Advanced Software Products Group, Inc. | April 2021

Our Data Is in the Cloud, Now What?

Maintaining Data Security in the Cloud Using MegaCryption

ASPG
Advanced Software Products Group, Inc.

Table of Contents

ABSTRACT

There is an emerging business trend toward migration to cloud computing due to the many benefits offered when compared against traditional privately owned and maintained data centers. However, security concerns are inherent with cloud computing, especially when it comes to transmitting and storing sensitive data. The introduction of data encryption helps solve this problem.

MegaCryption is a data encryption tool from Advanced Software Products Group, Inc. that combines data security, data integrity, and digital signature functionality all in one offering. Further, it is as easily installed on a cloud computing platform as it is onto a mainframe OS, making it an ideal tool to reduce vulnerabilities intrinsic in a cloud computing environment.

PROBLEM STATEMENT

Cloud computing is becoming a popular choice for businesses instead of a private data hub, and therefore concern about the security of their data is crucial. Vulnerable data can be stolen and used nefariously – sold, used for identity theft, or even ransomed back to the business. Additionally, it is often accessible by unauthorized users, which can potentially corrupt its integrity. A business's finances, continuity, and reputation will suffer as a result of data mishandling.

DATA CENTER 101

A data center is the hub of an enterprise's IT operations. Traditionally, it refers to the physical facility that houses all of the equipment necessary for data storage, data transmission, and data processing. It also includes the employees who utilize, maintain, and update equipment and data. While a private data center is appealing for many reasons, the cost to design, build and maintain one is often too high a financial burden for small-, or even medium-sized companies.

DATA CENTER VS. CLOUD COMPUTING SERVICE

The price tag required for a company's private data center adds up fast. Initially, there's an investment of IT equipment, and peripherals – miles of cables to connect and power the hardware, and racks to hold the servers and storage arrays. All this needs to be housed in properly-located (and often specially built) real estate, complete with manufacturer-recommended environmental controls installed, including but certainly not limited to fire suppression and backup power systems. To all of this add the IT professionals needed to design and build it to a business's precise specifications, and perhaps an in-house IT expert to maintain and update the data hub, and who will also need to safeguard the security of the data itself, and you have the basic ingredients for a private data center.

The list of capital expenditures merely begins with what's listed above - it ends with whatever else a business or organization requires to build and maintain a data center that meets their immediate and future needs. These high costs suggest that a private data center may not be a viable option for many businesses.

CLOUD COMPUTING 101

Cloud computing is a term generally used to describe data centers available to many users via the Internet. These online data centers avail users to resources such as data storage and computing power, but are managed by cloud service providers rather than the users themselves. In a nutshell, it is a virtual computing infrastructure, and is thus an ideal replacement of the traditional private data center.

Cloud service providers offer on-demand the entire infrastructure necessary to create, customize (and re-customize as needed in a just few clicks), and utilize the equivalent of a company's private data center. They also supply the technicians who maintain, protect, and update the infrastructure. Therefore, cloud computing is becoming more widely recognized as an option that lowers capital expenditures while providing approximately the same services as a private data center.

CLOUD SERVICE PROVIDER OFFERINGS

Every business has specific needs to be addressed in the customization of an in-house data center. Knowing this, cloud providers offer different platforms to meet different utilization needs. The service platforms generally used are:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Cloud service customers also choose which developmental model best fits their business's computing, storage, and transmission needs, and these are:

- Private Cloud, a single tenancy cloud service,
- Public Cloud, a multi-tenancy cloud service, and
- Hybrid Cloud, a combination of Private and Public cloud use.

Because cloud implementations typically rely heavily on virtualization, they offer clients economy of scale, ease of configuration, and a high degree of portability. In addition, virtualized environments allow cloud service providers to offer a dynamic setting capable of scaling to satisfy their clients' changing needs. Cloud providers maintain the infrastructure, so a company can allocate funds that it otherwise would have spent on building and maintaining a private data center to costs related to its actual endeavor. It also allows for its employees' focus and time to be centered back on its own business.

Upon considering the multiple service options and deployment models available, a sizeable reduction in capital expenditure, and an ability to be up and running in just a few clicks, it is easy to see why cloud computing has become a popular choice for many organizations. It is no surprise that the research firm Gartner Peer Insights predicts that 80% of enterprises will have closed their traditional on-premise data centers by 2025 in favor of cloud computing.

CLOUD COMPUTING – THE ELEPHANT IN THE ROOM

While the benefits of cloud computing are many, it also brings to the table new security challenges. Per Eugene Schultz, chief technology officer at Emagined Security, "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into."

One of these holes is the potential for data from many companies to be stored on servers used by cloud providers, opening the door for hackers to steal a vast amount of sensitive information in a single attack, called hyperjacking. Beyond hacking and hyperjacking, according to the Cloud Security Alliance, the top three threats in the cloud are insecure interfaces and APIs, data loss and leakage, and hardware failure requiring disaster recovery. Another security challenge occurs when cloud service technicians accidentally or deliberately alter or delete data. Hence, data security is the primary concern with cloud computing.

Cloud service providers are only responsible for the security of the cloud infrastructure. The tenant remains responsible for the security of their data. For example, in the IBM Cloud, where there are varying degrees of shared responsibility for the protection and maintenance of applications, runtime, middleware, O/S, virtualization, servers, storage, and networking, only data security is the sole responsibility of the client across every cloud service model offered.

THE IMPORTANCE OF DATA SECURITY

Data security refers to both the practice of putting in place safeguards to protect an enterprise's sensitive data, such as financial records or the personal information of employees or customers, and to the physical and technological safeguards themselves. One method for evaluating and reducing the risk that comes with storing or moving any data has three core elements:

- **C**onfidentiality, which ensures data is accessed only by authorized individuals,
- **I**ntegrity, which ensures that data is reliable and accurate, and
- **A**vailability, which ensures that data is available and accessible when needed.

Known as the CIA Triad, this is a security model and guide used by businesses and organizations to protect their sensitive data from theft or unauthorized access, and it is an excellent example of a business protocol for data security.

Company data is a valuable asset. It is created, collected, transformed, stored, and exchanged daily. Because of its value, it is vulnerable to DOS attacks, malware injection, database invasions, theft, corruption, and ransomware attacks, to name just a few. However, the consequences of lax data security practices do not end with the act of theft or the corruption of the integrity of sensitive data. The damage to a business from an attack on or mishandling of their data also include reputation damage, the disintegration of consumer confidence, brand erosion, and even costly fines and litigations.

Fortunately, many mitigating strategies exist that a company may employ to enhance its data security. These include, but are certainly not limited to:

- Authentication to verify if a user's credentials match those stored in the company's database (i.e., passwords, PINs, security tokens, swipe cards, and biometrics),
- Discretionary, role-based, or mandatory access control,
- Backups and recovery,
- Encryption,

- Data masking,
- Tokenization,
- Deletions and erasure to permanently remove or archive data that is no longer required.

Of these, many cloud computing, data security, and IT experts agree that there is, “no better way to secure critical data than through cryptography – especially when that data is stored in the cloud,” (Tom Field, Senior Vice President, Editorial, Information Security Media Group) and that, “information in motion and information at rest are best protected by cryptographic security measures.” (Ralph Spencer Poore, Chief Cryptologist for Cryptographic Assurance Services LLC)

Additionally, IBM writes about data center security, “logical security controls should include data encryption.” Nate Lord states, “Companies should implement data security solutions that provide consistent protection of sensitive data, including cloud data protection through encryption and cryptographic key management.” Finally, in her blog article The Importance of Data Encryption in Cyber Security, Lucy Manole mentions that sensitive and valuable information must be protected by data encryption.

CRYPTOGRAPHY AND THE CLOUD

Data encryption is the mathematical transformation of data utilizing various algorithms to convert the information to unreadable ciphertext. Decryption (reverse transformation) is possible only with the use of keys available only to authorized users.

Because the encrypted data is gibberish, its confidentiality is protected, rendering its theft a useless endeavor. The requirement of keys ensures the prevention of unauthorized access, and therefore the integrity of the encrypted data is assured. Cryptography is a vital tool for any business wishing to avoid data loss, damage to its reputation, lawsuits from compromised customers, and fines for not maintaining governmental regulations regarding encryption and data security.

CONCLUSION

Cloud computing is becoming more popular with companies and organizations of all sizes and business types. Paths through the cloud may not be secure, and cloud storage may be used by multiple clients, creating issues with data security. By all accounts, data encryption helps solve the problem of insecure data at rest (stored data) or in transit (data exchanged between databases, mobile devices, and the cloud) by rendering it useless to potential thieves and inaccessible to, and therefore incorruptible by, unauthorized users. Use of cryptographic functions such as encryption, decryption, key management, and signature processing represent a highly effective approach for protecting a critical business asset – data.

MegaCryption is an industry-leading encryption tool specifically designed to keep data secure. Using both symmetric and asymmetric algorithms, MegaCryption makes unauthorized access to the data impossible, maintaining its integrity. It utilizes both private and public key infrastructure options, a wide variety of cryptographic algorithms, and compliance with widely recognized crypto techniques and standards. MegaCryption runs on many platforms including z/OS, Linux, UNIX, and Windows.   Such compatibility is essential for organizations competing in a global marketplace. It's also a valuable tool for a company faced with disaster recovery. With its many features and timely updates that meet, and exceed, industry standards, MegaCryption provides a simple, effective solution to a complicated problem.

References

1. IBM Cloud Education. "Data Centers." *IBM Cloud Learn Hub,* www.ibm.com/cloud/learn/data-centers, January 24, 2020. Accessed February 3, 2021.
2. Khan, Shafat. "Cloud Computing Paradigm: A realistic option for the Business Organizations – A study." *Journal of Multi Disciplinary Engineering Technologies,* Vol. 12, Issue 2, December 2018.
3. "Cloud Computing." *Wikipedia: The Free Encyclopedia*. en.wikipedia.org/wiki/Cloud_computing Wikimedia Foundation, Inc. 22 July 2004. Web. 10 Aug. 2004. Accessed February 3, 2021.
4. Odin-Ayo, O. Ajayi and C. Okereke. "Virtualization in Cloud Computing: Developments and Trends." *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS),* Jammu, 2017, pp. 24 – 28, doi: 10.1109/ICNGCIS.2017.10.
5. Moore, Susan. "The Data Center Is (Almost) Dead." *Smarter With Gartner,* www.gartner.com/smarterwith gartner/the-data-center-is-almost-dead/, August 5, 2019. Accessed February 4, 2021.
6. DeGroot, Juliana. "What is Data Security?" *Digital Guardian, Data Protection 101,* www.digitalguardian.com/blog/what-data-security, December 10, 2020. Accessed February 4, 2021.
7. Looker Data Sciences, Inc. "Data Security." *Looker.com Definition,* www.looker.com/definitions/data-security Accessed February 4, 2021.
8. BuckBee, Michael. "Data Security: Definition, Explanation and Guide." *Inside Out Security Blog, Data Security*, www.varonis.com/blog/data-security/, Updated January 29, 2021. Accessed February 18, 2021.
9. Lord, Nate. "Cryptography in the Cloud: Securing Cloud Data with Encryption." *Digital Guardian, Data Protection 101,* www.digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption, September 11, 2018. Accessed February 3, 2021.
10. Manole, Lucy. "The Importance of Data Encryption in Cyber Security." *HAKIN9 Blog,* www.hakin9.org/the-importance-of-data-encryption-in-cybersecurity/, August 28, 2019. Accessed February 4, 2021.
11. Field, Tom. "Cryptography in the Cloud." *Bank Info Security,* www.bankinfosecurity.com/cryptography-in-cloud-a-3305/op-1, January 28, 2011. Accessed February 3, 2021.
12. Reich, Jeff. "Overcoming Fear of the Cloud." *Bank Info Security,* www.bankinfosecurity.com/interviews/overcoming-fear-cloud-i-738, September 22, 2010. Accessed February 3, 2021.
13. Arora, Rachna and Parashar, Anshu. "Secure User Data in Cloud Computing Using Encryption Algorithms." *International Journal of Engineering Research and Applications (IJERA),* Vol 3, Issue 4, Jul – Aug 2013, pp. 1922 – 1926.
14. IBM Corporation. "Cloud-native security practices in IBM Cloud." www.ibm.com/cloud/architecture/files/ibm-cloud-security-white-paper.pdf, Copyright IBM Corporation 2019, 2020. Accessed February 25, 2021.

15. IBM Global Solutions. "MegaCryption." *Business Partner Application Showcase IBM PartnerWorld Global Solutions Directory,* www-356.ibm.com/partnerworld/gsd/solutiondetails.do?solution=3287&lc=en&stateCd=P&tab=2. Accessed February 3, 2021.
16. AIT News Desk. "MegaCryption 6.5.0: Optimized Compression and Authentication Features Added to z/OS Cryptographic Toolkit." *AIT News Desk,* *www.aithority.com/security/megacryption-6-5-0-optimized-compression-and-authentication-features-added-to-z-os--cryptographic-toolkit/*, June 8, 2020. Accessed February 28, 2021.