WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Secure & Control Sensitive Data in Cloud Environment

Amol A Wable

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India
amolwable957271@gmail.com

ABSTRACT

Cloud Platform provides on-demand, elastic computing as a utility service, and it is transforming a variety of computer sectors. With the widespread usage of cloud computing to store sensitive information on servers, networks, applications, storage, and services. In today's digital environment, keeping sensitive data safe from theft and susceptibility isn't as simple as locking the file cabinet - especially with the increased adoption of cloud computing. Even if you take every precaution with your online accounts and personal information, there are several ways for that information to get up in the data management systems of another person or firm, making it vulnerable to data theft or data leaks. They don't know where their sensitive data is because they don't have policies in place to categorize it systematically and consistently, and as a result, they don't have controls in place to ensure that all kinds of data are handled effectively. Doing the basics effectively is the best approach to secure sensitive data (like blocking and tackling in football). Understand what data is important, establish rules for managing it, install technical controls to ensure it is handled correctly, and educate your users about their responsibility in data security. This paper covers the difficulties of handling sensitive data and maintaining control over the cloud environment. In order to accommodate the security of sensitive data in a cloud environment, a framework is presented. This study discusses three levels of data classification, encryption, and cloud misuse prevention. The research should result in a validated architecture for securing and controlling sensitive data in the cloud.

INTRODUCTION

Enterprises use 80 different third-party cloud services to collaborate, communicate, develop, manage contracts and HR functions, authorize signatures, and support other business functions that handle and store sensitive data in a cloud environment. Software as a service refers to these types of apps. Organizations are also launching applications and complete businesses on public platforms, infrastructures, and platforms as a service (Infrastructure as a service).

Organizations are also using public platforms (platform as a service) and infrastructures to launch applications and complete enterprises (Infrastructure as a service). By 2020, 76 percent of businesses will be using Amazon Web Servers (AWS) and 63 percent would be using Microsoft Azure. All of these public cloud services are vital and productive, and they even offer a more secure environment than traditional data centers. They do, however, pose distinct dangers to sensitive data processed and stored on these clouds, with the majority of those risks stemming from customer error in the setup and management of those services. Cloud computing systems offer substantial advantages over traditional data processing methods, such as the availability of automated tools to build, connect, configure, and reconfigure virtualized resources on demand. Organizations may simply implement cloud services, making it much easier to accomplish business goals.

The paradigm shift that comes with cloud computing usage is rapidly causing security and privacy concerns about aspects of cloud computing such as multi-tenancy, trust, loss of control, and accountability. As a result, cloud platforms that handle sensitive data must implement technical and organizational safeguards to minimize data security breaches that could result in massive and costly losses. The research on the security and privacy of sensitive data in cloud computing settings is summarized in this publication. We look for new developments in a cloud provider's orchestration, resource control, physical hardware, and cloud service management layers. We also look at the state-of-the-art in privacy-preserving sensitive data approaches for cloud computing, such as privacy threat modeling and privacy-enhancing protocols and solutions.

OVERVIEW OF FINDING SENSITIVE DATA ON THE CLOUD

Gather and classify the data:

Not all cloud-based data is equally sensitive. All of the data must be collected and classified. To give an example, high-risk sensitive data is any information that, if lost or exposed, could result in legal liability or reputational damage to a business. The value and sensitivity of data varies depending on the level of access granted to users and the level of interaction across cloud apps. Create policies for data classification and labeling (confidential, important, sensitive, private, etc.)

Analyze the data:
It's time to evaluate the data now that it's in a manageable context. When searching, it's critical to distinguish between material that is sensitive and data that is necessary but not sensitive. It's also crucial to figure out what information a user needs to keep and what information can be discarded.

Purge the data: After the data has been evaluated, it should be removed from the cloud platform. Once data has been determined as unneeded, a policy should be established for it to be purged. When performing data discovery in the cloud, however, it is critical to keep track of the data that is remediated.

Establish DLP policies:
While pre-built DLP templates cover a wide range of standards for identifying financial data, information security professionals should also construct custom templates that include regular expressions and keywords. Look for a system that uses Optical Character Recognition (OCR) to scan photos for sensitive data like credit card numbers, social security numbers, and other personally identifiable information.

Assess the security situation: Examine and report on the contents of previous file scans, as well as the number of existing non-compliance issues. Following this, the administrator can take corrective action in accordance with the organization's data security policy.

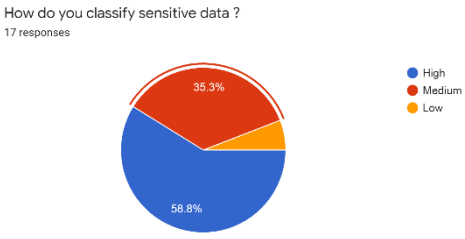
List data discovery scans: To ensure data compliance with GDPR, CCPA, HIPAA, and other regulatory laws, full or incremental cloud data discovery scans should be done on a regular basis. This cloud-based data discovery technique aids in the detection of out-of-compliance data that may be triaged or remedied promptly.

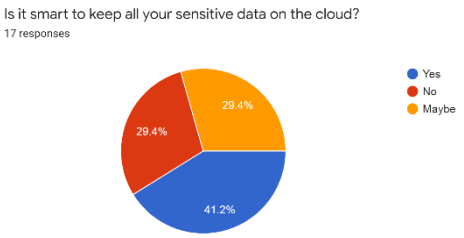
RESEARCH APPROACH

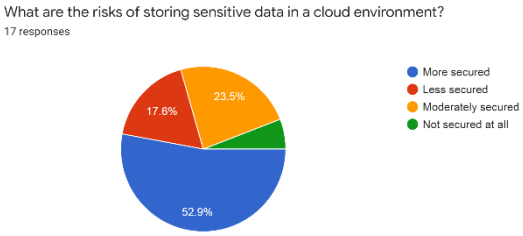
We first performed a survey of individuals using an online form creator and data collection via service chat, collecting data on people's awareness, and then structured the data and conducted experiments on the existing data using prior papers.

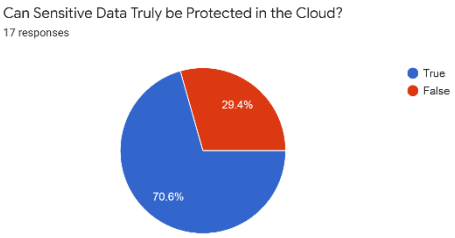
PUBLIC SURVEY
We sent our data collection utility on the survey bot to various people and collected data on many aspects of secure and control sensitive data in cloud environments after establishing our data collection utility on the survey bot.
These are some of the survey's questionnaires that have proven to be useful in my search for results..

Figures and Survey Results









How do you Protect Sensitive Data in the Cloud?

We live in a data-driven era. In one way or another, every organization handles data of varied degrees of complexity; nevertheless, despite the growing importance of data, we are not witnessing a proportionate increase in data security. The frequency of data breaches has climbed by a third, according to the 2021 Data Breach Investigation Report, as organizations migrate to the cloud at a quicker rate as a result of the COVID-19 pandemic. Data security must not take a second seat to productivity or operational agility as more firms return to normal operations.

When it comes to storing data online, enterprises should keep in mind that even if the right processes are in place, a major amount of the data kept in the cloud is not adequately protected by default security safeguards. Developers may leave sensitive material in a public repository in some instances. Because of this potentially serious error, as well as insufficient security controls on internet-hosted databases, sensitive data might be indexed by Google's public search engine, or a database port that permits access to information via a browser could be exposed if not adequately audited.

What strategy & policy can we put in cloud to keep the sensitive data secured?

According to my research, the three principles listed above can help protect sensitive data in the cloud.

Data Classification - Businesses must determine what data must be secured and develop a Data Classification Policy to categorize data according to its sensitivity. Three stages of data classification are required at the very least.

Restricted: This is the most sensitive information that, if hacked, might pose a serious threat. Only those with a need-to-know basis have access.

Confidential or Private: This is information that is moderately sensitive and poses a moderate risk to the firm if it is compromised. The company or department that owns the data controls access.

Public: This is non-sensitive information that, if accessed, would provide little or no harm to the company. Access is either weakly regulated or not at all.

Encryption - Encryption is a broad phrase that refers to a variety of methods for encrypting data. Companies must properly deploy and manage encryption. The use of strong encryption and proper key management are essential components of a successful encryption strategy. Before sharing important information via untrusted networks, encrypt it (Encrypted Email, Encrypted file storage).

Misuse of the Cloud- Saving data in the cloud is the same as storing it on someone else's machine. You don't have control over it once it's there. Before uploading data to the Cloud, encrypt it if it is classified or sensitive. If you're going to share keys with the Cloud provider, be sure you're familiar with their policies. What is their policy on backups? Who has access to your personal information? What is their policy on data breach notification?

Companies can sufficiently safeguard data against today's dangers by first identifying what they're seeking to protect and then devising a strategy to protect each level of data appropriately.

CONCLUSION

With the increased need for cloud storage systems, it's more important than ever to have a server company that can host services for customers connected to the network. Because of advancements in computing, communication, and networking technologies, technology has progressed in this direction. In today's digital environment, keeping sensitive data safe from theft and susceptibility isn't as simple as locking the file cabinet - especially with the increased adoption of cloud computing. Doing the basics effectively is the best approach to secure sensitive data. Understanding what data is sensitive, establishing rules for managing it, implementing technical controls to ensure it is handled properly, and educating your users about their role in keeping it safe are all important steps. This article examined several data security and privacy strategies, with a focus on data storage and use in the cloud, for data protection in cloud computing settings, with the goal of fostering trust between cloud service providers and consumers.

ACKNOWLEGMENT

It brings me great pleasure to offer my research paper on "Secure and Control Sensitive Data in the Cloud." I'd want to offer my heartfelt gratitude to all of the teachers who assisted us during the process. I'd want to express my gratitude for our lecturers' assistance and direction during the presentation of this study work. We owe a debt of gratitude to you, Mr. Head of Department. This appreciation would be incomplete without expressing our gratitude to our excellent Principal, who gave us with the necessary advice, encouragement, and all of the resources we needed to complete this project.

REFERENCES

[1] https://insights.comforte.com

[2] https://www.csoonline.com

[3] https://arxiv.org

[4] https://digitalguardian.com

[5] https://www.sciencedirect.com

[6]Figure and chart