The Role of Cloud Service Brokers: Enhancing Security and Compliance in Multi-cloud Environments

Comment [YA1]: Title is suiteable, quite clear and quite interesting. This title truly reflect the contents of the manuscript, catchy and scientifically appropriate.

Abstract

The goal of this study is to put encryption key management strategies into practice while taking legal restrictions and the necessity for data accessibility into account. In order to reduce the danger of unauthorized access to cloud resources, this article explores the creation of Identity and Access Management (IAM) solutions that successfully apply role-based access control and abide by the least privilege principle. The advancement of digital business is both facilitated and disrupted by the usage of cloud technologies. Spending on cloud computing platforms and infrastructure is expected to rise significantly, with a compound annual growth rate (CAGR) of 30% predicted for the period between 2013 and 2018. In comparison, the corporate IT industry as a whole is anticipated to develop at a rate that is quite slow—5%. Additionally, an increasing number of businesses—precisely 85%—are seeing the benefits of using several cloud platforms to boost employee productivity, encourage collaboration, and spur corporate innovation. Regulations and standards are quite complicated, with possibilities for repetition and occasionally discrepancies. Utilizing existing standard models, patterns, architectures, and best practices is one efficient way to manage the difficulties brought on by compliance complexity, uncertainties, and overlaps. Examining regulatory practices and looking for overlaps have been efforts.

Comment [YA2]: This abstract is good, clear, comprehensive and correct.

Keywords: cloud technology, compound annual growth rate, operationalize, Non-Functional Requirement.

Comment [YA3]: This Keywords is good, clear, comprehensive and correct.

1. Introduction:

The use of cloud technology concurrently facilitates and disrupts the progression of digital business. It is anticipated that there will be a significant increase in expenditure on cloud computing infrastructure and platforms, with a compound annual growth rate (CAGR) of 30% projected for the period between 2013 and 2018. In contrast, the entire enterprise IT sector is likely to experience a comparatively modest growth rate of 5%. Furthermore, a growing

proportion of organizations, precisely 85%, are recognizing the advantages of employing several cloud platforms to enhance staff productivity, foster collaboration, and drive business innovation. Nevertheless, the expeditious integration of several cloud platforms and providers presents a distinctive array of obstacles for information technology (IT) departments. In particular, due to the need for Chief Information Officers (CIOs) to effectively coordinate the processes of onboarding, administering, and delivering IT and business services from many portals and suppliers, they have encountered challenges in maintaining consistent performance, security, and control within the multi-cloud ecosystem (1, 2).

Over the past few years, there has been a significant increase in the adoption and utilization of cloud services. Based on the findings of the International Data Corporation (IDC), it is projected that the expenditure on cloud services by the public sector will amount to around $107 billion by the year 2017. Cloud service providers (CSPs), service brokers, and clients are progressively capitalizing on the various benefits offered by cloud computing, including flexibility, scalability, universal accessibility, inexpensive initial costs, flexible payment options, simplified metering, and quick monitoring. Notwithstanding the surge in demand and widespread use, the migration of a corporation to cloud computing is confronted with significant obstacles, namely compliance, security, and privacy concerns. There exists a considerable body of literature examining the topics of security and privacy in cloud computing. However, the focus of our discussion is specifically on compliance elements, as they are closely intertwined with these aforementioned traits. It is worth noting that there is a limited number of studies that primarily address compliance issues in cloud computing (3, 4).

Regulations refer to a collection of regulations that establish guidelines for the utilization of confidential corporate information. The primary objective of these regulations is to safeguard the privacy of consumers and provide security through the enforcement of traits such as confidentiality, integrity, availability, and accountability (CIAA). Compliance involves the act of ensuring adherence to the rules that are established to operationalize the policies outlined within the regulatory framework. According to the perspective held, legal compliance has the potential to emerge as the predominant Non-Functional Requirement (NFR) for a considerable multitude of software systems. Government and state rules are legally binding, whereas industry regulations are typically advisory in nature. Regulations exhibit variability across different

countries; nonetheless, it is common for several countries to adopt nearly identical laws that have been tailored to suit their specific local requirements. In this analysis, our focus is mostly on regulations within the United States. However, it is important to note that many of our findings and conclusions can be extrapolated to regulations outside of the United States. Compliance in cloud technology is a collective obligation that encompasses various stakeholders, including companies, service providers, service brokers, customers, and auditors, due to the inherent characteristics of cloud technology. As per the National Institute of Standards and Technology (NIST), companies have complete responsibility for all matters pertaining to compliance. Non-compliance can lead to financial penalties, legal actions, and a negative impact on a company's reputation (5, 6).

Frequently, the consideration of compliance and security is limited to either the testing phase or the last stage of development, potentially leading to the creation of apps that fail to recognize possible dangers. To ensure the construction of systems that possess high quality and adhere to rules, it is imperative to take into account the enforcement of regulatory measures across all stages of development, including requirements, design, implementation, and testing phases. The Resident Advisor (RA) highlights the importance of approaching the semantics of rules from a conceptual perspective, prior to delving into the intricacies of implementation (7).

1.1. What is cloud security?

Cloud security encompasses a comprehensive array of tactics and protocols that are specifically devised to protect data, apps, and infrastructure residing within a cloud-based ecosystem. Cloud service providers offer businesses the chance to eliminate the costs associated with establishing and managing their own computing infrastructure by granting access to pre-existing resources and services. However, the effectiveness and security of these services largely depend on the client companies themselves. The following are essential cloud security measures that should be implemented to ensure the protection and integrity of cloud-based systems and data (8, 9).

- Cloud security involves a variety of established procedures; it is important to consider the essential ones.

- The scope of responsibilities pertaining to cloud security
- The distribution of security responsibilities between cloud service providers and clients varies depending on the chosen cloud service model.

Infrastructure as a Service (IaaS) refers to a cloud computing model where the provider offers essential infrastructure components such as servers, network, and storage. However, it is the client's responsibility to ensure the security of the operating systems, applications, and data that they choose to deploy within the cloud environment (10).

Platform as a Service (PaaS) involves the provision of both infrastructure and a development platform by the service provider, encompassing operating systems and development tools. The responsibility for ensuring the security of the applications developed by the client, as well as the data processed by these applications, lies with the client (11).

In the context of Software as a Service (SaaS), the provider assumes the responsibility of delivering fully functional programs that are readily available for usage, while also ensuring the security of these applications. Nevertheless, it is important to note that the client retains accountability for the configuration and security of the data they store and process within these apps, as well as for the management of access to that data (12).

1.1.1. Data management.

This spans the fields of cryptography and key management. Cryptography is employed to safeguard data throughout its various stages, including storage (at rest), transmission (in motion), and consumption (in use). Key management is a critical process that encompasses the secure storage, generation, exchange, and utilization of cryptographic keys. Access management refers to the process of controlling and regulating the access to resources, systems, and information inside an organization. It involves implementing (13).

This pertains to the processes of authentication and authorization. Authentication is a process that validates the identification of an individual or a system that is seeking authorization to access a certain resource or service. Authorization is the process through which the permissions

and privileges granted to an authenticated user or system are determined, dictating what actions they are allowed to perform (14).

1.1.2. The adherence to security standards

In the realm of cloud security, there exists a range of security standards that may be deemed relevant and appropriate. General standards, such as ISO 27001, as well as industry-specific standards like PCI DSS for the payment industry or HIPAA for healthcare, can serve as benchmarks for organizations. By adhering to these standards, it aids in ensuring the maintenance of security and compliance with regulatory obligations. Furthermore, we possess a comprehensive piece regarding the adherence to HIPAA regulations in relation to cloud infrastructure. In this section, we provide an in-depth explanation of the Health Insurance Portability and Accountability Act (HIPAA), elucidating its purpose and scope. Furthermore, we delve into the technological measures implemented by our engineers to ensure compliance with HIPAA regulations, highlighting the intricacies involved in this process. Additionally, we shed light on the issues encountered by our engineers throughout the implementation phase, elucidating the complexities and obstacles they had to overcome. It is strongly advised to engage in reading activities (15).

1.2. What is a multi-cloud strategy?

The cloud sector is through a process of evolution, resulting in the emergence of numerous cloud providers, each presenting distinct services and conditions. The emergence of the multi-cloud strategy has resulted in a situation where over 76% of firms are presently utilizing two or more cloud service providers, and this inclination is anticipated to persist in its upward trajectory (16).

A multi-cloud strategy refers to the adoption of a comprehensive approach by an organization, wherein it leverages a combination of public, private, and hybrid cloud environments. Organizations are able to utilize the advantageous features and services offered by cloud providers in order to optimize certain business processes and adhere to regulatory requirements.

For example, a particular service provider may offer resources for high-performance computing, while another provider may specialize in advanced analytical tools or offer more favorable conditions for data storage. Additionally, several legislation require that citizen data be kept within specific geographical boundaries (17).

1.3. Navigating Multiple Clouds Presents Unique Challenges

In contemporary commercial environments, both business customers and application developers have increasingly high expectations for cloud-based services, necessitating prompt accessibility and limitless scalability.

The phenomenon of "shadow IT" arises as a consequence of business divisions engaging in direct acquisition of cloud services, when employees effectively circumvent established company policies and security procedures. This phenomenon commonly arises due to a lack of close alignment between information technology (IT) and the operational requirements of individual lines of business (18).

The proliferation of multi-cloud platforms amplifies the security vulnerability of the enterprise. Ensuring the security of firm data during its transition from on-premises infrastructure to various private and public cloud environments, and vice versa, emerges as a crucial yet complex task.

The management of a diverse range of public and private cloud platforms is a crucial responsibility for IT departments. These platforms exhibit varying capabilities, processes, pricing, and performance levels. This phenomenon not only incurs a significant amount of time but also has the potential to result in uncontrolled escalation of expenses if not effectively monitored and regulated (19).

Cloud brokers have emerged as proficient orchestrators capable of effectively managing the intricacies associated with numerous cloud ecosystems, hence facilitating the transformation of firms into digital corporations (20).

2. Definition of Cloud Services Brokerage

According to Gartner, cloud services brokerage (CSB) is a business model and IT role wherein an entity, such as a company, enhances the value of one or more cloud services (whether public

or private) on behalf of multiple consumers. This is achieved through three key roles: aggregation, integration, and customization brokerage. The cloud broker functions as a middleman between the buyer and sellers of cloud computing services, serving as a middle layer in this process. Despite being categorized as an emerging technology trend, it is projected that the worldwide Cloud Service Brokerage market will experience a compound annual growth rate (CAGR) of 29.6%, resulting in an increase from $5.24 billion in 2015 to $19.16 billion by the year 2020 (21).

2.1. Types of Cloud Brokers

There are two types of cloud brokers (22):

2.1.1. **Cloud Aggregator.** An aggregator refers to a mediator that consolidates and combines various service catalogs into a unified user interface. Subsequently, the client proceeds to choose a variable number of services that align with their particular business requirements, while ensuring that they are only obligated to remit a solitary payment to the broker. The cloud aggregator model is often regarded as a cost-effective and efficient strategy for clients in comparison to the individual procurement of each service. Aggregators fulfill a crucial role in the management of cloud provider partnerships and services within their capacity as resellers. In addition to cloud services, the broker may provide supplementary offerings such as security and governance, which will be further elaborated upon in subsequent discussions. In general, the primary objective of the aggregator is to systematically organize a comprehensive collection of services, so offering a unified interface for all business and IT services. This approach enhances flexibility and adaptability, while also yielding cost and time savings. Cloud integrators are entities that specialize in the integration of cloud computing technologies into existing systems and processes. Integrators enhance operational efficiency and mitigate business risks by implementing automated workflows across hybrid environments, utilizing a unified orchestration system. After the completion of the migration process, the integrator has the capability to offer continuous assistance to the organization as required..

2.1.2. **Cloud Customizers**. Customization refers to the process of making alterations to pre-existing cloud services in order to align them with the specific requirements of a

Comment [YA4]: Too many dots..., kindly just use one.

business. on certain instances, the broker may also undertake the development of further functionalities to be executed on the cloud, as necessitated by the organization. The aforementioned function plays a crucial role in the establishment of a comprehensive cloud infrastructure, characterized by enhanced visibility, adherence to regulatory standards, and seamless integration of fundamental IT operations.

3. Benefits Of Cloud Service Brokers And Multi Cloud Strategy:

Cloud service brokers provide solutions that turn IT into a growth accelerator for end customers. Additional benefits of cloud services brokerage include (23-35):

3.1. Providing Expertise

Cloud Service Brokers (CSBs) play a crucial role in mitigating the obstacles associated with the adoption, management, and customization of cloud services. This is achieved by addressing deficiencies in knowledge and skills that may exist among users. It is worth mentioning that brokers are frequently engaged to assess services offered by various vendors and furnish customers with guidance on using cloud services for the purpose of driving digital innovation. Upon the completion of the research, the broker provides the customer with a comprehensive compilation of suggested vendors, accompanied by a thorough analysis of service features, pricing breakdowns, service level agreements (SLAs), and additional relevant factors. The utilization of the broker's toolkit and knowledge facilitates the process of making decisions that are objective, accurate, and well-informed.

Comment [YA5]: Why are there no specific citations ?

3.2. Negotiating on Behalf of the Customer

Cloud brokers are occasionally granted the authority to engage in contract negotiations with cloud service providers on behalf of their clients. In such instances, the broker is bestowed with the power to engage in service contracts with many vendors, so presenting a commendable approach to cost reduction. Furthermore, it is common for CSBs to possess established affiliations with several vendors, and in certain instances, they may already have prearranged contractual agreements in place. This advantageous situation facilitates the expeditious acquisition of vendors by CSBs. The aforementioned advantage is typically prevalent in the context of cloud aggregators.

Comment [YA6]: Why are there no specific citations ?

3.3. Simplifying Operations

Cloud service brokers (CSBs) have the potential to mitigate redundancies, enhance resource efficiency, and enable the IT department to effectively manage cloud consumption expenses. Moreover, the implementation of a real-time integrated perspective of both on-premise and public cloud resources offers the company the advantage of reducing errors associated with the management of numerous cloud platforms throughout the entire business.

Comment [YA7]: Why are there no specific citations ?

3.4. Specialization

Organizations are afforded the opportunity to enhance the efficiency of their infrastructure for particular workloads by leveraging specialized services offered by various cloud providers. As an illustration, a corporation may opt to utilize a cloud service that provides substantial bandwidth to facilitate the processing of extensive data sets. Conversely, another service may be employed to cater to applications that necessitate a heightened level of dependability and accessibility. This enables enterprises to optimize the benefits offered by individual cloud providers, taking into account the unique demands of their workloads.

Comment [YA8]: Why are there no specific citations ?

3.5. Cost efficiency

Facilitates the ability of enterprises to enhance cost optimization. Cloud providers may present different pricing structures and terms for their services. Organizations have the option to select from these suppliers based on their present requirements and financial resources. This may entail the utilization of cost-effective services for non-essential workloads or the adoption of more costly yet dependable services for applications of utmost importance. Additionally, we possess a collection of publications wherein we elucidate the methods for enhancing infrastructure and development expenditures through the lens of our firsthand expertise.

Comment [YA9]: Why are there no specific citations ?

3.6. Disaster recovery

It improves the dependability and accessibility of the systems within the firm. In the event that a particular cloud provider experiences difficulties, an alternative provider can effectively sustain service provision. This practice mitigates the potential for operational interruptions and guarantees the uninterrupted functioning of the enterprise. Furthermore, the adoption of a multi-cloud approach enables enterprises to enhance their disaster recovery capabilities by leveraging the distribution of data and applications across several cloud platforms.

Comment [YA10]: Why are there no specific citations ?

3.7. Avoidance of vendor lock-in

Organizations can mitigate the risk of excessive reliance on a single cloud provider by employing numerous cloud providers. This approach offers increased adaptability in contract negotiations and resource allocation, so safeguarding the business against potential price fluctuations or modifications in services imposed by a sole provider.

Comment [YA11]: Why are there no specific citations ?

3.8. Improved security and compliance

The utilization of several cloud environments can enhance security measures by distributing data across various platforms. Additionally, certain cloud providers may offer enhanced security measures and compliance with specific standards that are essential for particular business sectors.

Comment [YA12]: Why are there no specific citations ?

4. Multi-cloud security challenges

Along with these advantages, multi-cloud environments present a series of unique challenges (36-46).

4.1. Staff training

Professionals employed in multi-cloud environments are required to possess a comprehensive understanding of fundamental cloud security principles as well as the distinctive attributes associated with each individual cloud platform. This may involve receiving instruction in the utilization of specialized security tools and interfaces, as well as comprehending the unique

security policies implemented by each cloud service provider. Providing extensive training to employees in these domains may necessitate substantial allocation of time and financial resources.

Comment [YA13]: Why are there no specific citations ?

4.2. Cloud migration management

The process of transferring data and apps from one cloud platform to another requires careful and thorough preparation and implementation. The task at hand encompasses the imperative of safeguarding the integrity and confidentiality of data during its transfer, while also overseeing the regulation of data access on the newly implemented platform. The execution of this procedure can be intricate and necessitates significant endeavors to ensure its fulfillment.

Comment [YA14]: Why are there no specific citations ?

4.3. Security policy management

Maintaining consistent security rules in a multi-cloud environment can provide significant challenges. Each cloud provider may possess distinct methods and protocols for managing security, hence exhibiting potential variations in comparison to alternative platforms. The aforementioned situation may give rise to challenges in upholding coherence and efficacy in security protocols.

Comment [YA15]: Why are there no specific citations ?

4.4. Encryption management

Managing encryption keys in a multi-cloud context might present a challenging undertaking. The accessibility of keys across various cloud platforms must be ensured, while simultaneously guaranteeing their secure storage and usage. Specialized encryption key management systems that offer support for multi-cloud setups may be required in this scenario.

Comment [YA16]: Why are there no specific citations ?

4.5. Resource management

The management of resources in a multi-cloud context presents challenges arising from variations in pricing structures and reporting procedures among different cloud service providers. This may need the deployment of specialist techniques for monitoring resource allocation and optimizing financial expenditures.

Comment [YA17]: Why are there no specific citations ?

4.6. Monitoring challenges

The task of monitoring activity and security events in a multi-cloud environment presents difficulties owing to the disparities in logs and audit data offered by different cloud platforms. The implementation of centralized security monitoring systems that include the capability to aggregate and analyze data from many sources may be necessary.

Comment [YA18]: Why are there no specific citations ?

4.7. Multi-cloud security threats

Multi-cloud systems may present distinct security risks as well. The emergence of these threats can be attributed to a multitude of variables, encompassing intricate configuration setups, failure to adhere to legal mandates, susceptibilities in access and identity management systems, as well as vulnerabilities spanning across diverse layers such as networks, apps, and APIs.

Comment [YA19]: Why are there no specific citations ?

4.8. Multi-layer threats

Within a multi-cloud context, there are numerous potential risks that manifest across various tiers, encompassing networks, application programming interfaces (APIs), and applications. At the network layer, potential issues may arise due to misconfigurations of network devices, such as firewalls and load balancers. These misconfigurations can result in the occurrence of distributed denial-of-service (DDoS) attacks or unauthorized interception of data. At the application level, potential threats encompass vulnerabilities present in application code, thereby enabling SQL injections or cross-site scripting attacks. Additionally, vulnerabilities in APIs may grant attackers the ability to circumvent access controls or manipulate API functionality through injection attacks or brute force attacks utilizing credential stuffing.

Comment [YA20]: Why are there no specific citations ?

4.9. Encryption threats

Encryption serves as a fundamental technique for safeguarding data within cloud environments; nevertheless, it also introduces distinct vulnerabilities. The loss or compromise of encryption keys might result in the loss of data accessibility or data disclosure. This phenomenon may arise as a result of an external assault, internal abuse, or mere inadvertence. Certain cloud providers may employ proprietary key management systems that may lack compatibility with other systems.

Comment [YA21]: Why are there no specific citations ?

5. How To avoid threats; best practices

In the contemporary landscape, characterized by the growing prevalence of multi-cloud systems, ensuring the security of these environments has emerged as a crucial concern. The following are a set of recommended procedures that can enhance the security of multi-cloud settings (47-54).

Comment [YA22]: Kindly..., it would be best to cite the related statement.

1. The concept of team education. It is imperative to ensure that the team possesses a profound comprehension of multi-cloud security principles, encompassing the intricacies associated with operating on diverse cloud platforms and adhering to various security procedures.

2. The formulation of an incident response strategy. The development of comprehensive incident response plans that take into account the unique characteristics of each cloud environment is crucial. These plans should encompass methods for effectively identifying, isolating, and minimizing problems.

3. The allocation of responsibility. The delineation of security responsibilities between a corporation and cloud providers must be explicitly established, taking into account the nature of service provisions, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Additionally, careful consideration should be given to the particulars of Service Level Agreement (SLA) contracts, as well as the features of Service Level Objectives (SLO) and Service Level Indicators (SLI).

4. The consolidation of security tools. across order to achieve consistency and expedite incident response across all cloud environments, it is imperative to establish uniformity in security tools and their corresponding usage rules.

5. One important aspect to consider in maintaining a secure environment is the implementation of consistent security policies. The objective is to formulate and execute cohesive security rules that can be uniformly enforced across various cloud platforms, thereby guaranteeing a consistent standard of safeguarding measures.

6. The first concern is security. Incorporate security concepts into the first stages of development and deployment procedures, as well as consider pre-established criteria when selecting cloud providers.

7. Identity and access management (IAM) is a crucial aspect of information security and data protection. It refers to the processes and technologies used to manage and control user identities and their access to various systems, applications, and resources within an organization. IAM encompasses the establishment, maintenance, and termination of user This paper aims to explore the development of Identity and Access Management (IAM) solutions that effectively implement role-based access control and adhere to the least privilege principle in order to mitigate the risk of illegal access to cloud resources.

8. The topic of discussion is data encryption. Encryption methods should be implemented across all stages of the data lifecycle, including storage, transmission, and processing, in order to guarantee the confidentiality and integrity of the data.

9. The topic of discussion pertains to the administration of encryption keys. This study aims to implement encryption key management solutions that consider legislative constraints and the imperative to provide data accessibility as needed.

10. Ensuring security measures across diverse cloud platforms. Utilize security capabilities, such as CloudGuard offered by Check Point, to ensure persistent safeguarding of data and apps during their transition across diverse cloud platforms.

11. Guaranteeing perceptibility within a multi-cloud framework. Utilize monitoring and analytics technologies, such as Splunk or Datadog, to facilitate comprehensive oversight and management of all cloud environments, hence enabling prompt identification and mitigation of security events.

12. The implementation of routine security testing. It is recommended to regularly do security audits and penetration tests in order to identify and address vulnerabilities in a timely manner, as well as to assess the efficacy of existing security measures. One such approach is employing tools such as OWASP ZAP for the purpose of conducting penetration testing, or alternatively, engaging the services of external businesses to perform comprehensive security audits.

5.1. Finding and using the right cloud security solutions (55-61)

Comment [YA23]: Kindly..., it would be best to cite the related statement.

- It is imperative to carefully choose cloud security solutions that align with the specific demands and capabilities of each firm. The following are the overarching procedures for selecting and implementing appropriate cloud security solutions.
- • Gaining comprehension of the specified criteria
- Please outline the primary security needs, encompassing the necessary level of safeguarding for data and applications, adherence to regulatory standards, and the unique attributes of the cloud infrastructure in question.
- • Evaluating the existing solutions
- Conduct a comprehensive analysis of the market and assess the existing cloud security solutions, taking into account their functionality, compatibility with your specific cloud environment, and associated costs.
- • Conducting a comparative analysis and critical assessment of potential solutions
- The selected solutions can be compared by assessing their performance across various critical characteristics, including the degree of security, adaptability, scalability, and financial implications.
- • Performing a proof of concept
- Conduct a proof of concept utilizing the chosen solutions to validate their efficacy and compatibility inside your cloud infrastructure in realistic scenarios.
- The execution of the selected solution
- Once a suitable solution has been chosen, proceed with its implementation, ensuring seamless interaction with your cloud environment and existing security protocols.
- The process of monitoring and making necessary adjustments
- Following the implementation of the solution, it is imperative to consistently monitor and make necessary adjustments to its settings and parameters in response to evolving situations and security demands.

- Regular review and updating are essential components of maintaining accuracy and relevance.
- It is vital to engage in periodic evaluations and revisions of one's cloud security solution in order to ascertain its pertinence and efficacy in light of perpetually evolving threats and security prerequisites.

Conclusions:

Comment [YA24]: My suggestion... is that the **Conclusion** should be made into a separate chapter
(in this case is **Chapter 6**).

The current study entails a comprehensive analysis of the existing practices in regulatory compliance. This investigation is conducted through an examination of recent scholarly publications and a review of various industrial methodologies. Regulations and standards have a high degree of complexity, potentially displaying redundancy and sometimes inconsistencies. One effective approach to managing the challenges associated with compliance complexities, uncertainties, and overlaps is to utilize established standard models, patterns, architectures, and best practices. Efforts have been made to examine regulatory policies and identify instances of overlap. Nevertheless, there has been a lack of initiative in enhancing the precision of their software architecture at a more advanced level, which might potentially provide guidance for design and implementation endeavors. The implementation of these standardized methodologies has the potential to enhance compliance, security, privacy, and the overall software quality within cloud systems. This study investigates the extent to which publications and industry have taken into account this specific feature as an indicator of their capacity to manage the growing complexity. Although there are various factors that influence compliance, we have prioritized the correct utilization of architectures as a crucial feature.

An RA (Risk Assessment) has been developed for the purpose of complying with the Health Insurance Portability and Accountability Act (HIPAA), as well as a CSRA (Cloud Security Risk Assessment) specifically designed for cloud-based systems. These assessments were conducted using a five-step process as outlined in the proposal. The utilization of architectural patterns can serve as a shared medium of communication among various stakeholders in the field of

architecture, including architects, developers, business owners, managers, service providers, and auditors. Additionally, it can serve as a point of reference for the development and execution of automated systems utilized in the realms of testing, auditing, and compliance verification. There is a pressing need to develop more research areas (RAs) focused on services, platforms, regulations, and policy-based systems in order to enhance the overall quality of software. The use of abstract compliance architectures that offer enhanced flexibility and adaptation to emerging rules holds significant importance in persuading the sector to embrace them. It is imperative to integrate the efforts focused on compliance with those dedicated to security, so establishing a cohesive approach that encompasses both facets..

Comment [YA25]: If you consider this statement to be an ***important finding*** in this manuscript, you should ***highlight*** it and *reformulate* the sentence so that it appears to be an ***important*** and interesting (***eye-catching***) sentence.

Comment [YA26]: Too many dots..., kindly just use one.

References:

1. Amazon. Amazon web services: risk and compliance. http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf.
2. Amazon. AWS compliance. https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.
3. Amazon Web Services. Risk and compliance. https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.
4. Avgeriou P. Describing, instantiating and evaluating a reference architecture: a case study. Enterp Archit J. 2003. Available online:http://www.rug.nl/research/portal/files/14407113/2003EnterpArchitJAvgeriou.pdf. Accessed 22 Apr 2016.
5. Booch G, Rumbaugh J, Jacobson I. The unified modeling language user guide. 2nd ed: Addison-Wesley; 2005.
6. Brandic I, Dustdar S, Anstett T, Schuman D, Leymann F, Konrad R. Compliant Cloud Computing (C3): architecture and language support for user-driven compliance management in clouds, Proceeding CLOUD '10 Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing. Miami, Florida, USA: 2010; 244–51.
7. Buschmann F, Meunier R, Rohnert H, Sommerlad P, Stal M. Pattern-Oriented Software Architecture: A System of Patterns, vol. 1.Wiley; 1996.

8. Cisco. Cisco compliance solutions. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/pci-compliance/pci-dss-30-wp.pdf. Accessed 22 Apr 2016.

9. Cisco. The risk management framework: building a secure and regulatory compliant trading architecture. http://www.cisco.com/web/strategy/docs/finance/risk_mgmt_C11-521656_wp.pdf.

10. COBIT. IT Governance Framework - Information Assurance Control, ISACA. http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx.

11. Dasgupta D, Naseem D. Security and compliance testing strategies for cloud computing. https://umdrive.memphis.edu/g-mis/www/memphis/step/STEP2012/STEP2012Proceedings3.pdf.

12. Dasgupta D, Naseem D. A framework for estimating security coverage for cloud service insurance, Proceedings 7th Cyber-Security and Information Intelligence Reserach Workshop, Oak Ridge, TN, October 12-14, 2011.

13. FedRAMP. FedRAMP compliant cloud systems. https://www.fedramp.gov/resources/documents.

14. FedRAMP. Federal Risk and Authorization Management Program (FedRAMP). https://www.fedramp.gov/resources/documents.

15. FedRAMP. FedRAMP Third Party Assessment Organizations (3PAOs). https://www.fedramp.gov/resources/documents.

16. Fernandez EB, Yuan X. Semantic analysis patterns, Proceedings of the 19th Int. Conf. on Conceptual Modeling, ER2000. p. 183–95.

17. Fernandez EB, Larrondo-Petrie MM, Sorgente T, Van Hilst M. A methodology to develop secure systems using patterns. In: Mouratidis H, Giorgini P, editors. Integrating security and software engineering: advances and future vision. IDEA Press; 2006. p. 107–26.

18. Fernandez EB, Mujica S. Two patterns for HIPAA regulations, Procs. of AsianPLoP (Pattern Languages of Programs) 2014. Tokyo: 2014.

19. Fernandez EB, Monge R, Hashizume K. Building a security reference architecture for cloud systems. Requir Eng. 2015; doi:10.1007/s00766-014-0218-7.

20. Fernandez EB, Yimam D. Towards compliant reference architectures by finding analogies and overlaps in compliance regulations, Procs.12th Int. Conf. on Security and Cryptography (SECRYPT 2015), Colmar, France, July 2015.

21. FISMA. Federal Information Security Management Act FISMA. http://www.healthinfolaw.org/federal-law/federal-information-security-management-act-fisma.

22. Fowler M. Analysis patterns – reusable object models. Addison-Wesley; 1997.

23. Gartner. http://www.gartner.com/newsroom/id/2352816.

24. GLBA. Gramm-Leach-Bliley Act. http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

25. Hamdaqa M, Hamou-Lhadj A. Citation analysis: an approach for facilitating the analysis of regulatory compliance documents, Procs. 2009 6th Int. Conf. on Information technology: New Generations. IEEE; 2009. p. 278–83.

26. Warmer J, Kleppe A. The object constraint language. 2nd ed. Addison-Wesley; 2003.

27. Breaux TD, Anton AI. Analyzing regulatory rules for privacy and security requirements. IEEE Trans Soft Eng. 2008;34.

28. Elgammal A, Turekten O, Heuvel WJ, Papazoglou M. Formalizing and applying compliance patterns for business process compliance. J Softw Syst Model. 2016;15.

29. Fernandez EB. Security patterns in practice: building secure architectures using software patterns2013 2013//.

30. Gikas C. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Inf Secur J. 2010;19.

31. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB. An analysis of security issues for cloud computing. J Internet Serv Appl. 2013;4.

32. Massey AK, Smith B, Otto PN, Anton AI. Assessing the accuracy of legal implementation readiness decisions2011 2011//.

33. Ruiter J, Warnier M. Computers, privacy and data protection: an element of choice2011 2011//.

34. Silva CMR, Silva JLC, Rodrigues RB, Nascimento LM, Garcia VC. Systematic mapping study on security threats in cloud computing. IJCSIS. 2013;11.

35. Yimam D, Fernandez EB. Building Compliance and Security Reference Architectures (CSRA) for cloud systems2016 2016//.

36. HIPAA. HIPAA Administrative Simplification. https://www.fedramp.gov/resources/documents.

37. HIPAA. Understanding Health Information Privacy. http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/understanding-hipaa-notice.pdf.

38. Hitachi. Compliance architecture. http://hitachi-id.com/compliance/compliance-architecture.html.

39. IBM. IBM Cloud computing. http://www.ibm.com/cloud-computing.

40. IBM. Security compliance services. http://www-935.ibm.com/services/us/en/it-services/security-services/compliance-and-regulatory-services.

41. IDC. International Data Corporation. http://www.idc.com/prodserv/subservices.jsp.

42. Stricker V, Lauenroth K, Corte P, Gittler F, De Panfilis S, Pohl K. Creating a reference architecture for service-based systems a pattern-based approach. 2010; doi:10.3233/978-1-60750-539-6-149. IOS Press.

43. Target. Response & resources related to Target's data breach. https://corporate.target.com/about/payment-card-issue.aspx.

44. Taylor RN, Medvidovic N, Dashofy N. Software architecture: foundation, theory, and practice. Wiley; 2010.

45. VMware. Compliance reference architecture framework. https://solutionexchange.vmware.com/store/products/vmware-compliance-cyber-risk-solutions.

46. Walker M. Architecting regulatory-compliant architectures. https://msdn.microsoft.com/en-us/library/bb233047.aspx.

47. IEEE. IEEE 1471–2000 recommended practice for architectural description of software-intensive systems. 2000. https://standards.ieee.org/findstds/standard/1471-2000.html.

48. ISO. ISO Information Security Standard. Available: http://www.iso27001security.com.

49. Kruchten P. The rational unified process, an introduction. 3rd ed. Addison-Wesley; 2003.

50. Mather T, Kumaraswamy S, Latif S. Cloud security and privacy: an enterprise perspective on risks and compliance. O'Relly Media; 2009.

51. Microsoft Azure. Microsoft Azure Trust Center. http://azure.microsoft.com/en-us/support/trust-center/compliance.

52. PCI guidelines. PCI cloud guidelines. https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.

53. Sony. Sony freezes 93,000 online accounts after security breach. http://www.forbes.com/sites/parmyolson/2011/10/12/sony-freezes-93000-online-accounts-after-security-breach.

54. SOX law. The Sarbanes-Oxley Act. http://www.soxlaw.com.

55. Millard C. Cloud computing law. Oxford University Press; 2013.

56. Netschert BM. Information security readiness and compliance in the healthcare industry. Stevens Institute of Technology; 2008.

57. NIST. Guidelines on security and privacy in public cloud computing. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Accessed on April 22, 2016.

58. Oracle. Cloud reference architecture. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Accessed April 22, 2016.

59. OWASP. Cloud-10 regulatory compliance. https://www.owasp.org/index.php/Cloud-10_Regulatory_Compliance.

60. PCI-DSS RA. PCI-compliant cloud reference architecture. http://www.hytrust.com/solutions/compliance.

61. PCI DSS standard. Official source of PCI DSS Data Security Standards. https://www.pcisecuritystandards.org/security_standards/index.php.

SPECIAL COMMENT

This **manuscript** has been **well written** following the way of writing a **Research Article**. Research **objectives**, **Hypotheses, Justification** of the Study, **Scope** of the Study, **Methodology**, have all been well and clearly stated. **The methods** used in solving the problem, the **significance** and **urgency** of the problem under study, but the **significant findings** have not been ***explained explicitly and clearly***. I think this manuscript is ***scientifically correct***. Analysis and discussion are also presented sequentially and well structured, but are not detailed and not comprehensive. In the Results and Discussion section *should* ***not only mention*** about the ***results obtained*****, but also** *discuss key findings, claims, limitations of the study*, **etc.** ***Your key findings should be written in this section*** and ***discussed in depth*** **and** *comprehensively based on* ***reputable*** and ***sufficient*** *references*. My suggestion is that the **conclusion** should be made into a *separate chapter* (in this case it is **Chapter 6**). All references **have been cited properly** and **correctly**, and these **references** are **dominated by Textbooks, Journals** and **Proceedings** ***(Conference Article), Websites*** and **Standards.** The number is sufficient **(61 references).** Kindly..., reference would be best to cite the related statement. I suggest that the author writes suggestions for further research and acknowledgments to related parties at the end of the manuscript. I believe that the author has *adequate understanding* and *knowledge* of the issues covered in this manuscript.