Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 263 (2025) 548–556

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Industry Sciences and Computer Science Innovation

Leveraging cyber resilience using cloud services

Luís M. Noronha[a], Carlos Coutinho[b]

[a]School of Technology and Architecture, Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal
[b]Information Sciences and Technologies and Architecture Research (ISTAR), Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal

Abstract

Public cloud services consist of infrastructure, platforms or software hosted by third-parties which are made available over the Internet to end users. Organizations have adopted cloud services when selecting new applications or migrating application workloads to cloud providers, mainly because of their flexibility, scalability, and low entry cost. Security has been a topic of debate because of privacy concerns and the public cloud's inherent exposure to the Internet. The current work intends to assess how cloud services can be a strategic tool in improving an organization's cybersecurity posture. Not only some attack vectors can be reduced but cyber resilience can be setup faster using readily available cloud services. In this article we perform a systematic literature review on these topics, and design a decision support system to help application architects select cloud services from different Cloud Service Providers and make the best use of them to improve an organization's security posture and cyber resilience.

Keywords: Cloud Services; cybersecurity posture; IoT; Resilience; Risk;

1. Introduction

Cloud computing is the delivery of computing services over the Internet ("the cloud"). In the phrase Cloud Computing, the term Cloud (also phrased as "the Cloud") is used as a metaphor for "the Internet" and is believed to be derived from the cloud symbol that is often used to represent the Internet in flow charts and diagrams. The National Institute of Standards and Technology (NIST) defines cloud computing as, a template for providing the suitable and when needed access to the internet, to a collective pool of programmable grids, storage, servers, software, and amenities that can be rapidly emancipated, with little communication and supervision from the provider[1].
According to Gartner in the last five years public cloud services saw an yearly average growth of 23% [2], confirming earlier predictions by Forbes of 19,4% [3]. More and more companies are adopting cloud services which provide several benefits, mainly cost savings, high availability, and easy scalability [4]. Nevertheless cloud computing services are perceived to pose security risks, especially in the public cloud domain, and multiple articles have been written regarding how to address mainly privacy issues.

10.1016/j.procs.2025.07.066

1.1. Cloud Service Delivery and Deployment Models

According to NIST[5], cloud computing is provided in three different delivery models:

1. Software as a Service (SaaS) – a service model in which a cloud user has control on application configurations.
2. Platform as a Service (PaaS) – a service model in which software developers retain a moderate amount of control and customization over deployed applications application-hosting environment, using programming languages, services and tools provided by the cloud service provider (CSP).
3. Infrastructure as a Service (IaaS) – a service model in which a cloud user has control over everything in the cloud except for data center infrastructure.

Starting from the infrastructure layers (network, storage, servers and virtualization) and all the way to the final application layer, each delivery model includes further layers being managed by the cloud provider.
NIST also defines four cloud deployment models:

1. Public cloud - they are operated by service providers using the Internet to provide multiple resources, applications and storage to the general public. Examples of public clouds are Amazon Web Services (AWS), Microsoft Azure Services or Google Cloud Platform;
2. Private cloud - run on data centers owned by a single organization, providing services to different business units. They can exist on or off premises;
3. Community cloud - they are provisioned for exclusive use by a group of entities with shared concerns. It may be owned by one or more of the group members, or operated by a third party. One example is Microsoft's Azure Government Community Cloud, which delivers cloud services that follow FedRAMP or Department of Defense (DoD) cloud computing security requirements exclusively for U.S. Government agencies.
4. Hybrid cloud - is composed of two or more distinct cloud infrastructures (private, community, or public) which are bound together by standardized or proprietary technology.

1.2. Security Standards and Risk Assessment Frameworks

Entities operating in a regulated environment such as healthcare and financial sectors may need to comply with rules such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS) or Sarbanes-Oxley (SOX) [6]. Other companies if either operating in the European Union (EU) or treating personal data of EU individuals will need to comply with the General Data Protection Regulation (GDPR). On the other hand, entities may want to attain certifications such as the ISO 27001:2022 (Information Security Management Systems) or SOC 2 (Service Organization Controls) for managing customer data to prove that they are reliable and to drive their business growth.
Different Risk Assessment methodologies and frameworks have been developed regarding cybersecurity over the years such as ISO/IEC 27005:2022, guidance on managing information security risks, and the NIST Cybersecurity Framework (CSF), now in its second version [7]. NIST CSF is a voluntary framework designed to help organizations manage their cybersecurity risks. Another security standard which is commonly referenced in NIST CSF is NIST's SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations).
Looking specifically at cloud computing standards, Cloud Security Alliance (CSA) issued a cybersecurity control framework for cloud computing: the Cloud Controls Matrix (CCM). It provides guidance regarding 17 domains and defines almost 200 controls. CSP services can be awarded the CSA STAR Certification which in its Level 2 is a third-party independent assessment of a CSP's service security. It combines requirements from the ISO/IEC 27001 management system standard together with the CSA Cloud Controls Matrix.

1.3. Security Posture

The Committee on National Security Systems defines security posture as "the security status of an enterprise's networks, information, and systems based on cybersecurity resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes" [8].

Sometimes the driver to assess and improve an entity's cybersecurity posture are compliance or certification requirements, but security posture is most commonly triggered by the increasing number of observed cyberattacks and perceived risk to company business.
Security posture assessment is influenced by different computerized systems characteristics: a system which is located on-premises and isolated from external networks will be scored differently than a system which resides on a public cloud, running over IaaS or PaaS services.
Companies aiming to achieve security certifications such as the ISO 27001 should look at their security posture, because a good and mature security posture shows concern over security risk mitigation and facilitates obtaining the intended certification.
The following literature review will assess how cloud services have been put in the spotlight in the context of risk management and security posture.

2. Literature Review

2.1. Research Methodology

The current research used the methodology proposed by author Kitchenham[9] for conducting a Systematic Literature Review (SLR) with additional contributions from authors Webster and Watson[10]. The review is structured in three major phases: planning the review, conducting the review and reporting the review[9].

2.2. Planning the Review

2.2.1. Need for a Review

Cloud services security has seen addressed in articles most of time as a privacy concern, inherent to its management by a thir party, the CSP (Cloud Service Provider). Several articles address first and foremost ways to mitigate privacy concerns, e.g. employing cryptography [11] and blockchain [12]. Articles expressing that "security isn't necessarily always a cloud inhibitor" [13] are rare but show that there is room to focus on cloud security advantages.
Different cloud service models (SaaS, PaaS or IaaS), in the context of each cloud type, pose different security advantages that can improve a company's cybersecurity posture. A common attack vector are software vulnerabilities, but a CSP-managed solution SaaS has often a shorter time to remediate compared to an on-premise solution. The goal of the review is to identify whether cloud services have been assessed in scientific articles as having the potential to influence positively a company's security posture and make its IT systems more cyber resilient.

2.2.2. Objective

The current research aims to answer the following questions:
Q1: How can cloud services improve an organization's cybersecurity risk posture?
Q2: How can cloud services make an organization more cyber resilient?

2.3. Conducting the Review

2.3.1. Literature database search

The research included studies that provided guidance on cloud services and cyber resilience based on the paper or article title. We included studies from Computer Technologies and scope, but only written in English. We also focused on conference papers, journal articles and book chapters. We therefore started the literature search by using the keywords "Cloud services" in the Title and with the mandatory words cybersecurity and risk. We searched IEEE Xplore, Scopus, Springer Link, EBSCO and Web of Science, five frequently used databases by researchers across various disciplines. First search at abstract level provided a total of 407 results (Initial). Springer Link results were limited to "Computer Science" only. First step was to remove 26 entries which were found to be duplicates, already existing in other databases (Filter 1). On the next filter we excluded 3 magazine short articles (Filter 2). In case of Springer database we excluded preview-only articles, and focused on titles with the cloud keyword, resulting in a total of 137 articles (Filter 3) which were further reduced to 120 by considering only the ones published in the last 10 years,

since 2015 (Filter 4).
Finally, some articles did not have their full text available. Nevertheless, assessing their abstract and interest some of them were able to be obtained, finishing with a total of 108 articles (Filter 5).

The below table illustrates the number of articles by research terms that were found in the research:

Table 1. Filters used in the SLR protocol.

	Filter 1	Filter 2	Filter 3	Filter 4	Filter 5
IEEE	40	40	40	30	30
Springer Link	283	283	42	41	41
EBSCO	8	5	5	3	3
Scopus	47	47	47	43	33
Web of Science	3	3	3	3	1
Total	381	378	137	120	108

From the group of 108 articles we found that 45 of them addressed cloud and security resiliency, which helps assess our second question formulated in the literature review objectives.

2.4. Cloud delivery models and Security Concerns

We found that the most referenced cloud delivery model is IaaS, being referenced in 71 articles, 56% of total articles assessed, although SaaS is also addressed in many articles (68).
Regarding SaaS and its security challenges, an earlier article by Walters [14] focused on SaaS and the importance of multi-factor authentication (MFA) to prevent breaches. A later article by Murray et al. (2015)[15] covers security concerns of the three cloud computing delivery models and discusses existing cloud-based security tools for each model. They refer previous work by Subashini et al.[16] who designate the following security elements that should be a concern in SaaS application development and deployment:

- Data security
- Network security
- Data locality
- Data integrity
- Data segregation
- Data access
- Authentication and authorization
- Data confidentiality
- Web application security
- Data breaches
- Virtualization vulnerability
- Availability
- Backup
- Identity management and sign-on process

Murray et al. (2015) go on to detail some tools regarding Identity as a Service (IDaaS) and Security as a Service (SECaaS), services which can outsource some of your cybersecurity processes, providing data protection, e-mail security, VoIP security, database security, and general network security.

2.5. Security Standards and Cloud Security Requirements

Companies often operate on a regulated environment, where regulations dictate requirements for doing business and certifications are valued by customers. A group of three information security standards and regulations stands out from the articles as exhibited in Figure 1: ISO 27001, HIPAA and GDPR.
Kun [17] addressed the challenges to regulate cloud service providers in EU financial sector and the implementation of the Digital Operational Resilience Act (DORA). The author further explains how DORA is combining with GDPR and Network and Information Security Directive (NIS 2) to regulate CSPs activity in the EU.
Periasamy J K et al.[18] address data breach prevention in their work and the importance of safeguarding integrity, confidentiality and trustworthiness of sensitive information. Privacy standards such as GDPR and HIPAA were

developed with the intent to ensure data privacy.
Other standards such as COBIT, SOX and PCI-DSS are also addressed in the articles but to a lesser extent.

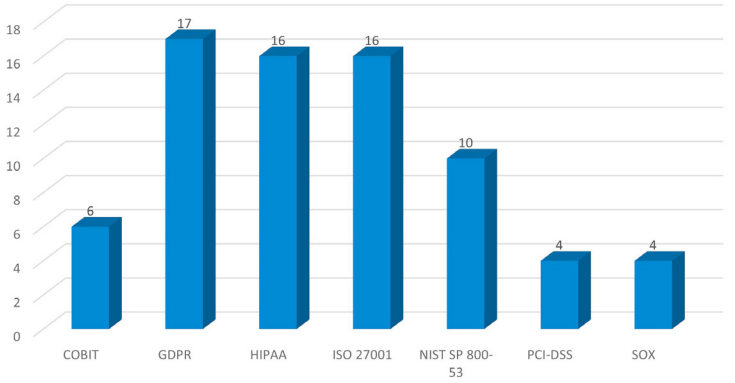

Fig. 1. Articles by Security Standard and Regulation

Regarding risk assessment and cybersecurity frameworks related to cloud services in particular the current research found articles referencing CSA's Cloud Controls Matrix (CCM), NIST's Cybersecurity Framework and FedRAMP. ISO 27005 and FISMA are not specific to cloud services and are a good basis to compare IT system risk score before and after migrating to different cloud services or models.

Finally, vulnerability and threat frameworks are another valuable tool used in articles (see Figure 2). Ammi et al.[19] referenced several of these vulnerability frameworks in their article, namely MITRE's CVE and ATT&CK, proposing a cloud-native architecture to implement a cyber threat intelligence solution.

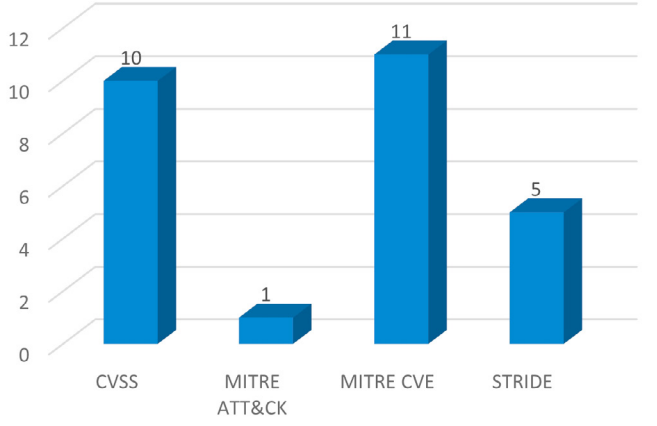

Fig. 2. Articles by Vulnerability and Threats Framework

2.6. Risk Assessment

Over 40 articles addressed risk assessment and tools/techniques on how to mitigate them. For instance, Sen et al.[20] provide a risk assessment framework for organizations considering migrating their applications to a cloud platform. Starting from an application's design they go through the threats that applications may be exposed to

but also how much of that threat is enhanced by being hosted on a cloud platform. This will help clients design and develop applications with much more preparedness towards the security uncertainties associated with a cloud platform .

2.7. Risk Mitigation Strategies

Murray et al.[15] state that cloud service security can be provided via encryption of data — both at rest and in transit — and access control (Identity Access Management). When dealing with cloud applications they also state the importance of two-factor authentication in access control and recommend a hybrid model, where personal information is managed on private cloud and not on public clouds, a tactic to reduce direct exposure. They further state that a well-designed identity management is also an enabler for compliance.

Another tactic to mitigate risk is to subscribe cyber insurance. Two articles in particular addressed the usage of cyber insurance products to mitigate cyber risk:

- Hoang et al.[3] developed a stochastic programming approach for risk management for CSPs, specifically applied to mobile cloud computing. A budget is used by the CSP to invest on security measures and the remaining capital in insurance policies.
- Dasgupta and Rahman[21] defined a framework called MEGHNAD in order for CSPs to estimate the security coverage for a customer's desired insurance tier. E.g. Tier I provides an Expected Security Coverage (ESC) of 90-99% and Tier II provides an ESC of 80-90%. They listed 50 security tools in six defense levels, in order to determine an Optimal Security Toolset, comprehending a multi-objective of coverage, cost and performance. The framework contemplates the possibility of having dependency and exclusion constraints between different tools.

Nevertheless, the focus of the above articles is as not as much on improving security posture by using cloud services but instead on applying mitigation to applications which are already running on cloud services.

2.8. Cloud recommendation systems and security posture

Cloud services recommendation systems help cloud service consumers compare services offered by different CSPs and recommend solutions based on the consumer requirements, but alto taking into account potentially incompatible cloud services. An extensive Systematic Literature Review has been performed by Aznoli and Navimipour[22]. They classified cloud recommendation system's mechanisms into four categories - collaborative filtering, demographic-base, knowledge-based and hybrid - and grouped the articles among 5 publishers along these categories. They found that the recommendation systems provided higher scores accuracy and scalability but the lower scores were on trust and security, Trust and security are therefore the two areas less taken into account in cloud services recommendation systems.

Abdel-Basset et al.[23] presented a framework for evaluating cloud computing services using a neutrosophic multi-criteria decision analysis (NMCDA) approach. They then applied the framework to a case study, assessing three cloud SaaS storage solutions. The ranking of the three solutions also matched the results of an inquiry to 200 users from various organizations on the performance of each solution according to the presented criteria (security, performance, accessibility, scalability and adaptability).

The CloudPerfect project is an European Union initiative that tries to help cloud adopters to identify what cloud services from the different cloud providers best match their application requirements, using previous data gathered from CSPs (Quality of Experience). The latest article by Psychas et al.[24] presented an EPR/CRM use case, with the application deployed at the IaaS level. The results focus on performance and security is not addressed as a decision parameter in this use case.

When considering security posture Coppola et al.[25] starts from NIST's Cybersecurity Framework (CSF) to design a Cloud Security Posture Management (CSPM) tool with emphasis on Amazon Web Services (AWS). The tool is intended to be capable of interfacing with AWS security services such as Amazon GuardDuty, AWS Security Hub

and AWS Inspector. This way the tool can detect misconfigurations and swiftly point possible remediation actions. In a SANS book by Kim et al.[26] Kyle Dickinson also explains how CSPM tools can continuously monitor an organization's application landscape posture, whether the CSPM tool is implemented as a SaaS (e.g. AWS Security Hub), or a managed service. Although using the above mentioned CSPM tools is beneficial when applications are running in a cloud environment, a focus was not placed in performing posture assessment before migrating to the cloud.

3. Decision Support System

Our goal is to design and develop a Decision Support System (DSS) that builds on top of NIST's recent CSF 2.0, queries the potential cloud adopter's application on categories that can benefit from using cloud services and recommends the possible options and their security posture improvement expectation. A business application may see its security risk being lowered by using cloud-native services (e.g. PaaS SQL services, containers), instead of a simple lift-and-shift of a virtual or physical machine to the cloud, or by using complementary security services - which themselves are constantly evolving - provided by each CSP.

3.1. Concepts

Very often the same requirement appears in different versions of the same standard (e.g. NIST CSF 1.1 and NIST CSF 2.0). On other occasions the same requirement can be mapped to different standards (e.g. NIS2's article 21.2.c) "business continuity, such as backup management and disaster recovery, and crisis management" can be mapped to ISO 27002's controls 5.29, 5.30, 8.13 and 8.14) This in turn inspired us to elaborate a concept model with three major concept groups:

- Questionnaire questions and options
- Security Requirements and relation to Standards (or Regulations)
- Vendor Solutions

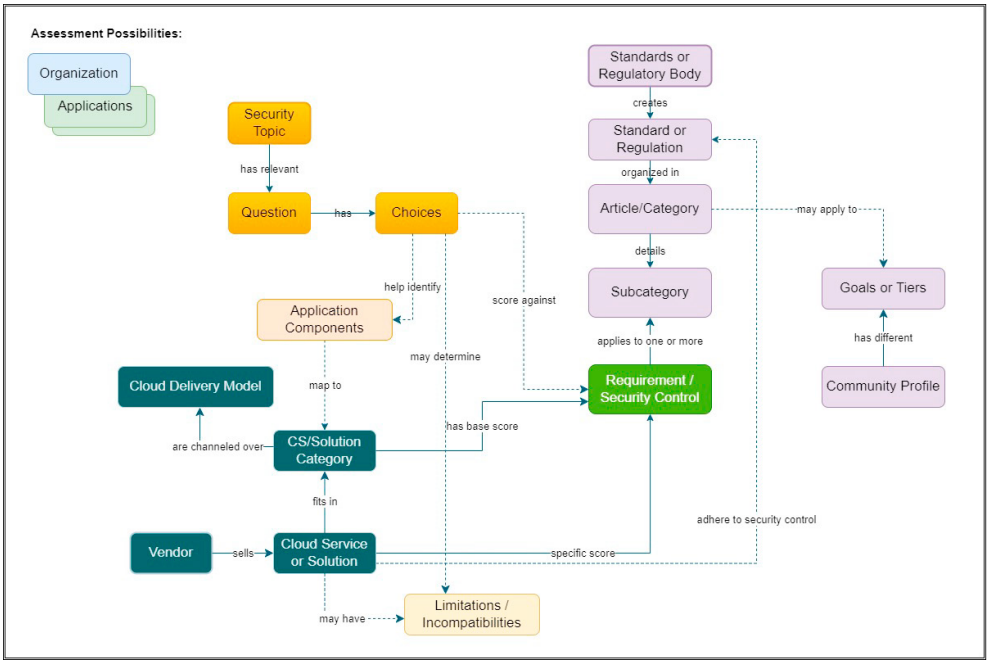

Fig. 3. Decision Support System Concept Model

In Figure 3 you can find the current concept model. The model is well suited to use scores in a scale similar to CSF's Tiers (scoring from Tier 1 - Partial - up to Tier 4 - Adaptive) or CMMI Institute's Levels of Maturity (0 - Incomplete to 5 - Optimizing). Different organization groups may have different business goals which in turn can select or prioritize certain security subcategories. The model can therefore accomodate CSF's Community Profiles which are thoroughly available for CSF v1.1.

3.2. Architecture

The decision support application is designed to use PaaS components. It uses a Kubernetes pod at the front-end User Interface layer containing a Content Management System, three microservices at the backend layer used for:

- storing questionnaire answers;
- producing a report/recommendation;
- searching CSP catalog APIs and updating data

, and a container with a database for storing the application's data (see Figure 4).

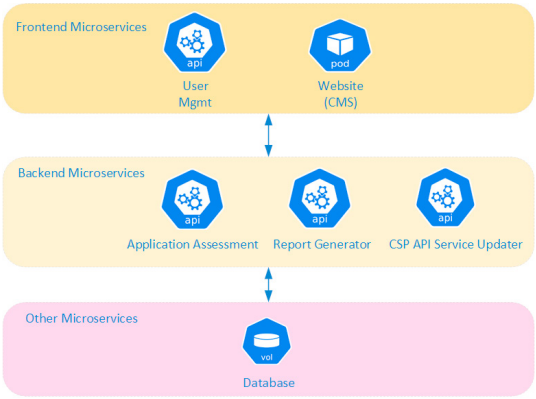

Fig. 4. Decision Support System Architecture

4. Conclusions and Future Work

We observed in the SLR an increasing number of articles over the years addressing cloud services security, which shows the topic's growing relevance in today's world. A large number of articles recommended using SaaS and a cloud-native approach because they make business sense, but we found little evidence in literature of articles addressing whether using cloud services — compared to have solely on-premises applications — could improve an organization's security posture. The Decision Support System being developed is expected to be a valuable tool for potential or already existing cloud adopters that wish to improve their cybersecurity risk posture. The application can be further developed to interface with CSPs APIs in order to help update the service catalog and obtain service pricing.

References

[1] N. Subramanian, A. Jeyaraj, Recent security challenges in cloud computing, Computers & Electrical Engineering 71 (2018) 28–42. doi:10.1016/j.compeleceng.2018.06.006.
URL https://www.sciencedirect.com/science/article/pii/S0045790617320724

[2] Gartner, Inc., Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach $679 Billion in 2024.
URL https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240

[3] D. T. Hoang, D. Niyato, P. Wang, S. S. Wang, D. Nguyen, E. Dutkiewicz, A stochastic programming approach for risk management in mobile cloud computing, in: 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1–6. doi:10.1109/WCNC.2018.8377035.
[4] M. Sterbak, P. Segec, J. Jurc, Automation of risk management processes, in: 2021 19th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2021, pp. 381–386. doi:10.1109/ICETA54173.2021.9726596.
[5] NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Standards Roadmap, Tech. Rep. NIST SP 500-291r2, National Institute of Standards and Technology (Jul. 2013). doi:10.6028/NIST.SP.500-291r2.
URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf
[6] A. G. Krishna, D. S. Rathore, N. S. Singh, H. M. Anitha, Securing Data Workflows: An Insight into Cloud Security, in: 2021 International Conference on Advances in Computing and Communications (ICACC), 2021, pp. 1–5. doi:10.1109/ICACC-202152719.2021.9708115.
[7] G. M. Nist, The NIST Cybersecurity Framework 2.0, Tech. Rep. NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD (2023). doi:10.6028/NIST.CSWP.29.
URL https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[8] CNSS, CNSSI 4009 - Committee on National Security Systems (CNSS) Glossary, publisher: Committee on National Security Systems (CNSS) (Mar. 2022).
URL https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[9] B. Kitchenham, Procedures for Performing Systematic Reviews, Keele, UK, Keele Univ. 33 (Aug. 2004).
[10] J. Webster, R. Watson, Analyzing the Past to Prepare for the Future: Writing a Literature Review, MIS Quarterly 26 (Jun. 2002). doi:10.2307/4132319.
[11] X. Liu, R. H. Deng, P. Wu, Y. Yang, Lightning-fast and privacy-preserving outsourced computation in the cloud, Cybersecurity 3 (1) (2020) 17. doi:10.1186/s42400-020-00057-3.
URL https://doi.org/10.1186/s42400-020-00057-3
[12] D. Gautam, S. Prajapat, P. Kumar, A. K. Das, K. Cengiz, W. Susilo, Blockchain-assisted post-quantum privacy-preserving public auditing scheme to secure multimedia data in cloud storage, Cluster Computing (Apr. 2024). doi:10.1007/s10586-024-04412-8.
URL https://doi.org/10.1007/s10586-024-04412-8
[13] C. Jenkins, The three pillars of a secure hybrid cloud environment., Computer Fraud & Security 2013 (6) (2013) 13 – 15.
[14] R. Walters, The cloud challenge: realising the benefits without increasing risk., Computer Fraud & Security 2012 (8) (2012) 5 – 12.
[15] A. Murray, G. Begna, E. Nwafor, J. Blackstone, W. Patterson, Cloud service security & application vulnerability, IEEE, 2015, pp. 1–8.
[16] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) (2011) 1–11. doi:10.1016/j.jnca.2010.07.006.
URL https://linkinghub.elsevier.com/retrieve/pii/S1084804510001281
[17] E. Kun, Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act, Computer Law and Security Review 52, type: Article (2024). doi:10.1016/j.clsr.2023.105931.
[18] Periasamy J K, Cindy Catherine A, Elamathi R, Subhiksha S, Guarding Against Data Breach, in: 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), 2023, pp. 1–5. doi:10.1109/ICCEBS58601.2023.10449222.
[19] M. Ammi, O. Adedugbe, F. M. Alharby, E. Benkhelifa, Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence, Cluster Computing 25 (5) (2022) 3629–3640. doi:10.1007/s10586-022-03576-5.
URL https://doi.org/10.1007/s10586-022-03576-5
[20] A. Sen, S. Madria, Application design phase risk assessment framework using cloud security domains, Journal of Information Security and Applications 55 (2020) 102617. doi:10.1016/j.jisa.2020.102617.
URL https://www.sciencedirect.com/science/article/pii/S2214212620307821
[21] D. Dasgupta, M. M. Rahman, Estimating Security Coverage for Cloud Services, in: 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, 2011, pp. 1064–1071. doi:10.1109/PASSAT/SocialCom.2011.246.
[22] F. Aznoli, N. J. Navimipour, Cloud services recommendation: Reviewing the recent advances and suggesting the future research directions, Journal of Network and Computer Applications 77 (2017) 73–86. doi:10.1016/j.jnca.2016.10.009.
URL https://www.sciencedirect.com/science/article/pii/S1084804516302375
[23] M. Abdel-Basset, M. Mohamed, V. Chang, NMCDA: A framework for evaluating cloud computing services, Future Generation Computer Systems 86 (2018) 12–29. doi:10.1016/j.future.2018.03.014.
URL https://www.sciencedirect.com/science/article/pii/S0167739X17327814
[24] A. Psychas, J. Violos, F. Aisopos, A. Evangelinou, G. Kousiouris, I. Bouras, T. Varvarigou, G. Xidas, D. Charilas, Y. Stavroulas, Cloud toolkit for Provider assessment, optimized Application Cloudification and deployment on IaaS, Future Generation Computer Systems 109 (2020) 657–667. doi:10.1016/j.future.2018.09.016.
URL https://www.sciencedirect.com/science/article/pii/S0167739X17329357
[25] G. Coppola, A. S. Varde, J. Shang, Enhancing Cloud Security Posture for Ubiquitous Data Access with a Cybersecurity Framework Based Management Tool, in: 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2023, pp. 0590–0594. doi:10.1109/UEMCON59035.2023.10316003.
[26] Kim et al., Cloud Security Practical Guide to Security in the AWS Cloud, Vol. I, SANS, 2020.