by the use of cloud computing.

RESOURCES

[1] The American Council of Technology (2011), Shared Interest Group: Enterprise Architecture, The Role of Enterprise Architecture in Federal Cloud Computing A White Paper from the ACT and IAC partnership in Fairfax, Virginia, Available at http://www.actgov.org/knowledgebank/whitepapers/documents/shared%20interest%20groups/enterprise%20architecture%20SIG/role%20of%EA%20in%federal%20cloud%20compete%20-%EA%20SIG-%2001-2011.pdf, and retrieved on 07-02-2012.

[2] Bruening and Treacy (2009), The Bureau of National Affairs, Inc., Privacy and Security Law Report, Available at http://www.hunton.com/files/Publication/6acf0d97-7c21-42d1-ab48315a04601152/Presentation/PublicationAttachment/37dc2129-4f0c-45a0-8417-651e05dc423f/CloudComputing_Bruening-Treacy.pdf, retrieved from the WWW on March 12, 2012.

[3] Clark, K., Brazier, F. M. T., and Warnier, M. (2011), Botclouds: The coming of cloud-based