Managing Data Protection and Privacy on Cloud

Satyavathi Divadari, J Surya Prasad and Prasad Honavalli

September 25, 2024

Managing data protection and privacy on cloud [1]

Satyavathi Divadari [1], Dr. Surya Prasad J [2], Prasad Honnavalli [3]

[1] CyberRes - A Micro Focus Line of Business
PES University,
Bangalore, India
satyavathi.d@gmail.com

[2] PES University,
Bangalore, India
surya@pes.edu

[3] PES University,
Bangalore, India
prasadhhb@pes.edu

Abstract: When pandemic rose in 2020, people were fighting against Covid-19 virus and organizations had accelerated their digitization and cloud adoption rapidly [1] to meet the online based business during the lockdown. This chaos helped fraudsters and attackers taking advantage of the momentary lack of security controls and oversight. Federal Investigation Bureau (FBI) Internet Crime Compliant Center (IC3) 2020 reported highest number of complaints in 2020 (791k+) compared to prior five years (298k+ in 2016), with peak losses reported ($4.2 Billion in 2020 compared to $1.5 Billion in 2016) [2]. Majority of these incidents were connected to financial fraud, identity fraud, and phishing for Personally Identifiable Information (PII).

Considering the severity and impact of personal data exposure over cloud and hybrid environment, this paper provides a brief overview of prior research and discuss technical solutions to protect data across heterogeneous environments and ensure privacy regulations.

Keywords: Multi-Cloud, Hybrid-Cloud, Cyber Security, Data Privacy, Data Breaches, Encryption, Data Governance, Data Discovery, Tokenization, Blockchain, Format Preserving Encryption, Regulations, Covid-19, Pandemic

1. Introduction

With the increased Cloud adoption by organizations, Data proliferation is greater than ever with the low-cost availability of advanced compute and storage and always-on high-speed networks. Given such a large accumulation of data, sensitive and confidential information is getting added to the pile.

Protection of personally identifiable information (PII), and sensitive personal information (SPI) against leakage or exposure is essential for people who own the data as well as the organizations that are its custodians.

1.1 Impact of Data Leakage on Individuals

With the digitally scalable, always-on, and reliable cloud-based infrastructure, data is heavily accumulated on single place, hackers and other adversaries are breaching it, collecting the data, and trading it. The data includes patient health information, and financial information, and other identity linked data on dark web [3] [4]. Financial institutions and insurance organizations use such data procured from authorized agents to decide on insurance policy issuance or sanctioning personal loans. While such claims sound like a science fiction movie to some, there are numerous proof points that confirm it is true. Figure 1.1 indicates an example of data monetization on dark web [4]

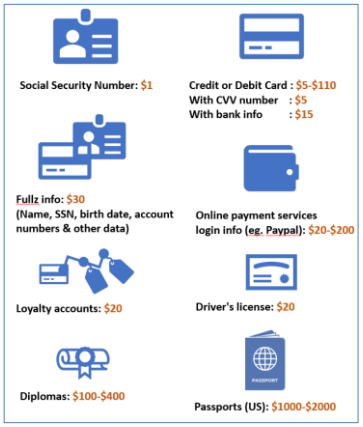

Figure 1.1: Cost of leaked data on dark web

1.2 Impact of Data Leakage on Organizations

With the continued threat of hackers and data exposure, Government and regulatory authorities across the world strengthened the data protection laws, that include European Global Data Protection Regulations (GDPR), California Consumer Privacy Act (CCPA), Personal Data Protection Bill (PCPB), and The Health Insurance Portability and Accountability Act (HIPAA). FTC enforced $5 Billion penalty and extended privacy restrictions on Facebook [5] in a historic resolution with a highest penalty as of 2019, and substantially strong obligations on organizations to enhance accountability of protecting data security and preserving end user privacy.

This case and similar instances demonstrate that enterprises are accountable to maintain strong security protection mechanisms and data privacy enforcement to maintain compliance with the regulatory requirements and stay abreast of continued cyber-attacks.

Data Discovery and Protection Methods

Organizations implement numerous safeguards and controls to discover and protect sensitive data against various types of cyber threats on the expanded threat landscape that include on-premise, cloud, hybrid cloud, or multi-cloud.

2.1 Data Discovery

2.1.1 Identification of Sensitive Information

Deployment of privacy and security controls to comply with legislation begins with the identification of sensitive data that is being collected and processed across the enterprise.

In a simple excel or a database like the one in Figure 2.1, it is easy to classify different fields as personal information (PII) or as sensitive personal information based on the standard definition of PII.

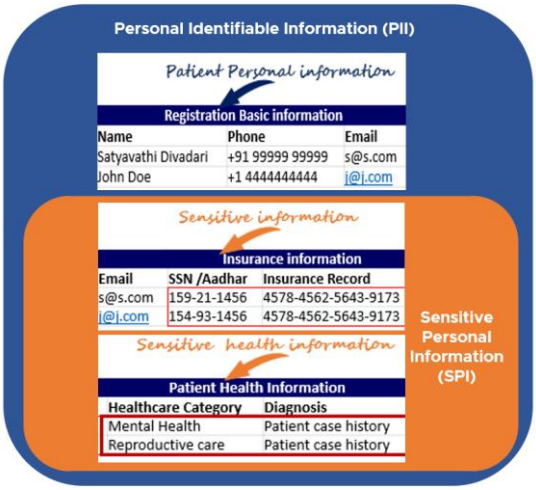

Figure 2.1: Example of Data Classification

With the heaps of data being collected across cloud, and on-premises data centers, customer, and third-party storage, identifying and classifying critical and sensitive information is a complex challenge to handle. Unless one knows the data type/content, it is difficult to protect.

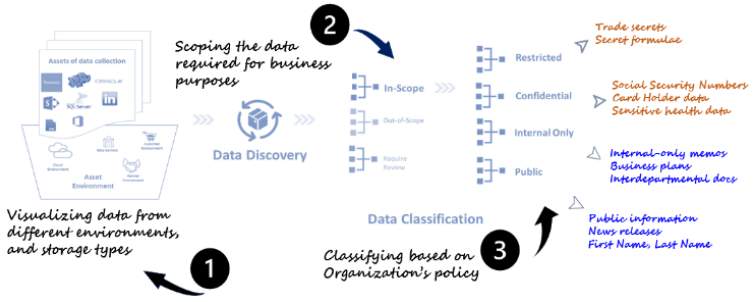

Figure 2.1.1: Data Discovery across different environments

The above complexities can be handled by a centralized data governance solution that supports three key requirements, as shown in figure 2.1.1.

1. Visualize data elements on several heterogeneous storages located on-premise, cloud, and external environments to know and identify the critical data assets from others. Centralized data asset awareness is the key to protection and oversight.

2. Analyzing, and scoping in the information relevant to current business requirements helps in reducing the cost of storage by eliminating unnecessary data and archiving data required for long-term needs.

3. Classification of data assets based on the organization's policy helps in segregating the data that require higher protection than others.

2.1.2 Data Discovery on Popular Cloud Platforms

IDC Research in 2018 [7] predicted that customer workloads will increasingly migrate to cloud platforms. They predict that more data will be stored in the public cloud than in consumer endpoint devices by 2020, and storage on public cloud exceeds the storage on-premise by 2021 as shown in figure 2.1.2.

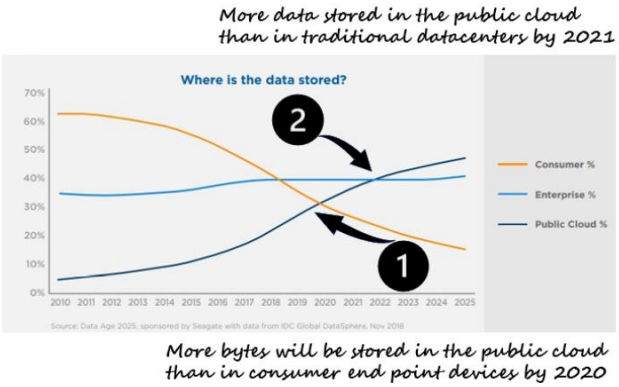

Figure 2.1.2: Data storage trends on public cloud vs others

The above trend necessitates the need to study the mechanisms of how data discovery and classification can be carried out on popular public cloud platforms.

2.1.3 Data discovery and classification in the cloud (AWS, Azure, GCP)

Amazon Web Services (AWS) Macie [9] discovers sensitive data among unstructured data that is stored in Amazon Simple Storage Service (S3) [10] as per definitions by data privacy regulations such as GDPR, PCI-DSS, and HIPAA. Macie can read several types of unstructured data in S3 buckets that include .txt, .json, .xml, Avro,.csv .tsv, .doc, .docx, .xls, .xlsx, .pdf, .tar, .zip, .gzip and Parquet.

Amazon SageMaker [11], AWS Glue [12], and supporting tools help in data labeling the structured data stored in tables, databases, data stores, etc., on the AWS infrastructure platform.

In the Microsoft Azure platform [13], sensitivity labels, information types, and discovery logic has been built into the databases such as Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics.

Google Data Catalog [14] offers a fully managed, scalable metadata management service to discover, classify and manage data with underlying machine learning-based Data Analytics.

Scanning, discovering, and classifying information across resources such as consumer endpoints, file repositories, and data stores on data centers, and cloud storage is an enormous task and necessitates automation technologies to improve efficiencies and accuracy.

2.1.4 Data Discovery: Heterogeneous Environments

There are many third-party tools that help in data discovery and classification across heterogeneous environments mentioned above. Here is an example of a tool, File Analysis Suite from Micro Focus [8], which can scan across cloud, on-premise, and public repositories and tag the resources with data classification labels.

The mentioned technology enables connections to different cloud as well as on-premise environments such as Google Drive, Microsoft share point repositories, Local file servers, and other content repositories. It allows the user to define different data classification tags for example payslip, credit card data, driving licence, etc.,

Once tags are created, data stored in different repositories are tagged and grouped under the respective classification groups, such as financial data, contact data. They are given ratings like partially sensitive, sensitive, highly sensitive, etc., to make it useful for the next level of the decision on protection controls. Figure 2.1.4 demonstrates an indication of tags.

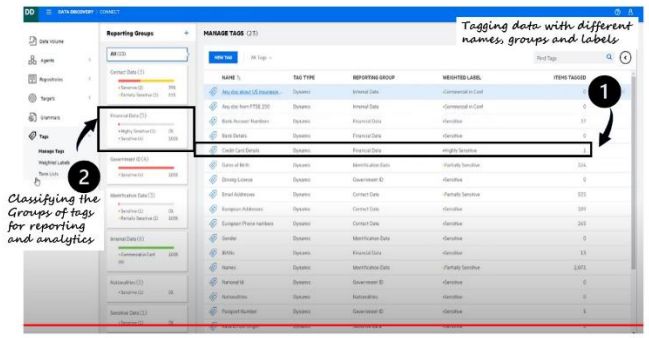

Figure 2.1.4: Example of data discovery across hybrid cloud

3 Data Protection

While encryption is the first technique that instantly comes into mind when data protection controls are planned, it is just one of the methods. To maintain the strongest compliances like GDPR, comprehensive protection of data is needed. This paper recommends a five-step approach to comprehensively address data security and privacy concerns.

Step 1: Assessing the risk of the data

As per FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) PUBLICATION 199 [42], Data classification levels are expected to be defined based on the potential data breach impact on the business in the event of security breach to Confidentiality, Integrity or Availability. Hence the risk exposure level is directly

proportional to the sensitivity level of the data. Highly sensitive data means higher risk exposure to the organization, in the case of leakage or cyber-attack, and that requires equally stronger controls to protect and preserve the data.

Cost and efforts could be reduced considerably by performing risk assessment before control implementation.

Step 2: Enforcing Zero Trust principles to access data

With the extended use of remote working employees, network security devices no more act as a perimeter. Zero trust adoption calls for the least privilege principle, and access should be based on the risk level of the asset. Identity and Access Management acts as a new perimeter or a gateway to deliver the right access to the right assets. Additional authentication levels with fine-grained access controls are required to exercise privileged changes to higher risk or sensitive data.

Step 3: Encryption

High-risk data [15] is the prime target for attackers, as it gets them the financial advantage or recognition. Data Encryption makes their efforts ineffective because they could not retrieve the data itself, but a concealed version. We will discuss different techniques of encryption in the next section while the data is at rest, on the move, or while it is in use.

Step 4: Backup and Archives

Important data assets [16] required regular backups to reduce the risk of accidental loss or disruption due to human error or technical misconfiguration or protect from ransomware attacks. Protecting archival data as per contractual or regulatory requirements by storing the data securely as per the classification is a complex problem to be handled.

Step 5: Secure Data deletion:

Data is deemed as securely deleted [17] from the system only when the data is made completely inaccessible or unusable to anyone that, including adversary or cyber attackers. Deletion of data securely is crucial to ensure that sensitive data will not land in hands of adversaries or hackers.

3.1 Encryption methods for cloud

Increased use of cloud and concerns around data privacy called for a requirement that was once a research question [18] posed by Rivest, Adleman, and Dertouzos in 1978, that is“ Can computations be conducted on encrypted data, the need to decrypt it, while conserving the data integrity?”

After that intriguing question, several encryption methods were developed to meet the requirements of conducting analytics or permutations on the encrypted data. Format Preserving Encryption and Tokenization are two such approaches.

3.1.1 Format Preserving Encryption

Conventional encryption methods AES-CBC [19] impacts data structures, schemas, and applications design as the encrypted text format in length and structure changes completely. Whereas Format Preserving Encryption (FPE) preserves the data structure and database schemas as is. Thus, making the applications perform operations on the encrypted format at all times and improving the performance of the application processing. Figure 3.1.1 below indicate comparison of traditional encryption vs FPE.

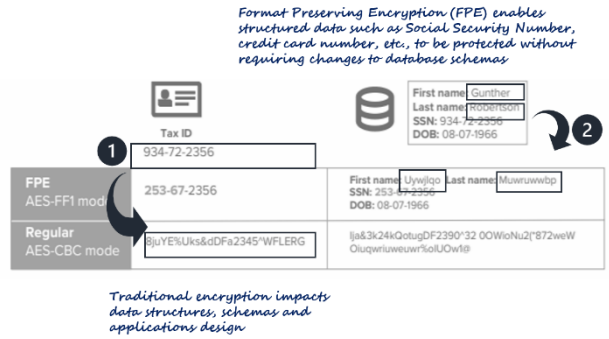

Figure 3.1.1 Traditional Encryption vs FPE

FPE uses the NIST-standard FF1(radix) mode of the Advanced Encryption Standard (AES) approved algorithm [20] that uses Format-Preserving Feistel-based encryption.

Other FPE methods FF2 [22] and FF3[21] have certain concerns related to encryption methods. FF2 was never got approved. FF3 method was exploited by researchers with a cryptanalytic attack (2017) making the encryption unacceptable for general-purpose usage because the anticipated 128-bit security level was not met. In response to the attack, NIST reverted FF3 to FF1 (FF3-1) in a revised version of FPE in the 2019 release [27].

1. Data was split into 2 portions
2. A keyed round function, with modular addition, applies on one data portion and it changes the other data portion.
3. The actions of these two portions were switched in the following iteration.

Ten iterations must be performed to complete the Encryption.

Similar steps are applied in decryption

1. Data is split into 2 parts. But the order of the round indices is reversed
2. A keyed round function, with modular subtraction, is applies on one data portion and it changes the other data portion.
3. The actions of these two portions were switched in the following iteration.

Ten iterations must be performed to complete the Decryption

The structure was explained in Figure 3.1.2 below for both encryption and decryption. Four iterations are listed in the figure below, but ten rounds are specified for FF1.

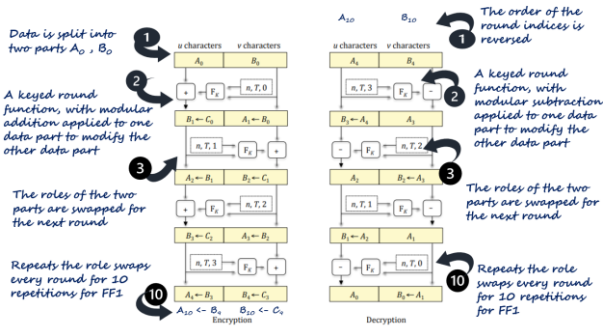

Figure 3.1.2: Feistel Structure for FPE FF1

3.1.2 Business Uses of FF1 mode of FPE

Sensitive data protection is the main usage of FPE. This includes protection of Payment Card Information, Bank Account details, Social Security Number, etc., encrypting the personally identifiable information (PII) such as these will make the information less vulnerable to focused attacks.

Field-level encryption of personally sensitive data eases the transaction by anonymizing the data in retail, health care, and financial applications that help in conducting analytics and transactions on the data without decrypting the data. As FPE preserves the original data format and length, systems that recognize a certain format treat that data as the original and carry on with the transactions on the encrypted data. Data remain encrypted unless there is a request from the data owner or other exceptional reasons. For example, a law enforcing authority is investigating a fraudulent case and is interested to know the financial details and sensitive information such as Aadhar, in that case, the ciphertext will be decrypted into plaintext by the authorized people after seeking the right permissions.

Multiple vendors offer FPE in their products and services, including Micro Focus Voltage SecureData, HashiCorp, Comforte, and Futurex.

3.1.3 Tokenization

To make the business transaction of physical assets easier, usage of digital substitutes of asset representations such as tokens or smart contracts are increasing rapidly [41].

Now a days, Gold, Diamonds, Real Estate Properties, and many more precious assets are getting tokenized. Considering the value of such transactions, addressing financial fraud, tax avoidance, and investor protection are the major concerns of the Governments. To meet the regulatory compliance requirements and to protect the sensitive data, tokenization need to be securely handled.

As per Payment Card Industry Data Security Standard (PCI-DSS) Guidelines [6], a method by which a substitute value, called a “token,” swaps the primary account number (PAN). The process of tokenization may or may not revert a token back to the original PAN.

The token's security and reliability rely primarily on the unfeasibility of establishing the original PAN with the knowledge of just substitute value (i.e., token)."

To meet regulatory compliance requirements and to protect sensitive data, tokens are used as a substitute for original data. For example, a token represents a credit card number, there is no way to associate the token to the card itself. However, it fulfils the purpose of completing the transaction whatever the worth the token was issued for.

Such solutions alleviate the responsibility of PCI compliance and privacy-related concerns, but they have other challenges.

With the raised interest in the use of tokenization to meet compliance, different methods arrived to fulfil different business use cases.

1. Reversible tokens

Tokens that can be converted back to the original plain text. They are either cryptographically created ciphertexts, or data maps using relational database functions. Format Preserving Encryption is one of the encryption methods used to create reversible tokens.

2. Irreversible tokens

Tokens can never be converted back to the original primary account number PAN. They are either Authenticatable or Non-Authenticatable.

The authenticatable token is like a hash function to authenticate whether the PAN was used in creating the token. This procedure cannot be reversed to reconstruct the PAN itself.

Whereas Non-Authenticatable can never be linked to a specific PAN, however, they could be linked to a consumer or account within the merchant.

The most discussed tokenization method in recent times is blockchain-based tokenization.

3.1.4 Blockchain-based tokenization and previous research

Blockchain-based transactions, commonly knowns as ledgers or tokens, are immutable [30] with timestamps that evade tampering of the information. Timestamp monitoring and access trails offer traceability and risk of counterfeit transactions.

With such strong claims, the Tokenization of valuable assets is getting implemented using blockchain technology [31].

Researchers analyzed its business use cases in real estate finance [33], renewable energy and green buildings [34], critical infrastructure such as energy microgrid transactions [35], smart city infrastructure with intelligent transportation [36]; [37], Pharmaceutical industries, and medical research [38],[39,[40].

3.1.5 Concerns and Future research possibilities

While blockchain technology seems to gain the robust attraction of adoption, the representation of virtual assets with tokens has been a highly mystifying matter [30].

The first point of concern by the asset owners is that token issuers control profits and cash flows connected to the token, thus diminishing the value of ownership of the associated assets. Another concern is about the separation of claim and ownership rights of tokens vs assets and interlinked components.

With the value and strength of the technology offered by blockchain, there are many business use cases with tokenization that could be powered by blockchain while addressing the dilemmas of usage, access, and ownership. We foresee a strong possibility to conduct future research in the adoption of blockchain-based tokenization.

4 Conclusions

Hyper-scale digital transformations and cloud adoptions are growing rapidly with the new trend of remote workers and digital businesses during the pandemic. With the increased business demand on the cloud, adversaries are attacking organizations with advanced threats and exploits are exposing sensitive data to the public. Governments are strengthening laws and regulations to enhance accountability on organizations for their security and privacy practices.

Cloud service providers are offering native tools to discover, classify and protect the data and workloads on their platforms. Security companies are coming up with advanced technologies to address the hybrid and multi-cloud complexities to secure the data across the lifecycle from discovery to destruction.

Regular data encryption techniques are not effective to provide protection while running data analytics on a cloud platform for banking, healthcare, and e-commerce industries. Field level encoding technologies, for instance, Format preserving encryptions and tokenization, preserve the data in original format, while running the transactions, support in managing the performance of applications. We propose to reassess the Blockchain-based tokenization for various business purposes, along with strong process definitions around ownership and responsibilities of tokens and their associated assets.

References

[1] De, Rahul, Pandey, Neena, Pal, Abhipsa, 2020/06/01, 102171, "Impact of Digital Surge during Covid-19 Pandemic: A Viewpoint on Research and Practice", International Journal of Information Management, volume 55, DIO:10.1016/j.ijinfomgt.2020.102171

[2] Internet Crime Complaint Center(2020), “Internet crime report. Washington, D.C:Federal Bureau of Investigation.”, Federal Burea of Investigation. Accessed on Jan 18,2022 at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[3] Wilson, Emily. "Disrupting dark web supply chains to protect precious data." Computer Fraud & Security 2019.4 (2019): 6-9, https://doi.org/10.1016/S1361-3723(19)30039-9

[4] Stack, Brian. "Here’s how much your personal information is selling for on the dark web." Experian. Haettu 4 (2018): 2021. Accessed on Jan 18, 2022 at https://www.courts.ca.gov/opinions/links/S248130-LINK1.PDF

[5] Juliana Gruenwald Henderson, July 24, 2019, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook", Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions accessed on Jan 8, 2022

[6] Hildegard Ferraiolo, Ramaswamy Chandramouli, Nabil Ghadiali, Jason Mohler, Scott Shorter, "Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)", NIST Publication, NIST.SP.800-79-2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-79-2.pdf

[7] David Reinsel, John Gantz, John Rydning, November 2018, “DATA AGE 2025: The Digitization of the World From Edge to Core”, An IDC White Paper – #US44413318, Sponsored by Seagate, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[8] File Analysis Suite, Micro Focus documentation, https://www.microfocus.com/documentation/file-analysis-suite/3.6/

[9] Discovering sensitive data with Amazon Macie, Amazon Web Services, https://docs.aws.amazon.com/macie/latest/user/data-classification.html

[10] Amazon Simple Storage Service User Guide, Amazon Web Services, https://docs.aws.amazon.com/AmazonS3/latest/userguide//Welcome.html

[11] Amazon Sage Maker user guide, Amazon Web Services, https://docs.aws.amazon.com/sagemaker/latest/dg/whatis.html

[12] Amazon Glue user guide, Amazon Web Services, https://docs.aws.amazon.com/glue/latest/dg/security.html

[13] Microsoft Azure Data Discovery & Classification documentation https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview

[14] Google Data Analytics Products, Data Catalog Overview, https://cloud.google.com/data-catalog

[15] Yang Tao, Zhu Lei, Peng Ruxiang, “Fine-grained Big Data Security MEthod Based on Zero Trust Model”, 2018 IEEE 24th Intrenational Conference on PArellel and Distributed Systems

[16] Jianping Zhang, Hongmin Li, "Research and Implementation of a Data Backup and Recovery System for Important Business Areas", 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics

[17] Joel Reardon, David Basin, Srdjan Capkun, “SoK: Secure Data Deletion”, 2013 IEEE Symposium on Security and Privacy.

[18] V. Vaikuntanathan, "Computing Blindfolded: New Developments in Fully Homomorphic Encryption," 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011, pp. 5-16, doi: 10.1109/FOCS.2011.98.

[19] S. Frankel, R. Glenn, S. Kelly, September 2003, The AES-CBC Cipher Algorithm and Its Use with IPsec, IETF, https://www.ietf.org/rfc/rfc3602.txt

[20] Bellare, Mihir & Ristenpart, Thomas & Rogaway, Phillip & Stegers, Till. (2009). Format-Preserving Encryption. 295-312. 10.1007/978-3-642-05445-7_19.

[21] Morris Dworkin, NIST Special Publication 800-38G (2016), “Recommendation for Block Cipher, Modes of Operation:Methods for Format-Preserving Encryption”, 10.6028/NIST.SP.800-38G

[22] M. Bellare, P. Rogaway, and T. Spies, The FFX Mode of Operation for FormatPreserving Encryption, Draft 1.1, February 20, 2010, http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec.pdf

[23] M. Bellare, P. Rogaway, and T. Spies, Addendum to “The FFX Mode of Operation for Format-Preserving Encryption”: A parameter collection for enciphering strings of arbitrary radix and length, Draft 1.0, September 3, 2010, http://csrc.nist.gov/groups /ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec2.pdf

[24] E. Brier, T. Peyrin, and J. Stern, BPS: a Format-Preserving Encryption Proposal, [April 2010], http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/bps /bps-spec.pdf

[25] M. Dworkin and R. Perlner, Analysis of VAES3 (FF2), Report no. 2015/306, IACR Cryptology ePrint Archive, April 2, 2015, http://eprint.iacr.org/2015/306

[26] J. Vance and M. Bellare, An extension of the FF2 FPE Scheme: Submission to NIST, July 2, 2014, http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/dff/dff-ff2-fpe-scheme-update.pdf

[27] Morris Dworkin, Recommendation for Block Cipher Modes of Operation, Methods for Format-Preserving Encryption, Draft NIST Special Publication 800-38G Revision 1, February 2019, https://doi.org/10.6028/NIST.SP.800-38Gr1-draft

[28] PCI Security Standards Council, Tokenization Product Security Guidelines, version 1.0, April 2015, https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

[29] D. Mazzei, G. Baldi, G. Fantoni et al., A Blockchain Tokenizer for Industrial IOT Trustless Applications, Future Generation Computer Systems (2019), doi:https://doi.org/10.1016/j.future.2019.12.020.

[30] All you need to know about tokenization, its benefits, challenges and future outlook. https://e27.co/academy-tokenization-benefitschallenges-future-outlook-20181109/. Accessed 8 Jan 2022

[31] Chen Y (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. Business Horizons, 61(4): 567–575

[32] Nakamoto S (2008). Bitcoin: A peer-to-peer electronic cash system. Available at: bitcoin.org/bitcoin.pdf

[33] Stein Smith S (2020). Stablecoins & the decentralized organization. In: Stein Smith S, ed. Blockchain, Artificial Intelligence and Financial Services. Cham: Springer

[34] Uzsoki D (2019). Tokenization of infrastructure: A blockchain based solution to financing sustainable infrastructure. International Institute for Sustainable Development

[35] Mengelkamp E, Gärttner J, Rock K, Kessler S, Orsini L, Weinhardt C (2018). Designing microgrid energy markets. A case study: The Brooklyn Microgrid. Applied Energy, 210: 870–880

[36] Gong Y, Liao J H (2019). Blockchain technology and simulation case analysis to construct a big data platform for urban intelligent transportation. Journal of Highway and Transportation Research and Development, 13(4): 77–87

[37] Zhong B J, Adriaens P (2020). Digital financing model for bridges in Washington State. In: International Conference on Transportation & Development. Seattle, WA, 300–308

[38] Pêgo, Ana, et al. "Blockchain and Clinical Data Economics: The Tokenization of Clinical Research in the EU." Political and Economic Implications of Blockchain Technology in Business and Healthcare, edited by Dário de Oliveira Rodrigues, IGI Global, 2021, pp. 269-291. https://doi.org/10.4018/978-1-7998-7363-1.ch011

[39] Agbo CC, Mahmoud QH, Eklund JM (2019) Blockchain technology in healthcare: a systematic review. Healthcare 7(2):56

[40] Yaqoob, I., Salah, K., Jayaraman, R. et al. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput & Applic (2021). https://doi.org/10.1007/s00521-020-05519-w

[41] Prof. Dr. Tim Weingärtner, Tokenization of physical assets and the impact of IoT and AI, Lucerne University of Applied Sciences & Arts – School for Information Technology

[42] Federal Information Processing Standard (FIPS) 199, Standards for Security ; Published. March 1, 2004