

Report on solution for laurel Technology Solutions expansion outside of Europe

Bernadette Murphy

30/11/23

Introduction

The main aim of this report is to conduct a thorough analysis of available information and identify the best technological options for expanding a business. The report will provide a comprehensive evaluation of the advantages and disadvantages of current technological solutions, as well as the challenges that businesses typically face when dealing with big data during expansion.

Considering the significance of Big Data in modern life and businesses, it is crucial to integrate critical tools and information. As per Hariri et al. (2019), Big Data refers to the vast amount of data generated every second, taking into account the size and scale of the dataset (Géczy, 2014). Therefore, the report will provide a detailed analysis of the company's current data management practices, highlighting areas for improvement.

Furthermore, the report will investigate potential future issues that may arise during the expansion process. It will focus on analyzing the legal policies of the General Data Protection Regulation (GDPR) in the countries where the business intends to expand. The report's evaluation will be based on Laurel Technology Solutions LTD, a Small to Medium Business situated in the UK that operates from a single office. Currently, customer data is stored across various off-the-shelf systems and different locations. Therefore, the company is looking to consolidate the data as it plans to expand to East Asia. The report will provide a detailed analysis of the current data infrastructure, including the data storage, data processing, and data analysis approaches. It will evaluate the strengths and weaknesses of the current data infrastructure and provide recommendations on how to improve the data management practices of the company.

Furthermore, the report will also provide an overview of the potential technological solutions that can be implemented to support the expansion plan. It will evaluate the latest technological advancements in the field of data management and identify the most suitable solutions for the company. The report will also provide an analysis of the costs associated with implementing these solutions and the potential return on investment.

In conclusion, the report aims to provide a comprehensive evaluation of the data management practices of Laurel Technology Solutions LTD and provide recommendations on how to improve the data infrastructure to support the expansion plan. The report will also provide an overview of the potential tech-

nological solutions that can be implemented to support the expansion plan and evaluate the costs associated with implementing these solutions.

Overview of current infrastructure

The current data storage system utilized by the company is not in line with industry standards, which can lead to difficulties in accessing and utilising data. The Financial department stores credit card information, while the Human Resource department stores employee data in a separate location. This approach creates a "silo" effect on data storage, making it challenging to access all the necessary information when needed and poses a risk to data security. The absence of a comprehensive and centralized database that includes all customer information hinders the organization's ability to streamline data analysis and utilization. To resolve these issues, the company plans to merge all data into a single centralized location. Doing so will facilitate business expansion, ensure easy accessibility of data, and reduce the risk of data loss or unauthorized access. We will conduct a thorough analysis of the current data storage system and recommend possible solutions to ensure the organization's data storage system complies with industry standards, is secure, efficient, and easily accessible. Finally, we will provide a recommendation to improve the current system's performance and ensure the security of the organization's data.

Big data issues

To help small to medium-sized businesses access information on their employees and customers, big data can be classified into different categories, such as unstructured, structured, and semi-structured data. Before deciding on the method of storing data, it is essential to consider its intended use. Storing this information in a central database is the most suitable option for this scenario. However, there are several ways to implement this, so let's explore the different storage methods.

One possible solution is to use SQL language, where different SQL commands can be written to create a database that stores all the files. Alternatively, Python can be used to develop a program that converts files into a central database.

Let's delve into relational databases and how SQL can be used to query them. Relational databases or RDBMS are a type of database management system designed for online transaction processing (OLTP) applications. They have been popular for several decades, and some of the most commonly used relational databases are MSSQL, MariaDB, and PostgreSQL. They are used by various applications such as e-commerce, banking, and hotel reservations, as they are excellent at handling transactional data that requires complex join queries between tables. When managing data, relational databases follow the principles of atomicity, consistency, isolation, and durability, also known as ACID. Atomicity means that when a transaction is executed, it is done so from beginning to end, and if there is an error, the entire transaction is rolled back. Consistency ensures that all data is committed to the database once the transaction is complete. Isolation means that multiple transactions can

run simultaneously in isolation without interfering with each other. Durability ensures that in the event of any interruption like network or power failure, the transaction can recover to the last known state.

Relational databases are highly efficient in managing complex data that requires intricate join queries between tables. They are specifically designed to adhere to the principles of ACID, which are crucial for fulfilling the transactional data requirements of several applications. Typically, businesses move data from relational databases to data warehouses to perform advanced reporting and data aggregation, enabling them to make more informed decisions.

The JSON file that needs to be converted into a database consists of a massive amount of data, including confidential credit card information and other significant data, making it an excellent fit for a relational database. The researcher chose a relational database created in Python rather than SQL. While the Python language is relatively straightforward to learn, people who are already familiar with it may find creating a database challenging. One must know how to manipulate Python to transfer all the data into a relational database while ensuring that private information is secured and GDPR requirements are met.

Developing a central database to store company data is a crucial task, and for this purpose, Python ETL will be used. However, it is important to thoroughly evaluate the Python ETL tools available in the market, as there are several commercial ETL and data integration tools, including IBM and Oracle. By critically assessing the Python ETL tools, we can choose the one that best aligns with our specific requirements and ensures the smooth functioning of the central database.

Security considerations

Data security is critical for companies that store sensitive information. One of the ways to achieve this is through the use of Transport Layer Security (TLS) technology, which ensures encryption and secure communication between web applications and servers. TLS is also essential for securing emails and voice over internet protocol (VOIP) calls.

Another way to secure data is through hashing, which uses algorithms to convert data into fixed values. Although SHA-1 is a commonly used algorithm that produces a message digest of 128 bits, it has been found to have security flaws. Intruders with adequate resources can use 2⁶³ hash processes to create collisions, which means they can generate two different messages with the same hash value. Additionally, attackers can manipulate input data to obtain the desired output through a chosen plain text attack. Therefore, companies should be aware of the vulnerabilities of SHA-1 and take appropriate measures to protect sensitive data. Hiring technicians who can protect against these kinds of attacks may be necessary.

EAP-TLS is another widely used security protocol that offers secure communication between two parties. The algorithm ensures message integrity through hashing and signing processes. In the first process, the message is converted into a unique, fixed-length string of characters, known as a hash. In the second process, the message is signed using the RSA signature algorithm, which is preferred over other signature algorithms due to its processing speed. How-

ever, the security of the RSA digital signature depends on the properties of the hash algorithm used in the signature process. Several types of attacks can be launched on the RSA digital signature, including key-only, known message, and chosen message attacks, which rely on the characteristics of the hash algorithm. Hence, it's crucial to choose a secure hash algorithm to ensure the security of the RSA digital signature.

Each interaction between two parties using TLS involves a cypher suite, which is a combination of cryptographic algorithms that define the encryption type, key exchange method, and message authentication code for a particular session. A cypher suite plays a vital role in ensuring secure communication by determining encryption keys that protect transmitted data. TLS provides a secure and transparent channel through which data or information can be transmitted without obstruction. It's critical to have secure internet communication to prevent sensitive information from falling into the wrong hands. For instance, clients can lose money if credit card numbers are intercepted. TLS ensures that data is transmitted in a clear and unimpeded way, providing a secure medium for information passage.

The high development in the systems administration innovation drives a normal culture for exchanging information very definitely. Subsequently, it is more powerless to copy of information and rearranged by programmers. The data must be safeguarded while communicating it, Delicate data like Visas, banking exchanges and government-managed retirement numbers should be secured. For this numerous encryption methods are existing which are utilized to stay away from data robbery. In late long periods of remote correspondence, the encryption of information assumes a significant part in getting the information in on the web transmission centres principally around its security across the remote. Encryption is an exceptionally normal procedure for advancing data security. The advancement of encryption is moving towards an eventual fate of vast potential outcomes. Regular new strategies for encryption methods are found. This paper holds a portion of those new existing encryption procedures and their security issues. The exhibition of that large number of encryption procedures is considered and talked about remembering UMARAM and UR5 for later parts of the paper.

An examination is directed between the consequences of the chosen different encryption calculations utilizing different settings such as various information types, different parcel sizes, and unique key sizes. If there should arise an occurrence of changing bundle size, (throughput, power utilization in $\mu\text{Joule}/\text{Byte}$, and power utilization by working out distinctions in battery rate were determined) in the event of encryption cycles to work out the execution of every encryption calculation. In the event of changing information types like sound, (throughput, power utilization in $\mu\text{Joule}/\text{Byte}$, and power utilization by working out the contrast in battery rate was calculated) in instances of encryption cycles to work out the execution of every encryption calculation.

Issues present with the expansion scenario

Expanding business operations to a foreign country can be challenging, especially when it comes to complying with local laws and regulations. In the case of South Korea, the country has its own set of data protection laws that com-

panies must follow. To operate in South Korea, a company must comply with the country's General Data Protection Regulation (GDPR), which may differ from GDPR requirements in the UK.

In February 2020, the National Assembly in South Korea passed several amendments to the Personal Information Protection Act (PIPA), which came into effect on August 5, 2020. These amendments aimed to centralize personal information protection services within the Personal Information Protection Commission (PIPC). They also introduced new requirements, restrictions, and measures, including updated definitions for pseudonymous and anonymous processing and various penalties. Therefore, it's essential for a company that plans to expand its business to South Korea to familiarize itself with and adhere to these new regulations.

The Personal Information Protection Act (PIPA) is an extensive law that governs the collection, use, and processing of personal data in all sectors. The definition of personal data under PIPA is broad, including any information that can be used to identify a living person on its own or in combination with other data. Companies must follow PIPA's guidelines to protect personal data.

To support the statute, there is an Enforcement Decree, which is the primary regulation implementing the law, as well as guidelines issued by the regulator. Companies must follow these guidelines to ensure they are in compliance with PIPA.

In early 2023, significant amendments were made to the PIPA, which were implemented in stages, with the most notable change taking effect on September 15, 2023. These amendments aimed to strengthen data protection and privacy regulations in South Korea. The amended statute relies on changes to the Enforcement Decree, which is currently in draft form. However, it's expected that the draft will be adopted largely unchanged. This chapter on Korea reflects those amendments and notes any outgoing rules that still retain relevance.

Therefore, it's crucial for a company that plans to expand its business to South Korea to read up on these laws and ensure they abide by them when working in Korea. Failure to comply with these regulations can result in penalties and legal action.

Moreover, AI-related personal data protection has been a significant concern in South Korea. The Lee-Luda (also referred to as "Iruda") case led to the development of specific policies and regulations. The Lee-Luda case is particularly significant for AI governance in Korea because the Personal Information Protection Commission (PIPC) ruling was the first to make a judgment on the violation of the Personal Information Protection Act (PIPA) due to the development and operation of AI. Following the Lee-Luda case, Korean society became more aware of the risks posed by security breaches in the era of smart data technology. Legislators began to establish legal frameworks for the protection of personal data while developing AI products and services. Therefore, companies that plan to develop or operate AI products and services in South Korea must ensure that they comply with these regulations to avoid any legal issues.

Future suggestions

In order to ensure the smooth functioning of a company, it is crucial to store all the necessary information in a central database that has been specifically created for this purpose. This will not only streamline the process of accessing the data but also minimize the risk of data loss or theft.

When contemplating an expansion of the company to other nations, it is of utmost importance to take into consideration the GDPR regulations of those countries. This will help the company avoid any potential legal issues that may arise from not adhering to the specific guidelines set by those nations.

It is also essential to calculate the travel expenses and analyze the potential productivity of expanding to a specific country. This will help the company to determine the feasibility of such a move and minimize any unforeseen costs that may arise from travel and procurement of necessary equipment.

Moreover, it is crucial to ensure that the majority of the profits generated from the expansion will be allocated towards growing and developing the business, rather than being spent on travel and acquiring devices. By doing so, the company will be able to maximize its profits and achieve sustainable growth.

Finally, when it comes to storing the information, it may be beneficial to consider a different method of storage, as storing all the information together in one central database may not be the most secure method. In this case, the company could store the information separately in partitioned tables and use SQL to create and query this database, which will not only ensure the security of the data but also provide a more efficient method of accessing the information. Data storage is a critical aspect of modern life, and there are many different options available for it. However, with the ever-increasing amount of data, the need for more secure and efficient methods of storing data is becoming increasingly important. In the future, new and innovative technologies may be considered for data storage, such as DNA storage, which has the potential to revolutionize the way we store information.

DNA storage is a fascinating and unusual technology that utilizes the molecule responsible for storing biological data to store digital information. Harvard scientists were able to encode a 53,400-word book in HTML, eleven JPEG images, and one JavaScript program onto DNA in 2012. This technology boasts an incredible storage density of 2.2 petabytes per gram, which means that a DNA hard drive the size of a teaspoon could hold all of the world's information, including every song, book, and video ever created. DNA storage is also well-suited for long-term storage, as it can last up to 400,000 years, making it an excellent option for archiving important information.

Although DNA storage is still in development and too expensive to implement at present, it may become a feasible option in the future. An article by Melanie Pinola in October 2015 investigated this method, which could potentially revolutionize data storage.

Another possible solution for data storage is cloud storage, which is currently available. Infrastructure as a Service (IaaS) provides computing resources, such as storage and processing power, that can be split, allocated, and resized as needed. Service Providers (SPs) deploy the software stacks that run their services, creating ad-hoc systems. Cloud storage can be used alongside databases as a backup solution, providing a more secure and efficient method of data storage.

There are various distributed storage frameworks available. Some are designed for specific purposes, like storing web emails or digital images, while others can store any kind of digital data. These systems can range from small projects to large-scale ones that require entire warehouses to house the hardware. These facilities that house the distributed storage systems are known as data centres.

Cloud storage is a cutting-edge resource that offers businesses an array of possibilities. Meanwhile, disk drives provide an alternative way to store data, but it may not be the most effective or secure method. The first disk drive was introduced in 1961, and since then, disk drives have undergone significant emotional improvements to meet performance requirements. Despite this, the performance gap between memory and disk drives has widened to a significant extent, and it continues to expand by approximately 50

Furthermore, energy efficiency has become a crucial challenge in designing disk drive storage systems. Although the architectural design of disk drives has reached a turning point, allowing their performance to advance further while maintaining high reliability and energy efficiency, traditional disk drives are facing design constraints and challenges.

This article sheds light on the evolution of disk drives over the past fifty years, detailing how they have been developed to meet challenging customer needs. It offers a brief introduction to the development of disk drives, providing a comprehensive analysis of disk performance and power usage. It also describes the innovative disk drive models discussed in the industry, and how new types of storage media impact the design of traditional disk drives.

A disk controller, a complex and vital component, is responsible for controlling the disk drive. It consists of specially designed chips that can skillfully process digital signals. The disk controller is made up of several parts, each with its unique function. The storage interface offers a standard protocol for communication between the disk controller and other components such as IDE, SCSI, FC, SATA, etc., enabling the disk drives to communicate with its user. The disk sequencer, a critical component, manages data transfer between the storage interface and the repository. ECC, another key part, attaches ECC codes to the user's data and verifies and corrects data before transmitting it through the storage interface. The servo control system, a meticulously designed mechanism, identifies the current position of the disk head, allowing the VCM to control track following and seeking. The microprocessor, the heart of the disk drive system, controls the disk drive system. The buffer controller provides control and signal processing for the bank of buffer memory, storing data and using it as temporary storage for read/write operations. In conclusion, the disk controller is a work of engineering art that enables the disk drive to function seamlessly and efficiently, providing us with the technology that has become an integral part of our daily lives.

Conclusion

The previous section covered several approaches to storing customer data. In this particular case, the method of choice is Python code that facilitates the transfer of data to a centralized database. This consolidation process streamlines data access. Sensitive data is secured via hashing, while future developments may include stronger encryption methods. Encryption, which was previously mentioned in the security considerations section of the paragraph, may be one such method. The report evaluates the data management practices of Laurel Technology Solutions LTD, suggests improvements to support the expansion plan, and analyzes potential technological solutions.

1 Bibliography

2 Works Cited

Cloudflare. “What Is Transport Layer Security? — TLS Protocol — Cloudflare.” *Cloudflare*, 2021, www.cloudflare.com/learning/ssl/transport-layer-security-tls/.

Deng, Yuhui. “What Is the Future of Disk Drives, Death or Rebirth?” *ACM Computing Surveys*, vol. 43, no. 3, 1 Apr. 2011, pp. 1–27, <https://doi.org/10.1145/1922649.1922660>.

Ko, Haksoo, et al. “Structure and Enforcement of Data Privacy Law in South Korea.” *International Data Privacy Law*, vol. 7, no. 2, 24 Apr. 2017, pp. 100–114, <https://doi.org/10.1093/idpl/ix004>. Accessed 20 Mar. 2020.

“Pros and Cons of 11 Payment Gateways for Web, Mobile & Apps.” *Dotknowledge.uk*, dotknowledge.uk/articles/view-article/pros-and-cons-of-11-payment-gateways-for-web-mobile-apps.

Salloum, Salman, et al. “Big Data Analytics on Apache Spark.” *International Journal of Data Science and Analytics*, vol. 1, no. 3-4, 13 Oct. 2016, pp. 145–164, <https://doi.org/10.1007/s41060-016-0027-9>.

Solove, Daniel J. *Digital Person : Technology and Privacy in the Information Age*. New York, New York University Press, 2006.

Smallcombe, Mark. “Structured vs Unstructured Data: 5 Key Differences.” *Integrate.io*, www.integrate.io/blog/structured-vs-unstructured-data-key-differences.

Younas, Muhammad. “Research Challenges of Big Data.” *Service Oriented Computing and Applications*, vol. 13, no. 2, June 2019, pp. 105–107, <https://doi.org/10.1007/s11761-019-00265-x>.