Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(7):275-281**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Privacy in Cloud Computing: Best Practices for Protecting Sensitive Data, DLP Solutions

Ravindar Reddy Gopireddy

Cyber Securirty Engineer

Abstract The rise of cloud computing has upended the way organizations save and manage information. Cloud services have many benefits, such as scalability and flexibility of infrastructure resources that may help cost reduction, however, Cloud-based data services also mean challenges to keep your sensitive information secure. We develop enhancements to its capabilities with support for Data Loss Prevention solutions up until July 2020 that might be a crucial asset when protecting sensitive data in the cloud. Adherence to these methods and approaches will enable organizations in improving their data protection plans while lowering the risks pertaining with cloud computing.

Keywords Cloud computing, Protecting Sensitive Data, DLP Solutions, Data Loss Prevention, Cloud-based data services

1. Introduction

From storage and processing to data management, cloud computing - or rather the cutting-edge applications built on it - is a staple in technological needs of businesses across sizes. Benefits include cost saving, scalibility and the fact that data and application can be reached from anywhere with a change of paradigm. But, then there is another horn and data privacy & security issues.

When it comes to sensitive data stored in clouds, the risks are slightly amplified by a few threats may cause unauthorized access and subsequent loss of such information that was stolen. So, it is very important for organizations to ensure the privacy of this data so that they do not lose their customers trust and also loose compliance with regulations like General Data Protection Regulation (GDPR) or Health Insurance Portability Accountability Act (HIPAA).

This document sets the best practices to follow in order to protect data at rest on cloud using an overview of DLP effectiveness prior July 2020. Its goal is to provide organizations with Blueprints for Critical Activities in the Cloud fast enough so that they can be used to improve how data protection strategies.

2. Effective Practices for Protecting Sensitive Data in Cloud Computing

Protecting sensitive information from unauthorized access or disclosure is paramount for organizations as data and applications are moved to the cloud. Cloud computing is a dynamic and complex system, which presents the need of different challenges in it own. The complexity makes to build robust Data Protection Strategies for Cloud internationally partore onarticulate idea best practices for cloud data

Protection is important to protect sensitive information access from unauthorized, otherwise might lead compliance violations and open up security holes. This post articulates

the primary strategies and approaches with which organizations can properly secure their sensitive customer data so that they remain complaint from a regulatory standpoint, while also preserving trust with all of their constituents.

2.1 Data Encryption

At a basic level, data encryption is principal to secure the sensitive information in cloud. It works by further scrambling data to make it practically illegible to unauthorized access, providing another level of security that even if someone did gain entry into the application environment, they would not be able view important records.

Data Encryption and in Transit

Data should be encrypted both when stored (at rest) and when being transmitted (in transit). Encrypt data at rest, which means that even if someone gains physical access to the storage device they can't view or use any of it. Doing this is called encrypting data in transit, meaning that even if attackers intercept the information while it's being transmitted over a network they won't be able to read its contents. Data confidentiality is maintained using strong encryption algorithms such as AES-256

Key Management

Good key management practices are essential to ensuring that encrypted data remains secure. Enterprises shall use Hardware security modules (HSM) to create, store and control an access over encryption keys. Key Management Best Practices - We recommend key rotation, secure storage of keys, and the use of a cloud provider's KMS (key management services) as some best practices for managing your encryption keys. Good key management means that should the encrypted data become accessible, it can not be read without having access to those keys.

2.2 Access Controls

It is important to implement strong access control systems which will enable only the right people have your data. Access controls limit the access of users on who uses your network, reduce data breaches and prevent unauthorized access.

Identity Access Management (IAM)

IAM Policies - to manage user identities and resources access control. IAM systems deliver centralized management for users, authentication, and authorization. MFA is one a great way to enforce such security and provides users with an extra layer of protection by requiring that any user must provide two or more different verification factors, which authenticate the claimed identity. An example would be the user knows (password), has and is same, (security token) or simply what we are seeing on our phones for biometric verification.

Role-Based Security

RBAC restricts the data access based on the role that is assigned to a user in an organization. It keeps in mind the principle of least privilege, i.e. users should be able to access only that amount and type of information required by their job. To complement this, RBAC also requires roles and permission to be defined first associated with the ou user needs one of these roles therefore assigning users for each role based on what they might need in different stages so when a new joiner joins we can simply provide him/her all necessary permissions matching their job description without getting confused between those domain bound rising operation scale.

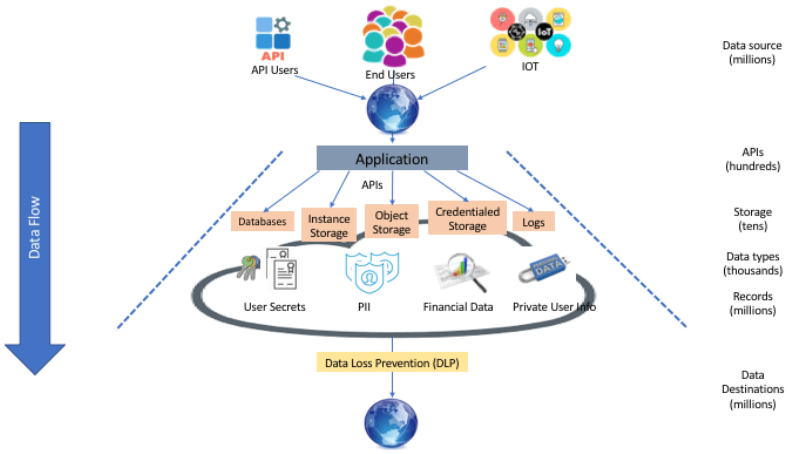

Figure 1: Data Flow and Protection in Cloud Applications: Data Sources, Storage, and DLP Integration

2.3 Data Classification and Policy Enforcement

The previous word of wisdom still holds as the strongest, and simplest way to protect sensitive data by breaking it down into classes with corresponding security. Data classification is the process by which organizations work to understand both how valuable or risky a piece of data may be and then helps them determine what standard security controls need to protect it, in order help protects it properly.

Sensitive Data Identification

Automated tools can be used to identify and categorize sensitive data for organizations. Data classification: Advanced data identification and labeling products that scan your data repositories for these labels or protectively categorize the services based on its policies, tags, content headers (key words header), etc. This is a useful process for organizations to determine where sensitive data lives and how it moves so that they can secure assets accordingly.

Policy Enforcement

Once data classification is complete, organizations can then enforce policies on them. These could be encryption, access controls, data retention policies and blur on fields etc. For effective data privacy, compliance with these policies must be audited and monitored on a regular basis. With the right policy enforcement tools, you can automate their application to apply security policies in a consistent way across your organization.

3. Data Loss Prevention (DLP) Solutions

DLP solutions are designed to prevent data breaches by monitoring, detecting, and blocking sensitive data from being shared or transferred inappropriately. These solutions help organizations enforce data protection policies and prevent accidental or malicious data loss.

3.1 Symantec Data Loss Prevention

Symantec DLP provides comprehensive protection across endpoints, networks, and storage environments. It offers content discovery, monitoring, and policy enforcement capabilities, making it a robust solution for preventing data loss.

Features

- **Content Discovery:** Identifies and classifies sensitive data across the organization.
- **Data Insight:** Provides visibility into data usage patterns and helps identify potential risks.
- **Policy Enforcement:** Blocks or alerts on activities that violate data protection policies.

3.2 McAfee Total Protection for Data Loss Prevention

McAfee DLP offers a centralized management console for administering data protection policies across the organization. It provides granular controls to prevent data loss through various channels such as email, web, and removable media.

Features

- **Unified Management:** Centralized console for policy administration and monitoring.
- **Granular Controls:** Fine-grained controls to prevent data loss across multiple channels.
- **Comprehensive Coverage:** Protects data across endpoints, networks, and cloud environments.

3.3 Forcepoint Data Loss Prevention

Forcepoint DLP leverages behavioral analytics to identify and mitigate insider threats. It integrates with cloud services to extend data protection to cloud environments, ensuring consistent policy enforcement.

Features

- **Behavioral Analytics:** Detects anomalies in user behavior that may indicate data theft or misuse.
- **Cloud Integration:** Extends data protection policies to cloud environments, ensuring consistent enforcement.
- **Policy Enforcement:** Blocks or alerts on activities that violate data protection policies.

3.4 Digital Guardian Data Loss Prevention

Digital Guardian DLP uses agents installed on endpoints to monitor and control data access and transfer. This approach ensures comprehensive visibility and control over sensitive data.

- **Agent-Based Protection:** Monitors and controls data access at the endpoint level, providing detailed insights into data movements.
- **Encryption and Device Control:** Encrypts sensitive data and controls the use of removable media to prevent data exfiltration.
- **Comprehensive Visibility:** Provides detailed insights into data usage and movements, helping organizations identify and mitigate risks.

Figure 2: Effectiveness of Various DLP Solutions

The bar chart compares the effectiveness of various DLP solutions in terms of coverage, policy enforcement, and user satisfaction. This chart helps readers quickly grasp how different solutions measure up against each other, aiding in the selection of an appropriate DLP solution.

4. Challenges

While we have come a long way with Data Loss Prevention (DLP) solutions, and best practices for securing sensitive data in the cloud, there are still challenges that need to be worked around. These are the issues that need to addressed to ensure proper data privacy and security.

4.1 Complexity of CloudgetToken with Separate Environments

Cloud environments are dynamic and distributed, making it extremely difficult to implement and maintain a security policy universally. Cloud environments may consist of public, private and hybrid clouds having

different security needs. Further complicating the protection of data privacy in cloud computing, is this possibility/actuality that responsibility for security falls in a jointly shared domain between customer and CSP (shared responsibility model).

Ultimately, organizations need to understand the different cloud service models (IaaS, PaaS and SaaS) and their resulting security implications. Combining automated security tools, clear policies and continuous monitoring of the environment is crucial to effective manage these environments so all cloud platforms maintain consistent security measures.

4.2 Evolving Threat Landscape

Cyber threats change on a regular basis as new attack vectors and techniques are developed. Cybercriminals are constantly, and rapidly, evolving their methods of attack to outplay the security defenses in place at organizations.

These threats are constantly evolving, so DLP solutions need to be able to respond by adding a layer of advanced threat detection and response. DLP solutions can be further improved thanks to artificial intelligence (AI) and machine learning (ML), which are able to process vast amounts of data, establish noiseless patterns among them, and predict potential threats. These tools assist organizations in spotting anomalies, reacting to incidents live and reducing the damage of data breaches.

4.3 Regulatory Compliance

For many organizations, navigating that increasingly complex landscape of data protection regulations is a considerable challenge in and of itself. Organizations that deal with sensitive data are required to follow regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) or California Consumer Privacy Act(CCPA) with respect to how they collect, store, process and protect this information.

Compliance with these regulations must be sustained through active data protection policy updating and enforcement. Compliance is never static - organizations must keep up to date on regulatory requirements and take action to ensure that they are in continuous compliance. These measures involve performing regular audits, educating employees on data protection requirements and deploying new technologies to assist with regulatory compliance.

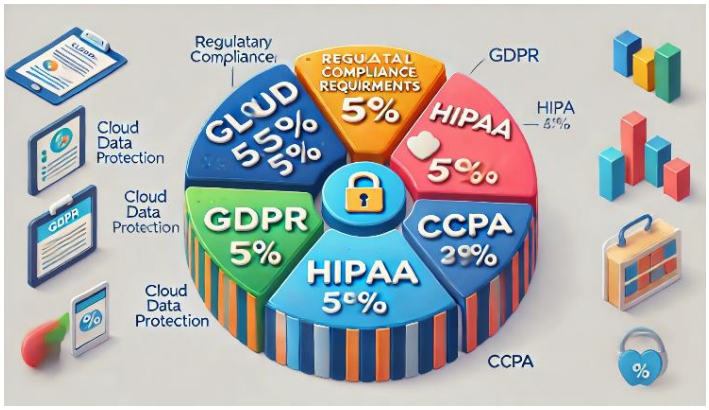

Figure 3: Breakdown of Regulatory Compliance Requirements for Cloud Data Protection

The pie chart shows the breakdown of regulatory compliance requirements, highlighting the percentages for GDPR, HIPAA, and CCPA. This visual aid emphasizes the importance of compliance with multiple regulations and helps organizations prioritize their data protection efforts.

4.4 Integrating Emerging Technologies

Tomorrow, new capabilities are offered in technologies such as blockchain and the Internet of Things (IoT) to better secure data; however, these may introduce more complexity. This includes secure, transparent audit trails using blockchain and compliance-oriented data management platforms. On the other side, integrating blockchain to existing systems and scaling it might not be as easy.

What's more these all are connected to the internet denoting that there is an increased attack surface which results in higher chances of hacking, thus it becomes imperative for security measures as data generated and transmitted by a n number of IoT devices. This work would inform future research on creating security solutions that combine to solve the challenges presented by new technologies in tandem.

5. Future Research Directions

The security community must explore several critical avenues to address emerging issues listed above and better the data-privacy-security nexus diligently in their cloud environments

- **Advanced AI and ML Algorithms:** Innovation in developing more advanced AI and ML algorithms to enhance threat detection, anomaly detection techniques, automation response capabilities of the DLP tools.
- **Blockchain Integration:** Researching the viability of blockchain implementation to filter data safely, verify courses and make regulation more efficient.
- **Security of the IoT:** This would include developing systematic and comprehensive security framework towards ensuring secure communication among data generated by various devices.
- **Cross-Platform Security:** Enable unified security policies and tools that can be consistently applied across multi-cloud, and hybrid cloud environments.

6. Conclusion

Organizations across sectors are focusing on ensuring that sensitive data in their cloud computing environments remain secure; as a result, protecting them has become the top priority. Data privacy and security threats rise with cloud adoption I hope my research has provided some best practices for securing these sensitive organizations data in the cloud and analyzed how well Data Loss Prevention (DLP) solutions prior to July 2020 could protect them.

Strong data encryption, access controls, rapid classification of data collation and monitoring paired with advanced DLP solutions help organizations to a significant extent in building fool proof strategies for protecting their information. These controls reduce the risk of unauthorized access, data breaches and information leakage to keep sensitive data safe.

But, the complexities of cloud environments and shifting threat landscapes makes for ongoing work - not to mention environment-specific challenges in regulatory compliance and emerging tech integration on top. In the future, research based on more advanced AI and ML algorithms should be developed for blockchain integration with IoT security along with cross-platform-security.

No matter how much, but the purpose of this article is to explain how important it is to protect sensitive data inside cloud computing environments. However, organizations must stay watchful and upgrade their security methodologies on an ongoing basis - implementing advanced technologies to keep the data safe. In turn, they foster goodwill and trust with their clientele while shoring up regulatory adherence for the parties of interest on each side.

It emphasizes the need for proactively develop a holistic data privacy and security solution in cloud computing. With the cloud landscape shifting so should our approaches and technologies in securing sensitive data. Persistent research and innovation will help us meet the next-generation threats and make cloud environments even more secure.

References

[1]. Dai, X., Wang, Z., & Zhang, Y. (2013). Data Security and Privacy Protection of Cloud Computing. Advanced Materials Research, 846-847, 1570 - 1573. https://doi.org/10.4028/www.scientific.net/AMR.846-847.1570.

[2]. Gugelmann, D., Studerus, P., Lenders, V., & Ager, B. (2015). Can Content-Based Data Loss Prevention Solutions Prevent Data Leakage in Web Traffic?. IEEE Security & Privacy, 13, 52-59. https://doi.org/10.1109/MSP.2015.88.
[3]. King, N., & Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Comput. Law Secur. Rev., 28, 308-319. https://doi.org/10.1016/J.CLSR.2012.03.003.
[4]. Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, 10. https://doi.org/10.1155/2014/190903.
[5]. Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., & Buyya, R. (2016). Ensuring Security and Privacy Preservation for Cloud Data Services. ACM Computing Surveys (CSUR), 49, 1 - 39. https://doi.org/10.1145/2906153.
[6]. Singh, N., & Singh, A. (2018). Data Privacy Protection Mechanisms in Cloud. Data Science and Engineering, 3, 24-39. https://doi.org/10.1007/s41019-017-0046-0.
[7]. Muhasin, H., Atan, R., Jabar, M., & Abdullah, S. (2018). The Factors Affecting on Managing Sensitive Data in Cloud Computing. Indonesian Journal of Electrical Engineering and Computer Science. https://doi.org/10.11591/IJEECS.V11.I3.PP1168-1175.
[8]. Xiong, J., Li, F., Ma, J., Liu, X., Yao, Z., & Chen, P. (2015). A full lifecycle privacy protection scheme for sensitive data in cloud computing. Peer-to-Peer Networking and Applications, 8, 1025-1037. https://doi.org/10.1007/s12083-014-0295-x.
[9]. Itani, W., Kayssi, A., & Chehab, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 711-716. https://doi.org/10.1109/DASC.2009.139.
[10]. Walia, M., Halgamuge, M., Hettikankanamage, N., & Bellamy, C. (2019). Cloud Computing Security Issues of Sensitive Data. Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing. https://doi.org/10.4018/978-1-5225-7335-7.CH004.
[11]. Sun, P. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. IEEE Access, 7, 147420-147452. https://doi.org/10.1109/ACCESS.2019.2946185.
[12]. Yuan, Z., & Liu, X. (2016). A Survey of Data Security and Privacy Protection in Cloud Computing. https://doi.org/10.2991/MEICI-16.2016.135.