Data Encryption

Prasanthi Desiraju, Vittorio Pepe, and Will Shin

MSDS 485 Data Governance, Ethics & Law

May 30, 2021

ENCRYPTION – HOW DOES IT FIT?

With recent advances in technology, data is proving to be a strong asset. It helps Organizations build digital transformations and propels them against competitors. But the main challenge we face is the readiness of data, as there is always a risk of gearing in the wrong direction if we hold on to low-quality unreliable data. Furthermore, even with high-quality data, an additional risk posed in this digital realm is data security, ensuring data does not fall into the wrong hands, making it vulnerable to a wide range of data breaches and privacy risks. Thus, every organization needs to establish data governance frameworks to progress in data-driven technology and decision-making successfully. Data Governance helps ensure high-quality data throughout the lifecycle while accounting for the data's integrity, security, and consistency. The framework employs people and processes to enable appropriate and authorized handling of data across the organization, thus minimizing the risks posed by the unintended use of data. Here, we focus on the security aspect of data governance and how encryption can help make the data governance processes more effective by establishing the confidentiality of data.

Encryption is the process of converting a message or a file to appear entirely random for a non-authorized system and helps protect the data in transit. It is a means of scrambling plain text into an alternative form known as ciphertext such that only the authorized systems can decipher back the original information. Encryption is a more advanced and computationally intensive technique that induces confusion (scrambling) to plain text messages to maintain data confidentiality. The scrambled message is further encoded based on some algorithm to ensure data usability during the transit.

The encryption process involves a key to decipher the text, and the strength of the system depends on the strength of the key, and the length of the key is usually 128, 192, or 256 bits. There are two widely used encryption approaches, symmetric and asymmetric. The former uses a single key for encryption and decryption of data and is speedier; the latter uses two separate keys, one public key and one private key, and provides additional security. Figure 2 shows an example of a symmetric encryption process, where the messages can be deciphered only by the parties who have the ten-digit key.

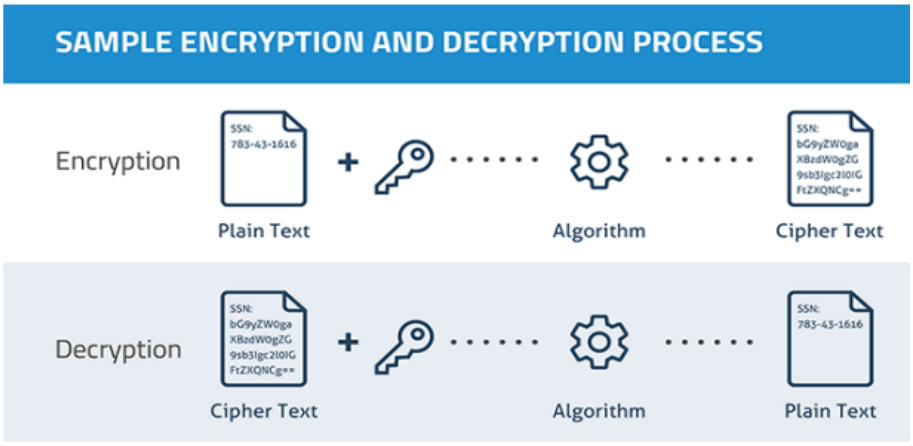

Figure 1: Encryption Process [1]

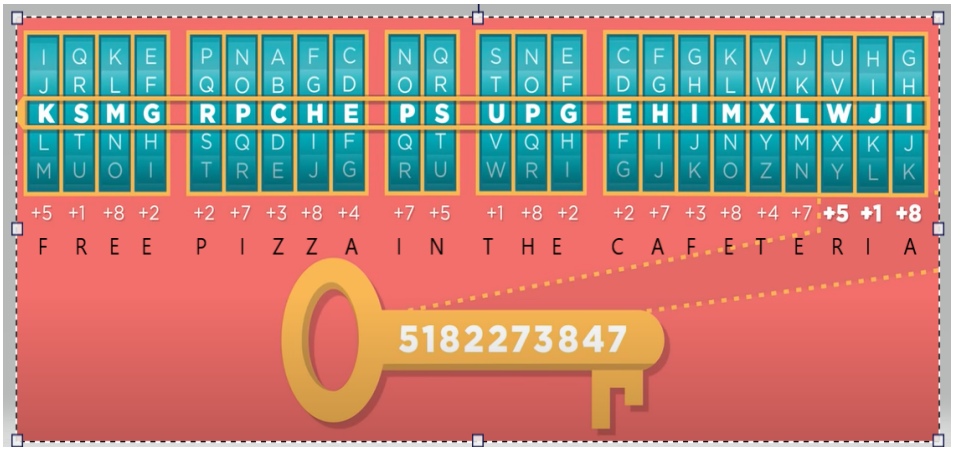

Figure 2: Symmetric Encryption with 10 digit key [2]

RISKS ASSOCIATED

In today's landscape, the occurrence of data breaches must be considered as a certainty, it is not a matter of 'if' but a matter of 'when' the next data breach will occur. Keeping this in mind, failing to adopt proper encryption policies results in increased risk associated with data breaches. If the data is adequately encrypted, the consequences of a data breach can be greatly reduced, being the data unusable by the hackers.

There are two possible scenarios:

- Unencrypted data
- Poorly managed encryption, i.e., use of outdated algorithms or not proper management of certificates and keys

The main consequences of having the company data exposed in a data breach are the exposure to the risk of fines by the competent authorities and forensic investigations to address the root cause, with the relative legal costs. The company also would have to provide some kind of compensation for the customers affected that can range from monetary compensation to services like credit monitoring and identity theft protection, in case of personal data.
But the most significant risk of all that is difficult to monetize is the impact that such events can have on the brand image and reputation [7].

The Yahoo! data breach reported in 2016 is an example of how critical it is to manage encryption properly. Yahoo! was attacked by hackers in 2013 and 2014, bringing affected users from the initial estimate of 500 million to three billion [8]. The hack was discovered only in 2016, and it is to the day the most significant data breach on records [9].

The data that came into possession of hackers may have included names, passwords, security questions, and answers, as well as other personal information like dates of birth and email addresses. Although some of the information was encrypted, the algorithms used were not of the higher standards, and the perpetrators were able to reverse the encryption. Another factor contributing to the breach's size is the poor management of certificates and their expiration dates, allowing the hackers to use some of them to access the network and decrypt communications.
The consequences of this data breach have been reported in 117,5 million costs in compensation due to class action and a loss of value of the company that had to accept a rebate of 350 million on the acquisition offer by Verizon in 2017 [10] [11].

ENCRYPTION LAWS

This paper focuses on the regulations and laws that require encryption, also known as data encryption laws, data privacy laws, or data protection laws. These laws span across different industries, and there are global laws and laws specific to industry and sector. For example, GDPR is applicable only when dealing with EU citizen data, whereas laws like Payment Card Industry Data Security Standard (PCI DSS) apply globally to any Organization dealing with payment information such as credit cards. [3]

ISO/IEC 27001:2013 (ISO27001) an international standard for information security that covers data protection. Several of the ISO27001 requirements also fulfill those of the GDPR and Data Protection Act (DPR), and implementing such standards help reduce the likelihood of breaches and potential deviations from existing laws. This framework will put the Organization in a better position to handle data security and serve as a good starting point. Regarding ISO

270001, organizations must comply with implementing a cryptographic policy (A.10), and below are some of the considerations to be considered while designing this policy. [4]

1. Training users on how to protect information and use Cryptographic controls.
2. Risk Assessment Procedure: Test the quality and strength of the encryption algorithm.
3. Implement encryption for data at rest, information in transit, data transfers involving email, mobile, or any such portable devices.
4. Build Strategy for storing encryption keys
5. Adhere with encryptions laws

Additionally, it is ideal to not restrict to a location and adopt a high level of data confidentiality and protocols throughout the Organization, even if required by a specific location. This helps organizations to be on top and quickly adapt to any new laws that come into place. Some of such laws are described in detail here [3]

1. PCI DSS – Global: A global council established these standards, and any business that handles, processes, or stores any form of payment information should ensure that they are using encryption to make the information unreadable. It applies to both the data at rest and in transit. PCC DSS 4.0 is the latest updated set of policies to account for the cloud, and serverless computing landscape, which serves as a reminder to the firms that new laws will be introduced with the technology and security needs to be an integral part of the design to stay ahead.

2. Healthcare Insurance Portability And Accountability Act (HIPAA) – United States: This encryption law applies to U.S. organizations that handle patient's sensitive and confidential personal information, and it requires organizations to protect the data against anticipated threats, unintended use, or disclosure of such information. It is required by the firms to implement security measures to ensure the confidentiality, integrity, and availability of all electronic health information at rest and in transit. A brief from regulation § 164.312 specifically illustrates the technical safeguards implemented by any such organization dealing with health information.

    - Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.
    - "Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

We have many more such laws like European Banking Authority – (EU), California Consumer Privacy Act (CCPA), etc., which emphasize the need for encryption while dealing with sensitive data. Failure to comply with these laws can result in fines causing both financial and brand damage. But most of the laws do not dictate the encryption technique and mostly a technique of choice. This is one of the key decision-making points that help build a robust and secure system - how the vendor/cloud service provider chooses to apply encryption and store and handle the keys.

BLOCKCHAIN

In simple terms, blockchain holds anything that has “value” and is immutable. It plays a significant role in digital transformation by making it easier to send and receive value in an easy yet most trusted way. Just as today’s internet lets us share information, blockchain lets us share value (Ex: money, contract, gold). As an analogy, blockchain technology can send money as easily as sending an email, just by adding the recipient's address and the amount. Blockchain technology records information encrypted and is essentially a digital ledger of decentralized, duplicated transactions and disturbed across the entire blockchain’s network of computer systems. Blockchain is a chain of blocks where each block contains a number of transactions, and each time a new transaction occurs, it is recorded onto every participant’s ledger. These transactions are recorded with an immutable cryptographic signature called a hash. The key terms involved in blockchain are decentralized and distributed; distributed refers to duplicating and sharing the information across participants of the network; decentralized ledger refers to not having it on a single server or a bank account or a firm responsible for exchange of information. Blockchain works on a peer-to-peer (P2P) network, which simply means we have multiple nodes and do not need a central server.

Blockchain is a different way of validation or accounting compared to traditional ways where each transaction is written to a block of data, and those blocks are chained together, as shown in figure 3, instead of some central database system.

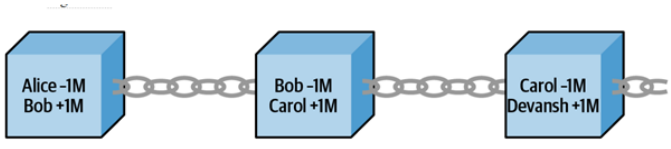

Figure 3: Money transfer between 3 people represented by blocks. [5]

Examples built using blockchain technology include Bitcoin, a peer-to-peer electronic cash system, Ethereum to run decentralized applications (DApps) and a smart contract platform, and so on. These smart contracts help provide better eCommerce solutions when buying from a new business party, where there is always a risk of less than good intent from one of the parties. For example, blockchain allows the use of escrow accounts to enable the seller to check that the money is ready for them, and the buyer can receive and check the goods before releasing the payment.

Example Application

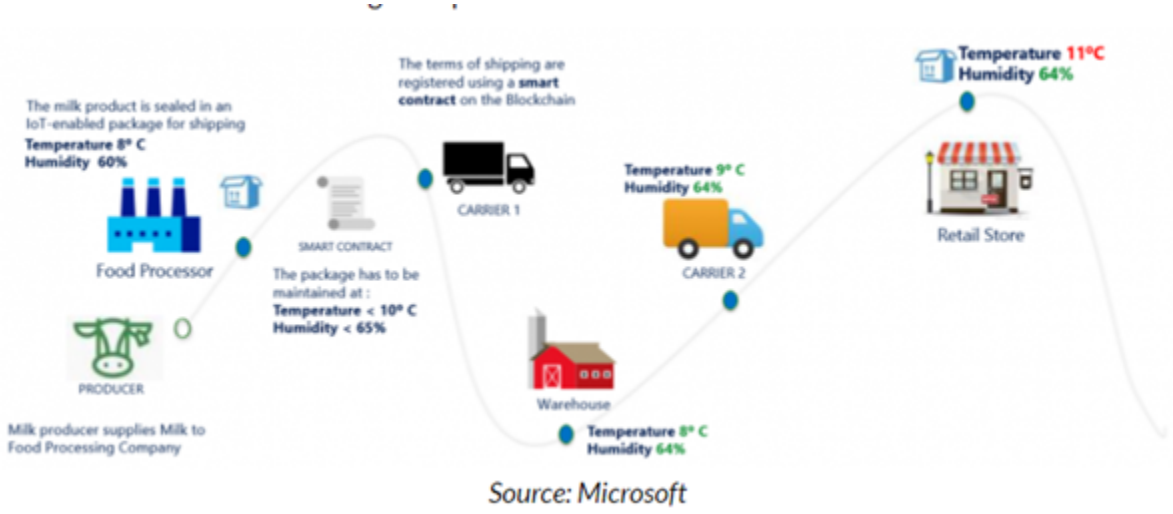

Figure 4: Supply Chain Life Cycle - With Smart Contracts [5]

The above example illustrates how the integration of IoT devices with blockchain can increase the efficacy of the supply chain and not depend on a centralized control mechanism facilitating things to be flexible. While IoT can collect the telemetry data at each stage of the supply chain, blockchain smart controls can validate this data in a completely trusted and transparent manner. As shown in the above example, the results can be backtracked quickly and

efficiently to analyze at what stage the product went out of compliance and make corrections accordingly. [5]

Blockchain Technology in Social Media: [6]

Blockchain sure seems to be a promising technology to improve the social media experience and build a safe and trustworthy platform for people. There are several ways blockchain technology can help improve social media platform, and some of them are illustrated below:

1. In-App Payments: Make secure and safe transactions with third-party transfers with the help of smart contracts without worrying about the legitimacy of involved parties.
2. Improved Security: The encryption powers of blockchain seem to have better value to share the authorized data with authenticated systems and make the process transparent to the users. In addition, the technology can be leveraged for additional security measures such as user verification and eliminate the prevalence of bots in social media platforms.
3. Authenticate Legitimacy of Content: Instead of having a single host/server controlling or validating the content, a decentralized platform is best suited to curb untrustworthy content yet protect the freedom of speech.

RECOMMENDATION

As in other cybersecurity topics, there is not a solution that covers all the risks associated. A satisfactory solution can be implemented only through a continuous investment process in people, process, and technology. Nevertheless, some basic steps should be followed to minimize data risks [12]:

1. Collaboration: having an encryption strategy requires the participation of all stakeholders, being management, operations, and IT. The process starts by identifying and prioritizing the risks that are unique to your company and its business.
2. Data Classification: encryption should be only a part of a broader IT security effort. Data classification policies and tools should be used to identify and separate data in different groups with different levels of sensitivity so that encryption policies can be applied following prioritization criteria.
3. Key Management. Encryption is safe as long as the keys associated with it are appropriately kept safe. If someone has access to keys, the encryption becomes transparent. It is necessary to implement a centralized system that can safely store the keys and certificates, allowing a single point of analysis and management.
4. Test different solutions. There are several encryption techniques that can cover different aspects (encryption data at rest, data in motion, and data in use). There are several aspects to consider as performance, feasibility, and need for security monitoring (see point 7). The best approach is to engage with vendor-independent suppliers that can advise and support during the test phase.
5. Access Control. If someone accesses the network with forged credentials, encryption no longer has any protective effect on data. It is necessary to evaluate the access points and define proper access control using more sophisticated technology like multi-factor authentication.
6. Communication and training. After the solution and the infrastructure are in place, there is the equally critical phase of informing and training all involved parties, employees, and business partners alike. All the parties should be well aware of the policies and tools

available and should be made aware of the company's stance on data security risks and consequences of no compliance.

7. SSL Decryption. If this kind of encryption is used, there is also the need to have a decryption tool that allows the monitoring of this kind of traffic. Some attacks could come through encrypted communications, and regular network monitoring tools cannot detect the threat.
8. Blockchain. Evaluate if any process would benefit from a blockchain solution, like vendor management, procurement, or shipping. Blockchain usually has the added complication that must be agreed upon between the parties involved, but once a common solution is devised and implemented, it can greatly improve transaction security. And it has the advantage of being natively encrypted.

REFERENCES

[1]. 2021. *Encryption - Library & ITS Wiki*. Accessed May 25. https://mediawiki.middlebury.edu/LIS/Encryption.

[2]. khanacademy. 2019. "Encryption and Public Keys | Internet 101 | Computer Science | Khan Academy." *YouTube*. YouTube. April 23. https://www.youtube.com/watch?v=6-JjHa-qLPk.

[3]. "10 Data Privacy and Encryption Laws Every Business Needs to Know." 2021. *Hashed Out by The SSL Store™*. March 11. https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/#takeaway-what-these-encryption-laws-mean-for-you.

[4]. "ISO 27001 Controls: What Is Annex A:10?" 2021. *Best Practice*. April 29. https://bestpractice.biz/iso-controls-27001-what-is-annex-10/.

[5]. "Your Supply Chain on the Azure IoT and Blockchain Cloud." 2021. *MSDynamicsWorld.com*. Accessed May 27. https://msdynamicsworld.com/story/your-supply-chain-azure-iot-and-blockchain-cloud.

[6]. Mire, Sam. 2019. "Blockchain For Social Media: 11 Possible Use Cases." *Disruptor Daily*. Disruptor Daily. January 3. https://www.disruptordaily.com/blockchain-use-cases-social-media/.

[7].“Unencrypted Data Represents a Huge Business risk” 2013, Mar 2. https://info.townsendsecurity.com/bid/63711/unencrypted-data-represents-a-huge-business-risk#:~:text=Unprotected%20sensitive%20data%20leads%20to,%2C%20public%2C%20and%20private%20companies.

[8] “Yahoo Triples Estimate of Breached Accounts to 3 Billion” 2017, Oct 3 https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804

[9] “List of data breaches’, retrieved on May 26, 2021. https://en.wikipedia.org/wiki/List_of_data_breaches

[10] “Yahoo data breach: How to file for $358 or more as part of claim settlement” 2019, Oct 15 https://www.cnet.com/how-to/yahoo-data-breach-how-to-file-for-358-or-more-as-part-of-claim-settlement/

[11] “Yahoo data breach: How to file for $358 or more as part of claim settlement” 2017, Feb 21. https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html

[12] ‘7 Key Elements of a Successful Encryption Strategy’ 2018, Nov 6. https://edge.siriuscom.com/security/7-key-elements-of-a-successful-encryption-strategy