Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach

Abstract

In today's digital age, businesses turn to cloud services to elevate their operations exponentially. While this trend harbors excellent potential, it is marred by significant concerns over the safety of data stored in the cloud. As the demand for cloud computing escalates, businesses grapple with issues ranging from data breaches and provider security to service availability and regulatory compliance. It becomes crucial for organizations to enact stringent security protocols not only to protect user information but also to smoothen operational processes, enforce regulatory compliance, and delineate user behavior norms. Cloud computing is a double-edged sword; it offers unparalleled opportunities and presents unique challenges, such as service discrepancies, legal tussles, and data protection qualms. To fortify cloud assets, businesses must adhere to foundational security guidelines covering confidentiality, risk analysis, e-discovery, business resilience, and third-party contract obligations. Risk assessment is pivotal, allowing businesses to identify, prioritize, and mitigate threats, influencing choices on service providers, security features, and service formats. Ensuring uninterrupted operations in the cloud entails safeguarding against threats like Denial-of-Service (DoS) attacks and weighing providers' Service Level Agreements. Data breaches, an ever-present threat, mandate a proactive and transparent approach from cloud vendors. Protecting sensitive data requires solid access controls, encryption practices, and legal conformity.

Moreover, e-discovery, vital in legal and corporate spheres, presents cloud challenges, emphasizing the need for impeccable digital records and data sanctity. The expanding cloud

Comment [41]: Consider rephrasing to:

In today's digital age, businesses turn to cloud services to boost their operations exponentially andwhile this trend presents excellent potentials, it is marred by significant concerns over the safety of data stored in the cloud. As the demand for cloud computing increases, businesses are faced with issues ranging from data breaches and provider security to service availability and regulatory compliance.

Comment [42]:

Comment [43]: Move to the background/ Introduction section

landscape also introduces legal gray areas, such as copyright breaches and data misuse, prompting a sharper focus on data security and precise contract terms.Therefore, while the cloud's advantages are manifold, they have intricate challenges. Businesses must prioritize impenetrable security, craft meticulous risk strategies, and fortify against potential threats to harness the full potential of cloud services while preserving their assets and reputation.From these results, it's evident that most respondents have a confidence level of 7, indicating a relatively high level of trust in the current cloud security measures.Organizations must continuously assess and adapt their cloud security strategies to keep up with the dynamic digital environment and evolving threats for long-term security and operational efficacy.

Keywords:Digital age, businesses, cloud services, data security concerns, cloud computing demand, data breaches, vendor security, availability setbacks, regulatory compliance.

Comment [44]: Move to the background/Introductory section

Comment [45]: Suitable for the conclusion section

Comment [46]: Not a suitable keyword for this work

Introduction

In this modern era of technological advancements, the growing ubiquity of cloud services among businesses is palpable. This shift towards digital transformation has the potential to catalyze operational efficiencies on an unprecedented scale (Barika et al., 2019). Yet, as with any transformative technology, the shift to cloud computing is not without its complexities. One of the foremost concerns remains the security and integrity of data hosted on the cloud (Chang et al., 2022).Businesses increasingly recognize the cloud's potential, but valid apprehensions temper their enthusiasm. These include potential data breaches, the overall security measures provided by cloud vendors, ensuring uninterrupted service availability, and addressing the ever-evolving regulatory landscape (Friedman & West, 2010; Harris & Khan, 2018). The demand for cloud services and the challenges accompanying their adoption are skyrocketing.

Comment [47]: Inappropriate, consider replacing it with a better suiting adjective e.g. popularity, adoption etc

Comment [48]: Apparent

Comment [49]: Consider integrating "**Cloud computing is a double-edged sword; it offers unparalleled opportunities and presents unique challenges, such as service discrepancies, legal tussles, and data protection qualms. "** sourced from the abstract to this section

A foundational principle for any organization seeking to adopt cloud services is the assurance of security measures that protect user information and facilitate the smooth functioning of their business processes. Security also aids in establishing clear operational standards, ensuring regulatory compliance, and setting boundaries for user behavior on cloud platforms (Gravel, 2023). But the journey of cloud computing is akin to traversing a two-pronged path. On one side, there's an abundance of opportunities waiting to be tapped; on the other, there are challenges like service inconsistencies, legal complications, and data protection dilemmas (Ermakova et al., 2020). One cannot underscore enough the importance of adhering to security protocols when venturing into cloud computing. Protocols that emphasize confidentiality, a thorough risk analysis, the practice of e-discovery, business resilience, and delineating third-party responsibilities in contracts are critical. Such measures prevent unauthorized access and ensure data remains inviolable (Fotiou et al., 2015).

Risk assessment forms the cornerstone of cloud security. By identifying, categorizing, and addressing potential threats, businesses can make informed decisions about their choice of service providers, security specifications, and the nature of the cloud services they opt for (Puchley& Toppi, 2018; Rajput, 2022). An inherent part of this digital landscape is the looming threat of Denial-of-Service (DoS) attacks, which can jeopardize operations. Thus, businesses must scrutinize Service Level Agreements offered by cloud providers to ensure continuous service availability (Carvalho et al., 2021).Data breaches remain a persistent concern in the cloud domain. Such incidents necessitate a proactive stance from cloud providers.

Moreover, data, susceptible information, requires rigorous access controls, advanced encryption methods, and legal compliance measures to remain secure (Iankoulova&Daneva, 2012). Additionally, the domain of e-discovery, which is paramount in legal and corporate

Comment [410]: Consider integrating this **". Risk assessment is pivotal, allowing businesses to identify, prioritize, and mitigate threats, influencing choices on service providers, security features, and service formats. Ensuring uninterrupted operations in the cloud entails safeguarding against threats like Denial-of-Service (DoS) attacks and weighing providers' Service Level Agreements. Data breaches, an ever-present threat, mandate a proactive and transparent approach from cloud vendors. Protecting sensitive data requires solid access controls, encryption practices, and legal conformity.**
" to this section. It wassourced from the Abract.

environments, introduces its challenges in a cloud context. It emphasizes the need to maintain pristine digital records and ensure data sanctity (Ritter, 2018).

Yet, the expanding horizon of cloud computing isn't without its legal ambiguities. Cases of copyright infringements, unauthorized data usage, and other legal complexities are rising. Such issues necessitate businesses to focus intently on data security and craft their contracts with laser precision to safeguard their interests (Morningstar Law Network, 2015).Furthermore, the rapid progression of cloud technology has prompted many to look at innovative solutions for bolstering security. For instance, integrating high-level programming languages like Python and SQL can strengthen cloud security frameworks and automate critical control processes (Olabanji, 2023). **T**he promise held by cloud computing is immense, offering numerous advantages to modern businesses. However, to fully reap these benefits, organizations must be prepared to confront and navigate the intricate challenges it presents. Prioritizing robust security mechanisms, adopting a comprehensive risk strategy, and being perpetually vigilant against potential threats will be paramount for businesses to unlock the cloud's full potential while safeguarding their assets and preserving their esteemed reputation (Posey, 2022; Reed, 2023).This paper aims to comprehensively dissect the required security requirements while designing and implementing applications, databases, systems, network infrastructure, and data processing in the cloud computing domain, all within the scope of an enterprise risk management framework.

Comment [411]: Not appropriate

Comment [412]: This should be an independent paragraph. You should consider elaborating more on this i.e. the objectives, research question, significance e.t.c

Literature Review

In recent years, the rapid expansion and adoption of cloud computing platforms have intensified the call for robust and comprehensive security measures. With the myriad benefits that cloud computing offers, such as flexibility, scalability, and cost-efficiency, come the

Comment [413]: "myriad **of** benefits"

challenges related to security, especially in the context of enterprise risk management (Harris & Khan, 2018).The orchestration of big data analysis workflows in cloud environments underscores the importance of establishing baseline security measures (Barika et al., 2019). As companies increasingly migrate their data and operations to the cloud, ensuring the integrity and confidentiality of data becomes paramount. The diverse research challenges Barika et al. (2019) highlighted underscore cloud security's intricate nature, particularly when integrating big data workflows.

Similarly, with next-generation network infrastructures, such as the 5G Cloudified Infrastructure, the necessity for optimal security risk management mechanisms has become more pronounced (Carvalho et al., 2021). Given the 5G's promise of higher bandwidth and lower latency, there's a simultaneous rise in potential security risks. Carvalho et al. emphasize the significance of risk management mechanisms tailored to these evolving infrastructure dynamics.Furthermore, the integration of fog computing into the cloud ecosystem has given rise to newer challenges. Chang et al. (2022) provide a comprehensive survey on Intrusion Detection Systems (IDS) for fog and cloud computing. Their work highlights the complexities introduced by the distributed nature of fog nodes, emphasizing the need for advanced IDS tailored to this unique environment.

While technological advances persist, the human aspect of cloud computing cannot be ignored. Ermakova et al. (2020) dive into the security and privacy requirements of cloud computing within the healthcare sector from a patient's perspective. With sensitive patient data at stake, their research pinpoints the elevated significance of eliciting and prioritizing security requirements, illustrating that cloud security isn't solely a technological concern but deeply rooted in human trust.On the policy front, Friedman and West (2010) discuss the intertwined

privacy and security issues in cloud computing. They provide a nuanced view, suggesting that while cloud providers can offer a level of security unattainable by individual users, the shared responsibility model of cloud security can lead to potential lapses if not handled diligently.

Offering access control as a cloud-based service has also been explored to enhance cloud security (Fotiou et al., 2015). Such approaches offer fine-grained access control, ensuring that data is accessible only by authorized entities, thus bolstering data protection in the cloud.As highlighted by Gravel (2023), recent industry insights emphasize the tangible measures enterprises can adopt as baseline security standards for their cloud environments. These measures, from regular vulnerability assessments to data encryption, provide practical steps for organizations to enhance their cloud security posture.However, new security challenges have arisen with the fusion of cloud computing and IoT termed the 'cloud of things' (Haq&Sholla, 2020). This blend of technologies brings opportunities and an array of potential threats, emphasizing the continuous evolution of the cloud security landscape.

While the vast benefits of cloud infrastructure are evident, such as increased flexibility and scalability, it comes with many potential security challenges (Iankoulova&Daneva, 2012). Rajput (2022) echoes this sentiment, emphasizing the significance of a dedicated risk management approach tailored for cloud computing.The legal dimension is an essential area that often becomes a focal point in cloud computing. The Morningstar Law Network (2015) provides insights into legal issues in cloud computing, ranging from cyber piracy, hacking, and intellectual property infringement. These legal challenges further accentuate the need for establishing clear-cut security requirements to ensure compliance and mitigate litigation risks.Another avenue that offers potential solutions to these security concerns is the application of high-level coding languages. Olabanji (2023) elucidates the prospects of leveraging languages

such as Python and SQL to fortify security systems and automate control processes in cloud environments. Such advancements can reduce the vulnerability of these systems and introduce automation to streamline the security mechanisms.

Enterprise Risk Management (ERM) plays an indispensable role in cloud security. Puchley and Toppi (2018) contend that transitioning from traditional risk assessment to strategic risk management can provide a more holistic perspective in identifying, assessing, and managing potential threats. Olaniyi&Omubo (2023) further underline the significance of compliance with frameworks such as COSO in IT auditing and Enterprise Resource Management. These frameworks offer a structured approach to ensuring that security controls and risk management processes are efficient and effective.However, even with strategic risk management, new challenges continually emerge. Posey (2022) delves into the complexities of ensuring business continuity in the cloud. Ritter (2018) addresses the intricacies of e-discovery in the cloud, emphasizing potential security and compliance issues that organizations must reckon with.

Reed (2023) introduces a comprehensive perspective on cloud security in his lecture series at the University of the Cumberlands, drawing attention to the multifaceted nature of this field. Parallelly, TsochevandTrifonov (2022) revisit cloud computing security requirements, reflecting on the evolving landscape and the necessity for organizations to remain proactive and agile. As cloud computing continues to evolve, establishing baseline security requirements remains a moving target. An amalgamation of technological advancements, user perspectives, and industry best practices shape the contemporary security landscape, underscoring the need for a holistic, adaptive approach to cloud security (Olaniyi et al., 2023). The literature suggests a pressing need for a multifaceted approach to establish baseline security requirements in cloud computing. From integrating high-level coding languages and adhering to established risk

management frameworks to navigating the legal maze and ensuring business continuity, enterprises must be adept at managing various challenges. As cloud computing continues to permeate various sectors, the focus on security will remain paramount.

Baseline Security Requirements Cloud ComputingWithin an Enterprise Risk Management Framework

The advent of cloud computing has undoubtedly ushered in numerous advantages and opportunities for various sectors of the economy worldwide (Gravel, 2023). Nonetheless, it has its fair share of challenges, risks, and obstacles, including issues related to system and service, legal disputes, information protection, ownership, sharing, and reliability (Harris & Khan, 2018).In order to guarantee the protection and safety of assets stored in the cloud, organizations must adhere to a set of baseline security requirements, including confidentiality and privacy, data infringement obligations and security, e-discovery, risk assessment, business continuity, legal problems, and third-party commitments in cloud computing agreements (Dunker & Bates, n.d.; Reed, 2023).

Risk Evaluation

Embracing cloud computing necessitates a strategic focus on risk evaluationfor organizations; thus, by systematically pinpointing, examining, evaluating, treating, and monitoring risks, businesses can exert control over likely dangers and defend their valuable resources (Rajput, 2022). Risk evaluation will enable organizations to prioritize selecting trustworthy cloud service providers, employ robust technical protection, establish robust controls, optimize their chosen service model, and devise plans to ensure uninterrupted service availability (Rajput in 2022). Cloud computing risk evaluation is vital for organizations to forecast harmful expectations, boost business opportunities, and furnish financial perspicuity for

proper budgeting (Rajput, 2022). Risk evaluation must factor in indemnification validations and consider the preference of law, risk transfer, and procurement guidelines and methods(Dunker & Bates, n.d.; Reed, 2023).Also, practical risk evaluation is crucial for making informed decisions and driving growth; thus, by adopting proactive risk management practices, organizations can improve their business processes, save costs, and stay competitive(Rajput, 2022).

Business Continuity

Cloud computing proffers a seamless answer for managing increased workloads by integrating virtual machines and mitigating the potential disruption caused by Denial-of-Service attacks (Posey, 2022). Therefore, by leveraging scalable assets, institutions can guarantee the stability of their business activities and operations (Posey, 2022). However, organizations must evaluate the critical aspect of business continuity when incorporating cloud computing into enterprise systems (Posey, 2022). Not all cloud service providers offer applicable service level agreements and adequate business continuity measures in case of service suspension or termination (Dunker & Bates, n.d.; Reed, 2023). Thus, when picking a cloud provider, organizations must prioritize dependability and reliability, considering the provider's established reputation and transparent data ownership policies. Also, it is necessary to comprehensively comprehend the costs related to data migration and establish the availability of emergency support services by the cloud provider (Posey, 2022). A suitable cloud computing infrastructure will embrace business continuity to reduce system downtime and facilitate prompt recovery, bolstering its operations' capacity to resist upheavals and disasters (Posey, 2022).

Data Breach Responsibilities and Security

Organizations' effectiveness now hinges on data exploration; however, failure to protect it can result in security violations (Barika et al., 2019). Database security is paramount when

choosing a cloud provider to ensure security, confidentiality, privacy, accuracy, and reliability (Barika et al., 2019). When choosing a dependable cloud computing provider, an organization must deal with possible data breaches that can significantly endanger security measures(Dunker & Bates, n.d.; Reed, 2023). Thus, the preferred cloud provider must have the infrastructure capability to promptly inform an organization in case of a breach (Dunker & Bates, n.d.; Reed, 2023). When crafting new initiatives, admitting the potential risks linked with intellectual property is paramount. Likewise, ensuring that the cloud provider abides by stipulated export controls is crucial to prevent unauthorized data transmission to other governments or nations (Dunker & Bates, n.d.; Reed, 2023).A good cloud provider must build security capacities and comply with standards to bolster dependability, privacy, precision, and integrity (Barika et al., 2019).

Confidentiality and Privacy

Confidentiality in cloud computing entails confidentially preserving data because employing third-party data storage comes with a very high risk due to privacy and accessibility concerns (Dunker & Bates, n.d.; Reed, 2023). Hence, protecting confidential information is paramount when data is no longer within the organization's control (Friedman & West, 2010). Hence, access control, encryption, and legal standards help maintain confidentiality and privacy to avert the disclosure of sensitive information that could hamper business activities (Friedman & West, 2010). Fotiou et al. (2015) proposed access control as a solution to problems envisaged by organizations planning cloud technology adoption. Access Control is a crucial element of Cloud Computing that furnishes information security for an organization by restricting access to data stored in the Cloud (Fotiou et al., 2015). Also, executing authentication measures such as multi-factor authentication, PINs, and passwords, access control guarantees that only authorized

personnel can access sensitive information (Fotiou et al., 2015). Institutions can customize access control based on employees' empowerment, functions, roles, and attributes, permitting verified individuals to access enterprise information. Access control enables organizations to outsource data storage and computation while controlling their sensitive business assets (Fotiou et al., 2015).The robustness of encryption, firewalls, authentication, intrusion detection and prevention systems, backup and recovery, and cloud storage auditing is crucial to protecting sensitive data from infringement, attack, and unauthorized access to cloud storage. Hence, an organization must consider the confidentiality and privacy level of a cloud provider before signing for the service (Barika et al.,2019)

E-Discovery

Cloud-based e-discovery has made security and compliance a severe challenge to institutions (Ritter, 2018). E-discovery platforms are crucial for validating, discovering, or revamping digital data in legal and corporate environments (Ritter, 2018) because E-discovery establishments and their legal consultants may have a legal duty to retain records for legal discovery (Dunker & Bates, n.d.; Reed, 2023). Therefore, stringent approaches are needed to guarantee that pertinent proof is available, as electronic information is admissible when needed (Ritter, 2018). Institutions must steer e-discovery initiatives to preserve data for investigations, negotiations, reports, and forensics because accurate digital information is vital for building trust and auditing (Ritter, 2018). Cloud computing will help institutions distribute complex applications across servers, firewalls, and IoT devices, reducing hardware and software needs (Ritter, 2018). Nevertheless, security and compliance crises exist around e-discovery in the cloud, and institutions must have valid documentation and execution logs to uphold data integrity (Ritter, 2018).

Legal Issues and Third-Party Obligations in Cloud Computing Contracts

Cloud computing is becoming indispensable in everyday business operations worldwide; however, its widespread use also raises several legal concerns that should be addressed proactively (Morningstar Law Network, 2015). The rules and regulations surrounding cloud computing keep evolving within the global ecosystem, especially in the United States and Europe, and the consequence affects vital sectors of the economy like financial, healthcare, technology, and social media, which use cloud-based products (Morningstar Law Network, 2015). Cloud computing attracts legal crises such as copyright violations, data infringements, security violations, HIPAA privacy breaches, data loss, management, e-discovery, hacking, and cyber threats, resulting in complex litigation across jurisdictions (Morningstar Law Network, 2015).Using cloud-based services in business can be risky, and it is essential to protect data security and address potential legal issues for the safety of all involved (Morningstar Law Network, 2015). Hence, data protection and contractual language are necessary considerations in cloud computing contracts due to the significance of legal concerns and third-party responsibilities (Dunker & Bates, n.d.; Reed, 2023).

Research Question

How do established security measures in cloud computing align with the perceived risks and challenges identified by professionals in the field, and how can an enterprise risk management approach enhance the baseline security requirements?This question seeks to understand the alignment between current practices and perceived threats while exploring the potential benefits of an enterprise risk management framework.

Comment [414]: No proper critique of the works of the authors mentioned. I.e. No decent comparison and contrast were made amongst their works to derive similarities and discrepancies. Research gaps were not properly identified. How relevant are the contribution of these authors to your work were not outlined i.e. how their studies, experiments e.t.c will be used to foster your work.

Methodology

To address the research question, we crafted a survey gauging the confidence in current security measures, scaled from 0 (no confidence) to 10 (extremely confident). We used the SurveyMonkey platform to deploy a structured questionnaire for this study's objectives. We gathered data from 121 professionals specialized in cloud technology, ensuring a diverse representation from different sectors within this field.

Comment [415]: What methodology did you used for the overall research? Agile? CRISP-DM? Water fall? Any justification?

What time period were these data captured?
What are the demographics of the participants?
Was any data protection policy(ies) considered?

Data Analysis

JASP was used to run linear regression. The "Scale" typically serves as the independent variable (x variable), and the "Number of respondents" serves as the dependent variable (y variable).

List 1 : The Linear Regression.

Linear Regression

Model Summary - Number of respondents

Model	R	R^2	Adjusted R^2	RMSE
H_0	0.000	0.000	0.000	13.304
H_1	0.696	0.484	0.427	10.073

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
H_1	Regression	856.809	1	856.809	8.444	0.017
	Residual	913.191	9	101.466		
	Total	1770.000	10			

Note. The intercept model is omitted, as no meaningful information can be shown.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p
H_0	(Intercept)	11.000	4.011		2.742	0.021
H_1	(Intercept)	−2.955	5.682		−0.520	0.616
	Scale	2.791	0.960	0.696	2.906	0.017

The statistical significance of the influence of current security practices (Scale) on confidence was tested. The obtained p-value of 0.017 is below the commonly accepted threshold of 0.05, implying that the scale of established practices is a significant predictor of confidence levels.

The profound insights from these experts formed the bedrock of our research conclusions and ensuing recommendations.Here's a breakdown of the results:

- No respondents rated their confidence as 0, 1, or 2.
- 4 respondents rated their confidence as 3.
- 7 respondents chose a confidence level of 4.
- 3 respondents rated their confidence as 5.
- 5 respondents gave a confidence rating of 6.
- The majority, 39 respondents, rated their confidence as 7.
- 24 respondents chose a confidence level of 8.
- 28 respondents rated their confidence as 9.
- 11 respondents expressed the highest confidence with a rating of 10.

These results show that most respondents have a confidence level of 7, indicating a relatively high level of trust in the current security measures.Organizations must continuously assess and adapt their cloud security strategies to keep up with the dynamic digital environment and evolving threats for long-term security and operational efficacy.

Comment [416]: What data processing tools were used for this analysis?
What are the experimental conditions, can the experiment be replicated? These are not evident from the discussions presented.
Is the quantity of data sufficiently representative of the overall population to be used as a premise for the inferences and conclusions derived?

The data analysis and associated discussions is scanty and not very informative, please reconsider elaborating on the implications of respective variables and values.

Conclusion

Cloud computing has advanced and benefited organizations, but its use by companies raises concerns and challenges like regulatory compliance, data breaches, and cyber-attacks (Harris & Khan, 2018). Therefore, prioritizing information security and privacy protection when utilizing cloud services is vital for institutions to benefit from cloud computing fully (Gravel, 2023). Businesses must thoroughly assess their cloud services and develop comprehensive risk management strategies that address potential issues, threats, and weaknesses; also, they must use strong encryption to protect data in cloud storage, set up reliable access controls, and conduct regular audits and monitoring (Harris & Khan, 2018). Risk managers concoct, execute and manage plans, regularly evaluating and reassessing potential risks by gathering pertinent data and modifying the risk profile (Puchley& Toppi,2018).Hence, Organizations can significantly enhance their data protection, optimize business processes, meet regulatory standards, and mitigate potential risks by implementing basic security requirements and establishing effective security policies and frameworks. Accordingly, an organization's failure to execute these measures can have detrimental consequences such as reputational damage, increased costs, and missed business opportunities (Gravel, 2023).The predictor "Scale" significantly affects the dependent variable, explaining approximately 48.4% of its variance. The model with the predictor is significantly better than a model without any predictors. The relationship between "Scale" and the dependent variable is positive, meaning as the value of "Scale" increases, the dependent variable also tends to increase.From these results, it's evident that most respondents have a confidence level of 7, indicating a relatively high level of trust in the current cloud security measures.Organizations have demonstrated commendable proficiency in evaluating and establishing baseline security requirements for cloud computing using an enterprise risk

management approach. However, given the dynamic nature of the digital environment and the constant evolution of threats, it's essential to recognize that there's always scope for further refinement and enhancement in these strategies. Continuous assessment and adaptation are crucial for ensuring long-term security and operational efficacy.

References

Barika, M., Garg, S., Zomaya, A., Wang, L., Moorsel, A., & Ranjan, R. (2019). Orchestrating Big Data Analysis Workflows in the Cloud: Research Challenges, Survey, and Future Directions. *ACM Computing Surveys*, 52(5), 1–41. https://doi.org/10.1145/3332301

Carvalho, Woungang, I., Anpalagan, A., & Traore, I. (2021). Optimal Security Risk Management Mechanism for the 5G Cloudified Infrastructure. IEEE eTransactions on Network and Service Management, 18(2), 1260–1274. https://doi.org/10.1109/TNSM.2021.3057761

Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Le Minh, T. D., Hall, K., Boddu, S., & Kobusińska, A. (2022). A Survey on Intrusion Detection Systems for Fog and Cloud Computing. *Future Internet*, 14(3), 89. https://doi.org/10.3390/fi14030089

Ermakova, Fabian, B., Kornacka, M., Thiebes, S., &Sunyaev, A. (2020). Security and Privacy Requirements for Cloud Computing in Healthcare: Elicitation and Prioritization from a Patient Perspective. ACM Transactions on Management Information Systems, 11(2), 1–29. https://doi.org/10.1145/3386160

Friedman, A.A., & West, D.M. (2010). Privacy and Security in Cloud Computing. *Issues in*

Technology Innovation. https://www.brookings.edu/wp-content/uploads/2016/06/1026_cloud_computing_friedman_west.pdf

Fotiou, N., Machas, A., Polyzos, G. C., &Xylomenos, G. (2015). Access control as a service for the cloud. *Journal of Internet Services and Applications*, 6(1), 1–. https://doi.org/10.1186/s13174-015-0026-4

Gravel, N. (2023, May 27). Baseline security measures for cloud environments. *Gray, Gray & Gray LLP*. https://www.gggllp.com/baseline-security-measures-for-cloud-environments/

Haq, B., A., &Sholla, S. (2020). cloud of things: architecture, research challenges, security threats, mechanisms and open challenges. Jordanian journal of computers and information technology (Online), 6(4), 415–433. https://doi.org/10.5455/jjcit.71-1592021856

Harris, M., & Khan, R.Z. (2018). A Systematic Review on Cloud Computing. *International Journal of Computer Sciences and Engineering*, 6. 632–639. https://doi.org/10.26438/ijcse/v6i11.632639

Iankoulova, &Daneva, M. (2012). Cloud computing security requirements: A systematic review. 2012 Sixth International Conference on Research Challenges in Information Science (RCIS), 1–7. https://doi.org/10.1109/RCIS.2012.6240421

Morningstar Law Network. (2015, March 15). The laws of cloud computing: Weathering the storms of cyber piracy, hacking, and IP infringement. https://morningstarlawgroup.com/insights/cloud-computing-legal-issues/#:~:text=Legal%20issues%20that%20can%20arise,lead%20to%20complex%20litigation%20and

Olabanji, S. O. (2023). Advancing Cloud Technology Security: Leveraging High-Level Coding

Languages like Python and SQL for Strengthening Security Systems and Automating Top Control Processes. Journal of Scientific Research and Reports, 29(9), 42–54. https://doi.org/10.9734/jsrr/2023/v29i91783

Olagbaju, O. O., Babalola R.O., & Olaniyi, O. O. (2023). Code Alternation in English as a Second Language Classroom: A Communication and Learning Strategy. *Nova Science*. https://doi.org/10.52305/YLHJ5878

Olagbaju, O. O., & Olaniyi, O. O. (2023). Explicit and Differentiated Phonics Instruction on Pupils' Literacy Skills in Gambian Lower Basic Schools. Asian Journal of Education and Social Studies, 44(2), 20–30. https://doi.org/10.9734/ajess/2023/v44i2958

Olaniyi O. O. (2022, April 26). Best Practices to Encourage Girls' Education in Maiha Local Government Area of Adamawa State in Nigeria. The University of Arkansas Clinton School ofPublic Service (Research Gate). https://doi.org/10.13140/RG.2.2.26144.25606

Olaniyi, O. O., Olabanji, S. O., &Abalaka, A. I. (2023). Navigating Risk in the Modern Business Landscape: Strategies and Insights for Enterprise Risk Management Implementation. Journal of Scientific Research and Reports, 29(9), 103–109. https://doi.org/10.9734/jsrr/2023/v29i91789

Olaniyi, O. O., Olabanji, S. O., &Okunleye, O. J. (2023). Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives. Journal of Scientific Research and Reports, 29(9), 73–81. https://doi.org/10.9734/jsrr/2023/v29i91786

Olaniyi, O. O., Abalaka, A. I., &Olabanji, S. O. (2023). Utilizing Big Data Analytics and Business Intelligence for Improved Decision-Making at Leading Fortune Company. Journal of Scientific Research and Reports, 29(9), 64–72. https://doi.org/10.9734/jsrr/2023/v29i91785

Olaniyi, O.O., Okunleye, O.J., &Olabanji, S.O. (2023). Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature. *Current Journal of Applied Science and Technology*, 42(25), 10–18. https://doi.org/10.9734/cjast/2023/v42i254181

Olaniyi, O.O., Olaoye O.O., &Okunleye, O.J. (2023). Effects of Information Governance (IG) on profitability in the Nigerian banking sector. *Asian Journal of Economics, Business and Accounting*. 2023;23(18):22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

Olaniyi, O.O. &Omubo, D.S. (2023). The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management. *The International Journal of Innovative Research & Development.* https://doi.org/10.24940/ijird/2023/v12/i5/MAY23001

Olaniyi, O.O. &Omubo, D.S. (2023). WhatsApp Data Policy, Data Security, And Users' Vulnerability. *The International Journal of Innovative Research & Development*. https://doi.org/10.24940/ijird/2023/v12/i4/APR23021

Posey, B. (2022, May 31). Business continuity in the Cloud: Benefits and planning tips. *TechTarget*. https://www.techtarget.com/searchdisasterrecovery/tip/Business-continuity-in-the-cloud-Benefits-and-planning-tips

Puchley, T., & Toppi, C. (2018). ERM: evolving from risk assessment to strategic risk management. *Healthcare Financial Management*, 72(4), 44–49. https://go.openathens.net/redirector/ualr.edu?url=https://www.proquest.com/trade-journals/erm-evolving-risk-assessment-strategic-management/docview/2036210031/se-2

Rajput, A. S. (2022, December 12). Risk management in cloud computing. *InterviewBit Technologies Pvt Limited.*https://www.scaler.com/topics/cloud-computing/risk-management-in-cloud-computing/

Reed, B (2023, June). Cloud Security. *Week 8 lecture, University of the Cumberlands*. https://us-lti.bbcollab.com/collab/ui/session/playback

Ritter, J. (2018, November 26). E-discovery in the Cloud introduces security and compliance issues. *TechTarget*. https://www.techtarget.com/searchcio/tip/E-discovery-in-the-cloud-introduces-security-compliance-issues

Tsochev, &Trifonov, R. I. (2022). Cloud computing security requirements: A Review. IOP

Conference Series. Materials Science and Engineering, 1216(1), 12001–.

https://doi.org/10.1088/1757-899X/1216/1/012001