Cloud Security Metrics and Measurement

Sina Ahmadi

February 5, 2024

ISSN: 2959-6386 (Online), Vol. 2, Issue 1, April 2023

Journal of Knowledge Learning and Science Technology

journal homepage: https://jklst.org/index.php/home

JKLST
EXPLORING THE INTERSECTION OF KNOWLEDGE, LEARNING, AND SCIENCE & TECHNOLOGY:
UNLEASHING THE POWER OF SYNERGY IN THE 21ST CENTURY

Cloud Security Metrics and Measurement

Sina Ahmadi[1]
[1] National Coalition of Independent Scholars (NCIS), United States

Abstract

This research aims to investigate the cloud security metrics by exploring the existing frameworks, integrated approaches and quantitative measurements to enhance overall security in cloud environments. This study explains several established frameworks and standards, such as the CSA Cloud Controls Matrix, NIST SP 800-53 and ISO/IEC 27001, which are important in guiding organizations towards strong security practices. Moreover, a qualitative research method has been used in this research study, conducting a literature review of past studies on the same topic. The challenges and limitations regarding cloud security have also been mentioned in this research study, which is helpful for future researchers to explore in detail and develop stronger strategies for enhancing cloud security as a whole. This research study states that the emerging threats and technologies related to cloud security must be explored continuously to develop a detailed understanding of cloud security measures.

Keywords: Cloud Security, Cloud Metrics, NIST, ISO 27001, Encryption.

Article Information:
Article history: *Received:*11/02/2023 *Accepted:* 25/03/2023 *Online:* 30/04/2023 *Published*: 30/04/2023
DOI: https://doi.org/10.60087/jklst.vol2.n1.p107

[i]**Correspondence author: Sina Ahmadi** **Email:** sina0@acm.org

Introduction

Cloud security can be defined as the collection of procedures and technology specially designed to address internal and external threats to business security [1]. In this modern world, organizations rely on cloud computing to enhance efficiency, scalability and flexibility. The complexities regarding cloud adoption keep increasing with the increase in its advancements. Organizations need to focus on cloud security because, in this digital world, most data are stored in clouds to be accessed anytime from anywhere. Organizations must also encourage using cloud-based tools and services as a part of their infrastructure. Moreover, cloud security metrics and measurements must also be considered for ensuring the security of the cloud data, whether it is related to an individual or an organization. When the clouds are secured from potential threats, mathematical models and comprehensive metrics are developed for effective cloud storage management.

The purpose of this research regarding cloud security is to explain quantitative metrics in detail for addressing confidentiality, availability and integrity. These important metrics contribute to a systematic approach for measuring and assessing the effectiveness of security controls included in cloud environments. Moreover, this research also explores some significant models that will reflect the overall security of the cloud system. When the loud ecosystems move to the next level of advancement, the requirement for enhanced and adaptable security strategies also increases. This research aims to provide valuable insights regarding cloud security by providing a structured framework for evaluating and measuring threats and risks in the system. With the help of effective metrics and measurements, organizations can not only stay updated with the current security trends. Still, they can also enhance the overall defensive system against emerging cyber threats. Figure 1 depicts the two pillars of cloud security.

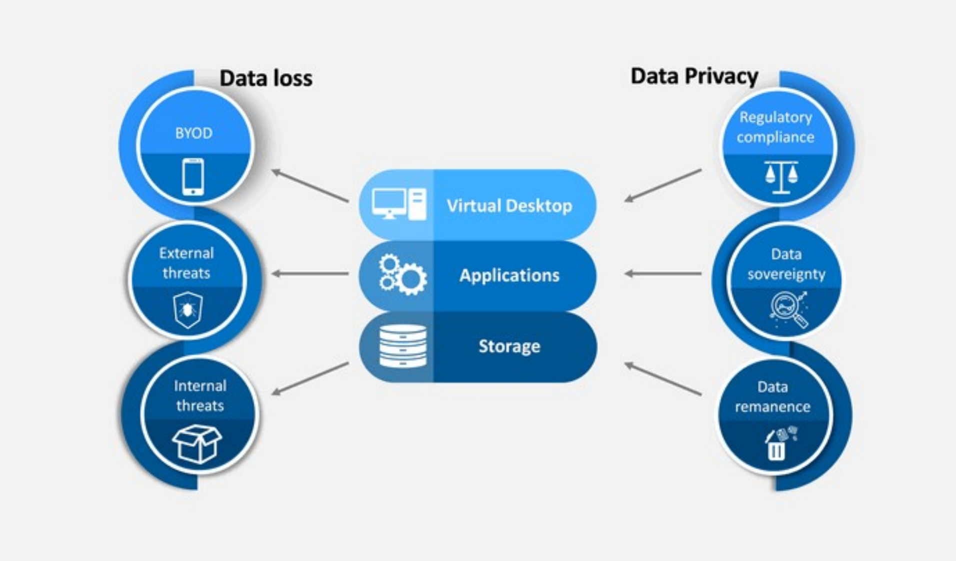

Figure 1: Cloud Security[2]

1. LiteratureReview

1.1. Existing Frameworks and Standards for Cloud Security Metrics

Assessing current standards and frameworks for security metrics is very important in cloud metrics. Currently, many different standards are being implemented in the industry. One of these is the ISO/IEC 27001. It is mainly a group of standards that help companies secure their private data. It provides detailed requirements for an information security management system and depicts a set of best practices. The standards describe the security controls that assist companies in mitigating information risks. [3] also conducted research in this regard. This standard mainly focuses on implementing and maintaining an information security management system (ISMS). Companies complying with this standard have a very secure and safe cloud network. It requires organizations to ensure that they encrypt their data both in transit and at rest. In this way, the integrity and confidentiality of data are maintained.

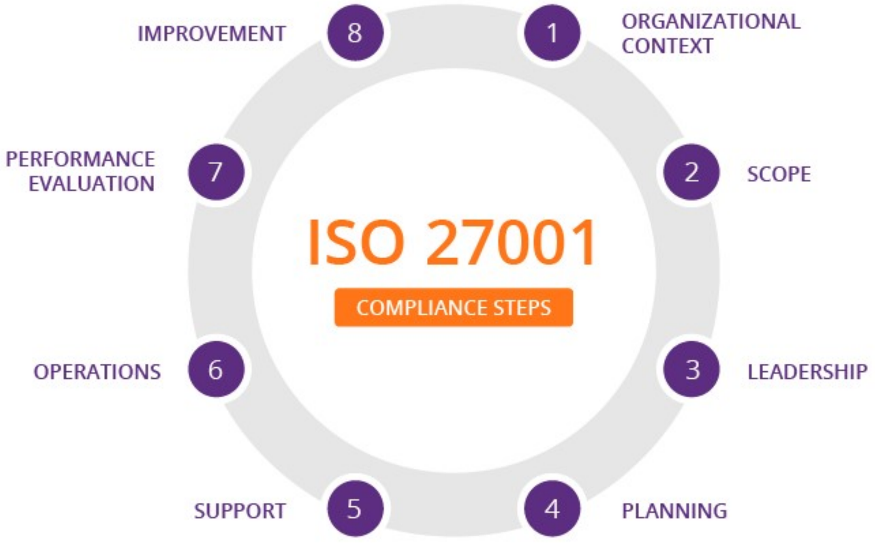

Figure 2: ISO/IEC 27001 Standard [4]

NIST SP 800-53 is another standard being implemented in the industry. This standard focuses on the shared responsibility model. It helps companies and cloud service providers understand their duties. It thus ensures that all the security measures are equally distributed. [5] conducted a comparative analysis of SP 800-53 with IEC 27001. NIST SP 800-53 is a compliance framework created by the National Institute of Standards in Technology. The main purpose of this standard is to develop a foundation of different guiding elements and controls that can help support a company's cybersecurity priorities and needs. All federal information agencies and systems must comply with this standard to secure their cloud environment.

The CSA Cloud Controls Matrix (CCM) is another framework to secure cloud environments. It contains around 197 control objectives that have been scattered in 17 different domains that are based on different aspects related to cloud security. [6] Cloud security level was also measured using this framework. It was found that CSA CCM can be used as a beneficial tool to conduct a detailed evaluation of a cloud implementation. It also provides useful guidelines on which security controls should be utilized by different users within the cloud. Each CCM control and its overall requirements mainly map onto different security regulations and standards that are accepted in the industry. It thus allows companies to understand and track the equivalent or similar requirements of such frameworks.

1.2. Quantitative Metrics for Confidentiality in Cloud Environments

Different quantitative metrics can also be used to assess confidentiality in cloud environments. It is one of the main pillars of information security, and quantitative metrics help companies identify such risks. Data encryption strength is one of these metrics used to measure the strength of different algorithms implemented on sensitive data. [7] also conducted research in this regard. It was seen that strong encryption mechanisms implemented on the cloud help greatly improve data confidentiality. Besides, access controls can also be used to analyze the effectiveness of cloud security strategies by assessing unauthorized access attempts and breaches. Another method is to analyze data masking and anonymization. These help analyse the extent to which private data is anonymized or masked. This helps in preventing unauthorized persons from gaining access to the data.

Formula 1 shows how to calculate the data encryption strength. Figure 3 shows data encryption flow.

$$DES = \frac{Number\ of\ Key\ Bits}{\mathbf{Data}\ Encryptio\quad Algorithm\ Strength\ Factor} \qquad (1)$$

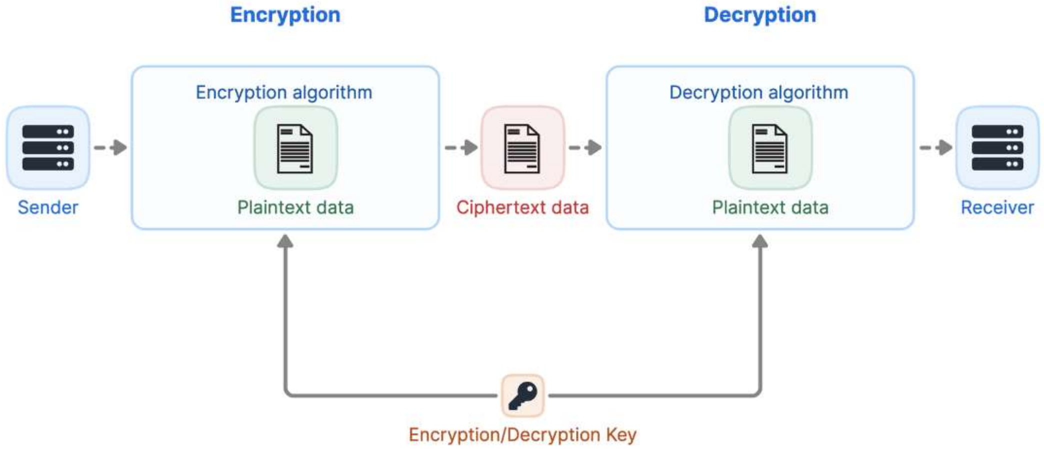

Figure 3: Data Encryption [8]

Some mathematical models can also be used to analyze confidentiality risks in the cloud. For instance, Bayesian Networks can analyze the probabilistic links between various variables that affect confidentiality. [9] also researched using Bayesian networks in a cloud environment for risk assessment. This approach provides a useful framework that helps ensure risk analysis's effectiveness. It also states that risk cannot be properly evaluated and described only by reference to describing probabilities. The mixture of probable consequences and related uncertainties mainly describes risk. A mathematical model to analyze probabilistic links between variables affecting confidentiality is introduced by Bayesian Networks. This model includes conditional probabilities and is represented in Formula 2.

Here, A and B represent events related to confidentiality, offering insights into the dependencies between variables.

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \qquad (2)$$

Entropy-based models can also be used to analyse the randomness and uncertainty in data. They thus provide a quantitative analysis of information content. Entropy mainly acts as an indicator of the extent of unpredictability or disorder in a dataset. [10] also held research in this regard. It is seen that when entropy is high, it means that the level of randomness is high in the data, which makes it less predictable. When this model is implemented on confidential data within the cloud, a high entropy value shows less confidentiality. This is because the data is difficult to understand. Entropy is usually calculated with the help of formulas like Shannon's entropy, which mainly quantifies the average level of uncertainty linked with every dataset. By managing and monitoring entropy levels, companies can implement strong measures to ensure the confidentiality of their data.

Another technique that helps analyse the confidentiality effectiveness of cloud networks is using Monte Carlo simulation. This technique involves repeated random sampling of input variables. [11] conducted research on different risk assessment models used in cloud environments. It was observed that Monte Carlo simulations help companies analyse different possible scenarios and their uncertainties. It utilizes different factors like encryption strength, data access patterns, etc., to develop a probabilistic view of the possibility of confidentiality breaches. In every simulation, input parameters are selected randomly based on their probability distribution. This method mainly helps companies analyse the range of probable outcomes and the relevant risks. Formula 3 shows the probability of a confidentiality breach. Figure 4 depicts Monte Carlo simulation.

$$P\ (Confidentiality\ Breach) = \frac{Number\ of\ Simulations\ with\ Breaches}{Total\ Numbe\ \ of\ Simulations} \quad (3)$$

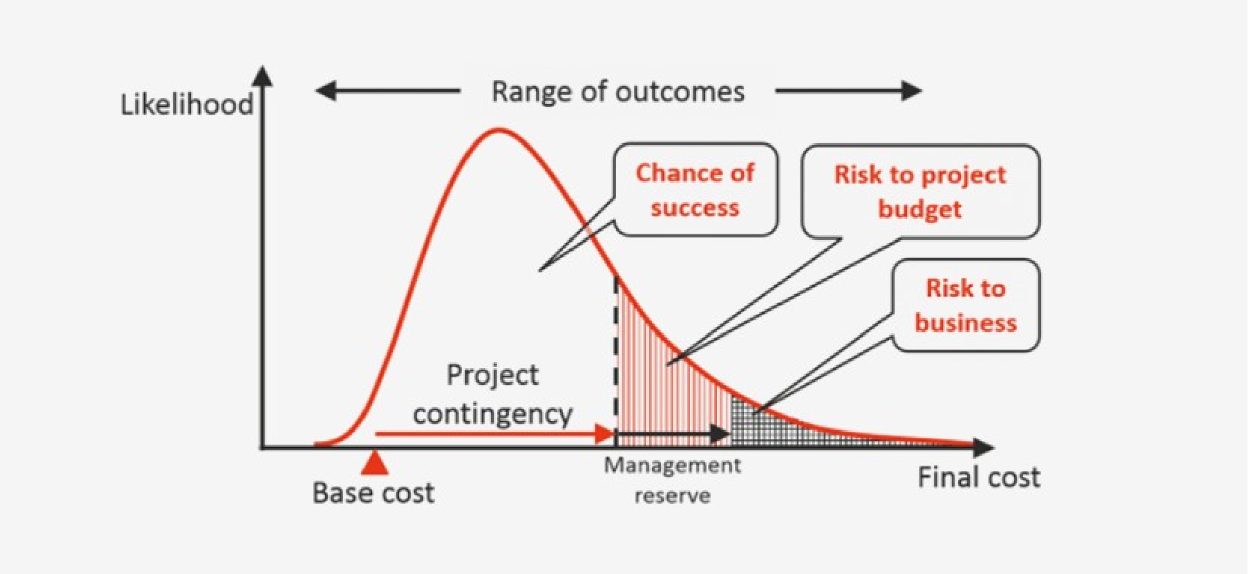

Figure 4: Monte Carlo Simulation [12]

1.3. Quantitative Metrics for Integrity in Cloud Environments

The integrity aspect of cloud environments can also be analyzed with the help of quantitative metrics. For instance, checksum verification is a common method used in this regard. [13] also researched one digital checksum verification. It is mainly a cryptographic value calculated based on a pile of data that can be used to assess the authenticity and integrity of that data. This technique provides various benefits in terms of integrity in cloud environments. Checksums also help in preventing data manipulation and unauthorized access. This method is considered more secure and effective than other version control systems. This is because they have strong mechanisms for file integrity preservation. Formula 4 shows how to calculate unauthorized access attempt rate.

$$UAAR = \frac{Number\ of\ Unauthorized\ Access\ Attempts}{Total\ Access\ Attempts}\ x\ 100(4)$$

Correct correction rates and error detection can also help analyse the integrity of cloud environments. These are the common quantitative metrics that help companies ensure the strong integrity of data. Errors can mainly occur because of different aspects like hardware failure, network problems, etc. It is important to analyze the frequency of errors to determine the status of data integrity. [14] also researched such metrics and their effectiveness with the help of a survey. It is seen that when the error detection rate is low, it means that the strategies implemented by the company are not effective in detecting errors. Besides, if the rate of uncorrected errors is high, it shows that the detection of errors is being done, but the mechanisms applied to correct them are not effective, which can lead to integrity issues.

Thus, companies must use correction mechanisms and error detection metrics like parity bits or Reed-Solomon codes. All these mechanisms can be measured in terms of their effectiveness by the ability to detect and mitigate risks. If the integrity of the company's data is compromised, it is important to analyze the main causes, such as system failure or security breaches. In this case, proper remediation strategies are also needed to overcome the issue. These can include the use of error detection algorithms or the use of strong correction methods [14]. However, proper monitoring of such metrics is highly needed to ensure the effectiveness of such methods. The integrity aspect of cloud environments can be quantitatively assessed using Checksum Verification. Formula 5 shows the calculation for a checksum.

$$Checksum=Modulo\ Sum\ of\ Data\ Bits \quad (5)$$

This cryptographic value verifies the authenticity and integrity of data, aiding in preventing unauthorized access and data manipulation.

Correct Correction Rates (CCR) and Error Detection Rates (EDR) are quantitative metrics for assessing integrity. They can be calculated as per formulas 6 and 7.

$$CCR = \frac{Number\ of\ Corrected\ Errors}{Total\ Errors\ Detected}\ x\ 100 \quad (6)$$

$$EDR = \frac{Number\ of\ Undetected\ Errors}{Total\ Errors\ Detected}\ x\ 100 \quad (7)$$

1.4. Integrated Approaches: Assessing Overall Cloud Security

It is very important to analyze the overall cloud security with the help of the analysis of integrity, availability, and confidentiality. This is also known as the CIA triad, used to check cloud security. [15] also researched security problems in the cloud and assessed the use of the CIA triad. The elements of this triad act as holistic metrics that help determine a company's overall cloud security level. If one element of this triad is disturbed, it also disturbs the others. Therefore, a balance of these elements is important to ensure the cloud environment's security. The CIA triad thus helps companies clearly analyse their current security situation. They ensure that their efforts to keep their data private are effective and do not lead to security issues.

Some companies also use multi-factor evaluation models to analyze their cloud security. These models mainly involve user behaviour analytics, threat intelligence, etc., to check cloud security. [16] also conducted research in this regard. It has been observed that multi-factor models provide a detailed analysis of a company's current cloud security situation. They help companies adapt to the current threats and technological advancements related to cloud environments. Using these elements helps ensure that the company's security evaluations are accurate and can identify the complexities present in cloud environments.

1.5. Challenges and Limitations in Cloud Security Metrics

While measuring cloud security, many companies face different challenges. Many firms need to use standardized metrics, making it difficult to compare their security measures efficiently. Every cloud service provider might have its metrics, making it hard to develop a universal standard for evaluating cloud security. [17] also researched the challenges faced by companies in this regard. Besides, cloud technologies are continuously evolving in the industry, which can create issues for companies while keeping their security metrics current. These advancements in the industry demand companies to continuously analyze their security measures and develop universal cloud security metrics.

The current approaches that measure cloud security face some limitations as well. These models depend on quantitative metrics, which overlooks the qualitative security metrics. According to [18], security does not relate only to numbers in the cloud environment. It also includes an analysis of the overall security context and the influence of vulnerabilities on security controls. This dependence on quantitative metrics can develop wrong perceptions of security in the company and make it vulnerable to external threats.

2. Problem Definition

Moving the important business stuff to the cloud comes with cool perks, like being flexible, scalable, and saving money. Cloud setups keep changing, and attackers keep getting trickier [19]. It's super important to understand and measure how secure things are. The problem is that there needs to be no standard way to put a number on security. This makes it a real challenge for companies. They want to check, compare, and strengthen their cloud security, but with clear metrics, it is easier.

2.1. Lack of Standardized Metrics

The absence of standardized metrics for assessing cloud security creates a real problem for organizations trying to figure out how secure their cloud systems are [20]. Everyone is using their own methods to measure security, leading to a confusing and complicated situation. This lack of a common ground makes it challenging to compare security measures effectively and puts a damper on collaboration and information-sharing among different organizations in the industry. Clear and common rules or criteria are needed to simplify things. A unified approach to metrics would make it easier for organizations to assess and improve their cloud security and foster better communication and understanding across the board. In the age of widespread cloud computing, having a standardized framework is essential to build trust, ensure systems can work together, and tackle the ever-changing challenges of cybersecurity in the digital world.

2.2. Dynamic Nature of Cloud Environments

Cloud setups are always in flux, with new resources always coming up. This constant evolution makes traditional security metrics not cut it [21]. Metrics that can keep pace with the rapid changes in the cloud environment are needed, unlike the old ones that need help to keep track of all the ins and outs. That's why organizations must focus on crafting metrics that can adapt on the go. This way, they can get an accurate picture of how secure their stuff is, even with all the constant changes in the cloud. It's like having metrics that can roll with the punches and still provide the lowdown on your security controls in the ever-shifting world of cloud computing. It's all about staying flexible and up-to-date in this dynamic cloud landscape.

2.3. Confidentiality, Integrity, and Availability Challenges

In the cloud world, keeping the info safe has its own set of challenges for each key area: keeping things private (confidentiality), making sure stuff stays accurate (integrity), and making sure everything is always accessible (availability). When sharing resources, keeping things confidential becomes complex. Storing and processing data everywhere can mess with its accuracy, and relying on outside service providers can make things less available when needed.

The real challenge is that cloud setups are all connected and spread out, making it tough to measure how well the security is doing [22]. To understand how safe the info is, specific ways need to be found to measure each of these challenges. Taking a big-picture view and looking at how all these things work together is crucial. It helps organizations stay on top of weaknesses and boost overall info security in the ever-changing and complex world of cloud computing.

2.4. Adaptability to Emerging Threats

Keeping up with the ever-changing threats to cloud systems can be a real challenge for the usual security models [23]. As cyber threats become fancier, organizations need security measures that can quickly adapt to the new risks. Making mathematical models becomes important to see how safe things are right now and to check how well security measures can roll. These models should look at how good an organization is at spotting, dealing with, and fixing new threats quickly and efficiently. By making adaptability a big part of the check-up, organizations can get better ready to stay strong against the ever-changing cyber threats. This ensures that their security measures stay operative and flexible in the always-shifting and challenging world of cloud computing.

2.5. Regulatory Compliance and Industry Standards

Certifying that cloud security aligns with rules and standards is important for any organization tapping into cloud services [24]. The tricky part is that these standards often require straightforward measurement guidelines. Companies need to be able to show they're on the compliance train. To tackle this, it's crucial to define clear and easy-to-measure metrics that align with rules and industry expectations. These metrics aren't just for ticking compliance boxes; they also help in building a strong and widely accepted method to check how secure your cloud setup is. With these solid measurement criteria, organizations can confidently navigate the tricky world of regulatory compliance. This shows everyone they're very serious about security and keeping their operations in the best shape in the ever-changing cloud scene.

3. Methodology and Approach

3.1. Challenges in Traditional Data Warehousing

This research study employs a qualitative research methodology that involves conducting a literature review of the studies conducted by past researchers. The reason behind selecting this research method is to provide authentic information by gathering relevant information from research papers on cloud security measures and metrics conducted by different researchers. The qualitative research method helps provide deep insights regarding cloud security with diverse perspectives, experiences and challenges. The purpose of this research method is to gather the richness of this topic and determine the complexities faced by different people and organizations when dealing with the challenges regarding cloud security measures. Moreover, this research methodology is explanatory and provides detailed information regarding cloud security in the context of different industries and organizations.

3.2. Data Selection

The data selection method for this research study is quite simple, as research articles and other relevant studies were selected from Google Scholar from 2020 to 2023. It is a simple criterion that involves those studies that involve the experiences of organizations and individuals regarding cloud security metrics and measures. The selected participants include IT managers, cloud architects, and cybersecurity professionals involved in the research studies for conducting a detailed literature review. Moreover, all the data has been selected based on themes created based on cloud security measures and metrics.

3.3. Data Collection

The data collection method includes document analysis of the studies related to cloud security measures and metrics. This type of analysis includes examining existing studies, organizational documents, industry reports and academic papers that play an integral role in understanding cloud security in detail. Moreover, a literature review has also been considered a major source for collecting detailed data for this research study. It plays a vital role in providing existing knowledge, gaining insights regarding the evolution of cloud security measures and identifying gaps. The academic papers have been selected from reliable and authentic journals to determine the current state of cloud security practices. Moreover, the document analysis allows the extraction of useful patterns, themes and findings from a wide range of sources to determine the latest trends and best practices.

3.4. Analytical Process

The analytical process involves a thematic analysis approach, which shows the research has been conducted based on several themes related to cloud security measures and metrics. The data collected from the document analysis and literature review will be coded systematically and categorised to identify useful patterns and themes. This analysis will be iterative, refining themes with the emergence of new data. All the identified themes will then be with the insights obtained from the literature review. This, in turn, contributed to a deep understanding of cloud security metrics and measurement.

4. Results and Discussion

4.1. Diversity in Current Cloud Security Metrics

In cloud security, organisations use a mix of ways to check how safe their stuff is in the cloud. Some stick to well-known standards like ISO 27001 or NIST, while others use measures that suit their particular cloud setups. The thing is, because there's no one-size-fits-all standard, everyone's doing their own thing. This makes it tough to compare and determine how well the performance is compared to others.

So, a common set of measures that everyone can use is needed. That way, everyone will speak the same language when discussing how secure their cloud stuff is. This helps to see the deficiencies and tells how to do better. Especially because the cloud is always changing, having a shared set of measures means we can keep up with the new challenges and ensure the security stays strong.

4.2. Adaptability Challenges in Dynamic Cloud Environments

The study talks about how using regular security measures in the always-changing world of cloud computing is tricky. When companies are growing and dealing with different workloads, the usual security metrics need to move more quickly to catch the rapid changes in how resources are added or removed. The metrics that work fine for old-school setups don't cut it in the fast, ever-shifting cloud scene.

So, dealing with this compliance challenge means switching how security metrics are thought and used, which is necessary. Instead of sticking to fixed measures, the focus needs to be on making changes in real time. This way, the metrics stay up-to-date in the always-changing world of cloud computing. It's all about ensuring security measures can keep pace with the constant changes in cloud setups. This shift is about recognizing the need for security metrics to easily match the active changes in cloud setups, creating a stronger and more reactive security system that can handle new challenges and evolving threats.

4.3. Confidentiality Metrics: Navigating Shared Resources

Analyzing how well the information is kept confidential in shared cloud resources is important to the study. Even though sharing resources in the cloud can save money and make things more competent, keeping data confidential comes with challenges. The research points out that the current methods used to measure confidentiality are only sometimes operative in dealing with these challenges. The discussion explores the complexities of shared environments and suggests improvements to the metrics used to navigate shared cloud infrastructures securely. Finding the right balance between maximising resources and protecting data becomes important. The research suggests metrics that keep data safe and work well in the collaborative nature of cloud environments. As more organizations use shared resources in the cloud, it becomes crucial to have a customized approach to measuring how well we keep information confidential. This ensures a smooth combination of efficiency gains with strong data security practices.

4.4. Integrity Metrics in Distributed Cloud Environments

Exploring how data stays safe in distributed cloud systems is a big deal. The research looks at how well the current ways of keeping data safe work and figures out where they can improve. There are unique challenges in these cloud setups, where data is stored and processed all over the place. Companies are increasingly using these systems, so it is important to know that the tools being used are safe for keeping the data safe and up to the task.

The study checks how well the current methods are doing and looks for new and clever ways to ensure the data stays intact in these distributed cloud setups. It understands that storing data in different locations differs from keeping it all in one place. For businesses using these distributed cloud systems, it's super important that the information is reliable and the same across the board. How things are happening now might be good, but it is also important to keep improving to ensure the data stays safe as things in the tech world keep changing.

4.5. Ensuring Availability: Metrics and External Dependencies

Checking how well cloud services stay up and running can take time and effort. The talk concerns the problems when important cloud services depend on other companies. The study looks into the issues that arise from relying on these outside people and shows how it can mess with the overall availability of services and what that means for companies. The study suggests a need to change how things are measured to handle these outside factors better. The goal is to give companies a clearer idea of their cloud services' readiness. With more and more companies using outside services in the cloud, it's a big deal to figure out how these dependencies affect the availability of services. This understanding is very important for making smart decisions and ensuring the cloud system is strong and reliable.

4.6. Security Measures and Emerging Threats

Examining security measures in response to evolving threats in cloud environments offers an inclusive view of the cybersecurity landscape. By uncovering the strengths and weaknesses in current security protocols when dealing with growing cyber threats, the analysis stresses the need for proactive and flexible security strategies. Recommendations propose mixing advanced threat intelligence and response capabilities into existing security models, highlighting the importance of dynamic cybersecurity approaches in the ever-changing realm of cloud computing. Recognizing the dynamic nature of cyber threats, organizations must go beyond traditional security measures and adopt innovative, adaptable strategies to minimize risks and safeguard sensitive information in the cloud effectively. The suggested addition of advanced threat intelligence guarantees a more responsive and tough security framework to protect against the continually changing tactics of malicious actors in the digital domain. The focus is on staying ahead of cyber threats through practical and flexible security practices.

4.7. Bridging Compliance Gaps with Quantitative Metrics

Looking at the hurdles of matching cloud security metrics with the rules and regulations gives some important insights. The discussion goes through the gaps in following the rules and explores ways to create numbers and measurements that fit better with the regulations. The results show how tough it is to meet various industries' different rules and security needs. Suggestions are made for using standard measurements that make it easier to follow the rules and stick to what the regulations want. These ideas give organizations a clearer way to follow the rules in their cloud setups. As the rules change, ensuring security measures fit in with what the rules say becomes important for organizations to handle the tricky regulatory landscape. It's all about committing to keeping data safe and following the rules in their cloud projects.

4.8. Toward a Unified Framework: Synthesizing Cloud Security Metrics

Pulling together insights from different metrics and challenges, this part supports a smart approach to creating a unified, adaptable, and all-encompassing cloud security metric framework. The discussion explores things that existing metrics share highlights key principles for a standard framework, and gives suggestions for future research and industry practices. The main idea is to boost collaboration among everyone in the industry to agree on cloud security metrics that can change with the fast-moving nature of cloud setups. The big goal is to guide organizations toward a more standardized and effective way of checking and strengthening their cloud security. By pushing for a united framework, the idea is to boost the industry's ability to handle new threats, compare how well everyone's doing, and ensure cloud security measures stay strong in a constantly changing tech world.

5. Conclusion

To conclude, this research study explores the cloud security metrics to provide a comprehensive overview of the existing frameworks, integrated evaluation approaches and qualitative measurements. Determining frameworks and standards shows the diverse strategies organisations adopt within cloud environments to deal with evolving cyber threats. The quantitative metrics related to integrity and confidentiality provide detailed analysis regarding specific security dimensions so that the role of encryption strength, advanced analytical models and access controls in protecting confidential data can be determined. Adopting integrated approaches inspired by multi-factor inspiration and the CIA triad shows the interconnected nature of availability, integrity and confidentiality in enhancing overall cloud security. Moreover, this research also highlights the limitations and challenges regarding cloud security and its future scope. Thus, organizations must consider integrating smart cloud technologies and focus on enhanced cloud security measures and metrics to enhance the overall security of a cloud-based system.

6. Future Scope

The determination and explanation of cloud security measurements and metrics highlight the current security challenges and offer opportunities for future development and research. The future scope of cloud security offers several advancements in the field so that the overall security of the cloud network can be enhanced. The most important factor related to the future of cloud security is the development of cloud security measures within organizations. The diversity in metrics in organizations and industries shows the need for an informed framework. Future researchers can focus on establishing a number of standardized metrics aligned with the industry's best practices, regulatory requirements and the flexibility of cloud networks. This initiative could facilitate easier benchmarking, collaboration, and information-sharing within the industry so that a more unified and useful approach to cloud security assessment could be developed.

Another important aspect to consider regarding cloud security metrics and measurements is adaptability. Future researchers can focus on creating security metrics that could respond to the changing nature of cloud deployments. This may include the metrics that can make real-time adjustments to reflect security measures accurately. Moreover, the future adaptability of cloud security results in managing workloads effectively and also contributes to addressing potential security threats and risks.

In addition, availability, integrity and confidentiality are important metrics to explore. Future research could also focus on these metrics for specific data types, critical services and applications. For instance, when security metrics are developed to address unique challenges regarding distributed data storage or shared resources, it provides organizations with detailed insights regarding their security requirements and measures. Also, the use of Machine Learning (ML) and Artificial Intelligence (AI) is included in the future scope of cloud security measures and metrics because these are the technologies that help enhance the ability of a cloud network system to detect threats timely and respond to them in real-time.

References

[1] S. S. Rupra and A. Omamo, "A cloud computing security assessment framework for small and medium enterprises," framework for small and medium enterprises. Journal, pp. 201-224, 2020.

[2] V. Ihnatiuk, "The Beginner's Guide to Cloud Security," 2023. [Online]. Available: https://boostylabs.com/blog/cloud-security.

[3] N. A. Kamaruddin, I. Mohamed, A. D. Jarno and M. Daud, "Cloud Security Pre-assessment Model For Cloud Service Provider Based On ISO/IEC 27017: 2015 Additional Control," Revolution, pp. 1-17, 2020.

[4] Imperva, "What is ISO/IEC 27001," 2023. [Online]. Available: https://www.imperva.com/learn/data-security/iso-27001/.

[5] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013," NIST Spec. Publ., pp. 10-13, 2022.

[6] A. Chandra, "Measurement of the Cloud Security Level at Company using Cloud Control Matrix," 2020.

[7] B. Seth, S. Dalal, V. Jaglan, D. N. Le, S. Mohan and G. Srivastava, "Integrating encryption techniques for secure data storage in the cloud," Transactions on Emerging Telecommunications Technologies, p. 4108, 2022.

[8] A. Diop, "A Primer on Cryptography," 24 October 2022. [Online]. Available: https://auth0.com/blog/a-primer-on-cryptography/.

[9] C. Chen, L. Zhang and R. L. K. Tiong, "A novel learning cloud Bayesian network for risk measurement," Applied Soft Computing, p. 105947, 2020.

[10] R. Jiang, Z. Ma and J. Yang, "An assessment model for cloud service security risk based on entropy and support vector machine," Concurrency and Computation: Practice and Experience, p. 6423, 2021.

[11] C. Bendicho, "Cyber security in the cloud: Risk assessment models," Intelligent Computing: Proceedings of the 2021 Computing Conference, pp. 471-482, 2022.

[12] B. Stanke, "What is the Monte Carlo Simulation?," March 2021. [Online]. Available: https://www.bobstanke.com/blog/monte-carlo-simulation-overview.

[13] M. Kara, A. Laouid, M. Hammoudeh and A. Bounceur, "One Digit Checksum for Data Integrity Verification of Cloud-executed Homomorphic Encryption Operations," Cryptology ePrint Archive, 2023.

[14] A. Li, Y. Chen, Z. Yan, X. Zhou and S. Shimizu, "A survey on integrity auditing for data storage in the cloud: from a single copy to multiple replicas," IEEE Transactions on Big Data, pp. 1428-1442, 2020.

[15] S. Goyal and R. Mathew, "Security issues in cloud computing," Proceeding of the International Conference on Computer Networks, Big Data and IoT, pp. 363-373, 2020.

[16] F. K. Mupila and H. Gupta, "A Multi-factor Approach for Cloud Security," Innovations in Computer Science and Engineering: Proceedings of 8th ICICSE, pp. 437-445, 2021.

[17] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," The Journal of Supercomputing, pp. 9493-9532, 2020.

[18] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," Network, pp. 422-450, 2023.

[19] M. M. Bazm, M. Lacoste, M. Südholt and J. M. Menaud, "Isolation in cloud computing infrastructures: new security challenges," Annals of Telecommunications, pp. 197-209, 2019.

[20] O. O. Akinsanya, M. Papadaki and L. Sun, "Towards a maturity model for health-care cloud security (M2HCS)," Information & Computer Security, pp. 321-345, 2020.

[21] S. T. Milan, L. Rajabion, H. Ranjbar and N. J. Navimipour, "Nature-inspired meta-heuristic algorithms for solving the load-balancing problem in cloud environments," Computers & Operations Research, pp. 159-187, 2019.

[22] W. Hassan, T. S. Chou, X. Li, P. Appiah-Kubi and O. Tamer, "Latest trends, challenges and solutions in security in the era of cloud computing and software-defined networks," Int J Inf &CommunTechnol ISSN, p. 8776, 2019.

[23] V. Sureshkumar and B. Baranidharan, "A study of the cloud security attacks and threats," Journal of Physics: Conference Series, p. 042061, 2021.

[24] H. L. Tsinale and O. C. Otieno, "Security and privacy determinants for a secured cloud-based electronic health record system," 2019.