Development of a Cybersecurity Framework for Cloud Environments Adapted to the Retail Sector

Tomás Tátá Isidoro
Instituto Universitário de Lisboa (ISCTE-IUL)
Lisboa, Portugal
tatss@iste-iul.pt

Carlos Coutinho
Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR
Lisboa, Portugal
carlos.eduardo.coutinho@iscte-iul.pt

Carlos Serrão
Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR
Lisboa, Portugal
carlos.serrao@iscte-iul.pt

***Abstract*— Retail companies are increasingly targeted by cyber threats that are becoming more complex and difficult to deal with as technologies evolve, particularly due to the complexity and volume of information involved in this type of business. Traditional solutions such as antivirus/antimalware are becoming insufficient to deal with mass attacks that are increasingly sophisticated given current computing power. The retail business, due to its characteristics, is becoming a greater target, due to the large number of transactions and potential points of intrusion, from employees to partners.**

This article proposes a cybersecurity framework to support the migration of on-premises systems to the cloud. This framework consists of controls aimed at increasing confidence in migration, which have been defined through the analysis of internationally recognized frameworks and the author's practical experience. The focus of this document is mainly on the retail sector and data protection.

Keywords — cloud, security, retail, migration, framework, dissertation

I. Introduction

Cybersecurity is the area of IT that seeks to protect computers, mobile devices, private information, and, above all, people from agents who seek unauthorized access to information and cause damage to organizations or individuals. Private and public companies are increasingly dealing with more constant and sophisticated cyber-attacks and threats, so it is necessary to develop a culture and awareness of cybersecurity to defend against cybercriminals [1], [2].

Even with all these advantages, such as the pay-per-use model, elasticity, cost savings, and rapid implementation, there are major concerns about migrating to the cloud. These include the exposure of sensitive data, the difficulty of implementing compliance requirements, internal and external threats, lack of control and visibility over migrated data, vendor lock-in, availability risks, and increased information security costs [2].

Retail has very specific characteristics, including large volumes of data and transactions associated with sales, returns, payments, and more recently, IoT devices. It is necessary to have an inventory that allows all this information to be stored and that can offer high availability, as downtime for this type of system can result in high costs for the organization. The management of confidential customer data and the inventory management are two of the requirements that make migration to the cloud quite complex and challenging. Given that cloud adoption in retail is still low, this document aims to create a best-practice guide for this migration, tailored to the needs of the retail sector.

One of the main objectives of this research is to create a guide to good cybersecurity practices when migrating on-premises systems to the cloud, with the aim of identifying and mitigating associated risks, alerting companies in the retail sector to the challenges of cloud security. On this basis, two research questions were defined: RQ1 - How can organizations' confidence in adopting cloud migration solutions be increased with regard to cybersecurity issues? and RQ2 - How can the developed cybersecurity framework add value to companies that migrate their local systems to the cloud?

These questions are essential to guide the author throughout this research and to help achieve the objectives set for this framework.

The first hypothesis (HRQ1) considers that the framework should include topics considered decisive, such as documentation with security criteria based on other frameworks, transparency in implementation, the possibility of generating audit reports, organization, and presentation of positive results, all of which can increase organizations' confidence in migrating to the cloud. The second hypothesis (HRQ2) argues that a framework that implements strategies such as cost and risk reduction metrics, well-defined security steps, and that ensures innovation and competitiveness, can effectively add value to organizations.

This paper will therefore focus on validating these hypotheses, seeking to demonstrate how a well-structured framework can answer the questions raised and assist organizations in the retail sector in the process of secure migration to the cloud.

II. Literature Review

The work involving this level of detail always needs to be carefully thought out and structured. To this end, two methodologies were used: Design Science Research (DSR) [3] and Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)[4]. The DSR methodology was chosen, as it is used in cases where artifacts are created to respond to specific and relevant real-world challenges.

As DSR is more oriented toward innovation and problem solving, it is not very specific when considering a procedure for conducting a literature review analysis. For this reason, a second methodology, PRISMA, was defined in order to enrich and reinforce the first step of the previous methodology.

PRISMA is a “statement or communication guide designed to help authors of systematic reviews communicate transparently, outlining the steps they took to arrive at their final synthesis and the results they found through their research”[4]. This method is divided into three functional

blocks, which allow us to identify the most relevant articles for the literature review.

Although the topic of cloud security is relatively recent, the literature review has already demonstrated many results from different types of sectors. The state of the art was divided into four areas: "Standards for best practices in Cybersecurity," "Cloud Migration," "Security in cloud migration," and "Cybersecurity Framework," allowing for a clear division of results in line with research needs.

A. Standards for best practices in Cybersecurity

Most authors use these frameworks as a basis for developing something new and often still largely unexplored. The most recognized organizations in the scientific community are the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), which have published several standards such as, ISO27001 [5], ISO27005 [6], and the NIST Risk Management Guide [7], which, although adapted for cloud technology, will be very important for the completion of this dissertation.

The Cloud Security Alliance (CSA) and the European Union Agency for Cybersecurity (ENISA) are also two organizations that contain documents providing relevant information on cloud migration and are therefore a key foundation for this dissertation.

Since the retail sector deals with a variety of data considered sensitive, it must comply with the General Data Protection Regulation (GDPR) by the European Parliament and the Council of the European Union, which is legislation that aims to protect people's rights with regard to the processing of their personal data [8].

In short, all frameworks developed are always based on standards accepted by the community.

B. Cloud Migration

The cloud is a very recent technology that is increasingly sought after by organizations in all types of sectors, as it allows for quick adaptation and configuration of services in a secure and easy manner. Even so, the total migration of a large infrastructure brings with it several concerns related to security, privacy, reliability, trust, total cost, changes in suppliers, and loss of control [9]. Theft and loss of information, third-party access, data traffic, and the impact of relying on external services in many cases are also concerns highlighted by organizations [10].

The main secret to a successful migration is transparency in the relationship with the supplier and choosing the right one. On the other hand, several articles demonstrate that customer satisfaction is, in most cases, much higher when using the cloud, due to its speed and the way information is organized. In addition to the above, the cloud has other features such as a resource pool, elasticity, the possibility of performing backups in other geographical areas, and self-service.

The success of the cloud always depends on the professional ties that are created between the customer and the service provider [11] .

C. Security in cloud migration

Data migration to the cloud raises security concerns due to the loss of control by organizations. The main risks involve data breaches, malware, insecure APIs (Application Programming Interface), and attacks such as DoS/DDoS (Denial of Service/Distributed Denial of Service) [12]. To mitigate them, solutions such as Secure Sockets Layer (SSL), Trusted Platform Module (TPM), privilege tickets, Zero Trust (ZT), and encryption (Password-Based Encryption (PBE), Advanced Encryption Standard (AES)) are used, in addition to authentication, access control, and configuration testing [11], [13].

Some authors emphasize that, in addition to encryption, it is essential to invest in continuous monitoring, real-time threat detection, and the use of artificial intelligence (AI) [14]. Attacks on the cloud are on the rise, especially on Software as a Service (SaaS) services, with attacks carried out via the domain name system (DNS), forms, and cryptojacking becoming more common and dangerous. [15].

D. Security in cloud migration

Cybersecurity in the cloud has been one of the topics of concern to the scientific community, where several authors have developed various frameworks with the aim of protecting sensitive data during migration using techniques such as encryption, authentication, and secure transfer.

One such example is the framework [9] , which focuses mainly on small and medium-sized enterprises (SMEs), assuming that one of the main problems in this type of organization is related to the lack of technical knowledge to implement solutions such as the cloud. The author of the framework [16], in an attempt to protect data, mitigate risks, and build a solid foundation of trust, created a structure that includes different phases of planning, negotiation, implementation, and verification.

All these types of analyses allow us to gather the most relevant points in order to develop a framework adapted to the retail sector that conveys confidence for its implementation by companies.

III. Cloud Models and Services

The main objective of this framework is to provide a guide to best practices that will help organizations, particularly those in the retail sector, to migrate to the cloud in a secure and informed manner. According to NIST, the cloud is a model that allows on-demand network access to a shared pool of configurable computing resources, such as servers, networks, storage, applications, and services, with minimal management effort [17]. These resources can be implemented in four different environments: public, private, community, or hybrid cloud. Detailing each of these environments, the public cloud is fully managed by the provider, where customer data, although separate, is stored in data centers shared between several organizations. The private cloud is also managed by the provider, but offers exclusivity to the customer, meaning that the entire infrastructure is dedicated to them. The community cloud is shared between several organizations and also managed by the provider. This type of cloud has very similar needs in terms of security, privacy, and regulation. Finally, the hybrid cloud is the most widely used by companies, particularly in the retail sector, as, among many advantages, it allows the use of a method called "cloud bursting" [18], [19].

This method allows resources to be added to machines hosted in the public cloud without affecting the load on the

private cloud. It is also used to deal with peaks in demand, for example during holidays or promotional campaigns.

In addition to cloud environments, there are also service models: infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS. IaaS places greater responsibility on the customer, with the provider only being responsible for the physical hardware and its security. PaaS also includes the provider's responsibility for operating systems and middleware, while security settings are shared. The SaaS model is almost entirely managed by the provider, who guarantees the entire infrastructure, platform, software, maintenance, and updates, so that the customer can implement their applications. In this model, security settings are mainly defined by the cloud provider [20].

A. Challenges in cloud migration

As with outsourcing services, concerns arise regarding data security and privacy. In the cloud, the organization remains responsible for choosing the type of cloud and provider, as well as for the security and privacy of the service. The NIST SP 800-144 guide [17] highlights some concerns such as the complexity of systems, the sharing of multi-tenant environments, the exposure of interfaces to the public, increased threats, and loss of control over data.

The factors described above prevent the organization from having complete control over its infrastructure, making the implementation of its own security policies a challenge. Recent studies, such as the "Study Cloud Migration" [21] or the "IBM Transformation Index [22]," indicate that most companies have already started or plan to start migrating to the cloud, but that companies such as SMEs face some difficulties due to a lack of technical knowledge, strategies, and resources, such as financial resources. The study also indicates that only 34% of these companies already have a defined strategy for migrating to the cloud. The study also indicates that only 34% of these companies already have a defined strategy for migrating to the cloud.

The hybrid cloud is the most widely adopted model (49% and 56% in the respective studies), while others opt for the lift and shift approach. Many companies admit that they lack the technical skills to manage cloud solutions, and 80% are transferring their infrastructure back to private clouds for reasons of latency, security, and compliance.

B. Basic principles for cloud migration

There is a set of frameworks that serve as the basis for the development of other approaches and methodologies, most of which are developed by renowned organizations in the field of cybersecurity and cloud computing. Support for these frameworks is essential, as it ensures that security principles are always complied with, thereby helping to increase the confidence of companies that may adopt the framework developed in this dissertation.

Among the main frameworks are ISO/IEC27001:2022 [5], ISO/IEC27002:2022 [23] and the NIST Cybersecurity Framework (CSF) 2.0 [7]. Each of these frameworks plays a specific role in defining guidelines, assessing risks, protecting data, or aligning security with the business, and they are fundamental to the construction of this document. All of them will be central to the description of each of the controls specified in the following chapter.

IV. FRAMEWORK DEVELOPMENT

This chapter aims to develop a framework for secure, structured, and conscious migration to the cloud. At the same time, it seeks to answer two research questions. The first subchapter presents a table with essential controls to reinforce companies' confidence in adopting cloud solutions. The second subchapter analyzes how the framework can generate value for companies migrating to the cloud, adapting it to the retail sector.

A. Controls that increase organization confidence in cloud migration:

Below are 10 controls and sub-controls that seek to help organizations increase confidence and security in cloud migration.

1. Identity and access management (IAM)

IAM is a key control in planning the migration of information to the cloud, as it ensures that only the right users have access to the respective resources, preventing intrusions by unauthorized parties. In the retail sector, much data is highly confidential, such as customer information, payment data, inventories, or commercial strategies, making the use of this control essential in these organizations.

IAM consists of several sub-controls that protect organizations from unauthorized access. These sub-controls include the documentation, approval, and implementation of IAM policies and procedures, with clearly articulated objectives, ensuring the confidentiality, integrity, and availability of data [24]. Some important policies that should be implemented are: identification of inactive users; granting only strictly necessary access; constant review of access; procedures for accessing and modifying critical files; strong authentication mechanisms and credentials; mandatory approvals by management; recording of approvals with dates and names; and annual revalidation of procedures.

It is important to ensure which cloud model the organization will use in order to clearly structure the obligations of the provider and the customer regarding the implementation of IAM-related measures [5] ,[24] and [25].

1.1. Multi Factor Authentication (MFA)

There are several types of authentication. One of the most widely used and well-known are passwords, which must contain different types of characters, length, history, and validity. The greater their complexity, the more difficult it is for an attacker to decipher them, thus preventing any type of attack of this kind. MFA aims to add other types of authentications in addition to the password, thus requiring two or more verification methods before accessing the organization's systems or applications [25].

This control should be applied to all types of users, including external users (e.g., outsourcing), and can be implemented through API or cloud service. Examples include SMS, email, smartphone apps, USB keys, biometric readers, among others [25].

Adaptive multi-factor authentication, a concept used in MFA, is also very useful, as it uses information from the organization's own users to determine whether to expand or reduce the complexity of the authentication steps. Examples include login failures, geographic location, devices, operating system [26].

In addition, it is increasingly possible to use artificial intelligence and machine learning as a means of analysis to identify suspicious activities, such as login attempts at unusual times, locations, and devices.

2. Zero Trust Architecture (ZT)

The next control, zero trust architecture, is very important for secure migration to the cloud. This assumes that there is no trust in assets (regardless of their owner) or users based solely on their location or similar information. The goal of zero trust is to propose an architecture that includes a security plan with these concepts, which is applied to all sectors of the company, thus protecting all of its assets [27].

In short, ZTA works simply. There is a flow that begins with an employee's request for access to information, which is validated by a PDP/PEP (Policy Decision/Enforcement Point) based on the organization's policies. Once approved, the request is directed to an area of trusted entities, allowing access to the resource [27].

When implementing ZTA, the organization must take into account several assumptions, including that no resource is 100% reliable during the entire time it is connected to the network, and must meet some minimum requirements, such as having a basic infrastructure with an internet connection, the ability to distinguish between company-managed and non-managed assets, and having traffic monitoring tools in place, among others. ZTA implementation usually occurs in phases, seeking to gradually implement the technology, as each company will have its own strategy and maturity in integrating this architecture [5], [27].

2.1. Network segmentation

Network segmentation is essential to protect an organization from attacks, both in a cloud and on-premises structure, and consists of dividing a main network into smaller ones that may or may not communicate with each other. This division can be done using physically or logically separated networks. Each subnetwork is usually associated with a specific group of devices with the same characteristics, such as POS terminals, printers, ATMs, among others [23]. Network segmentation may also be associated with other organizational needs related to trust levels, criticality, organizational structure, or any combination thereof.

Each subnetwork is then associated with a Virtual Local Area Network (VLAN), where different security rules can be implemented (usually through Access Control Lists (ACLs) and firewalls). These can be applied individually to each active device to restrict access, both internal and external. Wi-Fi networks require special attention, as it is common to have guest networks for visitors, which should only be used by them, where solutions based on captive portals with appropriate restrictions should be implemented.

3. Data encryption in transit and at rest

Encryption is a practice that is often ignored or considered irrelevant to businesses. However, it is a fundamental practice, especially in cloud environments, and failure to use it often results in major data leaks or information interception. The first step before an organization chooses the type, strength, and quality of algorithms is to classify the information and define the desired level of protection.

To implement this control, it is necessary to create a secure key management system to generate, store, archive, retrieve, distribute, remove, and destroy keys [23].

There are two types of data, in transit and at rest, which require different encryption strategies.

3.1. Data at rest

Data at rest is stored on static devices such as computers, smartphones, or removable disks.

There are three types of approaches to encryption: full disk encryption (FDE), which encrypts the entire disk and requires prior authentication to grant access; virtual disk or volume encryption, in which a file called a container, usually mounted as a virtual disk, is encrypted; and file and folder encryption, done individually, which is transparent to the user (unlike containers) [28]. While the user is working on a particular file, the operating system automatically encrypts and decrypts the content if the user is the owner of the information. The latter is useful in the retail sector, where files such as Excel or Word contain confidential information.

3.2. Data in transit

The second type of data is data in transit. Unlike static data, this type of data is typically transmitted over the internet, local network, or other channels containing a lot of confidential information. For this reason, an effective encryption method is necessary to protect all data being transmitted, such as Transport Layer Security (TLS).

This protocol consists of three subprotocols that ensure the correct encryption and decryption of information. Of all the versions of TLS, it is advisable to use 1.2 and 1.3 as they are more recent and ensure greater security. In the retail sector, TLS is essential for protecting confidential data and is one of the protocols that ensure compliance with international standards/frameworks [29].

4. Data backup and recovery

We are increasingly living in a digital world, where cyber-attacks, technical failures, and human error are a reality, and therefore organizations need to protect themselves by creating data backup and recovery mechanisms. By performing regular, remote, and automated backups, it is possible to ensure the normal functioning of the organization in the event of an attack, through the complete restoration of systems.

There are three backup methods: full (simple, but requiring more time and space), incremental (efficient in terms of storage, but more complex in recovery), and differential (balanced) [30].

For more critical systems, the cloud also offers several options for performing and storing backups by replicating data across regions or pairs of regions [20]. It is also important to ensure a second backup method in case the primary one fails.

5. Incident Response Plan / Continuous Monitoring

The cloud is becoming an increasingly desirable technology for organizations, with many already beginning to create and structure a migration plan. Before migrating the infrastructure, it is necessary to ensure that the organization has the capacity to analyze and resolve any type of security incident that may arise. This entire process should be structured and documented through an incident response plan, such as the NIST cyclical plan, consisting of the stages of

governance, identification, protection, detection, response, and recovery [7]. In addition to the plan, tools should be created to detect incidents through automatic alerts, which allow the impact and severity of the incident to be validated.

A hierarchical model should also be defined between technical teams through a Service Level Agreement (SLA) for incident response, which should be resolved as quickly as possible. All steps and operations should be fully documented. For rapid incident analysis, it is important to ensure a plan and monitoring tools are in place. Several cloud providers, such as Microsoft, offer monitoring tools (such as Azure Advisor, Azure Service Health, and Azure Monitor [20]) that allow, among many features, customizing recommendations and reporting problems in the customer's cloud services.

6. Cloud Asset Inventory and Management

An asset inventory contains the identification of all of an organization's resources and assets, making it a critical database that must always be updated and validated by different managers in a hierarchical manner. This inventory should serve as a basis for all departments, enabling cost management, the monitoring of compliance with internal security policies, and the validation of the proper use of resources [25]. The inventory should cover all physical, virtual, remote, and cloud assets, as well as software, services, and systems. The inventory should be aligned with IAM policies and updated with new cloud products. Google, for example, offers an asset management tool, CloudQuery, which provides a centralized inventory of your cloud resources, regardless of the provider [31].

In the retail sector, asset management and inventory are central elements for a secure and efficient transition to the cloud.

7. Secure Integration of IoT/IIoT/ and OT Devices in the Cloud

The digital transformation in the retail sector has driven the adoption of Internet of Things (IoT), Industrial Internet of Things (IIoT), and Operational Technology (OT) devices to optimize processes and improve operational efficiency. OT includes programmable systems and devices that interact with the physical environment, such as industrial control systems and building automation, while IoT/IIoT improves industrial and manufacturing processes. In the process of migrating to the cloud, the data transmitted by these devices is managed centrally, which minimizes resources. But on the other hand, it exposes devices to vulnerabilities due to their need for constant communication and limited security [32].

These devices, which are often obsolete, require demanding cybersecurity strategies such as the defense-in-depth strategy that uses layers of protection, such as antivirus, firewalls, VPNs, and machine learning technologies to detect anomalies and strengthen defenses.

8. Compliance and Risk Assessment

Finally, the last control is compliance and risk assessment, with compliance being important to ensure that everything is in line with organizational standards, laws, and regulations, and risk assessment allowing the identification of risks, the severity of their consequences, and the measurement of the level of exposure to external threats [33]. For control to be well executed, it is important that the direction of risk assessment and compliance is fully synchronized with the organization's objectives.

By ensuring that all controls comply with international standards, companies will feel more confident in implementing them. The same is true for risk analysis, knowing that all risks are assessed for the execution of each of the controls.

Compliance increases companies' confidence in adopting the controls developed, as they follow all international standards.

B. How this framework adds value to companies

The second part of this work seeks to answer the second research question through the practical application of the framework, demonstrating to companies that these recommendations follow all security standards, creating a climate of trust in cloud migration.

By using this framework, it is possible to make organizations aware that it is necessary to invest in the training of internal employees, for example through certifications, or by hiring external agents who can instruct teams. Migration should be initiated in accordance with the organization's financial capacity, always maintaining a solid and structured plan in order to prevent possible incidents.

Controls such as data encryption mechanisms, network segmentation, MFA, and IAM ensure that the organization's data is always protected, preventing possible intrusions. For proper management and control, the framework presents zero trust architecture, IAM, compliance, and risk assessment controls that ensure that all devices are controlled and monitored, allowing data visibility in both pre- and post-migration environments. It is expected that, by using these controls, the company will be able to achieve very positive results, starting with savings in time and costs, tailored to its needs, reducing the initial fears of organizations and demonstrating that, with a solid and well-segmented plan, it is possible to migrate to the cloud safely and without fear.

One of the best ways to demonstrate the application of the framework is through real-life scenarios. This document is prepared, for example, for different scenarios such as sales peaks (due to Black Friday, Christmas, campaigns, among others), due to its scalability and adaptability. One of the methods that guarantees this stability is cloud bursting, as mentioned above.

The framework also ensures that the technical teams and company management are in sync, ensuring that all decisions are made unanimously in accordance with the organization's objectives.

Finally, a realistic calculation of the possible cost of migration to the cloud was made for three generic types of companies: small, medium, and large. This calculation was performed for both a hybrid cloud and public cloud simulation, and the value was estimated using only the Linux and Windows operating systems.

V. CONCLUSION

Throughout this work, the author sought to answer the two research questions stated at the beginning of this document, with the main concern being the successful migration of organizations' on-premises systems, particularly those in the retail sector, to the cloud. The first research

question was answered by providing a list of strategic and technical controls that were able to reinforce the confidence of organizations by presenting theoretical and practical solutions to the main problems in this type of migration.

Through the second subchapter of the framework's development, it was possible to reflect on how it adds value to companies, going a little beyond risk mitigation. It became clear that an organized and structured approach allows technical objectives to be aligned with the organization's business strategy, optimizing resources and ensuring a safe, effective, and efficient migration. This work drew on the author's practical experience in the retail sector, thus answering many questions within this technology that these types of organizations seek answers to. Despite the complexity and effort involved, this process allowed for the consolidation of knowledge, the integration of best practices, and the proposal of a concrete solution to a current problem with a direct impact on organizational success.

In order to improve this work in the future, and to increase business confidence, it would be interesting to conduct an internal survey on the content of this framework, in order to validate the concepts in practice and create an application that can help organizations follow all the steps in a systematic and secure manner.

VI. Acknowledgements

This work was supported by Fundação para a Ciência e a Tecnologia, I.P. (FCT) [ISTAR Projects: UIDB/04466/2023 and UIDP/04466/2023].

VII. References

[1] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," in *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, Institute of Electrical and Electronics Engineers Inc., Jul. 2017, pp. 253–259. doi: 10.1109/INCISCOS.2017.20.

[2] Google Cloud, "Vantagens e desvantagens da computação em nuvem," https://cloud.google.com/learn/advantages-of-cloud-computing?hl=pt-BR.

[3] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to Design Science Research," 2020, pp. 1–13. doi: 10.1007/978-3-030-46781-4_1.

[4] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, *BMJ Publishing Group*. doi: 10.1136/bmj.n71.

[5] Iso, "ISO27001:2022," 2022.

[6] ISO, "ISO/IEC 27005:2022," *https://www.iso.org/standard/80585.html*, 2022.

[7] NIST - National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[8] Council of the EU and the European Council, "General Data Protection Regulation - What is the GDPR?," https://www.consilium.europa.eu/pt/policies/data-protection-regulation/.

[9] A. Roy and K. Patil, "Framework for Cloud Security Initiatives in Small and Medium-Sized Enterprises," in *2023 International Conference on Advancement in Computation and Computer Technologies, InCACCT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 444–449. doi: 10.1109/InCACCT57535.2023.10141743.

[10] S. Shakya, "AN EFFICIENT SECURITY FRAMEWORK FOR DATA MIGRATION IN A CLOUD COMPUTING ENVIRONMENT," *Journal of Artificial Intelligence and Capsule Networks*, vol. 01, no. 01, pp. 45–53, Sep. 2019, doi: 10.36548/jaicn.2019.1.006.

[11] C. Huang *et al.*, "Toward security as a service: A trusted cloud service architecture with policy customization," *J Parallel Distrib Comput*, vol. 149, pp. 76–88, Mar. 2021, doi: 10.1016/j.jpdc.2020.11.002.

[12] R. Bathini and N. Vurukonda, "A survey to build framework for optimize and secure migration and transmission of cloud data," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 2, pp. 812–820, Apr. 2024, doi: 10.11591/eei.v13i2.5181.

[13] A. Harikrishnan, "EVALUATING CLOUD MIGRATION SECURITY RISKS: DEVELOPMENT AND VALIDATION OF AN ENTERPRISE-LEVEL ASSESSMENT FRAMEWORK," *International Journal of Research In Computer Applications and Information Technology (IJRCAIT)*, vol. 7, no. 2, pp. 836–853, doi: 10.5281/zenodo.14045253.

[14] R. Dasari and G. R. M. Babu, "Revolutionizing Cloud Security: A Novel Framework for Enhanced Data Protection in Transmission and Migration," *Scalable Computing: Practice and Experience*, vol. 25, no. 6, Oct. 2024, doi: 10.12694/scpe.v25i6.3140.

[15] L. E. Bautista-Villalpando and A. Abran, "A Data Security Framework for Cloud Computing Services," *Computer Systems Science and Engineering*, vol. 37, no. 2, pp. 203–218, Mar. 2021, doi: 10.32604/csse.2021.015437.

[16] M. Aslam, S. Bouget, and S. Raza, "Security and trust preserving inter- and intra-cloud VM migrations," in *International Journal of Network Management*, John Wiley and Sons Ltd, Mar. 2021. doi: 10.1002/nem.2103.

[17] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing Special Publication 800-144," Dec. 2011. doi: 10.6028/NIST.SP.800-144.

[18] Microsoft, "What are public, private, and hybrid clouds?," https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/.

[19] Jon McElwee, "Cloud bursting for operational resilience," https://www.business-reporter.co.uk/technology/cloud-bursting-for-operational-resilience.

[20] Microsoft, "Introduction to Microsoft Azure Course AZ-900T00-A," https://learn.microsoft.com/en-us/training/courses/az-900t00.

[21] "Study Cloud Migration 2023," Feb. 2023.

[22] IBM Transformation Index: State of Cloud, "A comparative look at enterprise cloud strategy," Jul. 2022.

[23] ISO, "ISO27002:2022," 2022.

[24] "CCM v4.0 Implementation Guidelines Securing the Cloud with the Shared Security Responsibility Model About the CCM WG," 2024. [Online]. Available: http://www.cloudsecurityalliance.org

[25] "CIS Critical Security Controls® v8 CIS Critical Security Controls." [Online]. Available: www.cisecurity.org/controls/

[26] Amazon, "What is multi-factor authentication (MFA)?," https://aws.amazon.com/what-is/mfa/.

[27] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[28] K. A. Scarfone, M. P. Souppaya, and M. Sexton, "Guide to storage encryption technologies for end user devices - Special Publication 800-111," Gaithersburg, MD, 2007. doi: 10.6028/NIST.SP.800-111.

[29] K. A. McKay and D. A. Cooper, "Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations - NIST SP.800.52r2," Gaithersburg, MD, Aug. 2019. doi: 10.6028/NIST.SP.800-52r2.

[30] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, "Contingency planning guide for federal information systems - NIST Special Publication 800-34 Rev. 1," Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-34r1.

[31] Google, "Compute Engine overview - Google Cloud," https://cloud.google.com/compute/docs/overview?hl=pt-br.

[32] K. Stouffer *et al.*, "Guide to Operational Technology (OT) security," Sep. 2023. doi: 10.6028/NIST.SP.800-82r3.

[33] NIST - National Institute of Standards and Technology, "Guide for conducting risk assessments - NIST Special Publication 800-30 Rev1," Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.