International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019, ISSN No: 2348-9510

UNVEILING THE POWER OF DATA MASKING: SAFEGUARDING SENSITIVE INFORMATION IN THE DIGITAL AGE

Pavan Navandar
Independent Researcher

Abstract

Data masking, often referred to as data obfuscation or pseudonymization, is a crucial technique in ensuring the privacy and security of sensitive information. This white paper explores the fundamentals of data masking, its techniques, applications across various industries, benefits, challenges, and best practices. It aims to provide a comprehensive understanding of data masking and its role in safeguarding data privacy and security.

I. INTRODUCTION

In today's data-driven world, organizations collect, process, and store vast amounts of data, including sensitive information such as personally identifiable information (PII), financial data, and intellectual property. However, with the increasing frequency and sophistication of cyber threats, protecting this data from unauthorized access and misuse has become a paramount concern.

Data masking is a technique used to protect sensitive data by replacing it with fictitious, but realistic, data while maintaining its usability for various purposes such as application development, testing, and analytics. By concealing sensitive information, data masking helps organizations mitigate the risk of data breaches, comply with regulatory requirements, and uphold customer trust.

II. TECHNIQUES OF DATA MASKING

Data masking employs various techniques to conceal sensitive information effectively. These techniques Replacing sensitive data with fictitious but similar-looking data, Rearranging the order of sensitive data records to maintain referential integrity, Applying predefined masking formats such as randomization, tokenization, or encryption, introducing random noise to numerical data to obfuscate its original values, removing or obscuring sensitive data entirely from documents or records, the selection of a data masking technique depends on factors such as data sensitivity, regulatory requirements, and the intended use of the masked data.

III. APPLICATIONS OF DATA MASKING

Data masking finds applications across various industries and business functions, protecting patient health records and complying with HIPAA regulations, Securing financial transactions and adhering to PCI DSS standards, Safeguarding customer information and preserving consumer privacy, Masking sensitive data in development and testing environments to prevent data exposure, Concealing sensitive information while performing data analysis to ensure privacy and confidentiality.

IV. BENEFITS OF DATA MASKING

Implementing data masking offers several benefits to organizations, including:
Enhanced Data Privacy: Protecting sensitive information from unauthorized access and data breaches., Meeting regulatory requirements such as GDPR, HIPAA, and CCPA.
Enabling the use of realistic data for development, testing, and analytics without exposing sensitive information, Cost Savings along with reducing the risk of non-compliance fines, legal penalties, and reputational damage associated with data breaches, Trust: Building trust with customers by demonstrating a commitment to protecting their privacy and confidentiality.

V. CHALLENGES IN IMPLEMENTING DATA MASKING

Despite its benefits, implementing data masking poses several challenges, including
Dealing with diverse data types, formats, and structures across multiple systems and platforms, Balancing data security requirements with performance considerations, especially in real-time processing environments, Ensuring the usability and integrity of masked data for various applications and analytical purposes, adapting data masking strategies to keep pace with evolving regulatory landscapes and compliance requirements.
Insider Threats with mitigating the risk of insider threats and unauthorized access to masked data by privileged users.

VI. BEST PRACTICES FOR DATA MASKING

To overcome these challenges and maximize the effectiveness of data masking, organizations should adhere to the following best practices:
Data Discovery and Classification: Identify and classify sensitive data to prioritize masking efforts and ensure comprehensive coverage, develop a masking strategy tailored to the organization's specific requirements, considering data sensitivity, regulatory mandates, and business objectives, implement robust data governance policies and procedures to maintain data quality, integrity, and security throughout the masking process. Regularly monitor and audit data masking activities to detect anomalies, unauthorized access attempts, and compliance violations, foster collaboration between data security, compliance, and business stakeholders to align data masking initiatives with organizational goals and priorities.

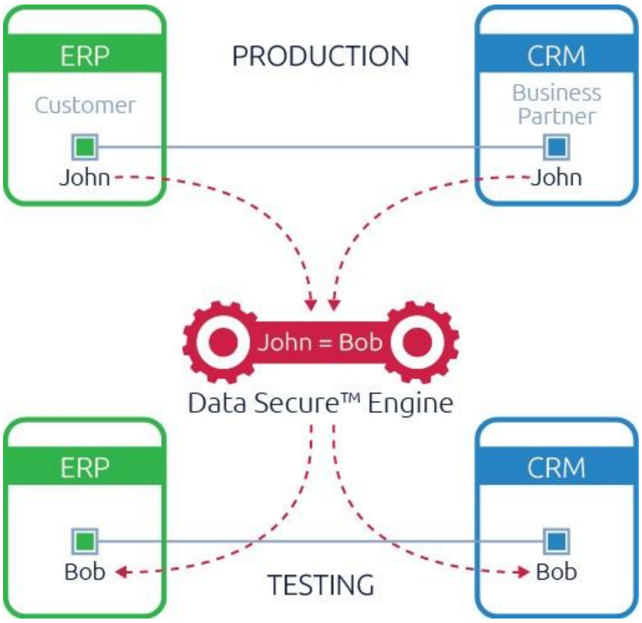
VII. FUTURE TRENDS IN DATA MASKING

Looking ahead, several trends are expected to shape the future of data masking, Adoption of Advanced Masking Techniques: The emergence of advanced masking techniques such as differential privacy and homomorphic encryption to enhance data privacy and security. Integration with Leveraging AI and machine learning algorithms to automate data masking processes, improve accuracy, and adapt to evolving threats. Increased adoption of cloud-native data masking solutions to address scalability, flexibility, and cost-efficiency requirements. Growing demand for privacy-preserving technologies that enable secure data sharing and collaborative analytics without compromising confidentiality.

VIII. CASE STUDIES

Several organizations have successfully implemented data masking to safeguard sensitive information and achieve regulatory compliance. Case studies highlighting these implementations demonstrate the effectiveness of data masking in real-world scenarios across various industries.
Data masking with pre-defined masking rules and empowers organizations to customize rules to scramble any non-key field on any client-dependent SAP table in a number of different ways (e.g. replace with data from mapping-table, replace with constant value, clear a field). These rules can be extended to cover more specific security needs relevant to an organization's business.

Data masking enables companies to comply with all well-known data protection standards such as Sarbanes Oxley, the UK/EU Data Protection Act (DPA), the BDSG (Bundesdatenschutzgesetz), and even the Payment Card Industry Data Security Standard.



How to implement a data security policy across your non-production SAP landscape. This usually commences with a workshop for training on Data Secure. The business units and functional teams identify the tables and data that need to be scrambled, then define profiles and create rules. The Basis team then takes charge of the technical implementation for Basis teams and security teams to do mass scrambling.

IX. CONCLUSION

In conclusion, data masking is a critical component of data privacy and security strategies, helping organizations protect sensitive information from unauthorized access and misuse. By employing effective masking techniques, adhering to best practices, and staying abreast of regulatory requirements and technological advancements, organizations can mitigate the risk of data breaches, achieve regulatory compliance, and preserve customer trust in an increasingly data-centric world.

REFERENCES

[1] Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security Survey 2015, September 30, 2014

PricewaterhouseCoopers, http://www.pwc.com/gx/en/consultingservices/information-security-survey/assets/the-global-state-of-informationsecurity-survey-2015.pdf

[2] NIST Cybersecurity Practice Guide, SP-1800-3: “Attribute Based Access Control,” NIST, https://nccoe.nist.gov/library/nist-sp-1800-3-attribute-based-access-controlpractice-guide

[3] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1, http://www.nist.gov/cyberframework/upload/cybersecurityframework-021214.pdf

[4] EMV Payment Tokenization Specification – Technical Framework, Version 1.0, March 2013, EMVCo, LLC, https://www.emvco.com/specifications.aspx?id=263

[5] EMV and Encryption + Tokenization: A Layered Approach to Security, A First Data White Paper, 2012, First Data, http://www.firstdata.com/downloads/thoughtleadership/EMV-Encrypt-Tokenization-WP.PDF

[6] What Every Card Not Present Merchant Should Know, Navigating Today’s Challenging Payments Ecosystem, 2014, Verifi Inc, http://www.verifi.com/wpcontent/uploads/2014/05/Verifi_eBook_web_noCNP.pdf

[7] Visa Best Practices for Tokenization Version 1.0, July 14, 2010, Visa Inc, https://www.visa-asia.com/ap/sg/merchants/include/ais_bp_tokenization.pdf

[8] Information Supplement: PCI DSS Tokenization Guidelines Version 2.0, August 2011, Scoping SIG, Tokenization Taskforce, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

[9] Tokenization Product Security Guidelines – Irreversible and Reversible Tokens Version 1.0, April 2015, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

[10] Implement Data Masking to Protect Sensitive Data: Part 1, Biswajit Maji, IBM, http://www.ibmbigdatahub.com/blog/implement-data-maskingprotect-sensitive-data-part-1

[11] Implement Data Masking to Protect Sensitive Data: Part 2, January 9, 2015, Biswajit Maji, IBM, http://www.ibmbigdatahub.com/blog/implement-data-maskingprotect-sensitive-data-part-2

[12] Data Masking Best Practice, an Oracle White Paper, June 2013, Oracle Corporation, http://www.oracle.com/us/products/database/data-masking-best-practices161213.pdf

[13] Security is Not Just External - Don't Forget the "Other" Security, http://www.securityweek.com/security-not-just-external-dont-forget-other-security, [Accessed on 08/03/2015].

[14] S. Schober, Real cost of data breaches still on the rise, http://www.cutimes.com/2015/03/01/real-costsof-data-breaches-still-on-the-rise

[15] W. Long, EU Data Protection Regulation: fines up to €100m proposed, http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed

[16] L. Whitfield, ICO spells out £500,000 penalty plans, http://www.ehi.co.uk/news/EHI/5542/ico-spells-out%C2%A3500000-penalty-plans [Accessed on 03/03/2015].

[17] R. Mckeane, EU data protection reform: 12 things businesses need to know, http://www.theguardian.com/media-network/olswang-partner-zone/2014/dec/04/eu-data-protectionreform-business-fines

[18] D. Worth, Target takes $162m hit from cyber-attack data breach, http://www.privacyrisksadvisors.com/news/target-takes-162m-hit-from-cyber-attack-data-breach-by-danworth

[20] Ponemon Institute, The State of Data-Centric Security, http://www.banktech.com/pdf_whitepapers/incoming/1411503329_ponemon_infa_security.pdf

[21] M. Greenway, Data Obfuscation - managing data privacy in development and test environments.

[22] Gartner, Magic Quadrant for Data Masking Technology, https://www.gartner.com/doc/2636081/magic-quadrant-data-masking-