ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

Review Article

Open Access

A Comprehensive Review on Ethical Considerations in Cloud Computing-Privacy, Data Sovereignty and Compliance

Ankur Mahida

Subject Matter Expert (SME), Barclays, USA

ABSTRACT

The way by which computing power and data storage are accessed has become dramatically changed through cloud computing, which is internet-based services made available on a need basis. Among the benefits come the new ethical issues that are related to privacy, data jurisdiction, and compliance obligations. The data of a customer becomes vulnerable when it is stored and processed off-site on a remote server, as impeding risks can arise from unauthorized access and secondary use of data without the customers' allowance. The jurisdictional authority over the data positioned globally and housed in numerous data centers is a big question to answer from the sovereignty perspective since a conflict of laws arises when they have to deal with privacy and government surveillance. In addition, how regulatory compliance is shared between cloud provider and user is complex and may end up confusing the two parties as different standards of security and privacy are most important. The following review draws out the significant problems, specific solutions, effects, and the scope of these ethical matters in cloud computing. It tackles privacy protections, location-based data sovereignty remedies, and the allocating burdens of compliance between the providing end and the customer clearly. Cloud computing can be adopted ethically by applying a proactive approach to the emerging ethical issues related to remote storage, access, and geography which it may hold.

***Corresponding author**

Ankur Mahida, Subject Matter Expert (SME), Barclays, USA.

Received: October 06, 2022; **Accepted:** October 10, 2022; **Published:** October 20, 2022

Keywords: Cloud Computing, Ethics, Privacy, Data Sovereignty, Compliance

Introduction

The most striking feature of cloud computing is that it has considerably swept the majority of businesses off their feet, and they find it to be the primary way to meet computing powers and data storage demands. Cloud computing relieves companies from the burden of buying and directing their servers and infrastructure by enabling them to pay only for what they need and obtain this as a service from established cloud providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform. As this is a pay-as-you-go system that is reliable across different services that can innovated and used in a more significant number of applications, the user is not forced to be under a specific cloud platform. Yet, while cloud use brings advantages, there are new ethical concerns related to privacy protection, jurisdictional authority on data, and regulatory compliance. Keeping the data and applications that belong to the owners of a business on distant servers of cloud computing providers actually transfers the risk of having unauthorized data access and usage to the cloud companies.

Additionally, with virtualized data centers in the world, the jurisdiction and sovereignty of data in these countries have also become a debate. Therefore, the cooperative responsibility of the cloud providers and customers to meet security and privacy regulations still needs to be defined. This article expounds on the emerging ethical dilemmas about privacy, data jurisdiction, and compliance sanctioned by the spread of cloud computing. It provides the shortcomings and the troubles within the mentioned areas and a recommendation on a positive, ethically responsible cloud adoption.

Problem Statement

The cloud computing revolution has not only increased the ethical tension on asking for compromises in privacy, jurisdiction, and regulatory obligations but has also intensified them as well [1]. The main reason for the breach of privacy is that customer data are no longer stored on local servers but on remote cloud provider servers. Hence, it introduces inevitable risks such as intrusion, leakage, and off-label processing of data by insiders or outsiders. Cloud providers, by virtue of the extended access they have to customer data and metadata required for service delivery, could at one point use such access for unethical things such as incorrectly sharing without consent or profiling illegally. Additionally, the customer needs a clearer view of how their data is being used, accessed, or protected, which is the case with cloud remote backup that contains the customers' data.

Furthermore, with the emergence of data centers that operate globally in multiple countries with the data stored in the cloud, the question of which country has the authority to regulate the data is complicated [2]. Customers need to gain knowledge of the physical locations of their data, which becomes a problem if different countries have different privacy, security, surveillance, and sovereignty laws. For example, the USA PATRIOT Act makes it possible for U.S. government agencies to get cloud data with the customers having no idea about it or not being asked for permission. This creates sovereignty conflicts with other nations.

Lastly, cloud regulation proves to be a challenging process due to the fact that it is not always clear which party - the vendor or the customer - is responsible for cloud governance [3]. Cloud providers may declare many guarantees of compliance.

Nevertheless, it is the customers who still might need to remain accountable for some regulatory issues, like HIPAA and PCI DSS, when using cloud services. The lack of clarification of the responsibilities of cloud providers versus customers in terms of compliance with obligations may result in the appearance of confusion and difficulties in proper compliance with standards established by the regulation in the field of security and privacy.

Solutions

In cloud environments, various technical and policy measures can be taken to address privacy concerns. Both in-transit and at-rest encryption of sensitive customer data defend from unauthorized access [4]. Implementation of robust access controls, like multi-factor authentication and the use of role-based limitations, also restrict the data viewing to authorized personnel only. In order to provide users with better control, cloud solutions should implement consent policies that enable secondary usage or sharing. There should be no access to customer data among providers, and a regular audit should illustrate strict data protection.

As to jurisdiction and sovereignty issues, the providers of the cloud can provide customers with options for data storage locations so that their preferences can be met with the applicable laws [5]. This shows that an EU-based company requests storage of its cloud data in EU data centers to follow GDPR standards. The providers should offer transparency about where the customer's data is stored physically, which law applies in the locality, and any possible government surveillance. Finally, customers may consider issues of data sovereignty when choosing a cloud provider, which would, in turn, help to mitigate risks.

Vendors should help with regulatory compliance by segmenting responsibilities through the use of contractual Service Level Agreements (SLA). The provider should mention those controls that are to be applied by the provider instead of the customer's duties [6]. The audit and certification of infrastructure implementation for compliance with HIPAA and other standards is a good sign of due diligence. Providers can also provide accessibility features for the validation step by customers to ensure the controls have not been compromised. Cloud migration risk assessment should be done by the customer to identify the control and to agree with the provider on the split of compliance responsibilities based on the cloud services being used.

An instance of privacy-enhancing mechanisms, location-based data storage choices, and both clear delineation of compliance responsibilities between cloud vendors and customers and the requirement for consent will help resolve the business ethical concerns associated with the issue of remote storage and processing of data.

Uses

Cloud computing has witnessed extraordinary growth in the number of adopters among organizations and industries that strive for lower cost-efficiency, greater agility, and innovation. The direct-on-demand services and pay-by-use pricing model of cloud infrastructure enable companies to cut down costs by getting rid of having to own and manage servers as well as data centers. The utilization of cloud services has reached new heights due to its flexibility and the possibility to scale dynamically according to evolving computing requirements.

A large proportion of cloud computing features are concerned with data storage and backup. It makes data storage convenient in that it can be accessed from any location [7]. At the same time, backup is ensured against loss of data. Cloud data storage facilities at AWS, Google, and Microsoft are highly scalable and flexible. Moving IT infrastructure to cloud servers enables organizations to stay safe even in case of disasters.

Since cloud web hosting is also very popular because of the cost and flexibility, the way businesses utilize the web has changed. With the IaaS and PaaS cloud services model, companies can easily roll out, host, and run websites and web apps without having a complex infrastructure dedicated explicitly to hosting [8]. With that in mind, negative impacts include spending practices, supply chain changes, and the inability of small businesses to establish an online presence.

Cloud analytics, which is like AWS Elastic MapReduce, is a powerful method to handle and yield valuable information from large datasets. Cloud analytics enables business intelligence, predictive modeling, extensive data analysis, and other complex functions that are unrealizable otherwise due to the lack of scalable computing capacity [9].

A lot of enterprises have moved applications like CRM, HRM, and ERP to the cloud as they enjoy advantages such as cost reductions, ease of accessibility, automatic updates, and scalability [10]. Cloud enterprise apps provide companies with the required tools instantly rather than installing on-premise. Cloud computing offers a huge economy of scale that, in turn, brings accessibility, resilience, and innovation, which helps cloud computing become pervasive in applications from data storage to analytics.

Impact

Cloud computing adoption undeniably offers compelling benefits to organizations by providing them with the flexibility to leverage such services into on-demand resources through the Internet [11]. While the use of the cloud avoids issues of damage to irreplaceable items, it also brings new risks if the computers are not adequately maintained.

Primarily, companies' proprietary customer data stored on cloud servers owned by third-party providers, which are accessible externally, augment the risks to privacy [12]. Customers' data might be exposed owing to breaches, access by unauthorized persons or internal staff, or abusing data access rights for unethical purposes. Inappropriate security controls and governance from the providers, the adoption of the cloud implies that taking over the complete overview of the sensitive data is not possible, and that way, there is a possibility of violations of privacy.

The model of sharing responsibilities between cloud service providers and users for the purpose of meeting the regulatory compliance requirements might make it difficult for complete compliance to be achieved [13]. Imbalances in the conditions that decide whether one party is responsible for the execution of each control under HIPAA, PCI DSS, and GDPR cause loopholes in the protection. Despite a shared yet ambiguous distribution of compliance responsibility, it will be more complicated to comply entirely with regulations in cloud services.

Moreover, the physical dispersion of data across various data centers maintained in different countries with different legislative controls makes translating backed information into authoritative replication complex [14]. From the customer's perspective, the very chance of losing visibility and sovereignty is the reason why data storage places can't be seen clearly and easily. Location is a driving force of the laws and protection for data as well as the chance of monitoring by the government that should attract the customers' concern. Hence, the legal and physical data location leads to significant sovereignty consequences in the cloud that, in turn, impact organizations.

Cloud technology empowers businesses to innovate while gaining efficiencies. Still, customers' privacy, compliance, and sovereignty risks are also magnified. They must be considered judiciously so that the technology can be adopted and utilized to its fullest effect in an ethical way. Proper governance is needed not to allow negative influences to occur.

Scope

The literature review in this paper focuses on the evaluation and identification of the significant ethical issues and dilemmas that cloud computing raises under the ethics of privacy, jurisdiction, and compliance. With an eye on cloud ethics, the focus of the review is on summarizing the fundamental concerns and problems that are raised by the functionality of paying-as-you-go cloud services, namely, remotely storing, processing, and retrieving user data. Privacy risks of fair use of customer data stored on cloud servers should be taken into account. It examines the lack of internal governance and regulation of proprietary data when using external cloud providers, thus handling outsourced data. Methods such as encryption, policies, and control are examined from a marked viewpoint.

On the topic of jurisdiction section, it asserts that the implications of availing data across the global data centers that subscribe to different sets of laws in other countries are considered. From the G2 point of view, there are sovereignty issues and conflicts between privacy regulations across borders when the location of storage of cloud data is unknown or uncertain. Ethical issues concerning government surveillance policies that obtain cross-border data were also covered. Compliance is part of the literature review, which includes a shared responsibility model that constitutes both cloud vendors and customers. It examines the problem of compliance with security and privacy regulations when responsibilities are not delineated. Ednethical allocation of compliance burdens is reviewed.

Besides describing the benefits and consequences in terms of the ethical issues mentioned above, the review will also cover cloud adoptions and their overall risks. It aims to delineate the challenges without going into the technical details. It primarily emphasizes an ethics-oriented interpretation of cloud privacy, jurisdiction, and compliance suitable to a cross-disciplinary audience. The literature underpins providing solutions analysis that are carefully considered to tread on responsibility in the cloud adoption process, which respects core ethical principles.

Conclusion

Cloud computing brings gigantic benefits of scale, accessibility, resilience, and efficiency by letting organizations use computing resources with instant provisioning over the Internet. On the plus side, using cloud services facilitates the advantages; however, there would be some new ethical challenges regarding personal data protection, jurisdictional authority, and regulatory compliance to be taken into consideration. Whenever private business data is stored in the public cloud, clients essentially deliver all supervision and control. Thus, privacy can be breached without their knowledge via unauthorized access or use. Cloud providers should endeavor to adopt measures such as technical encryption controls that are backed up with enforceable governance protocols of access restrictions and consent policies. Furthermore, the geographical distribution of data across infrastructures in different regions that follow diverse laws presents a compliance challenge where the role of a customer and a provider is unclear. Compliance resources should be shared in a straightforward structure of audits and controls that are conducted with transparency.

Similarly, jurisdictional conflicts between privacy laws are placed in danger over sovereignty concerns, which can be partially mitigated by allowing customers to select data storage locations that suit them with the regulations preferred. On the whole, although cloud computing makes a unique contribution to progress, customers and suppliers ought to follow privacy, security, and governance principles for ethical adoption. The options outlined in this review are encryption, location choices, access controls, and assignment of responsibilities, which could maintain a balance in the emerging ethical tensions with respect to remote storage and processing of data at scale in the cloud. Responsibly determining the cloud deployment capabilities will depend on a working partnership between the providers and users with implementable organizational policies and available technology. As adoption will not stop moving, the cloud ecosystem needs to keep evolving its ethical map.

References

1. Shepherd M, Turner JA, Small B, Wheeler D (2018) Priorities for science to overcome hurdles thwarting the full promise of the 'digital agriculture' revolution. Journal of the Science of Food and Agriculture https://onlinelibrary.wiley.com/doi/10.1002/jsfa.9346.
2. Schwartz PM (2018) Legal Access to the Global Cloud. Columbia Law Review 118: 1681-1762.
3. Gozman D, Willcocks L (2019) The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. Journal of Business Research 97: 235-256.
4. Keerthana N, Viji V, Musthafa A, Dilip K, Mohanraj E, et al. (2021) Securing data in transit using data-in-transit defender architecture for cloud communication. Soft Computing 25: 12343-12356.
5. Woods AK (2018) Litigating Data Sovereignty. The Yale Law Journal 128: 328-406.
6. Chen CM (2018) A review and analysis of service level agreements and chargebacks in the retail industry. The International Journal of Logistics Management 29: 1325-1345.
7. Deshpande PS, Sharma SC, Peddoju SK (2019) Security and data storage aspect in cloud computing. Singapore: Springer Nature Singapore Pte Ltd https://dokumen.pub/security-and-data-storage-aspect-in-cloud-computing-1st-ed-978-981-13-6088-6-978-981-13-6089-3.html.
8. Kim M, Ajay M, Vinod M, Rohit R, Valentina S, et al. (2016) Building scalable, secure, multi-tenant cloud services on IBM Bluemix. IBM Journal of Research and Development 60: 2-3.
9. Bibri SE (2018) The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. Sustainable Cities and Society 38: 230-253.
10. Attaran M, Woods J (2019) Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship 31: 495-519.
11. Kousalya G, Balakrishnan P, Pethuru Raj C (2017) The Hybrid IT, the Characteristics and Capabilities. Computer Communications and Networks 199-221.

12. Ghorbel A, Ghorbel M, Jmaiel M (2017) Privacy in cloud computing environments: a survey and research challenges. The Journal of Supercomputing 73: 2763-2800.
13. Ali O, Shrestha A, Chatfield A, Murray P (2019) Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly 37: 101419.
14. Coetzee S, Ivánová I, Mitasova H, Brovelli M (2020) Open Geospatial Software and Data: A Review of the Current State and A Perspective into the Future. ISPRS International Journal of Geo-Information 9: 90.