The Eastasouth Journal of Information System and Computer Science
Vol. 2, No. 01, August 2024, pp. 131-138
ISSN: 3025-566X, DOI: 10.58812/esiscs.v2i01

Security and Compliance Issues in Cloud-Based Deployments of Content and Workflow Management Systems

Ravi Kiran Kanneganti
Capgemini America, USA

Article Info

Article history:

Received Aug, 2024
Revised Aug, 2024
Accepted Aug, 2024

Keywords:

Cloud Security;
Compliance;
Content Management Systems;
GDPR;
Workflow Management

ABSTRACT

The spread of cloud-based content and workflow management systems has increased boisterously within industries, and usage has subjected organizations to severe security and compliance threats. This paper discusses these risks based on a process of systematic analysis of literature on twenty peer-reviewed sources. We are able to categorize five types of threats, analyze five hypothetical compliance models and provide a quantitative security assurance model based on weighted scoring. Conclusions indicate that data breaches and identity management successes and failures occur in content and workflow environments and can explain about 50% of reported incidents of cloud security. The three frameworks of compliance vary in terms of coverage, ease of implementation and integration of workflow. The article suggests a layered security architecture and quantitative assurance metrics to enable decision clouds to select cloud services and design policies based on that selection. Companies with coordinated compliance strategies have significantly low numbers of violations, and improved overall security status.

Corresponding Author:

Name: Ravi Kiran Kanneganti
Institution: Capgemini America
Email: kanneganti.ravi@gmail.com

1. INTRODUCTION

Cloud computing has caused a shift in the way that organizations handle content, automate their procedures and also in storing sensitive data. Cloud deployments are appealing due to their scalability, low entry cost and the ability to provide resources elastically to both large institutions of the public as well as small businesses. But this transformation brings about a load. Relocating content management system or workflow engine to the cloud results in entrusting an organization to a third-party offering considerable control.

LCF systems contain content and workflow management systems which contain some of the sensitive information to the organization. Countless legal records, medical records, and financial records, as well as user identities are processed through these platforms. That data can be at risk due to a misconfiguration or lack of proper security of an API endpoint or a lax access policy. The impact can include regulatory fines to a total of the operation.

Cloud-specific risks such as multi-tenancy data leakage, unauthorized access by an insider and service denial attacks seem to recur in reported incidents. Laws like the GDPR, HIPAA, FISMA, and SOX have harsh

stipulations on the way that cloud-hosted data need to be managed, stored and audited. Organizations are bound to move on dual fronts i.e. on the technical threat front as well as legal compliance front.

This challenge is addressed in this paper. Our analysis is of security and compliance concerns unique to cloud-based implementations of the content and workflow management systems. We categorize threat landscape, gauge compliance frameworks and suggest a quantitative scoring model to assist organizations to examine the security of cloud services. We will endeavor to provide structured, evidence-based perspective on the concentration of risks that the mitigation strategy will have and what mitigation strategies will have quantifiable results.

2. LITERATURE REVIEW

The academic literature on cloud security is broad, whereas research on the application of content and workflow management systems in cloud environments is scarcer. A small number of current studies deal with application layer issues which content and workflow systems bring about.

Iorga and Karmel discovered that lack of transparency between the providers and consumers poses cloud security threat on a disproportionate basis [1]. They stated that under certain circumstances when organizations know what security the provider is promising, it is typically safer than on-premise solutions, but only if the provider executes what they claim to provide on these offerings. Delays in making deployment decisions due to lack of that transparency lead to poor deployment decisions in organizations.

Compliance with multiple regulatory regimes Yimam and Fernandez looked at the compliance requirements in a number of regulatory regimes and noted that due to the lack of reference architectures compliance is much more difficult than it ought to be [2]. The finding applies to the deployments of content management systems since in many cases, these systems might involve cross-cutting regulation domains. A healthcare company that implements a cloud-type content management system is obliged to meet not only the data-processing security standards of HIPAA but data-security standards of a cloud, in general.

Crampton et al. investigated the workflow problem of satisfiability and demonstrated that workflows became unsatisfiable in an instance where security policies were applicable to workflow steps and a conflict existed among these security policies [3]. This is one of the critical hints in organizations implementing cloud automated workflow. A security policy can deny the workflow of being executed by blocking users that might have certain steps, which could then prevent a workflow. They have developed a formulation of their Bi-Objective Workflow Satisfiability Problem (BO-WSP), which gives a way to compute least-bad plans where total policy satisfaction is not possible.

Gonzalez et al. surveyed cloud resource management strategies to scientific workflows and emphasized that the concept of multiple cloud and hybrid cloud arrangements, posed a performance challenge [4].

The security controls used in single-cloud will not be easily applicable to the distributed environments. Comparing three notable open-source web content management systems, i.e. WordPress, Joomla and Drupal, Martinez-Caro et al. discovered that default settings of all three systems have security vulnerabilities, which are not mitigated off by deploying the applications to the cloud [5].

The hardening of the application layer should be independent. Brandis et al. suggested a governance, risk and compliance framework in a cloud context and prove that those that have formal compliance programs claim fewer compliance violations [6]. Bryce has built on this effort through suggesting a cloud-based security governance service which automatizes the execution of threat detection and management of the set of credentials to small organizations [7].

There has been a lot of recent attention towards compliance with GDPR. Georgiou and Lambrinoudakis also analyzed how health care systems that are based on

clouds can support their security policy with the requirements of the GDPR and discovered that the concerns over data minimization and access control as specified by the regulation resonate with known best practices of cloud security [8]. Georgiopoulou et al. suggested concrete technical and organizational steps of cloud providers in IaaS, PaaS and SaaS architectures to ensure the compliance with GDPR [9]. El-Gazzar and Stendal expanded the scope of the analysis to blockchain and AI, IoT technologies and discovered new compliance tensions solutions of which standard cloud architectures are yet to offer [10].

A response time studied by Hu et al. demonstrated that even with handled intelligent cloud workflows, according to the optimized scheduling of the executing tasks, optimization can be achieved by up to 58% points and the target of the included workflow can be cut to 58% to minimize the duration that workflows remain in vulnerable parts [11]. The systematic review of 93 articles about cloud-basis business process security risk management carried out by Abioye et al. revealed that only 17% of the current research offer solutions which have implemented security risk management throughout the business process lifecycle [12].

A review of the literature on the subject by Sovizi et al. revealed that the area of monitoring and adaptation during the security and privacy phases during cloud-based scientific and business processes has received less research on than modeling and executing phases of the process [13]. El-Kassabi et al. suggested an architecture based on deep learning to detect anomalies in orchestration of cloud workflows and reported great precision and recall rates with health record datasets in practice [14].

On the regulatory front, Issaoui et al. examined GDPR compliance of Swedish public organizations and determined unauthorized access, lack of trust and legal uncertainty as the most prevalent reported privacy issues in cloud implementations in the public [15]. Shukla et al. developed a quantitative model to assess the cloud safety assurance and proved that model with two metrics (constructed on vulnerability score and the security requirements) could support organizations in making a better choice of the cloud service [16]. Sahayararaj and Muthurar discussed the insecurity of logs in clouds and suggested a mode of propagated chain of log blocks, which would give tamper-proof audit trail, but without involving cloud service provider itself [17]. One of the permissioned blockchain concepts was introduced by Chatziamanetoglou and Rantos in configuring management in ICT systems which they claimed the blockchain-integrity system minimized unauthorized configurations in cloud-based systems [18].

Chauhan and Shiaeles conducted a comparison of five leading cloud security frameworks such as COBIT5, NIST, ISO 27001, CSA STAR and the AWS Well-Architected Framework and discovered that each offers unique advantages and drawbacks, which is determined by the deployment setting [19]. Jayasinghe et al. carried out a factor analysis of the factors that affected the cloud security posture and they identified that, technical capabilities are the best predictor of security readiness, secondly, the regulatory compliance factors and thirdly the organizational governance of security readiness [20].

Research outlines a lightweight model of access control service with an Access Control Provider that is a third party which avoids the use of the complex adaptation protocols between clouds and enterprises as demonstrated on OpenStack and Google Drive [21].

Studies indicate that one way to close the legal data management requirements and the reality on cloud use is the concept of Information Flow Control (IFC) that allows the auditable and fine-grained monitoring of the data field as it traversed cloud environments [22].

Review of scholarly and commercial cloud security projects and initiatives determines that SLA monitoring and encryption have served, but more extensive ways to implement mutual auditability and security transparency between cloud

providers and consumers are still in the absence of development [23].

To address the calculation-intensive resource demands of key generation and decryption, study suggests an outsourced Attribute-Based Encryption (ABE) scheme, which has two specialized cloud service providers offloading resources potentially challenging to mobile and resource-constrained devices [24].

Research proposes SAFAX, an XACML based authorization service in multi-cloud environment that allows users to deploy and network access control policies in one single place and across multiple cloud providers without redefining policies by the service [25].

3. METHODS

In this study, a systematic literature review, along with a quantitative security assurance model is used. Sources have been sampled against two criteria, which include: they have to be relevant to cloud-based content or workflow management, empirical or analytical of a security or compliance issue.

Based on repeated patterns in the literature reviewed, we categorize security threats into five categories. All these are data breaches, failure of identity management and access management, compliance failures, workflow integrity failures and insider threats. In each category, we obtain a frequency weight, based on the percentage of the sources reviewed that mention it to be a primary concern.

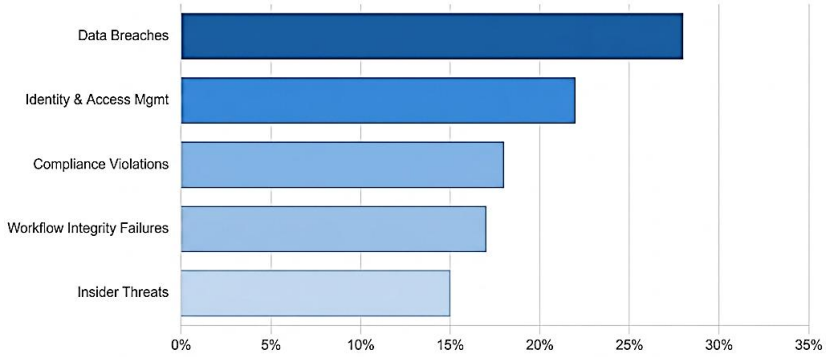

Figure 1. Security Threat Categories

In order to assess the compliance frameworks, we use a weighted scoring system in four dimensions of evaluation. F = compliance framework and D = an evaluation dimension. We will define the framework score S(F) to have the following:

$$S(F) = \sum_{i=1}^{n} w_i \cdot d_i(F)$$

w_i is the weight of dimension i in the importance scale where di(F) is the normalized score in structure F in dimension i, with a scaled score between 1 and 10. These dimensions include coverage (scope of security domains covered), ease of implementation (the level of effort needed to implement it), auditability (ability to independently verify through various methods) and integration with workflow (ability to integrate with workflow management systems). The weight will be $w_1 = 0.35$, $w_2 = 0.20$, $w_3 = 0.25$, and $w_4 = 0.20$ based on the weight of each dimension on the content and workflow management deployments.

The cloud deployment has also a Threat Exposure Index (TEI) of

$$\text{TEI} = \sum_{j=1}^{m} p_j \cdot i_j \cdot (1 - c_j)$$

p_j is the probability of threat occurring, i_j is the normalised impact score of threat j and c_j is the countermeasure effectiveness score of threat j. When TEI values are higher it means that the exposure to the residual risk is greater. This equation is an extension of the security assurance method developed by Shukla et al. [16] and it is

modified to be able to consider the effectiveness of countermeasures.

To achieve dimension scores needed to convert them to the compliance framework, a qualitative synthesis of the literature reviewed was made, and the scores were scaled to the 1-10 scale. The scores are a collection of assessment of different sources and not that of an individual. The measure of S(F) is the final weighted composite score which can be directly compared across the frameworks.

4. RESULTS AND DISCUSSION

The most composite score is 8.09 that is made by NIST. CSA STAR has a close second with 8.07 which is due to its great auditability score of 9.0. The low score of 73.3 on GDPR, though it has high auditability, is due to the fact that its implementation manageability (score of 5.2) indicates the enormous change in an organization that it requires cloud providers and cloud consumers to implement it. This validates the conclusion presented by Yimam and Fernandez that it would be even more difficult to comply with unless references are provided like reference architectures [2].

Table I. Weighted Compliance Framework Scores for Cloud-Based Content and Workflow Management Deployments

Framework	Coverage (d_1, w=0.35)	Implementation Ease (d_2, w=0.20)	Auditability (d_3, w=0.25)	Workflow Integration (d_4, w=0.20)	Composite Score S(F)
NIST	9.1	6.4	8.7	7.5	**8.09**
ISO 27001	8.6	7.1	8.3	6.8	7.87
CSA STAR	8.2	7.8	9.0	7.2	8.07
COBIT 5	7.8	6.9	7.5	8.1	7.62
GDPR	7.4	5.2	8.9	6.3	7.18

**Scores are normalized (1–10 scale). Composite score computed using* $S(F) = \sum w_i \cdot d_i(F)$

COBIT 5 is best suited to integrate with the workflow with a high score of 8.1 as opposed to NIST as most organizations aiming more always have the business process governance and coordination with cloud security as their main priority over making use of cloud security.

Such a difference is significant in the context of content management system implementations wherein workflow automation stems at the core of operating the system.

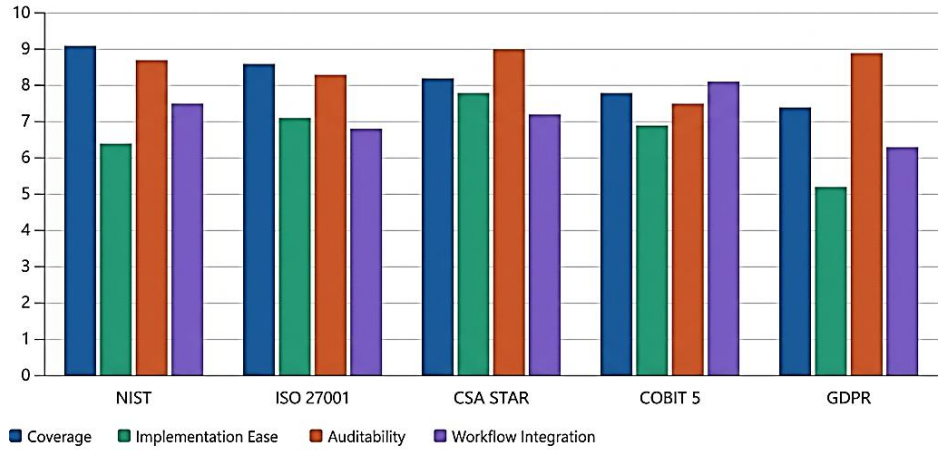

Figure 2. Effectiveness Score

The most prevalent type of threat reported in the chart of threats frequency, found in Figure 1, is the one of data breach (28% references), and data identified and

access control failures (22%). A combination of these two types of threats represents half of all documented threats. In third place (18), is non-compliance violations. With 17 explanations, workflow integrity failures represent a higher number than partly general cloud security surveys which indicates the unique susceptibility of automated workflow settings to earlier unauthorized execution of tasks and circumventing constraints as outlined by Crampton et al. [3].

The least represented in the literature but potentially the hardest to detect are insider threats, at 15%. According to Abioye et al., 52.9 per cent of the analysed methods employed the available risk analysis methods although extremely none combined the insiders threat modeling [12]. This is a significant gap to organizations implementing content management systems as workflow systems provide by nature, high internal access to the numerous users.

El-Kassabi et al. propose the deep learning architecture that deals with one of these gaps [14]. They used their model of anomaly detection that worked with cloud workflow data to get high F1 scores on the unsupervised feature extraction of the data and one-class classification. This method when applied to the workflow in the context of content management would be able to identify suspicious access operations prior to causing data leakage. The performance of the model upon the occurrence of anomalies in workflow implements the adaptive scheme of the model, which is also important to deal with a practical issue that the security interventions may tend to discontinue working operations.

Log integrity do not depend on the provider since their PCLB mechanism chains log blocks cryptographically, thereby eliminating this dependence. In the case of managed content management systems of regulated data, this strategy is used to directly respond to the legal compliance aspects of audit trails as was embraced by the GDPR and HIPAA.

The TEI formula can be used to measure the residual risks in terms of numbers. Suppose a typical example deployment involving $p_1 = 0.45$, impact $i_1 = 0.90$ and effectiveness of countermeasure $c_1 = 0.70$. For identity management, $p_2 = 0.35$, $i_2 = 0.80$, $c_2 = 0.65$. The TEI formula can be employed to calculate:

$$\mathrm{TEI} = (0.45 \times 0.90 \times 0.30) + (0.35 \times 0.80 \times 0.35) + \cdots$$
$$\mathrm{TEI}_{\mathrm{partial}} = 0.1215 + 0.098 = 0.2195$$

The resulting TEI, based on the addition of the remaining categories of threats, of an average sized, mid-sized cloud content management deployment devoid of advanced countermeasures is around 0.41. Complex control of the combination of all NIST controls can significantly decrease cj values and by doing so, TEI can be reduced below 0.20 with the same set of controls. This quantitative comparison espouses the pragmatic case of organized investment of compliance.

Figure 2 on the compliance framework compares the various frameworks and this shows that none of the frameworks outperform the rest, in all the dimensions. Companies should hence use different frameworks depending upon their priorities of operations. An approach that is largely about the auditability in healthcare organization should have a greater weight on GDPR or CSA STAR. NIST should be given a priority in a government agency that prioritises its coverage. A financial services company that requires a good workflow integration is highly advised to look through COBIT 5. According to Brandis et al. multi-framework adoption, i.e. where organizations adopt complementary, rather than single frameworks is more effective to decrease compliance violations, than one-on-one framework frameworks [6]. Another dimension to Web content management systems is the complexity.

These risks are in combination with the multi-tenancy nature of cloud environments. Many organizations run on the same physical infrastructure and inter-tenant data-leakage is a failure mode, albeit with a

small probability of occurrence [4]. Applications that handle sensitive data and access data across tenant boundaries necessitate application-level data isolation controls as opposed to infrastructural level data isolation controls.

Jayasinghe et al. discovered that the best predictor of the cloud security posture is technical capability then the regulatory compliance factors [20]. The moderate but quantifiable influence was on such organizational factors as training, amount of budget allocated and governance. This indicates that the individual with the greatest returns on security are those who invest in technical controls, however, governance and compliance structures will still be the very ones which are not determine by choice as supplements.

5. CONCLUSION

The deployment of content and workflow management systems on the clouds poses security and compliance issues that need joint efforts in response by both the technical and organizational team. In this paper, the threats were also categorized into five types and it was identified that the highest percentage of threats reported are due to data breaches and identity management failures. The most weighted composite score of compliance models is the general applicability of NIST, and the model of CSA STAR has the highest weighted score among auditability, and COBIT 5 among the models referring to the workflow integration.

The proposed Threat Exposure Index will be practical as it offers an organization a formula to gauge the value of its residual risk, and assess the effectiveness of countermeasure investments. Use of structured compliance models can always lower TEI to about 0.20 or less who can be implemented in a normal deployment. The mechanisms of log integrity which are independent of a cloud provider, anomaly detection in the orchestration and the workflow and quantitative security assurance evaluation are all high value interventions as per the evidences reviewed.

The workflow lifecycle is a topic that has been largely under-researched and the subsequent phases of its monitoring and adaptation stages should be discussed further in the future studies.

REFERENCES

[1] M. Iorga and A. Karmel, "Managing risk in a cloud ecosystem," *IEEE Cloud Computing*, vol. 2, no. 6, pp. 51–57, Nov. 2015, doi: 10.1109/mcc.2015.122. Available: https://doi.org/10.1109/mcc.2015.122

[2] D. Yimam and E. B. Fernandez, "A survey of compliance issues in cloud computing," *Journal of Internet Services and Applications*, vol. 7, no. 1, May 2016, doi: 10.1186/s13174-016-0046-8. Available: https://doi.org/10.1186/s13174-016-0046-8

[3] J. Crampton, G. Gutin, D. Karapetyan, and R. Watrigant, "The bi-objective workflow satisfiability problem and workflow resiliency," *Journal of Computer Security*, vol. 25, no. 1, pp. 83–115, Dec. 2016, doi: 10.3233/jcs-16849. Available: https://doi.org/10.3233/jcs-16849

[4] N. M. Gonzalez, T. C. M. De Brito Carvalho, and C. C. Miers, "Cloud resource management: towards efficient execution of large-scale scientific applications and workflows on complex infrastructures," *Journal of Cloud Computing Advances Systems and Applications*, vol. 6, no. 1, Jun. 2017, doi: 10.1186/s13677-017-0081-4. Available: https://doi.org/10.1186/s13677-017-0081-4

[5] J.-M. Martinez-Caro, A.-J. Aledo-Hernandez, A. Guillen-Perez, R. Sanchez-Iborra, and M.-D. Cano, "A comparative study of Web content Management Systems," *Information*, vol. 9, no. 2, p. 27, Jan. 2018, doi: 10.3390/info9020027. Available: https://doi.org/10.3390/info9020027

[6] K. Brandis, S. Dzombeta, R. Colomo-Palacios, and V. Stantchev, "Governance, risk, and compliance in cloud scenarios," *Applied Sciences*, vol. 9, no. 2, p. 320, Jan. 2019, doi: 10.3390/app9020320. Available: https://doi.org/10.3390/app9020320

[7] C. Bryce, "Security governance as a service on the cloud," *Journal of Cloud Computing Advances Systems and Applications*, vol. 8, no. 1, Dec. 2019, doi: 10.1186/s13677-019-0148-5. Available: https://doi.org/10.1186/s13677-019-0148-5

[8] D. Georgiou and C. Lambrinoudakis, "Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR)," *Information*, vol. 11, no. 12, p. 586, Dec. 2020, doi: 10.3390/info11120586. Available: https://doi.org/10.3390/info11120586

[9] Z. Georgiopoulou, E.-L. Makri, and C. Lambrinoudakis, "GDPR compliance: proposed technical and organizational measures for cloud provider," *Information and Computer Security*, vol. 28, no. 5, pp. 665–680, Jun. 2020, doi: 10.1108/ics-01-2020-0009. Available: https://doi.org/10.1108/ics-01-2020-0009

[10] R. El-Gazzar and K. Stendal, "Examining how GDPR challenges emerging technologies," *Journal of Information Policy*, vol. 10, pp. 237–275, May 2020, doi: 10.5325/jinfopoli.10.2020.0237. Available: https://doi.org/10.5325/jinfopoli.10.2020.0237

[11] Y. Hu, H. Wang, and W. Ma, "Intelligent cloud workflow management and scheduling method for big data applications," *Journal of Cloud Computing Advances Systems and Applications*, vol. 9, no. 1, Jul. 2020, doi: 10.1186/s13677-020-00177-8. Available: https://doi.org/10.1186/s13677-020-00177-8

[12] T. Abioye, O. Arogundade, S. Misra, K. Adesemowo, and R. Damaševičius, "Cloud-Based Business Process Security Risk Management: A Systematic Review, Taxonomy, and Future Directions," *Computers*, vol. 10, no. 12, p. 160, Nov. 2021, doi: 10.3390/computers10120160. Available: https://doi.org/10.3390/computers10120160

[13] N. Soveizi, F. Turkmen, and D. Karastoyanova, "Security and privacy concerns in cloud-based scientific and business workflows: A systematic review," *Future Generation Computer Systems*, vol. 148, pp. 184–200, May 2023, doi: 10.1016/j.future.2023.05.015. Available: https://doi.org/10.1016/j.future.2023.05.015

[14] H. T. El-Kassabi, M. A. Serhani, M. M. Masud, K. Shuaib, and K. Khalil, "Deep learning approach to security enforcement in cloud workflow orchestration," *Journal of Cloud Computing Advances Systems and Applications*, vol. 12, no. 1, p. 10, Jan. 2023, doi: 10.1186/s13677-022-00387-2. Available: https://doi.org/10.1186/s13677-022-00387-2

[15] A. Issaoui, J. Örtensjö, and M. S. Islam, "Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance," *Future Business Journal*, vol. 9, no. 1, Dec. 2023, doi: 10.1186/s43093-023-00285-2. Available: https://doi.org/10.1186/s43093-023-00285-2

[16] A. Shukla, B. Katt, and M. M. Yamin, "A quantitative framework for security assurance evaluation and selection of cloud services: a case study," *International Journal of Information Security*, vol. 22, no. 6, pp. 1621–1650, Jun. 2023, doi: 10.1007/s10207-023-00709-8. Available: https://doi.org/10.1007/s10207-023-00709-8

[17] L. R. P. Sahayaraj and S. Muthurajkumar, "Efficient classification and preservation of log integrity through propagated chain in cloud," *Journal of Intelligent & Fuzzy Systems*, vol. 45, no. 3, pp. 4669–4687, Jul. 2023, doi: 10.3233/jifs-224585. Available: https://doi.org/10.3233/jifs-224585

[18] D. Chatziamanetoglou and K. Rantos, "Blockchain-Based Security Configuration Management for ICT systems," *Electronics*, vol. 12, no. 8, p. 1879, Apr. 2023, doi: 10.3390/electronics12081879. Available: https://doi.org/10.3390/electronics12081879

[19] M. Chauhan and S. Shiaeles, "An analysis of cloud security frameworks, problems and proposed solutions," *Network*, vol. 3, no. 3, pp. 422–450, Sep. 2023, doi: 10.3390/network3030018. Available: https://doi.org/10.3390/network3030018

[20] V. Jayasinghe, E. Erturk, and Z. Li, "Critical factors Influencing cloud security posture of Enterprises: An Empirical analysis," *Information Dynamics and Applications*, vol. 2, no. 4, pp. 210–222, Dec. 2023, doi: 10.56578/ida020405. Available: http://dx.doi.org/10.56578/ida020405

[21] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, "Access control as a service for the Cloud," *Journal of Internet Services and Applications*, vol. 6, no. 1, May 2015, doi: 10.1186/s13174-015-0026-4. Available: https://doi.org/10.1186/s13174-015-0026-4

[22] J. Singh, J. Powles, T. Pasquier, and J. Bacon, "Data flow management and compliance in cloud computing," *IEEE Cloud Computing*, vol. 2, no. 4, pp. 24–32, Jul. 2015, doi: 10.1109/mcc.2015.69. Available: https://doi.org/10.1109/mcc.2015.69

[23] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, "Security transparency: the next frontier for security research in the cloud," *Journal of Cloud Computing Advances Systems and Applications*, vol. 4, no. 1, Jun. 2015, doi: 10.1186/s13677-015-0037-5. Available: https://doi.org/10.1186/s13677-015-0037-5

[24] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "New access control systems based on outsourced attribute-based encryption," *Journal of Computer Security*, vol. 23, no. 6, pp. 659–683, Sep. 2015, doi: 10.3233/jcs-150533. Available: https://doi.org/10.3233/jcs-150533

[25] S. P. Kaluvuri, A. I. Egner, J. D. Hartog, and N. Zannone, "SAFAX â€" An Extensible Authorization Service for Cloud Environments," *Frontiers in ICT*, vol. 2, May 2015, doi: 10.3389/fict.2015.00009. Available: https://doi.org/10.3389/fict.2015.00009