INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 04th Apr 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=Issue4

10.48047/IJIEMR/V10/ISSUE 04/125

Title **Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats**

Volume 10, ISSUE 4, Pages: 630-632

Paper Authors **1ShivaDutt Jangampeta,2Sukender Reddy Mallreddy,3Jaipal Reddy Padamati**

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats

[1]ShivaDutt Jangampeta, [2]Sukender Reddy Mallreddy, [3]Jaipal Reddy Padamati

[1]VicePresident, JPMorgan Chase, Dallas,USA, shivadutt87@gmail.com

[2]Salesforce Consultant, City Of Dallas, Dallas, USA, sukender23@gmail.com

[3]Senior Software Engineer, Comcast, Dallas, USA, padamatijaipalreddy@gmail.com

Abstracts

This review explains the various reasons for security data; to secure intellectual property rights (IPR), integrity, confidentiality, licenses, social partnership, distributed trust and building prestige. Also, the post reviews some of the most common data security risks and best practices of preventing them. These data security best practices are meant to manage data in accordance with established restrictions and maintain different data infrastructure requirements. Data security should be executed in every element of a data system because it can only take one loose link to break a secure chain.

Keywords – Data security, Data Infrastructure, Data System, Cyber Threat.

I. Introduction

There are many reasons for protecting data and data systems, ranging from the obvious ones, such as securing intellectual property rights, licenses, integrity, confidentiality, et al. to others expected to pop up in the future, including social partnership, distributed trust, and building prestige. Data systems should manage/handle data based on some established "restrictions" while maintaining other system requirements like data availability, scalability, provenience, and interoperability; and need to be protected from potential attacks. "Data security" comprises different technical and organizational facets of data infrastructures, such as physical access, policies, regulations, etc. It should be executed in every element of a data system because it only takes one loose link to break a secure chain [1]. However, whereas the definition of the "data security composition" may vary with the needs of different communities, an all-inclusive data infrastructure combines all the security facets of all communities.

A. What's Data Security?

Data security is a process/technique of protecting digital information from unintentional loss, alteration, divulgence, damage, corruption, and/or theft all around its whole life cycle. It covers virtually all data infrastructures, including hardware, software, consumer devices, and data storage systems; access, administrative, and supervisory controls; and enterprises' policies and processes. It incorporates tools and technologies to bolster the visibility of an organization's data and its utility [2]. These solutions adopt various techniques such as data encryption, masking, and redaction to safeguard data [1]. Data security helps businesses refine their auditing methodologies and abide by progressively strict data protection statutes.

B. Significance of Data Security

Enterprises are legally required to safeguard their corporate and consumers' data from accidental loss, manipulation, or falling into the wrong hands that may result in hefty financial losses, legal implications, and/or business closure [1]. As such, state and industry regulators, like the EU's General Data Protection Regulation (GDPR), Federal Risk and Authorization Management Program (FedRAMP), ISO 27001, Payment Card Industry Data Security Standard (PCI DSS), Gramm Leach Bliley Act (GLBA), National Institute of Standards and Technology (NIST), Health Insurance Portability and Accountability Act (HIPAA), etc. outline companies' obligations to secure data [3].

Owing to the objective of this review, the purpose of data security can be grouped into three categories: (1) Business Continuity, (2) Incident Handling, and (3) Authentication, Authorization, and Accounting (AAA).

(1) *Business Continuity*

Business continuity is guaranteed by the most obvious IT best practices. It comprises measures to ease and secure system operations, like data loss protection, incident recovery, and systemized data infrastructure procedures such as access control and rules governing access.

(2) *Incident Handling*

Incident handling comprises measures to prevent and mitigate losses like event analysis to learn about enhanced security procedures [3]. It requires well-structured knowledge and expertise such as contemporary considerations about complex distributed computing – often gained through handling a series of security incidents. As technologies and procedures around attack mitigation are constantly evolving, security pundits should have adequate expertise to successfully execute their jobs.

(3) *Authentication, Authorization, and Accounting (AAA)*

Authentication, Authorization, and Accounting (AAA) comprises measures to set users' rights to access organizations' data resources, detailing how and when those rights apply. Authentication is the technology/process that enables/requires entities (mostly human users) to correctly identify themselves, in terms of their exact attributes. Authorization is the establishment of rights (approval) of such users to carry out certain operations on a particular resource. Accounting gathers information about approved and declined access requests by users, and records the login details provided by users.

II. Data Security Risks and Challenges

According to the Economist [4], is no longer the globe's most valuable resource but data. However, compared to oil, data is harder to safeguard and easier to steal. Besides, data presents lucrative opportunities to not only entrepreneurs but also bad actors.

Lately, securing data has become undeniably hard for many businesses. Enterprises are facing a variety of threats, including insider threats (negligent, compromised, malicious, and malicious people), misconfigurations, and third-party risks:

a) *Insider Threats:*

End users, whether present or former staff members, subcontractors, or third-party business partners are some of the major threats to enterprise data security. Disgruntled and malicious insiders can misuse access rights to manipulate, steal, or damage data to satisfy their selfish interests in making profits.

Unintentional threats like a simple click on a phishing email could result in leakage of the user's credentials or the installation of malware or ransomware on the organization's computer system, leading to costly data breaches.

Negligence can lead to the accidental divulgence of valuable information. For example, an employee might send sensitive information to hackers or upload confidential files to unprotected cloud providers.

b) *Technical Misconfigurations*

Accidental divulgence of sensitive information may occur as a result of technical misconfigurations in cloud-based data systems.

c) Third-Party Risk

Vulnerable third-party data systems pose a significant risk to any organization. For instance, the infamous SolarWinds attack that occurred in 2020 enabled hackers to penetrate the vendor's client's networks [5].

III. Data Security Best Practices

To effectively mitigate the abovementioned risks, businesses should follow set data security best practices. IT pundits recommend tools, techniques, and solutions like:

- *Access Control:* This restricts who can read, modify, share, or delete data.
- *Data Backup:* A data backup is akin to an "insurance policy" in business. It helps a company recover data in case it is altered, corrupted, stolen, or deleted.
- *Data Encryption:* Security experts term it "a non-negotiable affair" for sensitive information whether at rest, in transit, or being used.

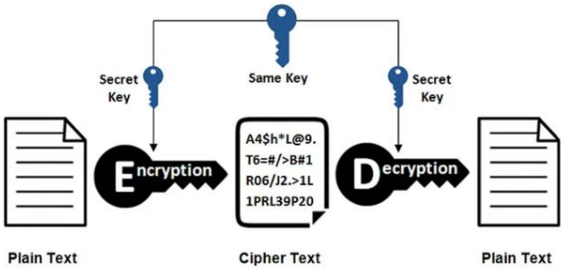

Fig. 1. Data encryption technique

- *Data Masking:* this involves substituting sensitive, valuable data with fake data when sharing information with certain users.
- *Database Security:* IT teams should ensure the organization's databases are impenetrable by hackers. They should enforce the "principle of least privilege," perform frequent access reviews, and constantly monitor database activity.
- *Endpoint Security:* some data security professionals focus majorly on network security while ignoring their endpoint devices or securing them with simple anti-malware solutions. Instead, IT experts should ensure all the endpoint devices connected to the company network are monitored to detect end-user attacks using next-gen solutions [6].

IV. Conclusion

With the immensely increasing volumes of valuable, sensitive digital data being used, stored, and transmitted via vulnerable systems, data security is becoming exceedingly critical to secure digital information from alteration, unauthorized access, theft, or damage. As such, businesses should implement proper data security controls/measures to protect valuable data.

References

[1] Foster, I. , Grid Computing: Making the Global Infrastructure a Reality. The Grid: A New Infrastructure for 21st Century Science. In Berman, F., Fox, G., & Hey, T., John Wiley & Sons, 2003.

[2] R. Perlman, An overview of PKI trust models. IEEE Network 6, pp 38-43., 1999.

[3] Jøsang, A. & Pope, S. , User-Centric Identity Management. AusCERT Conference., 2005.

[4] The Economist, The world's most valuable resource is no longer oil, but data., 2017.

[5] L. Constantin, SolarWinds attack explained: And why it was so hard to detect, News Analysis., 2020.

[6] Fortra's Alert Logic,, The Top Data Security Best Practices to Protect Against a Successful Breach, 2017.