International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I10P123

Volume 72 Issue 10, 160-172, October 2024
© 2024 Seventh Sense Research Group®

Original Article

Security Challenges and Solutions in Cloud-Based Software Systems

Zainulabdeen J Alibadi

Central Library, University of Kufa, Najaf, Iraq.

Corresponding Author : Zain.alibadi@uokufa.edu.iq

Received: 09 September 2024 Revised: 11 October 2024 Accepted: 24 October 2024 Published: 31 October 2024

***Abstract* - *This research focuses on the increasing security threats and challenges in cloud-based software systems and potential solutions. Topics talked about are data breaches, insecure APIs/shared technology vulnerabilities in a multi-tenant environment and insider threats. This research clearly indicates the glaring requirement for strong security practices, including encryption, Identity and Access Management (IAM), and continuous monitoring to diminish risks. In addition to the Typo3 example, we can see in case studies such as Capital One and Equifax the devastating effects of misconfigurations (CapitalOne) or unpatched vulnerabilities (Equifax). Other types of emerging threats are discussed, like ransomware, container vulnerabilities and supply chain attacks — all related to the dynamic nature of cloud environments as well. Moreover, a side-by-side comparison with the major Cloud Service Providers (CSPs) — AWS, Azure and Google Cloud.*

Keywords* - *Security challenges, Software, Cloud, AWS, Cloud Service Providers (CSPs).

1. Introduction

Software systems have traditionally been installed and run on the computer infrastructure of the organization that consumes them. As computer infrastructures become increasingly capable and expansive, the budgeting of resources to maintain and improve these infrastructures has similarly increased Cloud computing presents ways of using web-based applications, databases, and services that provide various types of functionality to the extent of replacing the client's computer infrastructure Cloud computing is a twofold construct On the supplier's side, cloud computing is a set of IT resources such as storage, processing, memory, and components like web servers and databases located in data centers These supplier-side resources are abstracted, commoditized, and easy to access at various service and price levels [1]. Developed cloud-based applications and services running on these resources are like traditional programs running on traditional server hardware. They are not affected by or aware of the low-level technologies surrounding cloud computing, such as virtualization and grid computing; today's clients of cloud services have a wide range of mobile client technologies to choose from for accessing the systems, devices, and data they need. As a result, these client-side technologies also differ in their levels of functionality, complexity, and the nature and extent of the cloud features that can be accessed; many traits describe cloud services, such as on-demand access and usage-based pricing, that have to do with the ease with which these services can be discovered, secured, deployed, and accessed Among these many traits are the highly available implementations, data storage execution, and scalability [2]. The existing body of research on cloud-based security challenges has extensively covered infrastructure security, including issues like data breaches, insufficient identity management, and insecure APIs. These studies have significantly advanced our understanding of securing cloud environments at the infrastructural level, emphasizing solutions such as encryption, authentication protocols, and secure network configurations. However, there is a noticeable gap in the literature regarding the specific vulnerabilities within cloud-based software systems, beyond just infrastructure concerns. As cloud adoption accelerates, more organizations are leveraging cloud-native applications and services, introducing new security challenges. These challenges often involve software-specific vulnerabilities such as insecure coding practices, third-party dependencies, and software misconfigurations within cloud ecosystems. While infrastructure security is essential, our research addresses this gap by investigating the vulnerabilities unique to cloud-based software systems. This is increasingly important as the shift to the cloud amplifies the complexity of securing the infrastructure and the dynamic, distributed applications running on top of it. By targeting software-level weaknesses, our work aims to propose more holistic security frameworks that align with the evolving threat landscape in cloud computing. Much of the current research on cloud security focuses heavily on infrastructure protection and generalized threat models. For instance, studies such as those by Smirnov et al. (2022) provide in-depth analyses of vulnerabilities like data breaches and insecure APIs. Yet, their focus tends to lean towards infrastructural concerns and basic security protocols rather than software-specific vulnerabilities. Our research, in contrast, seeks to expand this focus by delving into (software-level vulnerabilities) within cloud-based systems. While previous studies have addressed core issues related to hardware isolation and shared technology risks (Kumar & Gupta, 2021), the specific challenges posed by complex cloud-native applications, including dependency management and continuous integration/continuous delivery (CI/CD) pipelines, have been underexplored This work aims to fill that gap by offering a detailed examination of these software-specific threats and proposing security frameworks that are tailored to them. Another distinctive feature of this research is the emphasis on mitigating the risks associated with (dynamic cloud environments) Most existing solutions address static security models.

However, cloud systems are inherently dynamic, with applications and services frequently scaling and changing configuration based on demand. While Brown and Taylor (2023) explore the dangers of insider threats in dynamic cloud environments, they fall short in addressing the broader context of automated software orchestration and management tools, which can introduce new vulnerabilities if not properly secured.

By comparing our work with existing research, it becomes clear that the novelty lies in shifting the focus from traditional infrastructure-centric security concerns to the (complex, evolving vulnerabilities) found in cloud-based software ecosystems. Our approach not only identifies these specific risks but also integrates modern security measures, such as advanced monitoring tools and AI-based anomaly detection, to provide a more adaptive, resilient defense model that evolves alongside cloud software development practices.

2. Understanding Cloud-Based Software Systems

Cloud computing is an emerging technology that is currently gaining significant attention in the global sphere and is changing the way information technologies are viewed and utilized. It is rated as efficient, inexpensive, and effective in terms of delivering IT services in a distributed manner utilizing network communication. Different from stand-alone systems, cloud computing incorporates architectural elements that normally consist of processors, computer networks, memory, running applications, storage, and other components. Cloud computing is particularly a service that delivers information technology as a utility instead of a product, including capacity, virtual computing, and storage capacity. This technology gives organizations an opportunity to receive IT services on the basis of pay-per-use, and this feature is appealing, as the organization does not need to invest on a large scale in IT resources such as servers. Many service providers have capitalized on this demand, leading to different brands of cloud platforms in the market today. Some cloud platforms include known services that deliver hardware, software, virtual computing, and storage capacity to many subscribers. Note that the nature of cloud computing permits rapid access to dynamically provisioned and released resources over the internet on a web protocol, and payment is only made for the actual resources that were used [3].

2.1. Definition and Characteristics

Cloud computing, an IT paradigm, provides systematic, scalable, and virtualized resources to the client side through high-level services over the Internet Large scale network access, resource pooling, rapid elasticity, measured services, and on-demand self-service are five essential features of cloud computing Cloud computing is the latest platform as it concentrates the application software into the largest data centers and moves everything onto the internet However, there are some problems of software services caused by feelings of discomfort with privacy and security, as it concerns the application service accessing remote and unknown servers Users of the cloud system outsource their data to be maintained by servers responsible for their maintenance, and service providers of cloud computing have to provide service level agreements indicating service downtime and data center access for user data stored on the cloud. However, if the service provider does not comply with the provisions of the contract, it will expose the users to attacks on multiple security threats [4] The most common security threats are data leakage, stolen passwords, storage antivirus scanning requirements, insider fraud risk, loss of visibility and control, and DDoS prevention attacks.

Some reports forecast that security threats, including data leakage, insider fraud risk, and lost service control and data visibility, will outstrip traditional security issues, such as those for firewall attacks. Therefore, it is essential to investigate and address the concerns in cloud services in order to come up with an effective security policy. Cloud-based software services have been attracting attention, and more and more companies have started to provide software support and solution community functions [5].

2.2. Types of Cloud-Based Software Systems

Cloud-based software systems are a special type of Internet-based ICT systems. All they have in common are software characteristics, such as the capability to perform computation on incoming data, to be designed and implemented by means of programming languages, technologies, and tools, and to operate on different types of data.

They also have especially valuable characteristics, for example, covering a large and always updated software market, relieving clients from the difficulties connected with installing, managing, maintaining, updating, and supporting software, realizing the advantages of a pay-per-use commercial model, providing easy access to software applications, and the possibility of using those applications from various device types with different functionalities.

Fig. 1 Cloud-Based software systems

However, according to the type of software provided and the intended commercial target, cloud-based software systems can present many different peculiar characteristics and related implementation issues [6]. As for the provided software types, we can trace three macro-categories of cloud-based software systems One of these categories is the simplest and most traditional concept of software functionality, which is given by the possibility of consulting static content, making cloud-based software a slightly more sophisticated service instead of just a software application.

The other software type is cloud-based software for data manipulation, without any dedicated application to handle and manipulate uploaded information The third category of provided software functionality is the richest in capabilities, represented by cloud-based software systems that support commercial partners in carrying out software application functionalities, as is usually the case for email boxes, management consoles, document editors, calculation services, etc In fact, the functionalities of cloud-based software systems are usually supported by software components, which form the software applications that act as part of some dedicated cloud-based software system and follow the general model of ICT software systems [7].

3. Importance of Security in Cloud-Based Software Systems

The use of the cloud is increasing in all software areas due to development, flexibility, cost considerations, and process management activities. Security issues are also increasing due to the excessive use of the cloud. Therefore, security needs should be more important. Cloud software has its development and maintenance environments; software development environments in all areas must have security concerns and combined software development processes. The cloud software field needs to be more protected than traditional software. These requirements combine the fact that software development and cloud software should have a mechanism that focuses on solving their own security needs and concerns, present different manners of intervention according to area characteristics, and describe a security-based software development and process lifecycle [8] The security of cloud software and the fact that software has checked its components with different inspection mechanisms has always been important In this study, it was aimed to use known security mechanisms and adapt the development processes and metadata that software development processes use by describing them based on the security mechanisms of the cloud software integration tests and to share the four new models of Development Documents and Integration Testing with the project managers and software engineers by presenting four new models.

Furthermore, the software orientation of the operators is different from the development processes The term quality assurance is used at the service end Since the software and service models are different, they should have separate life cycles, but, in general, development teams agreed that integration testing should be performed by checking the outcomes encountered by integration testing as an integration factor in the timeline based on the common integration of the software model services Integration testing has suggested compliance for the integration factors to be verified However, linkage testing tools and methodologies are software-focused and require professional expertise [9].

4. Security Challenges in Cloud-Based Software Systems

As cloud-based software systems grow in size and popularity, they become increasingly important components of an organization’s IT infrastructure. Many organizations choose to host their software artifacts on cloud providers, deploying them on virtual instances and using additional cloud-supplied services. This is referred to as cloud deployment of software artifacts, in which software artifacts are hosted on clouds in the form of images. While the cloud offers a layer of abstraction to its hosted software artifacts, the owner of the software asset is ultimately responsible for its security. This chapter discusses attack surfaces present at the interface between hosted software artifacts and the cloud and proposes possible remediation strategies [10]. In our terminology, cloud deployment refers to the process of hosting software artifacts on clouds in the form of images. A cloud-based software system refers to a composite of a deployed software artifact and additional services provided by clouds. Cloud deployment not only relieves an organization from the burden of managing its own data centers but also offers several benefits, ranging from flexibility in managing peak loads and performance costs to agility in deploying products and meeting customer demands.

Fig. 2 Security challenges in Cloud-Based software systems

However, cloud deployment is not without traps: self-managed private cloud security vulnerabilities may affect cloud-hosted software artifacts; economic factors can result in completely unprotected derived clouds, and software artifacts retrieved from software artifact repositories may incorporate later discovered vulnerabilities [11].Cloud-based systems continue to face a wide array of security challenges, many of which remain unresolved despite the growing body of research dedicated to cloud security. One of the most persistent and critical concerns is the threat of (data breaches), where sensitive information is exposed or accessed by unauthorized parties. The researcher emphasize that these breaches are not limited to any particular type of cloud environment, affecting both public and private clouds equally due to their complex and interconnected infrastructures.

Another ongoing issue is the presence of (insecure APIs) (Application Programming Interfaces). As cloud services rely heavily on APIs for communication between different systems and applications, any vulnerabilities within these APIs can lead to significant security risks. Smirnov et al. also highlight that despite efforts to secure APIs through encryption and authentication, many APIs remain vulnerable to attacks such as Man-in-the-Middle (MitM) or injection attacks, further compromising cloud systems. Additionally, (shared technology vulnerabilities) are a significant concern in cloud environments, particularly in multi-tenant systems. In these setups, multiple clients share the same underlying hardware and software resources, which can lead to potential security breaches if the isolation mechanisms between tenants fail. Another researcher outlined, these vulnerabilities can expose one client's data or applications to other clients within the same environment, making shared infrastructure a weak link in cloud security.

Finally, (malicious insiders) pose a unique challenge in cloud-based systems. These individuals with authorized access to the cloud environment may intentionally or unintentionally exploit their access to compromise the system's security. The malicious insiders can be especially difficult to detect and mitigate due to their privileged access, making insider threats one of the most complex challenges in cloud security. These ongoing challenges illustrate that while progress has been made, cloud-based systems remain vulnerable to a range of security threats that require further research and development of robust security solutions.

4.1. Data Breaches and Data Loss

Data breaches, a subclass of security breaches, occur when data confidentiality is violated. Customer data compromised during a data breach can lead to various consequences, including damage to organizational relationships, a detrimental effect on a company's reputation, and the loss of competitive advantage. Additionally, theft of sensitive information can lead to identity theft or further criminal activities. Data loss can occur from the corruption of files, resulting in financial loss or violating data protection laws. Since the consequences of data breaches display phenomena unique to the cloud, their prevention must be different. One way a software system provider can address such security issues regarding data integrity in the cloud is through the use of cryptography. Using cryptography can help protect data confidentiality, ensure that the data is not tampered with, and confirm that data in storage is similar to the data sent to the CSP [12].

Cryptography has traditionally been used for the protection of PKI However, the use of cryptography may provide a degree of data integrity protection There are two ways in which a CSP, a customer, and/or a third-party supplier of cryptographic systems can achieve this: Cryptographic element protection may be deployed as part of a public cloud system where a user encrypts data before sending it to a public cloud The public cloud then stores the ciphertext and is unable to recover the plaintext without having access to the key information A second approach is to implement a private cloud system where all aspects of the cloud infrastructure are operated by the customer on the customer's behalf Draconian mechanisms can further ensure credit card data and data in pre-production hosting environments The element protection would necessitate storage of the key data on-premises and not at the CSP, reducing the probability of data breaches from insiders, including malicious or accidental data breaches such as accidental deletes or inserts in production databases [13].

4.2. Insecure Interfaces and APIs

Cloud-based software systems expose their interfaces and services for customers to use with flexibility and scalability, but insecure interfaces and APIs can cause damage. Exposed and insecure application programming interfaces and system interfaces are potential attack vectors for attackers using standard application exposure. Security problems are more likely to occur in default settings, especially in interfaces and API settings, when the vendors of the cloud-based software systems use technologies from other vendors. This is especially dangerous for web programs because they can manage cloud-based software systems in a trusted web browser. Even if an authentication mechanism is integrated with web programs, it may not achieve the required security level. Without the need for web security vulnerabilities such as cross-site scripting, insecure authentication channels can give attackers access to management services more easily [14]. These interfaces and APIs operate similarly in connection with web programs in combination with the mandatory requirements for cryptographic protocols and secure software systems. In the actual implementation, an attacker can penetrate almost any channel. In this way, during the entire system life cycle, an attacker can manage unauthorized external systems. Insecure interfaces and APIs also create bottlenecks in other mechanisms for protecting cloud-based software systems. For example, even if the software system security kernel at the client level is secure, extremely strong defenses do not respond to environmental weaknesses and software weaknesses. High API calls require detection and handling, which is an example of sensitive data leaving customer management. During the complex and fast service call process, the processing logic related to identifying exposed unused services is very complicated [15].

4.3. Insufficient Identity, Credential, and Access Management

The utilization of digital identities is increasing, challenging IT managers to manage change SaaS because it is delivered over the web to the consumer, both identifying individuals and setting the scope of the system being used. Knowing who is doing what within the system can be difficult because the actual consumers can be external to the organization. Application access controls sometimes need to be bypassed to enable soft organizational boundaries to exist in the cloud. Cloud computing user enforcement is accomplished through various digital rights management or accessibility enforcement solutions. SaaS vendors should use their identity services, single sign-on, and consumer roles to manage user identities, consumer credentials, delegation, consumer provisioning, consumer access, and incomplete management [16].

Credentials are especially vulnerable to proprietary mechanisms, insider attacks, and man-in-the-middle attacks. Vendor dependence on the integrity and reputation of the vendor has become a weak point in consumer trust. Misappropriation and damaged credentials can result in the first two risks. Consumers' rights should be used for consumer access management, and they need to verify that products and services are of high quality before making a purchase. Requirements for consumer involvement in the community, independent audits, and certification of robust and proven security capabilities need to be verified when evaluating a contextual application [17].

4.4. Shared Technology Vulnerabilities

There are two sources for shared technology vulnerabilities in the cloud: frameworks such as databases or application servers and libraries or engine-based services shared within applications. It is noted that these vulnerabilities are particularly difficult to eliminate. The only solution is to avoid using programmer-written code like this since it often won't contain any other code. Developer-written logic and services may contain shared technology vulnerabilities due to modular functionality and features, and framework issues could potentially impact all applications that employ the technology. While fixes or compensatory measures may exist to reduce exploitability, the bulk of vulnerabilities are, in fact, introduced with the technology design. Summary: Regardless of the focus on developer modules, repeatable projects of technology that are not specific to an application but are commonly found across applications make up a substantial portion of vulnerabilities. Attacking a cloud service model that utilizes a database vulnerability might indiscriminately attack multiple customer applications. Executing a privilege escalation on a shared business logic module may provide unauthorized access to a number of resources. Understanding that all developers must do their part to use and secure technology is important [18].

4.5. Insecure Data Storage

Data is often stored in an encrypted form but may still be vulnerable if the encryption is not properly constructed. Attackers look for encryption applications that don't securely store encrypted data The key management rule within the compliance section states that: "Keys and S-boxes that require protection shall be derived from a 56-bit key for a software-based implementation" Therefore, applications that are intended to implement DES-based encryption will usually support the ability to generate, import, and export keys A typical encryption application includes software plug-ins that integrate into the trusted computing base that can generate keys and carry out the encryption and decryption operations [19]. The application provides a user interface to access cryptographic services, and it has an access control list (ACL) that supports discretionary access and the ability to delegate access rights to others. By using a key control profile, the application ensures that a user's access is restricted to a cleared user group. Unauthorized decryptors embedded within applications that violate the system export a broad spectrum of encrypted sensitive data. These attacks can depend on one or a combination of encryption control points within many DES-based encryption applications.

4.6. Insufficient Due Diligence

Suppliers often fail to thoroughly investigate and validate that their selected cloud provider complies with established standards and best practices critical for the customer's internal governance standards and policies. The result is a solution that ends up being deployed in cloud environments that provide low levels of security and expose the organization to unforeseen and, oftentimes, unnecessary risks. For enterprises, recommendations have been made to ensure appropriate due diligence before entering cloud contracts. In security guidance for critical areas of focus in cloud computing, it is recommended that customers request proof of independent verification of compliance and internal controls. The software system executive tasked with signing the contract with these cloud providers needs to make sure they clearly define these contractual requirements and expect these critical security and governance questions to be answered [20].

Further elaboration on guidance for enterprise organizations looking to adopt cloud services includes credentials of both ethical and compliance experts within the cloud provider, legal to ethics consultancy service firms, and having cloud computing specialists determine if the supplier's chosen cloud provider offers experience in encryption, data residency, and data integration. Organizations must initiate a conversation about expected information protection when discussing with cloud service providers. Organizations should not wait until the service is being implemented before discussing safety requirements. Additionally, the organization should consider specific security concerns for different cloud delivery models. Specifically, organizations need to consider joiner, mover, and leaver business processes for operations that are no longer in the cloud (e.g., data archival with retrieval timeframes and costs). Cloud providers have different security profiles, and depending on which country's regulations apply, entities need to ensure that security measures are capable of complying. Defining the security measures through the use of local as well as internationally recognized security standards is another consideration for the cloud customer [21].

4.7. Account Hijacking

Account hijacking attacks can be damaging to the entire cloud ecosystem. Cloud service providers whose customer accounts have been hijacked can suffer damage to their reputation and risk legal liabilities. The attackers can exploit hijacked accounts to launch other attacks, such as email probing for confidential information, identity theft, and data access and manipulation. Attackers can use emails and other resources within the hijacked user accounts to send provocative emails to other accounts, install a virus, read the social security messages within the security information to capture the password for accessing an online bank account, get information on the arrival of the student's report, modify the arrival of the student's report, or change the instructor's evaluation for the student's exam. Businesses that rely exclusively on the cloud may face severe harm from hijacking in terms of operational disruption, loss of confidential information, financial loss, and damage to corporate reputation [22]. The design and implementation of a robust infrastructure that can resist account hijacking is critical to the mass acceptance of cloud computing. In recent years, there have been many proposals on this issue; again, multi-factor authentication is recommended. Incentives from cloud management and cloud consumers were recommended to further assist cloud computing in utilizing these proposals. Cloud management is also motivated to ensure the security and accountability of its systems to satisfy its users and minimize it becoming the responsibility of users of compromised systems [23].

4.8. Malicious Insiders

The ultimate insider is the cloud provider whose employees run cloud data centers, providing the cloud computing infrastructure to subscribers renting cloud services. The cloud provider and its employees have a level of access to a customer's cloud data and assets that is far higher than in traditional IT outsourcing scenarios. The provider can also conduct cloud forensic analysis on customer data, bypassing criminal investigations and negative publicity. A set of employee departments, including security functions, exists to protect cloud systems from internal and external attacks and from the consequences of operational errors. The insider is an individual or group representing a large organization to monitor data entities [24].

Employees conducting operations for the cloud provider are authorized to access customer data. Some accesses might be initiated manually, established by explicit customer requests or error notifications. In some cases, the accesses are performed automatically, using programmable automation systems such as monitored cloud service interfaces. Anomalous insider accesses might violate security and privacy expectations, and the insider can avoid detection inside traditional audit boundaries. Insider threats are recent examples of discovered insider physical access and digital rights management notices. Insider threat types related to digital risk management and legal aspects and rank their security threat potentials.

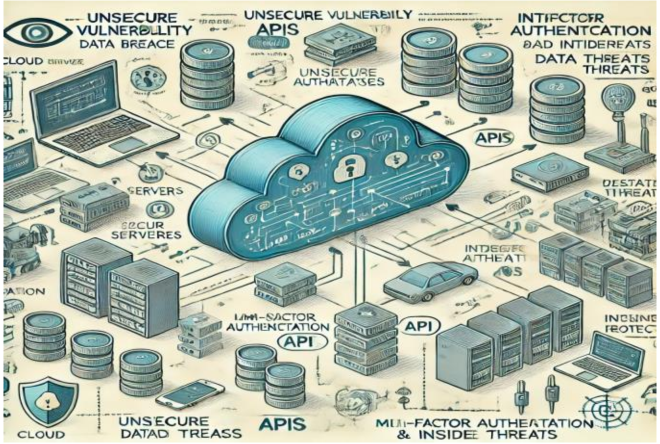

Fig. 3 Malicious insiders

A detailed analysis of insider threats to intellectual properties with suggestions for mitigation data management and cloud security measures can protect a customer's data, independent of the cloud provider employee status.

5. Security Solutions for Cloud-Based Software Systems

In software engineering and the development process, developers and testers should consider and handle all security aspects of software during its various phases. Security requirements are typically hidden requirements and are often omitted, leading to further threats. We can provide security solutions involving the following techniques in our cloud-based software application management to provide real strength against security threats. Several bug-tracking software applications are available in the security management of cloud-based software services. These software applications allow you to gather submissions of bugs and other issues from your team, others who have access to your service, and non-team members. These bug-tracking software applications will help your team keep track of outstanding issues for remediation.

Environment-aware solutions are designed to integrate software with security awareness primarily for software behaviors specific to online environments Such environment-aware solutions can detect certain patterns and states much more accurately than detection on underlying feature representations and have different performance depending on the specific risk of unsanctioned resource access With appropriate configurations within program logic, an appropriately designed integrated precision of almost 100% for over six months with no unsanctioned resource accesses occurring and persistent reasonable true-positive predictive performance can be achieved Such environment-aware solutions can be trained with minimal resource usage and used as introspection tools offering low CPU overhead and tight latency bounds but at a pace ideal for the demands of resource access policy enforcement in a cloud computing environment Such intelligent mechanisms can be integrated with security solutions to maintain effective and meaningful customization across different areas of cloud computing management.

5.1. Encryption and Tokenization

To secure the data, encryption and tokenization are the two primary methods most often employed Although they are both valuable in protecting data, the fundamental differences between the two mean that organizations might wish to apply the methods in unique ways First deployed over 2000 years ago, encryption is the modification of electronic data into another form called ciphertext For the data to be read, it requires a decryption key The data can be transformed easily and quickly both into cipher text and out of it, so a benefit of using encryption is that entire data fields or columns, specific pieces of data, and single characters or number values can be encrypted or decrypted tokenization is where a random token replaces the actual data The actual data would be stored securely in a separate location This added complexity acknowledges that encryption keys are often not isolated to the cipher text, and therefore are available to the data itself in some cases Both encryption and tokenization are capable of protecting sensitive data from being read by adversaries, but one key difference between the two is in how they protect data The main goal behind data encryption is to ensure the privacy of the data and protect it if it is stolen. Among the encryption techniques are Identity and Access Management (IAM). IAM is essential for controlling (who) can access (what) resources and under which conditions in a cloud environment. Cloud services involve multiple layers of access controls, making IAM solutions critical for maintaining a secure and scalable access framework [25]. IAM solutions generally offer the following key features:

5.1.1. Authentication

Ensures that only authorized users or systems can access cloud services (Multi-Factor Authentication (MFA)), which requires users to provide two or more verification factors (e.g., a password and a one-time code from a mobile device), is becoming a standard for securing cloud environments. Authentication can also be handled using identity federation services like (OAuth) or (SAML).

5.1.2. Authorization

Defines the permissions and access policies for users and roles within the cloud environment. Modern IAM systems use Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to determine what actions users can perform. These models ensure that users have the minimum permissions necessary to perform their tasks, a principle known as (least privilege).

5.1.3. Identity Federation and Single Sign-On (SSO)

Identity federation allows users to use their existing credentials from an external identity provider to access cloud resources. This reduces the need for multiple credentials and simplifies user management. Single Sign-On (SSO) is a related technology that allows users to authenticate once and gain access to multiple cloud services without needing to log in again.

5.1.4. Audit and Monitoring

IAM solutions often include logging and monitoring capabilities that track user activities and access patterns. This helps detect unauthorized access or suspicious activities and is critical for compliance and auditing purposes. Cloud providers like AWS offer tools such as (AWS CloudTrail), which logs IAM activity for auditing and monitoring.

Key Challenges and Future Directions

- Granular Control

One of the ongoing challenges with IAM solutions in the cloud is providing granular control without increasing complexity. Fine-grained policies can lead to configuration errors, inadvertently exposing sensitive data or services.

- Zero Trust Security Model

A growing trend in cloud security is adopting a (Zero Trust Model), which assumes that no user, whether inside or outside the organization's network, should be trusted by default. This model requires strict identity verification for every person and device attempting to access resources, aligning with advanced IAM practices.

- Encryption Across Multiple Cloud Services

As more organizations move to the (multi-cloud) environment.

5.2. Multi-Factor Authentication (MFA)

Implementation has security and review benefits when used in cloud services because you use at least two factors to identify yourself. MFA can be a one-time password based on a secret key secured by asymmetric cryptography, fingerprints, facial recognition, and social media. The main goal of MFA is to protect personnel and company data through the networks. Several companies have solutions to implement MFA based on services [26]. For companies, the strategy depends on the organization and the users who are using MFA. The general guideline is to adopt at least two different factors for organization-managed services. When using personal-managed services, a combination of username and password can be acceptable, and there is no need to add extra factors. Companies are encouraged to adopt third-party solutions for MFA to attain security and ease of usability, such as not needing to use an MFA server. By using several MFA solutions, the organization can acquire affordable prices. MFA normally includes cloud services but is not limited to them. This also becomes necessary for company-owned computer services with personal data. MFA is a crucial requirement but has the potential to skirt many real-world security realities. During implementation, weaknesses have the potential to create vulnerabilities that can lead to significant security problems and might become difficult to fix.

5.3. Regular Security Audits and Penetration Testing

In the context of cloud computing, the physical security of data centers and virtual systems becomes a concern for both companies and their third-party partners. Therefore, the security posture of the systems should frequently be tested to enable action in justified cases. These tests are generally classified as regularly performed remote and in-house penetration tests. Regular security audits are used to monitor the system and environment to find potential vulnerabilities, apply quick fixes if available, or make companies aware of the issues within their systems. In general, these tests are conducted by third-party companies that possess the necessary resources and knowledge to exploit potential vulnerabilities within the environment. However, apart from third-party validation, companies may need in-house testing to verify third-party validations and potential penetration precautions developed [27]. Regular security audits are generally conducted in two different ways: remote external network tests and remote external web application tests. Remote external network tests provide an understanding of exposed systems on the network and a pentester's ability to infiltrate from outside the network. Moreover, pen testers do not have access to the internal network to perform these tests, which simulate a real-world scenario. Additionally, synthetic data is used as much as possible in these tests. These are used to detect SQL injection, packet sniffing, and other network layer vulnerabilities.

5.4. Access Control and Privileged User Management

The continuous challenges in the context of access control in mission-critical software systems hosted in the cloud, due to the loosely connected shareholders' collaborations, raised the number of published works International government agencies and product developers are interested in adopting and developing security and privacy requirements from the start of the systems development Nevertheless, few papers seem to adopt a comprehensive approach to address issues across this supply chain Continuous challenges raised in the context of a distributed governance model and gaining collaborative intelligence to promote the perpetual development of innovative software systems are much less debated This chapter presents a major contribution with the empirical validation of the access control concept model in a case organization to depict how the concept is compared to current practices Access control and privileged user management policies, object models, techniques, and best practices usually focus on the cloud service provider and multi-tenant software systems Nevertheless, software systems are developed and managed by a pool of shareholders situated in different geographies and governed through a shared vision of reuse and cost This distributed governance model may have several hierarchies and is commonly used by companies to support control and management activities, achieve high maturity levels of software process standards, decrease risk, increase return on investment, and support integrity applications and complex external partners [28].

5.5. Data Loss Prevention (DLP) Tools

DLP is actually an approach and a set of technologies that allow companies to protect their sensitive information within an enterprise environment They prevent end users from accidentally or maliciously sharing sensitive information In recent years, DLP technologies have been employed to achieve security functionality when developing software applications These DLP technologies can be used as a new and effective means to ensure the privacy and security of cloud-based software systems In general, DLP technologies can be categorized into three types based on the way in which they perform data loss prevention First-generation data loss prevention technologies can be seen as mail firewalls; these technologies can detect sensitive objects and stop the leak of sensitive information Second-generation data loss prevention technologies take the form of restrictions based on file type, location, size, or other technical properties These features are usually available on any software that is in use within an enterprise Setting restrictions based on file type, location, and size is a critical function of data protection when sensitive information is sent outside [29] However, research has found that common data loss prevention methods do not provide effective protection of sensitive data. This indicates that setting a complex policy may not be the best way to manage sensitive data. This shortcoming is mainly due to the fact that data loss prevention technology, in general, mainly focuses on organizing, managing, and protecting data on-premise. The technology has been applied to cloud-based software systems for the first time. A classification rule and sensitive information types uniquely designed for auxiliary work are uploaded to the DLP server in the configuration of DLP. Then, the DLP cloud services are used and integrated with the cloud-based software platforms for which a software system is to be designed and developed. Finally, the client performance of the cloud-based software interacts with the human security administrator, who manually adjusts and checks the sensitivity types and file types.

5.6. Security Information and Event Management (SIEM)

SIEM is intended to help with establishing monitoring across systems and defining the information to be collected for centralized inspection and reporting As the enterprise data is quite spread, log super collectors usually have collection agents distributed across the network, and they all feed the documents and data entries to a shared data repository, making it scalable for very large enterprise environments During log analysis, several patterns can be detected based upon the inspection of infrastructure and its activities, and subsequent containment of the enterprise risks by applying prevention, detection, and alerting Context-based enrichment is applied by adding threat intelligence data during the analysis process in order to enhance correlation, and finally, near real-time reporting of enterprise events is used to provide true threat hunting services to enterprise information security SIEM platforms provide real-time analysis of security alerts generated by network hardware and applications Scope definition and incident diagnostics provide customers with an 'automated incident response' component of specialist security services .

The goal is to make it possible to detect, analyze, prioritize, and respond to threats and minimize risk on networks, servers, applications, and databases Due to the cloud nature of services that are offered in serverless and OaaS, the monitoring covers specific data points This definition is aligned with the possible security challenges and risks that are present in the analyzed cloud-based services However, the defined approach is a generic approach to enterprise information security, so in order to utilize its benefits, a tailored configuration is needed High-level SIEM stops being beneficial as soon as it reaches a scaling point of being a one-size-fits-all solution After that point, it is considered to be short-lived due to the quick evolution of OaaS and serverless FaaS that are constantly being redefined and offer custom solutions to their clientele in order to differentiate their offering from competitors [30].

6. Compliance and Regulatory Considerations in Cloud-Based Software Systems

While compliance and regulatory considerations are important from a business and a sociopolitical point of view, the adoption of cloud computing in most verticals assumes that service providers will manage such requirements. The complexity of the problem is magnified by the number of verticals that cloud computing impacts. Services management, auditing and reporting, data protection, retention, and deletion, as well as eDiscovery for litigation requests, must be managed in the cloud to satisfy this set of business and societal requirements. In this chapter, we will identify some of the key cloud challenges in both regulatory and cultural compliance that have been undergone when moving components of small cloud-based projects to full composition capability. Where specific regulatory and legislative requirements are relevant to the chapters covered in this text, a brief summary is provided in the sections of those chapters.

Legal requirements have a considerable impact on many IT capabilities, but this impact is often lost in discussions about the capacity of technology This deceit can create an implicit belief among customers that because their service or technology operates seamlessly, all the legally required accountability and reporting is automatic Working on two different applications during the past year, the experience is that ensuring compliance is complex and sometimes out of a company's control A website to assist in residency permit applications for clients of a company included two cloud-based services that retrieved personal governmental information on a tourist's movements to and from a country by translating the stamps affixed to that client's passport during each exit and entry No server was established to run the service; instead, a provider hosted this functionality After a year of smooth operations, the tourist office of the host country realized that no contract was signed with the provider, no processing criteria laid out, no defined service interruption clauses for failure of the service, no defined service-level agreement, no associated fee structure, no defined key performance indicators to track the service, no defined contract lifecycle documented, and no conditions for the provider discharging its operations to another provider Satisfaction by the provider was taken as adequate proof of concerns addressed by the tourist office of the host country

7. Case Studies About Security Breaches

Looking at examples of cloud security breaches in the real world provides an illuminating look into vulnerabilities and what can be done to reduce them. Here, we will explore some of the hilarious moments happening to a few organizations that adopted cloud computing. Two key examples include:

7.1. Capital One Data Breach (2019)

Over 100 million customer personal data was exposed due to unauthorized access via misconfiguration in the AWS web application firewall, this led. This case underscores the urgent need for cloud-hands-on executives to configure their security controls properly. Through the rigid application of Identity and Access Management (IAM) best practices, strong encryption standards can be put in place to diminish this type of breach.

7.2. Equifax Data Breach (2017)

A cybersecurity breach that occurred due to an unpatched vulnerability in a cloud-based application resulted that left nearly 147 million consumers' personal data at the fingertips of any efficient cybercriminal. The Equifax breach, in addition to the fact that there may be dozens of wide-reaching data breaches happening every year, and we just have no idea they are occurring, should make patch management a front-burner issue for any organization seeking to protect itself from potential cloud malware threats. At the end of these case studies, it makes overall sense to enforce cloud security transformation, such as encryption measures, proper configuration, and routine patching practice, that will secure vital information and guarantee that undesired situations do not happen again.

7.3. Emerging Threats

Fresh security threats are emerging that cast a wider net to target cloud systems. Key examples include:

7.3.1. Container and Microservice Vulnerabilities

With the rise of containers and microservices for application deployment, as organizations utilize these, more touch points are exposed, which drives up complexity in securing these environments. Attackers can exploit these weaknesses in cloud-native applications by weakening vulnerabilities that are exposed due to misconfigurations related to containers (such as Docker) or orchestrators, which could be Kubernetes.

7.3.2. Cloud Supply Chain Attacks

By attacking the cloud supply chain, a party exploits vulnerabilities in third-party software or services attached to cloud environments. By attacking the supply chain in this way, these actors can bypass traditional security controls and do some serious damage to cloud systems.

7.3.3. Ransomware in the Cloud

Ransomware attacks are also taking a new shape in attacking cloud-based data by encrypting or deleting crucial information stored on the cloud. This attack has been a growing menace with the increasing use of cloud storage, especially in hybrid or multi-cloud environments. It also points to the evolution of adaptive security solutions in dealing with new kinds of threats that are now becoming more common and that are best handled by agile tactics rather than static defenses.

7.4. Comparative Analysis of Cloud Service Providers(CSPs)

This section provides an in-depth comparison of the three largest Cloud Service Providers — Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) from a security standpoint and features.

7.4.1. Amazon Web Services (AWS)

Having a great reputation as the gold standard of security services, among which are strengthened features like IAM (Identity and Access Management), encryption at rest on multiple levels and compliance certificates: SOC 2, ISO 27001, FedRAMP. Other security services, such as AWS Shield for DDoS protection and CloudTrail to monitor API activity, are also available. On the other side, AWS has an architecture that is far more complex than ElasticSearch and this can be a problem – misconfigurations are one of the most common causes for data breaches. Education and governance are crucial to securing AWS environments.

7.4.2. Microsoft Azure

Integration with enterprise systems Azure integrates very well with most enterprises, especially those using Microsoft stacks. To secure the solution, it provides security features like Azure Active Directory for IAM, Role-Based Access Control (RBAC), and encryption services that are in place, such as Azure Disk Encryption. Furthermore, advanced threat protection in Azure is available through Microsoft Defender for Cloud. Though Azure has many different services, and we are focusing on three specific points that can be seen as weak links to a highly secure POC for any company.

8. Case Studies and Examples of Security Incidents in Cloud-Based Software Systems

In this chapter, we presented a case study to demonstrate how to apply the threat modeling process for ensuring the security and privacy of the mobile healthcare software system In this method, actors, assets, goals, resources, and constraints that might concern when considering the architectural security and privacy properties of mHealth software systems should be identified and built in a non-formal structure Time for providing this structure is in the phase of 'Construct Each Data Flow' We secured communication channels by constraint objects and encryption We identified threat agents and established an environment, respecting their capabilities We enumerated the data exchanges in DFD and IS diagrams We examined assets' RICA using threat and defense trees I think with a careful design, we've solved that problem Since the server operates that listens to the submitted mHealth information, they can compare submission data to the security portal data and they know that the requests originated from the mHealth application. The quality of the resulting secure software is determined by the software maintenance process that was used to manage the changes. This makes sense: if problems can be solved before building security and privacy into the software, there will be fewer ongoing concerns to manage during its operation. Functionally, maintaining secure software implies code structure, configuration, and constant enhancement and modification of sub-functions. Security and privacy maintenance ensures that unwanted actors do not enter, disrupt, or destroy functions and that sensitive information is hidden. This implies that architecture and design should be done with security and privacy in mind, using the threat model as a guide. These security and privacy issues are significant challenges for mHealth software systems that will be developed in the cloud.

9. Future Trends and Emerging Technologies in Cloud Security

In 2017 and beyond, as cloud infrastructure adoption accelerates, many organizations and developers have begun to offload more and more services to the internet As with locating the infrastructure on the internet, botnets and various forms of phishing, spam, and DDoS become real threats Because botnet agents are often distributed on end-user systems, related challenges must be addressed for secure cloud computing: managing service trust, accurate intrusion detection, and defending against denial of service With the accelerated trend to place large infrastructures, such as CRM software and core database services, on the internet to avoid building a parallel, Internet-facing infrastructure, organizations must now take steps to secure these systems the same way they have always sought to secure their data

Software systems in the future must increasingly offload their services to cloud infrastructure to “just-in-time” the services they need but don’t want to build Future trends such as botnet attacks, hybrid clouds, ultimate data centers, safe computing, service level management, and predictive security are explained security is now known to be the largest barrier to adopting cloud services As in other components of the infrastructure investment, management systems project new costs The irony here, as systems become more distributed to respond quicker to changes in characteristics, is that customers must consider the increased risks of are they building any new problems in, building in any new weaknesses?.

10. Conclusion and Recommendations

As a company moves its valuable data and systems from in-house hardware to cloud computing, it faces many new and specific threats. These include side-channel attacks that stem from sharing the hardware, and so cache-based attacks are a particular problem in the multi-tenant cloud environment. The increased use of APIs causes further threats. For instance, exploits have been developed that utilize device APIs to send high-frequency signals in devices, leading to device malfunctions. The growing complexity of large cloud-based systems also increases their vulnerability to human error, which is a major cause of security breaches This text has presented many different vulnerabilities that can affect cloud-hosted software systems.

We have also introduced a number of technologies to counter these threats: in particular, we focused on cloud container technology as a building block to provide secure containers to be shared by multiple developers or by the same developer across multiple machines. Finally, we have identified a number of useful further measures to improve cloud-resident software security that go beyond the key recommendations: using cloud certificates, encrypting data, and monitoring software, network, and cloud services to discover intruders We recommend applying the security technologies that we have presented systematically. Given the abundance of threats to defeat, it could otherwise be all too easy to follow security best practices only to be illustrated at well-known and well-understood chokepoints such as the web server.

It is also important to embed all of the individual security technologies we described within a holistic security strategy that requires the developer to enhance the company’s knowledge of threats over time and to ensure that the set of controls remains current to deal with the security vulnerabilities associated with continuously evolving cloud technologies. Finally, we recommend that cloud information security officers define the specific company security requirements for particular hosted cloud services in a security requirements document.

References

[1] Farhan Faridi et al., “Cloud Computing Approaches in Health Care,” *Materials Today: Proceedings*, vol. 51, no. 1, pp. 1217-1223, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Bo Li, and Subodha Kumar, “Managing Software-as-a-Service: Pricing and Operations,” *Production and Operations Management*, vol. 31, no. 6, pp. 2588-2608, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mayank Sohani, and S.C. Jain, “A Predictive Priority-Based Dynamic Resource Provisioning Scheme with Load Balancing in Heterogeneous Cloud Computing,” *IEEE Access*, vol. 9, no. 62653-62664, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Jaskaran Singh Saini et al., “Cloud Computing: Legal Issues and Provision,” *Security and Communication Networks*, vol. 2022, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Svetlana Syarova et al., “Data Leakage Prevention and Detection in Digital Configurations: A Survey,” *Proceedings of the 15th International Scientific and Practical Conference*, vol. 2, pp. 253-258, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Oleksii Smirnov et al., “Simulation of the Cloud IoT-Based Monitoring System for Critical Infrastructures,” *2nd International Conference on Conflict Management in Global Information Networks*, pp. 1-10, 2022. [Google Scholar]

[7] Iffat Fatima, and Patricia Lago, “Towards a Sustainability-Aware Software Architecture Evaluation for Cloud-Based Software Services,” *Software Architecture. ECSA 2023 Tracks, Workshops, and Doctoral Symposium*, Istanbul, Turkey, pp. 200-216, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] S. Vinoth et al., “Application of Cloud Computing in Banking and E-commerce and Related Security Threats,” *Materials Today: Proceedings*, vol. 51, no. 8, pp. 2172-2175, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Dervis Kirikkaleli, Hasan Güngör, and Tomiwa Sunday Adebayo, “Consumption-based Carbon Emissions, Renewable Energy Consumption, Financial Development and Economic Growth in Chile,” *Business Strategy and the Environment*, vol. 31, no. 3, pp. 1123-1137, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Rafiq Ahmad Khan et al., “Systematic Mapping Study on Security Approaches in Secure Software Engineering,” *IEEE Access*, vol. 9, pp. 19139-19160, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hussain Akbar, Muhammad Zubair, and Muhammad Shairoze Malik, “The Security Issues and Challenges in Cloud Computing,” *International Journal for Electronic Crime Investigation*, vol. 7, no. 1, pp. 9-28, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Nelson Novaes Neto et al., “Developing a Global Data Breach Database and The Challenges Encountered,” *Journal of Data and Information Quality*, vol. 13, no. 1, pp. 1-33, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Panjun Sun, “Security and Privacy Protection in Cloud Computing: Discussions and Challenges,” *Journal of Network and Computer Applications*, vol. 160, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Farhan Qazi, “Application Programming Interface (API) Security in Cloud Applications,” *EAI Endorsed Transactions on Cloud Systems*, vol. 7, no. 23, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Roy-Ivar Andreassen, “Digital Technology and Changing Roles: A Management Accountant's Dream or Nightmare?,” *Journal of Management Control*, vol. 31, pp. 209-238, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues, “A Signature-Based Wireless Intrusion Detection System Framework for Multi-channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks,” *IEEE Access*, vol. 12, pp. 23096-23121, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Umer Ahmed Butt et al., “Cloud Security Threats and Solutions: A Survey,” *Wireless Personal Communications*, vol. 128, pp. 387-413, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] Abhishek, Hrudaya Kumar Tripathy, and Sushruta Mishra, “A Succinct Analytical Study of the Usability of Encryption Methods in Healthcare Data Security,” *Next Generation Healthcare Informatics*, pp. 105-120, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Apeh Jonathan Apeh et al., “GRC Strategies in Modern Cloud Infrastructures: A Review of Compliance Challenges,” *Computer Science & IT Research Journal*, vol. 4, no. 2, pp. 111-125, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Hamed Tabrizchi, and Marjan Kuchaki Rafsanjani, “A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions,” *The Journal of Supercomputing*, vol. 76, pp. 9493-9532, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Fatemeh Khoda Parast et al., “Cloud Computing Security: A Survey of Service-Based Models,” *Computers and Security*, vol. 114, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Qianru Gong, “Research and Practice of Cloud Application Security Based on Multi Factor Authentication Technology,” *Forest Chemicals*, pp. 1578-1584, 2022. [Google Scholar] [Publisher Link]

[23] Tanweer Alam, “Cloud Computing and Its Role in the Information Technology,” *IAIC Transactions on Sustainable Digital Innovation*, vol. 1, no. 2, pp. 82-93, 2020. [Google Scholar]

[24] Peter Mell, and Timothy Grance, “The NIST Definition of Cloud Computing,” *National Institute of Standard and Technology*, 2011. [Google Scholar]

[25] Ayman Mohamed Mostafa et al., “Strengthening Cloud Security: An Innovative Multi-factor Multi-layer Authentication Framework for Cloud User Authentication,” *Applied Sciences*, vol. 13, no. 19, pp. 1-14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Avita Katal, Susheela Dahiya, and Tanupriya Choudhury, “Energy Efficiency in Cloud Computing Data Centers: A Survey on Software Technologies,” *Cluster Computing*, vol. 26, pp. 1845-1875, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Ze Jin et al., “P-Verifier: Understanding and Mitigating Security Risks in Cloud-Based IoT Access Policies,” *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles CA USA, pp. 1647-1661, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Fayazoddin Mulla Syed, and E.S. Faiza Kousar, “Role of IAM in Data Loss Prevention (DLP) Strategies for Pharmaceutical Security Operations,” *Revista de Inteligencia Artificial en Medicina*, vol. 12, no. 1, 2021. [Google Scholar] [Publisher Link]

[29] Gustavo González-Granadillo, Susana González-Zarzosa, and Rodrigo Diaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,” *Sensors*, vol. 21, no. 14, pp. 1-28, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[30] Frederik Wulf et al., “IaaS, PaaS, or SaaS? The why of Cloud Computing Delivery Model Selection: Vignettes on the Post-Adoption of Cloud Computing,” *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021. [Google Scholar] [Publisher Link]