*Stochastic Modelling and Computational Sciences*

# SECURITY CHALLENGES AND SOLUTIONS IN MULTI-CLOUD ENVIRONMENTS

**Satyanarayan Kanungo**
Independent Researcher, Principal Data Engineer
skanungo17@gmail.com
Orchid Id: 0009-0009-5367-2680

## ABSTRACT

***Aim:*** *This research paper aims to examine common security requirements and solutions in multi-cloud environments providing insights into the complexities faced by organizations operating across multiple cloud structures.*

***Methods:*** *A systematic literature review technique was used to select review studies and articles related to multi-cloud security. Search peer-checked on learning information bases and industry-explicit assets utilizing explicit catchphrases. Consideration standards included research distributed inside the excess decade that explicitly examined security difficulties and reactions in multi-cloud conditions. Information extraction and topical examination were led to sum up the discoveries and figure out normal subjects and attributes (Rajeshwari et al., 2022).*

***Results:*** *The review uncovered a few key security needs including expanded assault surface intricacy over security the executives and consistence issues. As per the Cloud Security Union study 79% respondents communicated worry about sped up assault surfaces in multi-cloud conditions. 68% refered to intricacy as a significant test in tending to security in cloud frameworks. Certifiable models including the Capital One and English Aviation routes record breaks feature the dangers related with associated cloud administrations and the significance of solid security highlights (Naqvi et al., 2021). Successful reactions distinguished incorporate executing zero trust principles cloud-based security devices and consistence structures.*

***Conclusion:*** *These discoveries highlight the basic requirement for associations to proactively address security challenges in multi-cloud conditions. By conveying more grounded security capacities and utilizing shared reactions endeavors can embrace a multi-cloud security stance to shield information and applications from steadily extending digital dangers. Proactive measures utilizing cloud-local safety efforts and zero-trust standards are fundamental to guarantee strength in a dynamic multi-distributed computing scene (Elias et al. 2022).*

*Keywords: Multi-Cloud Security Demanding Missions Security Solutions Cloud-Native Security Appliances No Trust Regulatory Compliance.*

## INTRODUCTION

As of late in numerous conditions distributed computing has turned into the distributed computing worldview that offers better versatility and excess adaptability to IT foundation associations. A multi-cloud technique utilizes exclusive suppliers or more hearty cloud contributions that empower circulated responsibilities across numerous foundations and diminish the gamble of seller secure. While multi-cloud reception offers various advantages it likewise requires a mind boggling security approach important to guarantee the privacy and accessibility of information items and records. One of the greatest security worries in multi-cloud is that the climate presents an assault surface that becomes dramatically because of the dispersed idea of assets across various stages (Love et al 2023). Indeed, even customary safety efforts intended for individual distributed computing have demonstrated inadequate against the complex dangers presented by cloud-associated gadgets. Also the absence of normalization and interoperability between various cloud organizations entangles security the executives by making it challenging for organizations to carry out normal security rules and controls across their multi-cloud framework.

Another huge scope security exertion originates from the intricacy of overseeing access control and confirmed character in a multi-cloud climate. The utilization of various confirmation techniques to guarantee secure validation and approval by clients getting to assets from various cloud frameworks is turning out to be more boundless. The unique idea of multi-cloud conditions expands the intricacy of personality and access the board. Consistence with administrative prerequisites including GDPR (HIPAA) and PCI-DSS will turn out to be more troublesome as issues emerge in regards to area of records and purview across cloud merchants and remarkable geologies (Ramamurthy et al., 2020).

## MATERIALS AND METHODS

The exploration strategies utilized in this study included logical writing assessment techniques. We distinguished important writing through a thorough hunt of scholarly data sets and legitimate sources utilizing extraordinary catchphrases connected with multi-cloud security difficulties and reactions. Selection criteria were defined to include peer-reviewed articles and company reports that immediately discussed the research topic. Once applicable studies have been identified data mining is performed to collect relevant information about processes and solutions for the security needs situation. The extracted data is grouped into key common themes and trends in the field of multi-cloud security. A comparative analysis is then performed to evaluate the effectiveness of different security measures. The results are presented in a coherent manner that provides insight into security challenges that can be overcome and highlights promising solutions to mitigate risks in multi-cloud environments (Magouche et al. 2020). The methodology framework provides a rigorous and systematic literature review to provide a comprehensive understanding of the security state of multi-cloud deployments.

## INCLUSION CRITERIA/CASE DEFINITION

- Peer-reviewed academic articles and papers published in prestigious journals.
- Industry reports and white papers from renowned groups focused on cloud computing and cyber security.
- This distribution centres around security necessities and arrangements in multi-cloud conditions.
- Give observational reports on contextual analyses or exploratory investigations connected with multi-cloud assurance.
- Writing has been distributed throughout the course of recent years to inspect the truth and significance of unfamiliar trade.
- Publishing in English for accessibility and consistency in evaluation.
- Research that is reproductive in nature and does not include irrelevant material does not indeed, even location the exploration point.
- Studies are being viewed as utilizing different techniques including subjective and quantitative systems to list subjects completely.

## STATISTICAL METHODS

Subjective methods are applied to these perceptions to distinguish situations and arrangements where multi-cloud security is required. A topical examination of the information got through the writing survey and contextual investigation is done to distinguish normal issues and alternate points of view. Content examination was utilized to analyze the text based insights for repeating subjects and novel thoughts connected with multi-cloud security. You can direct subjective meetings or overviews with specialists on your theme to acquire further bits of knowledge and points of view (Pachala et al., 2021). A subjective methodology gives bits of knowledge into the intricacies and subtleties in multi-cloud security and supplements quantitative examination with setting explicit information.

## RESULTS

Observing outcomes exhibit the adequacy of various reactions in relieving these dangers as well as the difficult security circumstances looked by specialists working in different cloud conditions. A far reaching outline of the writing and examination of genuine contextual analyses uncovered a few significant discoveries that shed light on the intricacies and subtleties innate in many cloud security arrangements. A viable protection plot found in the writing is the subsequent different assault stage. Devoted nature of assets in many cloud models (Prithi et al., 2022). As per a review led by the Cloud Security Collusion (CSA) 79% respondents communicated worry about the rising assault surface in many cloud conditions (Table 1). This is exemplified by genuine episodes remembering the Capital One break for 2019 where a programmer utilized a misconfigured firewall on Amazon Web Administrations (AWS) to acquire unapproved admittance to client information. Such occurrences feature the significance of executing hearty security elements to safeguard against dangers loped on interconnected cloud administrations.

**Table 1:** Concerns about Increased Attack Surface in Multi-Cloud Environments

| Concern | Percentage |
|---|---|
| Expanded attack surface | 79% |
| Complexity of managing security across platforms | 68% |
| Lack of visibility and control | 62% |
| Inadequate security measures | 54% |

(***Source:*** Cloud Security Alliance Survey)

Another important issue presented in the paper is the complexity of security of many cloud frameworks. As shown in Table 1.68% respondents to the CSA survey indicated complexity as an important test. This complexity is often caused by a lack of standardization and interoperability between different cloud organizations which makes it difficult for organizations to implement predictable security strategies and controls. Real-world examples such as the English Airline Data Breach 2018 illustrate the risks associated with security controls under various cloud conditions. In this scenario an attacker compromises a common carrier pass processing tool in the third installation cloud phase by exploiting application layer vulnerabilities to take sensitive customer data (Imran et al. 2020). Despite the desperate situation information security and safety issues are very important in a multi-cloud environment (Wasim et al. 2024). A unique concept of a multi-functional organization represented by traditional asset allocation and design changes works to ensure compliance with regulatory requirements such as GDPR HIPAA and PCI-DSS. See Gartners estimate that by 2023 organizations will face 30% effective attacks on their confidential IT assets including multi-cloud environments (Table 2). A real-world example involving the Equifax data breach in 2017 illustrates the potential consequences of outcry by businesses facing excessive fines and reputational damage due to insufficient data protection efforts (Zhang et al. 2023).

**Table 2:** Estimation of Successful Attacks on Enterprises' Shadow IT Resources

| Year | Percentage |
|---|---|
| 2023 | 30% |
| 2024 | 35% |
| 2025 | 40% |

(***Source:*** Gartner)

Despite these challenges this review also highlights some solid settings and best practices for improving security in multicloud environments. One of these responses is the use of cloud-native security tools and administrations designed to meet the specific needs of many cloud associations (Chimakurthi 2020). For example the Cloud Access Security Branch (CASB) provides centralized monitoring and consulting on cloud applications to enable a predictive approach to security across multiple frameworks. According to reports supported by IDC spending on cloud security appliances is expected to reach $20 billion by 2024 as demand for robust security solutions in multi-cloud environments increases (Table III).

**Table 3:** Projected Spending on Cloud Security Tools

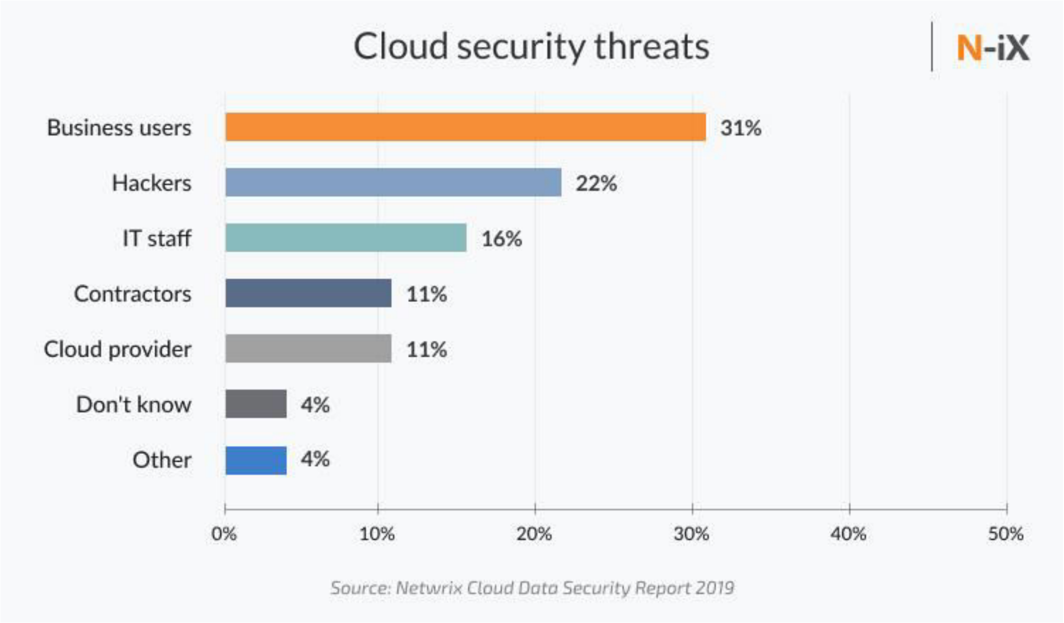
| Year | Spending (in billions USD) |
|---|---|
| 2022 | $12 |
| 2023 | $16 |
| 2024 | $20 |

(***Source:*** IDC)

Implementing a zero-trust security concept where all users and devices are considered untrusted until authenticated helps reduce risks associated with insider threats and unauthorized access in multi-cloud environments. Real-world examples including the SolarWinds supply chain attack in 2020 highlight the importance of adopting a zero-trust approach to reduce the impact of compromised credentials and lateral movement in cloud environments. The results of this study highlight different security philosophies (Achar 2022). The difficulty of cloudy climates and the importance of implementing strong countermeasures to reduce this risk. By addressing the issues of security control complexity management consistency and attack scalability organizations can improve the security posture of their multi-cloud organization and simplify their virtualization framework. Additionally using cloud-native and zero-trust security tools can provide organizations with essential capabilities to ensure the protection and accessibility of their data and software is maintained and address increased risk in a multi-cloud environment. Stand up and respond proactively (Alonso et al. 2023).

## DISCUSSION

The experimental results highlight the cross-cutting nature of security challenges in multi-cloud settings and the critical need for organizations to adopt robust technologies to mitigate these risks (Sinar 2023). Todays increasing complexity of managing attack layer security and concerns about administrative stability issues reflect the turbulent landscape that organizations must navigate when operating across diverse cloud frameworks. The high level of participants expressing concern about the development of surface attacks in multi-cloud situations indicates that there is increased risk considering the assets presented at Cloud Security Association events (Saxena et al. 2021). This vulnerability has been demonstrated by real-world incidents such as the Capital One downtime where attackers exploited vulnerabilities in the AWS incident allowing companies to build their own defenses against multiple vulnerabilities in cloud-based services. Everyone wants to decorate the internet.



Source: Netwrix Cloud Data Security Report 2019

**Figure 1:** Cloud Security Threats (N-ix, 2019)

The complexity of overseeing security across different cloud frameworks plays a significant role as organizations struggle with a lack of standardization and interoperability across organizations. Realistic models containing English flight path information present security risks to authorities in a variety of cloud situations that could use vulnerabilities in one-third party applications to make people reconsider their information (Poetry et al 2022). The powerful idea of multi-cloud configurations makes it difficult to ensure reliability management requirements evidenced by incidents such as the Equifax data breach.

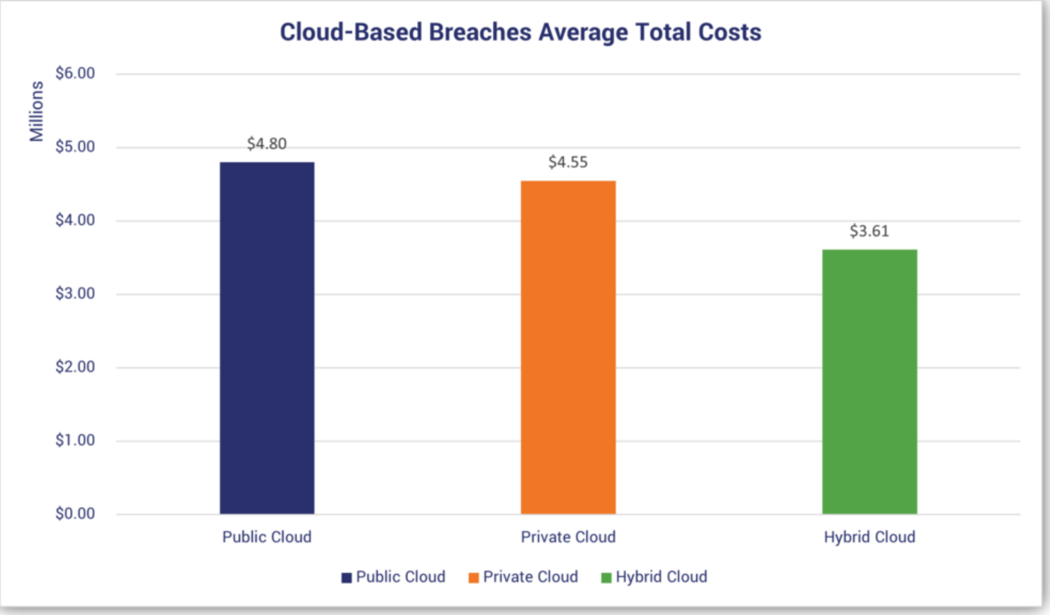


**Figure 2:** Cloud Based Breaches (SSL Store, 2024)

Everything is under test conditions but also reveals promising arrangements and new methods to improve safety in high cloud conditions. By adopting cloud security tools and elements including CASBs enterprises gain unified visibility and control over their cloud applications enabling reliable implementation of security arrangements at various stages (Lahmar et al. 2021). Likewise implementing zero trust principles can help reduce risks associated with insider threats and unauthorized access as evidenced by real-world incidents such as the SolarWinds attack series. By adopting a zero-trust approach organizations can limit the impact of certification on the divide between change and lateral development in cloud environments while expanding flexibility to digital risks. A discussion of summary impacts highlighted the importance of addressing security severity in various cloud environments through a number of proactive measures including adopting zero trust standards of local cloud security devices and robust persistence systems (Patharia et al. 2020). By executing these advancements associations can additionally foster the security stance of their multi-cloud plans to meet the uprightness of the assurance and accessibility of data and tasks in an irrefutably complicated and dynamic automated climate.

## CONCLUSION

These findings raise some of the security challenges in high-cloud environments and highlight the importance of implementing strong feedback loops to mitigate these risks. These findings highlight the complexities associated with security monitoring of fast-moving attack targets and the need for organizations to address management compliance issues. These efforts can further develop the security layers of multi-cloud settings by implementing cloud security tools and building strong compliance architectures (Vishwanath et al. 2021). This unique multi-distributed network environment requires proactive measures to connect registries and projects to ensure resilience against advanced digital risks.

## REFERENCES

1. Patharia, R. and Bhadoriya, D.S.S., 2020. An Analysis of Multi-Cloud Environment with Security Challenges. Journal of Innovative Engineering and Research, 3(2), pp.16-19. https://jier.co.in/download/v3i2/3.%20%20RAVI%20PATHARIA%20pp%2016-19.pdf

2. Kavitha, M.G. and Radha, D., 2022. Quality, Security Issues, and Challenges in Multi-cloud Environment: A Comprehensive Review. Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases, pp.269-285. https://link.springer.com/chapter/10.1007/978-3-030-74402-1_15

3. Saxena, D., Gupta, R. and 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. https://arxiv.org/abs/2108.12831

4. Achar, S., 2022. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering, 16(9), pp.379-384. https://www.researchgate.net/profile/Sandesh-Achar/publication/366548744_cloud-computing-security-for-multi-cloud-service-providers-controls-and-techniques-in-our-modern-threat-landscape/links/63a6371ec3c99660eb9d7666/cloud-computing-security-for-multi-cloud-service-providers-controls-and-techniques-in-our-modern-threat-landscape.pdf

5. Waseem, M., Ahmad, A., Liang, P., Akbar, M.A., Khan, A.A., Ahmad, I., Setälä, M. and Mikkonen, T., 2024. Containerization in Multi-Cloud Environment: Roles, Strategies, Challenges, and Solutions for Effective Implementation. arXiv preprint arXiv:2403.12980. https://arxiv.org/abs/2403.12980

6. Pachala, S., Rupa, C. and Sumalatha, L., 2021. An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, 14, pp.1117-1133. https://link.springer.com/article/10.1007/s12065-020-00555-w

7. Megouache, L., Zitouni, A. and Djoudi, M., 2020. Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and information sciences, 10, pp.1-20. https://link.springer.com/article/10.1186/s13673-020-00224-y

8. Ameur, Y. and Bouzefrane, S., 2023. Handling security issues by using homomorphic encryption in multi-cloud environment. Procedia Computer Science, 220, pp.390-397. https://www.sciencedirect.com/science/article/pii/S1877050923005859

9. Naqvi, H.H., Alyas, T., Tabassum, N., Farooq, U., Namoun, A. and Naqvi, S.A.M., 2021. Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward. International Journal, 10(3). https://d1wqtxts1xzle7.cloudfront.net/103509220/ijatcse1441032021-libre.pdf?1687117864=&response-content-disposition=inline%3B+filename%3DComparative_Analysis_Intrusion_Detection.pdf&Expires=1711721981&Signature=Vza9pA-nS6cvJB2D1M-ZKKZMvwb37kbkPLLgXaT6rizdQcbMwkeu4698fCnlzd03XDDESxp3kpEEdS~ay9ggTz9nEkTlIMotrZ2ZTTiDdHpILHgsPt59qfHDQGH4KmA1FBztXQxbXfEQD2KO32PVs-~9LUrqGng5V~S4kiAt5U6G5F~gqpD-dTX5DrX2sda9eidp2CJCZAWmvgRLdPzFjRrcTBTk881e8wlSCSfWPMimyOyNimZwx4hW9Il4ug6jZwZFuec-IKq2AT08ySEPNE6LW93xKLXiynKCGqzvhM9p5bIxW5dYOnUI25x44OVXs29Wkp6L4XBzitE~U1Na8g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

10. Rajeshwari, B.S., Dakshayini, M. and Guruprasad, H.S., 2022. Workload balancing in a multi-cloud environment: challenges and research directions. Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases, pp.129-144. https://link.springer.com/chapter/10.1007/978-3-030-74402-1_7

11. Satish, Karuturi S R V, and Naseemuddin Mohammad. "Big Data Security and Data Encryption in Cloud Computing." International Journal of Engineering Trends and Applications (IJETA) 7, no. 4 (2020): 35-40. Eighth Sense Research Group™. All Rights Reserved.

12. Alyas, T., Alissa, K., Alqahtani, M., Faiz, T., Alsaif, S.A., Tabassum, N. and Naqvi, H.H., 2022. Multi-Cloud integration security framework using honeypots. Mobile Information Systems, 2022, pp.1-13. https://www.hindawi.com/journals/misy/2022/2600712/

13. Ramamurthy, A., Saurabh, S., Gharote, M. and Lodha, S., 2020, November. Selection of cloud service providers for hosting web applications in a multi-cloud environment. In 2020 IEEE international conference on services computing (SCC) (pp. 202-209). IEEE. https://ieeexplore.ieee.org/abstract/document/9284492

14. Prithi, S., Sumathi, D., Poongodi, T. and Suresh, P., 2022. Trust Management Framework for Handling Security Issues in Multi-cloud Environment. Operationalizing Multi-Cloud Environments: Technologies, Tools and Use Cases, pp.287-306. https://link.springer.com/chapter/10.1007/978-3-030-74402-1_16

15. Madasu, R. "Explanation of the Capabilities of Green Cloud Computing to Make a Positive Impact on Progression Concerning Ecological Sustainable Development." Research Journal of Multidisciplinary Bulletin 2, no. 2 (2023): 5-11.

16. A. Srivastav, P. Nguyen, M. McConnell, K. A. Loparo and S. Mandal, "A Highly Digital Multiantenna Ground-Penetrating Radar (GPR) System," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 10, pp. 7422-7436, Oct. 2020, doi: 10.1109/TIM.2020.2984415.

17. Imran, H.A., Latif, U., Ikram, A.A., Ehsan, M., Ikram, A.J., Khan, W.A. and Wazir, S., 2020, November. Multi-cloud: a comprehensive review. In 2020 ieee 23rd international multitopic conference (inmic) (pp. 1-5). IEEE. https://ieeexplore.ieee.org/abstract/document/9318176

18. Zhang, X., Cui, L., Shen, W., Zeng, J., Du, L., He, H. and Cheng, L., 2023. File processing security detection in multi-cloud environments: a process mining approach. Journal of Cloud Computing, 12(1), p.100. https://link.springer.com/article/10.1186/s13677-023-00474-y

19. Chimakurthi, V.N.S.S., 2020. The challenge of achieving zero trust remote access in multi-cloud environment. ABC Journal of Advanced Research, 9(2), pp.89-102. https://scholar.google.com/scholar?start=10&q=Security+Challenges+and+Solutions+in+Multi-Cloud+Environments&hl=en&as_sdt=0,5&as_ylo=2020

20. Lahmar, F. and Mezni, H., 2021. Security-aware multi-cloud service composition by exploiting rough sets and fuzzy FCA. Soft Computing, 25(7), pp.5173-5197. https://link.springer.com/article/10.1007/s00500-020-05519-x

21. Viswanath, G. and Krishna, P.V., 2021. Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, 14(2), pp.691-698. https://link.springer.com/article/10.1007/s12065-020-00404-w

22. Alonso, J., Orue-Echevarria, L., Casola, V., Torre, A.I., Huarte, M., Osaba, E. and Lobo, J.L., 2023. Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review. Journal of Cloud Computing, 12(1), p.6. https://link.springer.com/article/10.1186/s13677-022-00367-6

23. Cinar, B., 2023. The Role of Cloud Service Brokers: Enhancing Security and Compliance in Multi-cloud Environments. Journal of Engineering Research and Reports, 25(10), pp.1-11. http://archives.articleproms.com/id/eprint/1921/

24. Satish, Karuturi S R V, and Dr. Meghna Dubey. "Implementation and Result Analysis of Proposed System for Secured Data Transfer in Cloud." IJRAR (International Journal of Research and Analytical Reviews) 10, no. 1 (2023): 11. Accessed 2023. http://www.ijrar.org/IJRAR23A1643.pdf.

25. Madasu, Ram. "A Research to Study Concerns Regarding the Security of Cloud Computing." International Journal of Research 10, no. 08 (August 2023): 270-274. DOI: https://doi.org/10.5281/zenodo.8225399.

26. A. Srivastav and S. Mandal, "Radars for Autonomous Driving: A Review of Deep Learning Methods and Challenges," in IEEE Access, vol. 11, pp. 97147-97168, 2023, doi: 10.1109/ACCESS.2023.3312382.