Ensuring Data Privacy and Compliance across Multiple Clouds With GDPR Regulations

Upesh Kumar Rapolu

Houston, USA
Upeshkumar.rapolu@gmail.com

Abstract

The following research paper has provided data encryption and compliance across multiple clouds by the utilisation of GDPR. This has provided a decent set of standards that has been crucial for protecting the data which the organisations need to comply with. At the same time, the research paper has analysed that the application of supportive cloud security platforms has enabled to ensuring of complete data privacy and compliance across multiple clouds regarding the GDPR regulations. Furthermore, this has transformed the path by fostering the latest technologies and best practices for encryption of the data followed by access controls and data governance.

Keywords: Data privacy, compliance, GDPR,m cloud security, access controls, data encryption, cloud security gateway, cloud security information and event management

I. INTRODUCTION

The research paper will provide a vivid explanation of the intricate application of GDPR to ensure data privacy and compliance across multiple clouds. This will be posed to the encryption techniques to safeguard sensitive data which are in transit and at rest. At the same time. The research paper will portray having a curated understanding of data encryption and protection and thus reflecting the access controls and identity management/. Furthermore, this will be regarded to be effective to shed its light on data compliance and governance. Moreover, this will be effective for the organisations to propose cloud security and monitoring that will help to maintain data privacy and compliance.

II. UNDERSTANDING DATA ENCRYPTION AND PROTECTION (DEP)

The following section describes data encryption and protection alo abbreviated as "DEP". It is defined as a systematic security method that is capable of scrambling data into a secret code or cypher text. This code is then used for reading purposes by authorised people. It integrates with encryption algorithms like Advanced Encryption Standard and a Key Encryption Key (KEK). This is used to encrypt and decrypt the confidential data[1]. The KEK is usually kept in a protected place like a Trusted Platform Module to ensure compliance with the GDPR regulations. However, this benefits the organisations to implement robust encryption and mechanisms. This is categorised into two parts Dtav at Rest and Data at Transit. On one hand, in Data at Rest encryption, the protected data is kept securely in cloud storage services such as Microsoft Azure Blob Storage. On the other hand, in Data at Transit encryption, the safeguarded data is transmitted successfully among cloud services like HTTPS or SSL.

Figure 1: Highlighting GDPR Regulations

III. DESCRIBING ACCESS CONTROLS AND IDENTITY MANAGEMENT (ACIM)

This section describes Access Controls and Identity Management also known as "ACIM". It is defined as a specific set of processes and technologies that are posed to be capable enough to manage the complete user access to the overall resources in an organisation. This also makes ACIM stand as an essential component in managing the overall security infrastructure of an organisation in a productive form. It generally performs in two halves. In the first half, ACIM gets utilised with authentication mechanisms which are capable enough to verify a user's identity. Then the system determines to choose the appropriate resources that can be used by a user to promote complete access[2]. In the second half, the system sets the stage by controlling and allowing users based on their identity and gets access to multi-levels which are authorised intricately. The organisation needs to get accustomed to robust access controls containing Role-Based Access Controls (RBAC) and Attribute-Based Access Controls(ABAC). RBAC provides the users with complete access based on their definite roles and responsibilities. Similarly, ABAC grants users comparisons based on their attributes followed by departments and job functions. Furthermore, this ensures that not only the right individuals can get complete access but at the same time it also lets the organisations strictly adhere to cybersecurity practices[3]. As a result, this enables IT administrators to stop unwanted access to organisational resources so that the individual can get complete access.

Figure 2: Defining Access Controls and Identity Management

IV. HIGHLIGHTING DATA COMPLIANCE AND GOVERNANCE TO ENSURE DATA PRIVACY

The following section reflects on the importance of data compliance and governance to ensure data privacy. On one hand, data compliance refers to the process of following laws along with regulations and guidelines which need to be followed to safeguard the confidential information of users. On the other hand, the implementation of data governance is termed to be crucial, as it takes informed consent from the individuals to share their data and use them. At the same time, data governance also establishes the successful handling of data and thereby protecting it[4]. As a result, this can be considered ethical to make justified decisions that are vital for all organisations. However, the organisation must use Data Classification (DC) to categorise the data based on their confidentiality. It also involves Data Retention (DR) which tends to store large volumes of data and delete them once they are used. On the other hand, organisations must also get familiarised with Data Subject Rights (DSR) that allow data subjected to access protection and thus keep secure personal data.

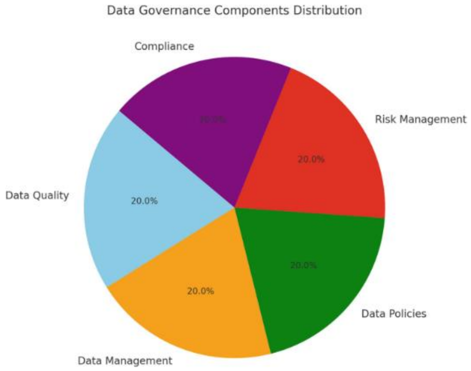

Figure 3: Understanding Data Compliance and Governance

V. PROPOSING CLOUD SECURITY AND MONITORING

This section elaborates on the importance of cloud security and monitoring which is applied intricately to manage the risks at the initial phases and protect the cloud-based asset in the field of data privacy. This stands to be necessary as it delves deep for identifying and responding to the security breaches across multiple c;louds. It is the companies that need to get accustomed to cloud security measures like CASB, CSG and SIEM. Firstly, CASB or Cloud Access Security Broker is used to provide complete monitoring and control to the cloud traffic[5]. Secondly, the application of Cloud Security Gateway (CSG) is used to nurture security entry points for cloud services. The integration of Cloud Security Information and Event Management helps to monitor and then analyse cloud security logs.

Figure 4: Nurturing Cloud Security and Monitoring

VI. CONCLUSION

This research paper has understood the importance of data privacy and its compliance across multiple clouds by the usage of GDPR. It has been analysed that fostering a comprehensive approach has been considered to be crucial to pose data encryption followed by access controls and cloud security. Moreover, the organisation needs to get familiarised with strengthening data encryption techniques which have been determined to protect confidential data and ensure compliance with GDPR regulations. This has served to be beneficial to make sure that the organisations maintain their data privacy and compliance across multiple clouds and has rendered complete data privacy and compliance.

Abbreviations and Acronyms

- AES - Advanced Encryption Standard
- GDPR - General Data Protection Regulations
- KEK - Key Encryption Key
- CASB- Cloud Access Security Broker
- CSG- Cloud Security Gateway
- ACIM- Access Controls and Identity Management
- CSIM - Cloud Security Information and Event Management
- DaR- Data at Rest
- DiT- Data at Transit
- DEP - Data Encryption and Protection
- HSM- Hardware Security Module
- RBAC- Role-Based Access Control
- ABAC - Attribute-Based Access Controls

Units

- Cloud Security Information and Event Management is measured in events per seconds (eps)
- Thus it is evident that the unit of measurement for access controls is usually calculated in Terms of Reference (ToR).

Equations

- The encryption formula $En(x) = [(x+ n) \bmod 26]$
- Data Retention (DR) = [{ number of users at the end of a time period / number of users at the beginning of a time period } X100]

ACKNOWLEDGEMENT

I would also like to acknowledge and express my sincere gratitude to the professors who have given their valuable time to complete my research project efficiently within the given timeline.

REFERENCES

[1] H. Li, L. Yu, and W. He, “The impact of GDPR on global technology development,” *Journal of Global Information Technology Management*, vol. 22, no. 1, pp. 1–6, Jan. 2019. [Online]. doi: https://doi.org/10.1080/1097198X.2019.1569186.

[2] M. Gal and O. Aviv, “The Competitive Effects of the GDPR,” *Ssrn.com*, Mar. 04, 2020.[Online]. Available:https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3548444

[3] M. Phillips, “International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR),” *Human Genetics*, vol. 137, no. 8, pp. 575–582, Aug. 2018[Online]. doi: https://doi.org/10.1007 /s00439-018-1919-7.

[4] R. N. Zaeem and K. S. Barber, “The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise,” *ACM Transactions on Management Information Systems*,vol.12,no.1,pp.120,Dec.2020.Available:https://www.researchgate.net/profile/Razieh-Nokhbeh Zaeem/publication/3436 81934_The_Effect_of_the_GDPR_on_Privacy_Policies_Recent_Progress_and_Future_Promise/links/60185126a6fdcc071bac1959/The-Effect-of-the-GDPR-on-Privacy-Policies-Recent-Progress-and-Future-Promise.pdf

[5] S. Sirur, J. Nurse, and H. Webb, “Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR),” Aug. 2018. Available: https://arxiv.org/pdf/1808.07338