

Reporting Date: 15th March 2024

TABLE OF CONTENTS

[ABSTRACT 2](#_Toc161415219)

[INTRODUCTION 3](#_Toc161415220)

[WHAT IS DATA ENCRYPTION? 3](#_Toc161415221)

[ENCRYPTION AND DECRYPTION 3](#_Toc161415222)

[TYPES OF DATA ENCRPYTION 4](#_Toc161415223)

[COMMON DATA ENCRYPTION TECHNIQUES 4](#_Toc161415224)

[PIPEDA 5](#_Toc161415225)

[KEYS PRINCIPLES OF PIPEDA 5](#_Toc161415226)

[RELEVANCE TO COMPANIES 6](#_Toc161415227)

[ADVANTAGES AND ADHERENCE 6](#_Toc161415228)

[CONCLUSION 8](#_Toc161415229)

[REFRENCES 9](#_Toc161415230)

# ABSTRACT

This week's project aimed to become acquainted with data encryption techniques and understand the significance of the Personal Information Protection and Electronic Documents Act (PIPEDA) in guaranteeing data privacy and security. For these purposes, different encryption techniques were considered that include symmetric encryption, asymmetric encryption, hashing, and digital signatures. These explanations shed some light on the reason why they are used to protect the sensitive information. Furthermore, outlining the PIPEDA principles also highlighted the significance of the implementation of diligent data management principles, which includes ideas such as consent, limitation on use, as well as, individual access rights.

The methodology included a comprehensive literature review of the encryption techniques and principles in PIPEDA, followed by a comprehensive summary regarding main findings and implications. Through considering the benefits offered by PIPEDA compliance and the repercussions of its violation, a more thorough understanding about the data privacy regulation can be achieved. The project emphasizes the credibility of sturdy encryption methods and lawful operations in order to create trust, reduce risks, and maintain privacy rights in a world that is increasingly digitally interconnected.

# INTRODUCTION

AutoBasket is a company founded by Larry and Veronica Smiles with the purpose of simplifying the grocery shopping experience for individuals and families. Situated in the heart of Toronto, the company's headquarters pulsate with the energy of a city known for innovation and diversity. The company's app automates grocery and recipe lists, linking recipes to required products, and streamlining the shopping process. Today, AutoBasket assists households across the world to save time and energy on their weekly grocery runs, making it easier for busy families and individuals to get everything they need for a great meal.

AutoBasket has hired us as interns to focus on all areas of development for the organization and to help create solutions to common issues within the industry. Our role as interns is not only focused on the knowledge you have learned in school but also on developing your soft skills, including presentations, teamwork, and leadership. This internship will provide us with valuable real-world experience and an opportunity to contribute to the continued success of AutoBasket.

# WHAT IS DATA ENCRYPTION?

Data encryption is a technique for safeguarding information by encoding it so that only individuals with the right encryption key may access it. Unauthorized access to encrypted data results in jumbled or unintelligible answers. The act of changing data from an understandable/readable format to a jumbled piece of information is known as data encryption. This keeps private information from being viewed by others while the data is in transit. Documents, files, communications, and any other type of network connection; all benefits from encryption.

# ENCRYPTION AND DECRYPTION

Data securing is done through encrypting or decrypting which is a process of transforming data into a legible format to deter attacks from unauthorized users.

* **Encryption**: The action of transitioning straightforward normal clear text into an encrypted form via employing a secret key and an encryption algorithm is what the word “encryption” refers to in straightforward language. The set of the key and the algorithm with their essential matching could and must be used to restore the text from its impenetrable form. Data can appear to be spoiled in case a stranger or hacker intercepts it, but such information cannot be recovered without the specific decryption key required for that encryption.
* **Decryption**: The contradiction of encryption or decryption will be done by a similar technique which use of a correct decryption key to change the ciphered text into a plain text. Consequently, decoding, which is how keyholders can access the original, readable data in a way that won’t cause unauthorized data leaks is how this instance shows it.

# TYPES OF DATA ENCRPYTION

Here are some common types of encryption and decryption techniques:

* **Symmetric Encryption**: Similarly to symmetric key encryption the same key is applied for both encrypting and decryption processes. DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Blowfish are illustrations to this statement. Symmetric encryption is indeed a faster technique than asymmetric encryption, however, it requires some sort of key exchange methodology to be carried out in a safe manner.
* **Asymmetric Encryption**: Being referred to as public-key encryption or quite often simply as private-key encryption, asymmetric encryption utilizes two types of keys: a public key for the encryption process and a private key for decoding. ​The public key is widespread and serve as an instrument to encrypt messages which are delivered by anyone and the private key is very confidential only the recipient has access to the decrypting messages. The RSA and ECC (Elliptic Curve Cryptography) are asymmetric cryptography algorithms.
* **Hashing**: Hashing makes use of a one-way encryption method that transforms raw data into a String of fixed-length characters, also known as the hash value or digest. Hashing is not an encryption or decryption tool, and is only used for verifying the integrity of data and keeping passwords safe. Hashing algorithm is the most important that people need to be aware of; for example, MD5, SHA-1, and SHA-256.
* **Digital Signatures**: Digital signature is based on an asymmetric algorithm that both provides authentication and deference to data. They do that by employing the hashing of the message with the sender's secret key. The receptor may decipher the signature with the sender`s public key to check for message intactness, and to prove the sender`s authenticity.

# COMMON DATA ENCRYPTION TECHNIQUES

There are different types of data encryption and techniques which have been used to approach security within various application. Here are some of the most widely used ones:

* **Advanced Encryption Standard (AES):** Before AES algorithm, AES was the international standard for implementing secret-key cryptography in hardware available. Its wide spread use directed to and significant impact on web encryption and data security is globally recognized. AES processes already encrypts data strings of 128 bits, and it allows using 128-, 192- or 256-bit key lengths. It's considered highly safe and precise, making it be applicable to many different fields.
* **Data Encryption Standard (DES):** DES is one of the first prevalent asymmetric encryption techniques conceived in the 1970s. While DES has the main disadvantage of being vulnerable to brute-force attacks, it has meanwhile developed as an open standard for secure data transmission. It works with 64-bit blocks and has a 56-bit key length. The later versions, like AES, operate on the variable block sizes. 3DES (Triplet DES) is double a version of DES that employs DES the algorithm triply to enhance an overall security level.
* **Rivest-Shamir-Adleman (RSA):** Through RSA digital signatures and secure communication channels can be secured. It is based on the arithmetical properties of prime numbers which a guarantee the safety of this system. Encryption with RSA in particular is done using the public key for encryption and the private key for decryption purposes. It pervasively is employed in secure email, SSL/TLS protocols, and certificates system.
* **Elliptic Curve Cryptography (ECC):** ECC which is an asymmetric cryptographic algorithm has its foundation in the mathematical structure of the finite field of curves over elliptic curves algebra. The fact that it gets the job done like RSA but invokes shorter key lengths makes it more efficient for the resource-constrained devices in settings like mobile devices and IoT (Internet of Things) devices. ECC is used for SSL/TLS, digital signature, both of these protocols, and cryptocurrency protocols among other.
* **Blowfish and Twofish:** The circular key size of the Blowfish we have is for the purposes of replacement of DES. It is useable with variable key lengths given up to 448 bits, with best known for its easy, and fast encryption process. Twofish is a considerable improvement on Blowfish and can operate with the next sizes, the block size (128 bits) and key length up to 256 bits. Unlike AES which has become the most popular alternative encryption algorithm, Twofish depending on its specific purposes finds its niche in some fields.
* **Format-Preserving Encryption (FPE):** Efficiently, FPE, or format-preserving encryption, is the kind of data encryption that enables the encryption of data with no change not being induced to its original format. Therefore, the encrypted data type, length, and form are identical to the original plaintext data. This will be helpful in systems which functionality or compatibility with other applications are depending on the format of data like this one. FPE ideation is about the encryption mechanism that renders an unreadable plaintext look like the ciphertext. Let's say the plain text is a 16-digit number for a credit card then the cipher text that FPE (frequency perturbation encryption) yields will also be a 16-digit number. This facilitates true plug-and-play encryption integration into systems which apply to specific data formats leaving the originator and the receiver to manage the encryption without clashing with existing data models or applications.

# PIPEDA

One important description of Canadian acts of legislation which is a controlling entity over information of personal information while conducting business is the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA kicked off on January 1, 2001, the legislation was passed in the wake of growing awareness among people about privacy while continual accrue of personal information by companies was socially acceptable.

# KEYS PRINCIPLES OF PIPEDA

* **Consent**: When the law is not in force yet, PIPEDA orders personal information should be collected, used, or disclosed only upon projects’ consent.
* **Limitation on Use**: Personal data can only be shared with a person as defined in the law and ought to be used for the purposes they were collected for unless otherwise stated in the law. Data collection should be openly and honestly explained by organizations, and applying such data to unattainable causes is forbidden.
* **Restricting Collection**: Companies must provide a rationale for the intended use of personal data they obtain and collect only the necessary amount of information. They have to limit the amount of data they collect to prevent abuses.
* **Accuracy**: It is essential to companies to secure the accuracy, completeness, and relevance of the people's personal data provided. They must exhibit sense of responsibility to avoid fake news and misinformation.
* **Protections**: Recognizing the fact that personal information can be used unauthorizedly for purposes that include access, use, disclosure or alteration, the PIPEDA requires enterprises to install security measures that will safeguard personal information from unauthorized use or access.
* **Openness**: Companies have to show respectability and acceptability on how they treat personal data and behave as responsible citizens in this new digital ecosystem. They should furnish people with straightforward information about how they carry out the procedures of gathering up, use, and disclosure.
* **Individual Access**: Individuals get the right to review any information held about them by the companies and in case of inaccuracy, to propose change or amendment.
* **Challenging Compliance**: In case someone believes that a company has done something and hence has breached the privacy act and PIPEDA, they have the right to lodge a complaint with the Office of the Privacy Commissioner of Canada. The co-chair, or the person with the highest rank, will have the capability to look into some complaints and ensure that rule-making is followed.

# RELEVANCE TO COMPANIES

Businesses, charities, and organizations under federal regulation are included in the states actors to which PIPEDA applies. It deals with the assembly, collection, retention and sharing of personal data both in hard copy media and electronic.

# ADVANTAGES AND ADHERENCE

The benefits for businesses that keep to the requirements of PIPEDA include a good reputation for privacy protection, reduction of legal risks and penalties, customer trust factor and many more. For non-compliance this could be led to penalties, regulatory measures, and a bad reputation for the organization.

Eventually, PIPEDA serves as a central body which is responsible for the protection of personal information as well as providing guidelines for legitimate data usage among the businesses. Adherence with PIPEDA not only guarantees compliance, but, in addition, creates trust and promotes favorable relationships with customers and company partners.

# CONCLUSION

In conclusion, it is evident that data encryption is crucial when it comes to the field of digital security, for it offers a range of protections from illegal access and guarantees the privacy and integrity of data. The use of encryption techniques, such as symmetric and asymmetric encryption, hashing, digital signatures, and many others, allows the transformation of data into a format that is just nearly impossible to decode for the parties except those having the appropriate private key. In this way, we not only encrypt the data during transmission but also at rest, which subsequently gives us a multi-pronged approach to the cyber-threat landscape.

Besides, there are regulations like the Personal Information Protection and Electronic Documents Act (PIPEDA). This leads to a trade that regulates responsible data handling practices. This especially refers to the personal information of consumers. Businesses that consider consent to be the most vital of the principles, in addition to limitations on use, accuracy, and individual access, will manage to earn the confidence of people that they will not misuse their earnestness while at the same time minimizing the legal risks and their status as upholders of privacy protection. To sum up, the fact that organizations follow PIPEDA does not only mean regulatory adherence; it also builds a transparent, reality-based culture that pay respect to privacy rights, and therefore these happen to be the basic elements of relationships with consumers and stakeholders in an ever digital community.

# REFRENCES

1. *data-encryption-methods-article*. (2023, 08 29). Retrieved from simplilearn: https://www.simplilearn.com/data-encryption-methods-article
2. *data-encryption-methods-types*. (2022, 11 22). Retrieved from splunk: https://www.splunk.com/en\_us/blog/learn/data-encryption-methods-types.html
3. *personal-information-protection-electronic-documents-act*. (2024, 03 15). Retrieved from hyperproof: https://hyperproof.io/personal-information-protection-electronic-documents-act/#:~:text=The%20Personal%20Information%20Protection%20and,disclose%20that%20individual's%20personal%20information