Chelonian Conservation And Biology

Vol. 16 No. 2 (2021) | https://www.acgpublishing.com/ | ISSN - 1071-8443

DOI: doi.org/10.18011/2021.04(1).1-12

SECURING MULTI-CLOUD ENVIRONMENTS WITH AI AND MACHINE LEARNING TECHNIQUES

Abhilash Reddy Pabbath Reddy

abhilashreddy511@gmail.com

Anjan Kumar Reddy Ayyadapu

anjanreddy8686@gmail.com

Abstract

This paper explores the security challenges faced in multi-cloud environments and how machine learning (ML) can be used to address them. Multi-cloud environments offer businesses flexibility and scalability, but also introduce complexities in securing data and applications. The paper discusses the challenges of distributed data, identity and access management, interoperability, and compliance. It then explores how multi-cloud security strategies can be implemented to mitigate these risks. Finally, the paper examines the role of machine learning in enhancing multi-cloud security by providing anomaly detection, intrusion prevention, and data encryption.

Keywords: Multi-cloud security, Machine learning (ML), Artificial intelligence (AI), Distributed data security, Identity and access management (IAM)

1. INTRODUCTION

The expression "multi-cloud" portrays how an association utilizes many cloud administrations to accomplish a business objective. This could entail utilizing different CSPs for dispersed applications, different cloud administration models, or a similar help model. A simple model would be a business that has a particular application utilizing multiple IaaS suppliers, or a business that chooses to isolate an application into multiple parts and has the parts utilizing different CSPs to meet its IaaS, PaaS, and SaaS needs. Joining a public cloud supplier with an individual server farm (confidential cloud) could be another model [1]. This can be required in the event that a business needs to maintain some level of command over the sorts of information or data that they contract with CSPs to store.

On the other hand, a multi-cloud application is an application that is separated into multiple parts and those parts are spread across multiple clouds. The possibility of multi-cloud applications depends on disseminated figuring, in which unique parts are intended to connect and impart in a brought together or facilitated manner to achieve a certain goal. These parts could be miniature administrations, containers, or administrations. All that about the cycle occurs like it were a solitary application. It is workable for multi-cloud applications to use different cloud administrations (IaaS, PaaS, and SaaS) from a few CSPs because of multicloud registering. This suggests that since CSPs can be picked in light of the requirements of the parts and applications, scattered parts can be put in various clouds for their tasks.

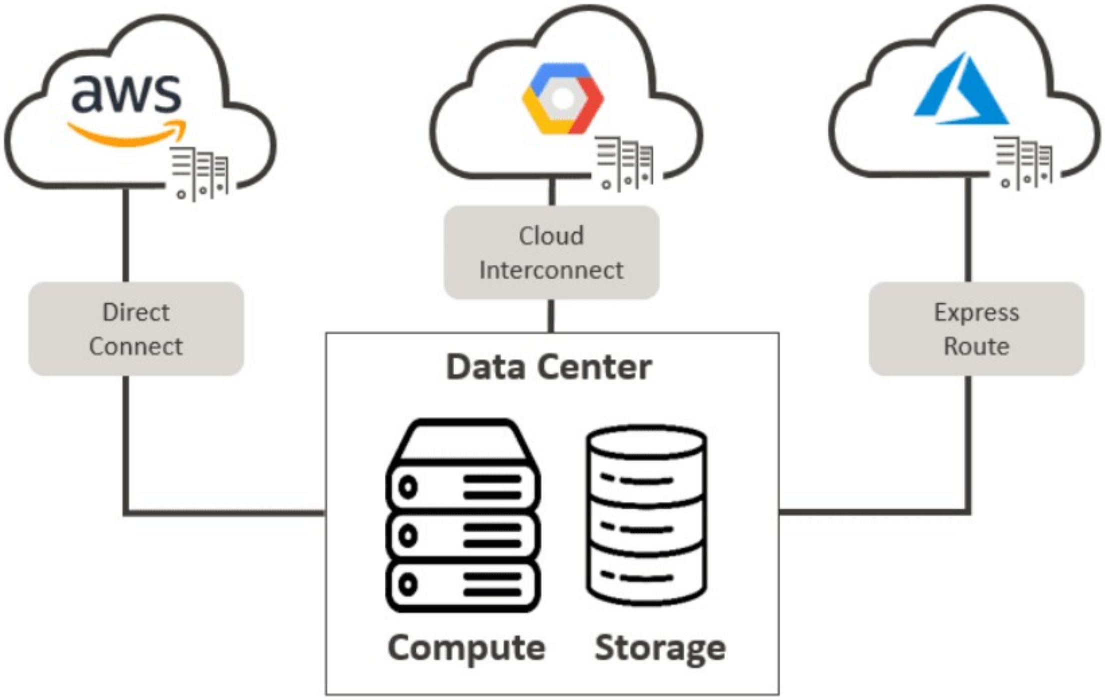

Figure 1: Multi-cloud Environment

A multi-cloud application should go through multiple transformative phases, including plan, improvement, sending, and run-time. The plan of the application is the most vital phase in making a multi-cloud application. During the plan stage, the application is demonstrated by characterizing the necessities (equipment, cloud assets, area, working framework, and so on) and the application design (i.e., the application parts, cooperations, and correspondence instrument). This will act as the establishment for making the multi-cloud application SLA [2]. The accompanying stage, called advancement, is building the parts of the multi-cloud application utilizing the apparatuses and innovations distinguished in the plan stage, like Java and JavaScript.

The multi-cloud application's sending in a cloud environment is the following stage simultaneously. Establishment, arrangement, testing, and provisioning of cloud assets, like servers and virtual machines, are all essential for it. The administrations and CSPs that meet the application necessities are recorded as of now. Thus, the organization script is created, which has every one of the pieces of information expected to do the sending. Three famous instruments for arrangement are Ansible, Manikin, and Cook. At long last, there is run-time. Right now, the multi-cloud application is conveyed on many cloud foundations and works on them. The application is held under perception to perceive how it performs and to track down any abnormalities or infringement. Notice of an abnormality is sent to start and implement the vital restorative measures, for example, countermeasures or security controls.

Organizations across a few clouds offer a method for enhancing the benefits and capacities of different cloud suppliers. It gives the opportunity to choose the best mix of CSP choices to best address application issues and corporate objectives. Significant factors like expense and execution can be augmented along these lines. The following segment records the benefits of multi-cloud registering.

1.1. Benefits of Multi-cloud Computing

An association might decide to run its tasks involving many clouds for various reasons. These legitimizations are ingrained in the benefits of multi-cloud processing, which incorporate keeping away from seller secure in, reducing expenses, offering CSPs more prominent decision and adaptability, debacle recuperation, overt repetitiveness in administrations, cost streamlining, load adjusting, and upgraded administration quality, among different benefits. Ventures should have an unmistakable comprehension of their requests and skill to settle on the best choices to meet them in the event that they are to completely benefit from multi-clouds. This beginnings with laying out the application needs (useful and specialized, for instance) and business targets (functional and monetary). Then, the right cloud administration model or models and CSPs that meet the rules are distinguished and picked [3]. The determination of a CSP and the help blend might approach the strong information and experience of inner IT staff. The following passages go over the upsides of having many clouds.

The utilization of many clouds aids in keeping away from merchant secure. This shows unequivocally the need to try not to be excessively subject to one cloud supplier. In this setup, at least two cloud specialist co-ops are utilized, and cloud clients have the opportunity to switch between them at whatever point they want to do as such because of elements like cost, unfortunate help, administration unavailability, or the disclosure of an unrivaled help presented by an alternate cloud supplier. It gives them decision adaptability, empowering them to change to the CSP that best addresses their issues. Interoperability across CSPs is the essential worry here, as it incredibly influences the seamless exchange of information between different cloud suppliers.

Through multi-cloud sending, cloud clients can fan out their dangers more than a few clouds, consequently controlling them. Information availability, catastrophe recuperation, and fail-over administrations are clear instances of this. It is feasible to ensure the ceaseless provisioning and activity of a help, for example, even if the essential cloud is unavailable or closed down, gave that multiple cases of the help are conveyed in around three different public clouds. This is a straightforward fail-over circumstance. Bunches may commonly be utilized to achieve this. Like information availability, the essential cloud houses the essential information, while two particular clouds — alluded to as auxiliary clouds — are provided by discrete CSPs and house its copies. At the point when extra clouds supply the information if the essential cloud fails, persistent availability is ensured. At the point when the information proprietor requirements to get to the information, information availability might be guaranteed with this setup.

Using many cloud suppliers' benefits is made plausible by multi-clouds. The qualities of CSPs are seen as their essential subject matters and are ingrained in the sorts of cloud models and administrations they give. For instance, CSP "A" could offer IaaS more really than CSP "B," undoubtedly because of CSP "B's" more noteworthy accentuation on PaaS. fluctuations in execution, cost, and inclusion are inborn in the arrangement of these administrations, and cloud clients take utilization of these differences by involving them as measurements to survey and assess CSPs' appropriateness for their tasks. Thus, cloud clients can now exploit these varieties to get the most ideal cloud administration from different CSPs [4]. This will try and give cloud clients the opportunity to choose the ideal mix of administrations and arrangements from different CSPs in view of how well they satisfy their needs. By doing this, organizations might cut costs and find some kind of harmony in their utilization of cloud administrations while likewise picking the best CSP to meet their particular necessities.

The use of various clouds may likewise be profitable in the space of information area, especially where information administration is relevant. For instance, it becomes essential to ensure that client information (connected with the utilization of a particular application) is saved in the assigned area assuming information security decides command that it be kept there. It becomes hard to meet information administration (information capacity) norms, in any case, if the expected CSP doesn't have a server farm at the area. This issue is tended to by the use of multi-clouds, by which client information can be kept in the nearby CSP's offices while the other application parts and basic administrations are facilitated by the other favored CSP. Powerful correspondence between the numerous CSPs under this framework requires appropriate consideration, particularly in the space of coordination and correspondence channel security.

The necessity for inactivity decreases and mystery is one more defense for utilizing a few clouds. For instance, regardless of the benefits of multicloud processing that have proactively been examined, a few organizations might in any case decide to try not to store delicate information on open clouds because of worries about information security. Thus, organizations might decide to reevaluate fewer delicate data to favored CSPs while maintaining more delicate information and data on-premise, or in their confidential cloud office. The organization currently has a colossal arrangement of command over its information. Multi-clouds can be used to diminish dormancy, particularly when a venture's clients are situated in a few regions. By utilizing a few CSPs arranged in the clients' locales, dormancy can be decreased by carrying the help nearer to the clients. Consumer loyalty and speedier response times will result from this.

The benefits of multi-clouds have been illustrated and investigated in the passages above. The expanded use of this has been credited to a few benefits. It is basic to recognize, by and by, that security remains a concern in spite of its developing prevalence. This is associated with the rising gamble level welcomed on by the multi-cloud environment's circulated structure. The security issues in multi-clouds are exacerbated by this rising level of hazard, which likens to rising dangers and weaknesses. Precisely distinguishing these security dangers and the countermeasures expected to address them are basic. By doing this, clients' trust in using multi-clouds develops and the multi-cloud environment turns out to be more protected.

1.2.Artificial Intelligence (AI)

The intelligence of PCs or programming, instead of the mind of living things, mainly individuals, is known as artificial intelligence (AI). A part of software engineering centers around making and investigating wise machines. These gadgets could be alluded to as AIs.

Artificial Intelligence is generally applied in government, industry, and the scholarly world. High level web search tools like Google Search, suggestion frameworks utilized by YouTube, Amazon, and Netflix, human discourse-based cooperation like Google Partner, Siri, and Alexa, self-driving vehicles like Waymo, generative and imaginative devices like ChatGPT and AI workmanship, and godlike play and examination in methodology games like chess and go are a couple of high-profile applications.

The principal huge scientist in the subject he named "machine intelligence" was Alan Turing. The scholastic field of artificial intelligence was laid out in 1956. The field had a few patterns of trust, known as AI winter, which were trailed by discouraging times and subsidizing misfortunes. After profound learning beat all earlier AI strategies in 2012 and the transformer design arose in 2017, subsidizing and interest in the field soar [5]. Accordingly, there was an AI spring in the mid-2020s, when significant progressions in artificial intelligence were spearheaded generally by American organizations, scholastic establishments, and labs.

1.3.Machine Learning

Machine learning (ML) is the investigation of the calculations and measurable models that PC frameworks use to complete a responsibility without express directions. It is at present one of the specialized disciplines with the quickest paces of headway due to the union of measurements and software engineering, as well as the groundworks of information science and artificial intelligence (AI).

PCs that utilization machine learning, a part of artificial intelligence, may learn without requiring any training. By utilizing experience to show itself, machine learning aims to increment PC execution. It makes PCs more equipped for dealing with issues after some time. This approach can be applied to deal with comparable difficulties later on.

The key parts of machine learning are the calculations that are utilized to train the models. The issue that should be tackled decides the sort of machine learning strategy that ought to be utilized [6]. The most vital phase in utilizing machine learning to take care of an issue is gathering information. From that point forward, the model is put to use by being trained, assessed, and carried out (Butt et al., 2020; Sarker, 2021). The three essential m subcategories

Utilizing strategies from directed machine learning, future results are conjecture. The essential capability of calculations for administered machine learning is to dissect and order input information in an OK way. This class designation is just conceivable with training utilizing a significant measure of exactly marked dataset with obvious classes.

Fostering a model utilizing training or named information that empowers us to conjecture the way of behaving of new information is the essential target of regulated learning. Directed learning can likewise be separated into two kinds of errands: relapse undertakings, in which the outcome is supposed to be a ceaseless worth, and grouping undertakings, in which the result is supposed to be a straight out esteem.

2. LITERATURE REVIEW

Selvapandian, D., & Santhosh, R. (2021) [7] To get past the disadvantages of brain network-based interruption location models, the work proposes a profound learning-based interruption identification framework for multi-cloud IoT environments. By expanding training proficiency, the proposed interruption recognition model raises identification precision. By utilizing the NSL-KDD dataset for exploratory assessment, the recommended model performs better compared to customary techniques, accomplishing 97.51% recognition rate, 96.28% discovery exactness, and 94.41% accuracy.

Dakalbab, F. M. (2021) [8] three essential review regions are recognized from the examination of 63 relevant examinations: (I) the different types of cloud security chances; (ii) the ML approaches applied; and (iii) the exhibition results. The creators have framed eleven cloud security domains. Besides, with 16% and 14% of clients, individually, conveyed refusal of-administration (DDoS) and information protection are the most famous Cloud security domains. Nonetheless, we found that 30 ML approaches were utilized; some were mixture, while others were independent. SVM is the most frequently involved ML in independent and half and half models. What's more, to show the viability of their proposed model, 60% of the distributions stood out their models from different models. Furthermore, a rundown of 13 unmistakable assessment measures was given. Genuine positive rate is the most frequently used measure, while it is the least to train time. At long last, among important investigations, KDD and KDD CUP'99 are the most utilized datasets out of the 20 that were found.

Viswanath, G., & Krishna, P. V. (2021) [9] The reason for this study is to make a safe system that limits insider assaults. Information transferring, cutting, ordering, encryption, dispersion, unscrambling, recovery, and combining processes are undeniably remembered for the recommended framework. The cross-breed encryption strategy was made to protect a lot of information preceding their stockpiling in many clouds. Cloud capacity environments that are refreshed progressively are utilized for the reenactment study. The encryption cycle was recorded at around 2630 KB/S by the recommended method. The results show the recommended calculation's predominance over the benchmark calculations.

Bucur, V., & Miclea, L. C. (2021) [10] a thorough way to deal with asset the board in a multi-cloud setting is portrayed in this work. By using multi-cloud innovation and industrially available answers for scale assets and further develop framework strength while remaining as cloud rationalist as could really be expected, this Programming interface aims to meet the steadily expanding asset necessities. Considering this, the work introduced here will include a structural examination of the asset the executives Programming interface, a significant level outline of the execution, and a trial intended to exhibit the reasonability and importance of the frameworks talked about.

Rao, P. (2021) [11] present a decentralized disseminated framework along with a model for a suggestion framework (Grid Factorization) trained on an Ethereum blockchain network through Unified Learning. To refresh confined things vectors, we exploit savvy contracts, which empower decentralized serverless accumulation. Additionally, we utilize homomorphic encryption (HE) to empower the encoded slopes to be shared all through the organization without undermining their security. Our discoveries lead us to presume that, while safeguarding our serverless model security and bringing the above transmission down to a focal server, training a model over a serverless Blockchain network involving savvy agreements will give a similar exactness as an incorporated model. Finally, we express that such an answer can offer endeavor cloud clients cash investment funds and worked on Nature of Administration (QoS) by offering straightforwardness, review prepared, and exhaustive bits of knowledge into inventory network exercises.

3. SECURITY CHALLENGES IN MULTI-CLOUD ENVIRONMENTS

The multi-cloud environment presents various issues for associations to deal with. Safeguarding information security and protection, taking care of character and access the executives entanglements, settling combination and interoperability issues, and ensuring administration rules are kept are the main worries of these difficulties. These troubles are exacerbated by the disseminated engineering of cloud foundation, the utilization of a few cloud specialist co-ops, and the intricacy of saving security across a few cloud stages. Information security and protection are issues when information is scattered among a few cloud specialist co-ops (CSPs). Access control procedures, client indexes, and confirmation components fluctuate broadly all through cloud stages. Associations find it trying to carry out uniform access the board across many clouds and authorize reliable security arrangements because of this absence of incorporation and concentrated control. It could bring about issues with inspecting and observing access occasions, wasteful requirement of access honors, and security weaknesses.

No matter what the cloud stage being utilized, organizations need to painstakingly carry serious areas of strength for out measures to safeguard information while it is moving as well as very still. Associations should reliably utilize encryption, access controls, and information security measures across all clouds to safeguard the classification and trustworthiness of information that is scattered among a few cloud suppliers. Since various cloud specialist organizations (CSPs) use different confirmation and approval frameworks, character and access the board turns out to be more perplexing in multi-cloud arrangements. The security environment is additionally muddled by the need to oversee encryption keys [12], safely communicate information among clouds, and guarantee consistence with information assurance regulation. Incorporated control is scrutinized by this shifted environment, which additionally raises security gambles.

Powerful correspondence and coordination across many cloud stages are hampered by the intricacy of exclusive advances and APIs, which conceals the difficulties of interoperability and reconciliation in multi-cloud frameworks. In the complicated universe of multi-cloud environments, associations need to consider the subtleties of information organizations, conventions, and security controls to ensure a protected and seamless domain of interoperability [13]. Associations should stick to the inside strategies and various administrative requests as commanded by consistence and administration. It is presently essential and challenging to review, screen, and uphold security guidelines across multi-cloud settings.

Enough security arrangements, such combined admittance control, are expected to address these muddled worries and assurance the illusive trifecta of secrecy, trustworthiness, and availability inside the multi-cloud setting.

4. MULTI-CLOUD SECURITY

The expression "multi cloud security" depicts the assortment of approaches, rules, rehearses, and innovative instruments planned to defend data, programs, and the connected framework of multiple cloud environments. An association utilizing a few cloud administrations from different cloud suppliers — a mix of public, private, and crossover clouds — is said to utilize a multi-cloud plan.

Moreover, as per Valtix's 2023 Multi Cloud Security Report, 95% of associations accept multi-cloud will be an essential need in 2023, however 58% are very certain about their ongoing security methodology.

Table 1: How many clouds does it take to run a company

Number of Platforms	Percentage
One Platform	43%
Two Platform	35%
Three or More platforms	22%

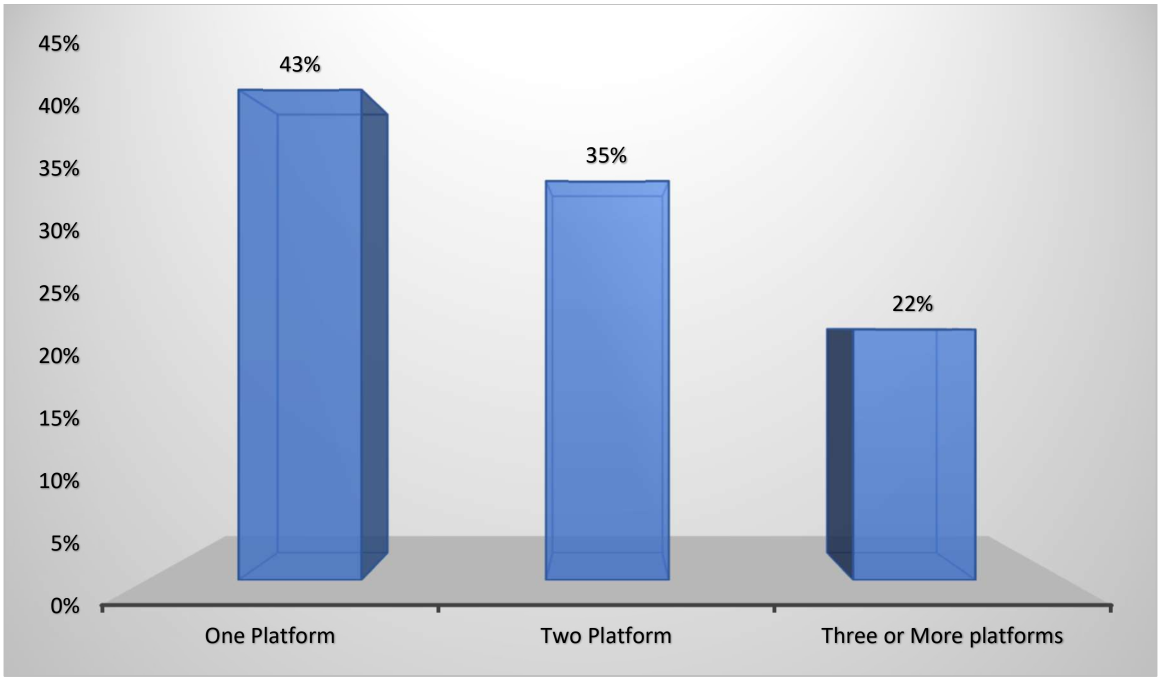

Figure 2: How many clouds does it take to run a company

Organizations are presenting themselves to new security risks as they move increasingly more to the cloud to exploit its benefits. Due to the expanded intricacy and necessity to get information across different stages, these dangers might be enhanced in a multi-cloud situation.

The rising utilization of cloud administrations and the complexity of cyberattacks have pushed the advancement of multicloud security. Getting a solitary cloud environment was the essential accentuation of cloud security from the start. However, when organizations started using an assortment of cloud administrations, obviously a more intensive way to deal with security was required.

4.1.The Advantages of Employing a Multi Cloud Strategy

Organizations can get to a more extensive scope of administrations and capacities across a few cloud suppliers because of multi-cloud figuring [14], which advances innovativeness and offers various benefits that can rouse unique idea and creative arrangements.

- **Cloud Agnostic:** Embracing a cloud-skeptic design is a fundamental initial phase in beginning the multi-cloud reception venture. This strategy makes it simpler to find and eliminate any implied conditions and suspicions that might be available in your framework and application. Your frameworks get more grounded, more adaptable, and easier to maintain in an assortment of cloud environments thus.
- **Flexibility:** As well as offering adaptability, a multi-cloud methodology dodges seller secure. Rather than being confined to one cloud supplier, associations are allowed to choose the best contributions from a few unique providers. Execution and adaptability are

likewise covered by this adaptability, permitting organizations to grow their tasks across a few clouds depending on the situation. To capitalize on each, organizations can, for example, consolidate Google Cloud Stage (GCP) for information examination and Amazon Web Administrations (AWS) for framework.

- **Uptime:** Organizations rely upon framework availability and trustworthiness, and a multicloud approach can work on these elements. Associations can keep a failure in one stage from influencing their whole business by spreading jobs more than a few cloud stages.

5. MULTI-CLOUD MACHINE LEARNING STRATEGIES

Building, training, and implementing artificial intelligence and machine learning models across several cloud platforms and providers is known as multi-cloud AI/ML, and it is a crucial component of a strong machine learning strategy. Organisations can approach AI initiatives with a multi-cloud strategy, responding on generic clouds such as Amazon's AWS or Google's GCP, as well as specialty AI-specific clouds like CoreWeave for highly available and competitively priced GPUs, rather than depending on a single cloud vendor [15]. Since AI is affecting more aspects of business and cannot be contained within a single cloud environment, this has grown in importance.

The significance of multi-cloud AI/ML can be attributed to multiple factors:

- **Avoids vendor lock-in:** By keeping away from over-dependence on any one cloud supplier, associations can furnish their AI frameworks with more noteworthy adaptability and convey ability. Multi-cloud makes it feasible for them to relocate between clouds or change suppliers later on.
- **Leverages unique strengths:** Only one out of every odd AI work is best served by a solitary cloud. With multi-cloud, you might take utilization of the particular benefits of a few suppliers. For example, you can use CoreWeave for GPUs and training/surmising, GCP for its modern ML foundation, Sky blue for big business AI abilities, and AWS for serverless AI.
- **Mitigates risks:** You lessen the risk of any one cloud tumbling down or losing administration by appropriating your AI jobs north of a few clouds. Overt repetitiveness is given by multi-cloud AI to keep your frameworks strong.
- **Enables hybrid cloud:** A multi-cloud AI methodology can consolidate on-premises framework to establish an adaptable crossover environment. This empowers organizations to take utilization of the cloud's adaptability notwithstanding their ongoing on-premise server farms and foundation.

6. CONCLUSION

In conclusion, protecting multi-cloud systems necessitates a multifaceted strategy that addresses the issues of compliance, identity management, and distributed data. Through the facilitation of anomaly detection, intrusion prevention, and data encryption, machine learning presents intriguing answers. In complicated multi-cloud environments, organizations may guarantee the confidentiality, integrity, and availability of their data and applications by fusing machine learning techniques with traditional security procedures.

REFERENCES

1. Anwarbasha, H., Sasi Kumar, S., & Dhanasekaran, D. (2021). An efficient and secure protocol for checking remote data integrity in multi-cloud environment. Scientific reports, 11(1), 13755.
2. Bhagavan, S., Gharibi, M., & Rao, P. (2021, December). Fedsmarteum: Secure federated matrix factorization using smart contracts for multi-cloud supply chain. In 2021 IEEE International Conference on Big Data (Big Data) (pp. 4054-4063). IEEE.
3. Bucur, V., & Miclea, L. C. (2021). Multi-cloud resource management techniques for cyber-physical systems. Sensors, 21(24), 8364.
4. Ramagundam, S., Das, S. R., Biswas, S. N., Morton, S., Assaf, M. H., & Ozkarahan, I. (2013). AMBA-BASED AHB MASTER/SLAVE MEMORY CONTROLLER DESIGN. Transformative Science and Engineering, Business and Social Innovation, 23.
5. Kavitha, S., Bora, A., Naved, M., Raj, K. B., & Singh, B. R. N. (2021). An internet of things for data security in cloud using artificial intelligence. International Journal of Grid and Distributed Computing, 14(1), 1257-1275.
6. Ramagundam, S., Das, S. R., Morton, S., Biswas, S. N., Groza, V., Assaf, M. H., & Petriu, E. M. (2014, May). Design and implementation of high-performance master/slave memory controller with microcontroller bus architecture. In 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings (pp. 10-15). IEEE.
7. Lahmar, F., & Mezni, H. (2021). Security-aware multi-cloud service composition by exploiting rough sets and fuzzy FCA. Soft Computing, 25(7), 5173-5197.
8. Naidu, P. R., Guruprasad, N., & Gowda, V. D. (2021, May). A high-availability and integrity layer for cloud storage, cloud computing security: from single to multi-clouds. In Journal of Physics: Conference Series (Vol. 1921, No. 1, p. 012072). IOP Publishing.
9. Naqvi, H. H., Alyas, T., Tabassum, N., Farooq, U., Namoun, A., & Naqvi, S. A. M. (2021). Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward. International Journal, 10(3).
10. Reddy, A. R. P. (2021). THE ROLE OF ARTIFICIAL INTELLIGENCE IN PROACTIVE CYBER THREAT DETECTION IN CLOUD ENVIRONMENTS. NeuroQuantology, 19(12), 764-773.
11. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. IEEE Access, 9, 20717-20735.
12. Komperla, R. C. A. (2021). AI-ENHANCED CLAIMS PROCESSING: STREAMLINING INSURANCE OPERATIONS. Journal of Research Administration, 3(2), 95-106.

13. Pachala, S., Rupa, C., & Sumalatha, L. (2021). An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, 14, 1117-1133.
14. Reddy, A. R. P. (2021). MACHINE LEARNING MODELS FOR ANOMALY DETECTION IN CLOUD INFRASTRUCTURE SECURITY. NeuroQuantology, 19(12), 755-763.
15. Ramagundam, S. (2014). Design and Implementation of Advanced Microcontroller Bus Architecture High-performance Bus with Memory Controller in Verilog Hardware Description Language (Doctoral dissertation, Troy University).
16. Paul, N. R., & Raj, D. P. (2021). Enhanced Trust Based Access Control for Multi-Cloud Environment. Computers, Materials & Continua, 69(3).
17. Ramagundam, S. (2021). Next Gen Linear Tv: Content Generation And Enhancement With Artificial Intelligence. International Neurourology Journal, 25(4), 22-28.
18. Robertson, J., Fossaceca, J. M., & Bennett, K. W. (2021). A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations. IEEE Transactions on Engineering Management, 69(6), 3913-3922.
19. Saxena, D., Gupta, R., & Singh, A. K. (2021). A survey and comparative study on multi-cloud architectures: emerging issues and challenges for cloud federation. arXiv preprint arXiv:2108.12831.
20. Selvapandian, D., & Santhosh, R. (2021). Deep learning approach for intrusion detection in IoT-multi cloud environment. Automated Software Engineering, 28(2), 19.
21. Viswanath, G., & Krishna, P. V. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, 14(2), 691-698.
22. Zhu, Q. H., Tang, H., Huang, J. J., & Hou, Y. (2021). Task scheduling for multi-cloud computing subject to security and reliability constraints. IEEE/CAA Journal of Automatica Sinica, 8(4), 848-865.