RESEARCH ARTICLE OPEN

# Handling Regulated data in Cloud Computing Environment with Potential Problem and Proposed Solution

By Azhar Ushmani

## I. INTRODUCTION

Cloud computing has become a popular model for organizations to store and process data. However, when regulated data such as personal health information or financial data is stored in the cloud, additional security considerations must be addressed. This paper examines the potential problems with handling regulated data in the cloud and proposes solutions to mitigate risks.

## II. POTENTIAL PROBLEMS

### 2.1 Data Privacy and Confidentiality

A major concern with regulated data in the cloud is unauthorized access and disclosure. The customer has limited control and visibility into the cloud provider's infrastructure. Sensitive data could be accessed by insiders or via vulnerabilities in the provider's systems (Jaatun et al., 2009).

Protecting sensitive user information is a major concern when using cloud services. Cloud providers must implement robust security measures to safeguard confidential data and ensure compliance with privacy regulations. Encryption of data at rest and in transit prevents unauthorized access. Access controls and identity management limit data exposure to authorized personnel only. Providers should disclose their security practices and allow audits to validate controls. Customers should understand where data is stored and ensure compliance with applicable regulations. Contracts should specify ownership rights, allowable uses of data, and breach notification policies. Multi-factor authentication adds an extra layer of protection for system access. Ongoing security training for cloud provider staff helps mitigate insider threats. Selecting reputable providers and monitoring for compliance gives customers assurance their data remains private and secure when using cloud services.

### 2.2 Data Security

Securing regulated data in the cloud is challenging. The customer relies on the cloud provider for security controls. Weaknesses in access controls, encryption, network security, etc. can expose data to attackers (Subashini & Kavitha, 2011).

### 2.3 Data Location

With cloud computing, data is stored on shared infrastructure across multiple locations. However, some regulations restrict data from being transferred outside national borders (Pearson & Benameur, 2010). This can conflict with the cloud model.

### 2.4 Legal and Regulatory Compliance

Handling regulated data in the cloud has unclear implications for compliance with regulations like HIPAA and PCI-DSS. Auditing cloud provider security is difficult for customers (Jansen & Grance, 2011).

## III. PROPOSED SOLUTIONS

### 3.1 Implement Strong Access Controls

Customers can require cloud providers to implement role-based access controls, multi-factor authentication, and encryption to restrict data access (Chen & Zhao, 2012). API keys can be used instead of passwords for applications.

### 3.2 Utilize Encryption

Encrypting regulated data before uploading it to the cloud can ensure confidentiality. Fully homomorphic encryption allows computations on encrypted data (Vaquero et al., 2011).

### 3.3 Select Cloud Providers Carefully

Choosing providers who contractually commit to meeting legal requirements, allow audits, provide

security certifications, and offer features like geo-fencing data can help reduce risks (Pearson, 2013).

### 3.4 Use Hybrid Architecture

A hybrid approach stores regulated data on-premises while extending into the cloud for scalability. This provides more control over sensitive data while still benefiting from the cloud (Bruin & Floridi, 2017).

## IV. CONCLUSION

Handling regulated data like healthcare records or financial information in the cloud raises important privacy and security concerns which must be addressed through strong access controls, encryption, prudent cloud provider selection, and hybrid on-premise/cloud architecture. With proper precautions, even sensitive data can be managed securely in the cloud.

## REFERENCES

Bruin, B., & Floridi, L. (2017). The Ethics of Cloud Computing. Science and Engineering Ethics, 23(1), 21-39.

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. Proceedings of the 1st International Conference on Computer Science and Electronics Engineering.

Jaatun, M., Pearson, S., Gittler, F., Leenes, R., & Niezen, M. (2009). Enhancing Accountability in the Cloud. International Journal of Information Management, 29(5), 324-331.

Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144.

Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London.

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

Vaquero, L. M., Rodero-Merino, L., & Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. Computing, 91(1), 93-118.