International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

Safeguarding The Cloud Frontier

Dr. Ashish Tiwari[1], Tushar[2] , Alhamd Khan[3] Nitish kumar[4]
[1]Associate professor, Dept. of CSE, Amity University, lucknow, India.
[2,3,4]UG Scholar, Dept. of CSE, Amity School of Engineering & Technology, India.
Emails: *atiwari3@lko.amity.edu[1], tusharsmail2313@gmail.com[2], alhamdkhan016@gmail.com[3], nitishgaming1710@gmail.com[4]*

Abstract
In today's cloud-centric environment, organizations face a growing array of security challenges that threaten data integrity, privacy, and compliance. This study explores the critical security risks associated with cloud computing, including data breaches, identity and access vulnerabilities, misconfigurations, and advanced cyber threats. It examines existing security frameworks, mitigation strategies, and best practices aimed at strengthening cloud security. Additionally, the paper emphasizes the importance of automation, continuous monitoring, and proactive risk management in addressing these challenges. By analyzing the evolving threat landscape, this research provides valuable insights into current security concerns and potential future advancements in cloud security.

Keywords: *Cloud Security, Cyber Threats, Data Protection, Identity and Access Management, Compliance, Security Automation, Continuous Monitoring, Risk Mitigation, Cloud Vulnerabilities, Threat Detection.*

1. Introduction
Adoption of cloud computing has given individuals and businesses brand new opportunities, but it has also created new challenges which need to be addressed right away. Organizations moving away from the more conventional on-premises infrastructure have a set of complex security issues to contend with including data security, access control, and compliance to regulations. In cloud security, a surmounting concern is the risk of data breaches and external unwanted access. Keeping sensitive data on a server which is managed by athird-party provider makes the information more prone to a cyber-attack and therefore enhances the requirement of encryption, multi-factor authentication, and access control. Aside from this, some businesses may considerably suffer from a loss in business continuity due to insider threats, data loss, service disruptions because of outages from the provider, or some misconfigurations. A shared sense of responsibility and visibility is another important concern. Customers are in charge of securing their applications and data while cloud providers are in charge of the infrastructure, and this lack of mutual understanding can lead to a plethora of security gaps ready for a range of uncharitable exploitive actions. To add on, organizations find it incredibly and unnecessarily challenging to monitor and address threats due to the lack of transparency in the cloud environments. Compliance with industry regulations and data privacy laws is another hurdle. Different regions and sectors impose strict rules on data storage and processing, requiring businesses to ensure their cloud solutions align with legal frameworks such as GDPR, HIPAA, or ISO 27001. Failure to comply can lead to severe penalties and reputational damage. Despite these challenges, organizations can enhance cloud security through continuous monitoring, advanced threat detection, regular audits, and employee training. By adopting a proactive approach to cloud security, businesses can mitigate risks while still leveraging the immense benefits of cloud computing.

2. Cloud Security Challenges
Think As cloud computing continues to revolutionize IT infrastructure, it also brings a unique set of security challenges. Organizations must address critical concerns such as data protection, regulatory compliance, and cyber threats

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

to maintain a secure cloud environment. The shared responsibility model divides security duties between cloud providers and customers, requiring businesses to take an active role in securing their applications and data. (Figure 1)

Figure 1 Showing Cloud Security Challenges

Key cloud security challenges pose significant risks to organizations relying on cloud infrastructure. One major concern is data breaches and unauthorized access, as storing sensitive information on remote cloud servers increases vulnerability to cyberattacks. Weak authentication, misconfigured access controls, or compromised credentials can expose critical data to unauthorized users. Another challenge is misconfigurations and human errors, where improperly configured cloud storage, databases, and permissions lead to security vulnerabilities. Simple mistakes, such as leaving databases publicly accessible, can result in massive data leaks. Additionally, the lack of visibility and control in cloud environments makes security management complex. Unlike traditional on-premises infrastructure, cloud platforms often restrict direct access to security configurations and activity logs, making it difficult for organizations to detect and respond to potential threats in real time. Compliance and regulatory risks further add to the complexity, as industries and regions impose strict data protection regulations such as GDPR, HIPAA, and ISO 27001. Organizations must ensure their cloud operations align with these legal frameworks to avoid hefty fines and reputational damage. Furthermore, advanced persistent threats (APTs) and ransomware attacks are becoming more sophisticated, targeting cloud environments with malware and persistent attack techniques to infiltrate and exploit cloud-based systems. Addressing these challenges requires robust security strategies, continuous monitoring, and proactive risk management to safeguard cloud infrastructure.

3. Strengthening Cloud Security

To mitigate these challenges, businesses must implement a multi-layered security strategy that addresses various aspects of cloud security. Strong identity and access management (IAM) plays a crucial role in restricting unauthorized access by enforcing multi-factor authentication (MFA), role-based access control (RBAC), and the principle of least privilege. Additionally, data encryption ensures that sensitive information remains protected both at rest and in transit through end-to-end encryption and secure key management solutions. Beyond access controls and encryption, automated threat detection powered by AI-driven security analytics enables real-time monitoring, helping organizations quickly identify and respond to anomalies or potential security breaches. To maintain a strong security posture, businesses must also conduct regular security audits, risk assessments, and vulnerability scans to ensure compliance with evolving regulations and industry standards. Furthermore, adopting cloud-native security solutions such as cloud security posture management (CSPM) and security information and event management (SIEM) enhances visibility, streamlines threat detection, and strengthens proactive risk management across cloud environments.

4. The Role of DevSecOps in Cloud Security

With increasing adoption of cloud computing, helping address the security challenges, many organizations have started adopting DevSecOps which engenders security within the Software Development Lifecycle. This strategy makes certain that security is built-in rather than bolted on to the process later on. Security automation is encapsulated security checks, vulnerability scanning, and compliance validation within the CI/CD pipelines. Additionally, real-time intrusion detection and response enhances security. Continuosly mitigating

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

and managing identified threats strengthens security posture. Apart from automation and monitoring, team collaboration is key by bringing together security, development, and operations to enable the securing of cloud applications and infrastructure. A predefined set of criteria assists organizations in determining the effective and potential impact of security risk enabling better allocation of resources. With these implementations, organizations are able to improve their cloud security posture while countering advanced threats and making use of the benefits from cloud computing.

4.1.DevOps: Automation and Collaboration for Software Delivery

DevOps has evolved into a decisive approach to modern software development, filling the gap between development and business teams. It emphasizes automation, cooperation and continuous delivery to speed up the software release cycle. One of his main practices is continuous integration, automating the creation and testing of code changes, ensuring seamless development. Continuous delivery further improves this process by automating software releases in different environments, reducing manual interventions and risk delivery. Another important aspect is infrastructure as code that allows teams to manage and deliver infrastructure per code to ensure consistency and scalability. The development of DevOps was closely linked to agile methods focused on automation and cloud integration in its current form. Research shows that Devops practices significant improvements in software training, quality and reliability profiles, contributing to the fundamental approach of modern companies seeking efficiency and innovation in software development.

4.2.DevSecOps: Integrating Security into the Development Lifecycle

DevSecOps represents the evolution of DevOps by incorporating security as a core component of the software development lifecycle. Its primary objective is to "shift left," ensuring that security practices are integrated early in the development process rather than being treated as an afterthought. One of the key aspects of DevSecOps is security automation, which involves automating security testing, vulnerability scanning, and compliance checks to enhance efficiency and consistency. Additionally, collaboration and shared responsibility play a crucial role, as DevSecOps fosters close cooperation between development, security, and operations teams to ensure seamless integration of security into the workflow. Another essential principle is continuous security, where organizations implement continuous monitoring and threat detection mechanisms to identify and address security issues in real-time. By embedding security throughout the development lifecycle, DevSecOps strengthens overall system security while maintaining agility and efficiency in software delivery. Research on DevSecOps focuses on the challenges of integrating security into existing DevOps workflows. Studies emphasize the importance of cultural change, automation tools, and security training to successfully implement DevSecOps practices. Challenges of Cloud Security. Cloud computing presents a distinct set of security challenges that demand thorough examination and attention. Shared responsibility model The shared responsibility model defines the division of security responsibilities between the cloud provider and the customer [2] The provider usually takes care of the infrastructure, while the customer is in charge of securing their data, applications, and operating systems that run on top of that infrastructure. Failing to comprehend this model can result in security weaknesses and loopholes.

- **Cloud-Specific Threats:** several cloud-specific threats have been identified in the literature:
- Sharing resources among multiple customers can lead to isolation challenges and increase the risk of data breaches.
- **Data Leakage:** sensitive information can be unintentionally or intentionally revealed due to misconfigurations, vulnerabilities, or malicious attacks.

Cloud services frequently utilize apis for communication, and insecure apis can be exploited to gain unauthorized access. Incorrectly configured cloud resources can create security vulnerabilities. The field of cloud security concentrates on devising efficient methods to combat these threats, such as

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

establishing strong access control measures, encrypting data, monitoring security, and managing vulnerabilities. (Figure 2)

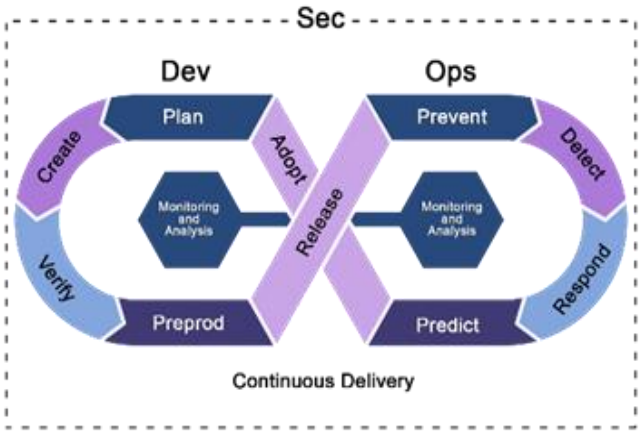

Figure 2 Showing DevSecOps Services

4.3.DevSecOps Implementation in Cloud Environments

4.3.1. DevSecOps Frameworks and Methodologies

Frame Work Sand DevSecOps: Security frameworks help identify, hierarchy, and mitigate threats, while DevSecOps ensures that security is integrated with the Software Development Lifecycle (SDLC) right from the beginning. While frameworks specify what security practices are necessary, DevSecOps is about how to carry them out and automate that. The five core functions of the NIST Cybersecurity Framework (CSF) align with DevSecOps: Identify (threat modeling), Protect (secure coding and automated testing), Detect (continuous monitoring), Respond (incident response), Recover (disaster recovery). DevSecOps complements ISO 27001 security governance, achieved by policies, procedures, and controls, with the integration of security into development mechanisms. CSA Cloud Controls Matrix (CCM) provides a cloud security control framework that, when combined with DevSecOps, enables automation for encryption, vulnerability management, and security integration in CI/CD pipelines. In cloud-native environments, successful DevSecOps adoption requires security automation, the use of Infrastructure as Code (IaC) for consistency, securing containers and APIs to reduce attack surfaces, and enabling continuous monitoring to detect and mitigate threats proactively.

Agile Security: Agile Security ensures that security is not treated as an afterthought but is integrated into every phase of Agile development. It follows core principles such as shifting security left by addressing it from the early development stages, promoting shared responsibility by involving all team members in security, ensuring continuous security assessments throughout development, leveraging automation for vulnerability detection and security testing, and fostering collaboration between development, security, and operations teams. In an Agile environment, security is embedded across different stages. During sprint planning, security requirements are defined early. Throughout development, secure coding practices and real-time static code analysis are implemented. The testing phase involves continuous security testing, including Dynamic Application Security Testing (DAST) and penetration testing. By integrating security at every step, Agile Security improves the overall security posture, accelerates time to market, reduces costs, and enhances team collaboration.

4.3.2. DevSecOps Maturity Models

DevSecOps maturity models help organizations assess their level of DevSecOps adoption, identify strengths and weaknesses, and prioritize improvements. The maturity stages begin with the initial or ad-hoc phase, where security is manual, reactive, and lacks collaboration. As organizations progress, they reach the managed or repeatable stage, where security practices are established, and automation begins. The next stage, defined or consistent, integrates security into the Software Development Lifecycle (SDLC) with increased automation and collaboration. In the proactive or predictable phase, security becomes fully integrated and automated, incorporating proactive measures and performance metrics. Finally, in the optimizing or continuous improvement stage, security is embedded as a core value, ensuring ongoing advancements and adaptation to emerging threats. The DevSecOps maturity model provides organizations with a structured roadmap, enabling them to conduct gap analysis, set priorities, and measure progress

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

effective. Tools and Technologies for DevSecOps in the Cloud Static Application Security Testing (SAST) analyzes source code to detect security flaws and ensure secure coding practices. Tools like SonarQube, Checkmarx, Fortify, and Coverity integrate into CI/CD pipelines, scanning code automatically and failing builds if critical vulnerabilities are found. This helps with early detection, reduces remediation costs, and improves code quality. Dynamic Application Security Testing (DAST) identifies vulnerabilities in running applications that are not visible in source code by simulating real-world attacks. Tools like OWASP ZAP, Burp Suite, and Qualys scan applications during the release process. While SAST detects early code issues, DAST focuses on runtime vulnerabilities, making both essential for security. Software Composition Analysis (SCA) scans open-source components for vulnerabilities, license issues, and outdated elements. Tools like Snyk, OWASP Dependency-Check, Black Duck, and JFrog Xray help mitigate risks by comparing dependencies against known vulnerability databases like NVD. (Figure 3)

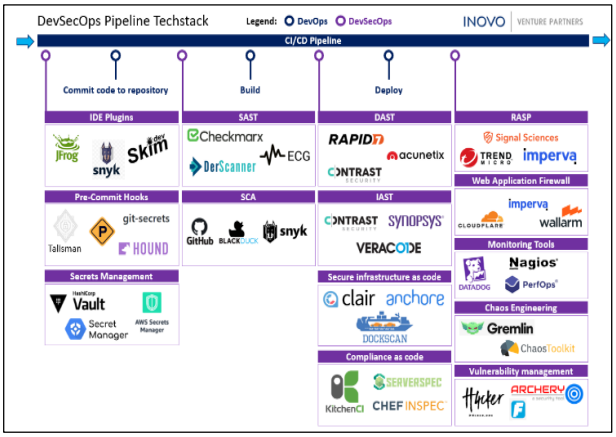

Figure 3 Showing DevSecOps Pipeline Techstack

5. Challenges and Best Practices

5.1. Challenges in Implementing DevSecOps in the Cloud

Cultural resistance is one of the key challenges in implementing DevSecOps, as development and security teams often work in silos, with security being perceived as a bottleneck. Overcoming this challenge requires strong leadership buy-in to champion the change, effective communication, and education to highlight the benefits of DevSecOps. Encouraging a culture of shared responsibility, where security is integrated into all processes, is essential. Demonstrating quick wins can also help build momentum and increase acceptance. Another significant challenge is the skills gap, as DevSecOps demands a unique combination of development, security, and operations expertise. Organizations can address this by investing in training programs to upskill existing staff, encouraging cross-training among teams, and hiring skilled professionals. Leveraging managed services can also help supplement resources where necessary. The complexity of cloud environments further complicates security management, as they are dynamic, distributed, and constantly evolving. Automation plays a crucial role in mitigating this challenge by enabling security testing, vulnerability scanning, and compliance enforcement. Using cloud-native tools specifically designed for cloud environments, implementing security controls within Infrastructure as Code (IaC), and establishing centralized logging and monitoring can help maintain security consistency. Another challenge arises when integrating DevSecOps with legacy systems, which often lack cloud-native security features and can be difficult to adapt. Secure API gateways can expose legacy functionality safely, while containerization improves security and portability. Organizations can also adopt an incremental migration approach, starting with less critical systems, or use a hybrid cloud strategy to bridge the gap between legacy and modern cloud-based systems. Cost is another major concern, as implementing DevSecOps involves investments in tools, training, and specialized personnel. To justify these costs, organizations should conduct a cost-benefit analysis to highlight the long-term value of DevSecOps. Prioritizing investments in high-risk and high-impact areas ensures maximum security with optimal spending. Additionally, using open-source DevSecOps tools and security solutions provided by cloud service providers can significantly reduce costs. By addressing these challenges with the right strategies, organizations can successfully implement DevSecOps in the cloud while ensuring security,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

efficiency, and scalability. (Figure 4)

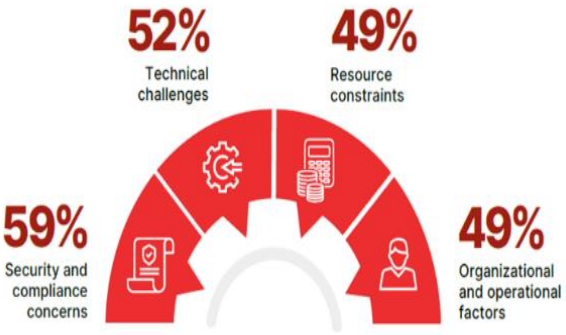

Figure 4 Survey Results: Key Factors Hindering DevSecOps Adoption

5.2. Best Practices for DevSecOps in the Cloud

Quality practices for DevSecOps in the cloud focus on integrating safety for the duration of the software program development lifecycle to ensure robust safety towards vulnerabilities. One vital approach is Shift Left safety, which entails incorporating protection early within the software program development existence cycle (SDLC) at some stage in the necessities and design stages to detect and address vulnerabilities before they become luxurious. Automation is some other key exercise, allowing security checking out, vulnerability scanning, and compliance tests to be carried out efficaciously and continuously with out guide intervention. Collaboration among improvement, protection, and operations teams is critical in breaking down silos and aligning protection desires, ensuring a unbroken integration of safety into the improvement process. additionally, non-stop tracking plays a vital role in DevSecOps by supplying actual-time protection tracking and hazard detection, permitting groups to perceive and reply to security incidents right away. sooner or later, protection education for all improvement crew individuals is critical to elevating consciousness and ensuring that protection remains a shared obligation, with everybody contributing to defensive sensitive information. by using adopting those best practices, organizations can enhance their cloud security posture while maintaining agility and efficiency.

6. Case Studies

Numerous businesses have effectively applied DevSecOps in the cloud, addressing security challenges whilst maintaining performance and innovation. Netflix faced the task of securing its massive, allotted cloud infrastructure whilst making sure rapid deployment cycles and integrating safety into its microservices architecture. to triumph over this, Netflix leveraged protection automation gear like security Monkey for vulnerability scanning and compliance exams. moreover, it adopted Chaos Engineering with tools like Chaos Monkey to proactively pick out and attach infrastructure weaknesses. by using promoting decentralized security, Netflix empowered improvement teams with shared safety obligation, main to stepped forward protection, faster deployments, and superior resilience.Capital One encountered challenges related to regulatory compliance and securing sensitive customer data while modernizing legacy systems and transitioning to the cloud. The company adopted a cloud-first strategy by migrating to AWS, ensuring scalability and security. It implemented Security as Code by integrating security controls within Infrastructure as Code (IaC) templates, enabling automated and consistent security enforcement. Additionally, Capital One embraced a DevSecOps transformation, upskilling its workforce and fostering a culture of security collaboration. The company also contributed to open-source security tools, benefiting both internal operations and the wider security community. These initiatives resulted in enhanced security, improved compliance, greater agility, and reduced costs Adobe faced the challenge of securing its cloud-based subscription services while keeping up with rapid innovation cycles. To address this, Adobe adopted a shift-left security approach, integrating security testing early in the software development life cycle (SDLC) with tools like Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). The company further improved efficiency through automation and orchestration, streamlining security processes and minimizing manual interventions. Investing in security training for employees helped build a security-aware workforce, ensuring best practices were followed. Additionally, Adobe utilized cloud-native security tools to enhance the security of its cloud workloads. As a result, the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

company reduced security risks, accelerated time to market, and strengthened customer trust. These case studies highlight how leading organizations have successfully embedded DevSecOps into their cloud environments, demonstrating the benefits of automation, early security integration, and a strong security culture.

7. Future Research Directions

future studies in DevSecOps is exploring diverse instructions to enhance security and performance in cloud environments. One full-size place is the combination of AI and gadget studying into DevSecOps. AI performs a critical role in threat detection through analyzing big datasets to identify vulnerabilities and unusual activities in real-time. system mastering improves static code evaluation gear by using gaining knowledge of from newly discovered vulnerabilities, improving computerized code scanning. moreover, AI-powered incident reaction automates reactions to detected threats, reducing the need for manual intervention. Predictive analytics further strengthens security through forecasting capability breaches based on ancient data, allowing proactive measures to be taken every other vital research region is serverless security, which presents unique demanding situations because of its occasion-pushed nature. making sure safety in serverless environments entails securing event resources and endpoints, managing access manipulate across multiple characteristic executions, and addressing delays in vulnerability patching, as cloud carriers manage infrastructure updates. high-quality practices for securing serverless functions include making use of the precept of least privilege to minimize get admission to risks, implementing continuous tracking and logging to locate anomalies, and securing APIs to shield towards malicious requests.DevSecOps for edge computing is also gaining attention, as distributed edge devices often operate with limited connectivity, making centralized security management difficult. To address these challenges, implementing a Zero Trust Architecture ensures continuous verification of device authenticity and security status. Encrypting all data in transit and at rest further enhances security, protecting sensitive information from breaches. Additionally, enabling automated security updates for edge devices ensures they remain protected against evolving threats without requiring manual intervention. As DevSecOps continues to evolve, these research directions will play a vital role in strengthening security frameworks across various cloud and computing environments.

Conclusion

The core finding is this: integrating security directly into the software development pipeline for cloud environments, through DevSecOps, is no longer optional. This proactive approach, marked by automated vulnerability scans, predictive threat modeling, and continuous monitoring, shifts security from a reactive to a preventative stance. Crucially, it fosters a collaborative security culture, where developers, operations, and security teams share ownership. Cloud adoption introduces distinct security hurdles, notably the complexities of shared responsibility, multi-tenancy vulnerabilities, the risk of data breaches. The ultimate benefit of DevSecOps lies in its ability to simultaneously enhance security and accelerate secure application deployment. By embedding security early, organizations minimize the risk of costly vulnerabilities, ensuring the dependability of cloud services. In a rapidly evolving cloud ecosystem, DevSecOps stands as an indispensable framework for maintaining robust security.

References

[1]. M. Tajammul, R. Parveen and I. A. Tayubi, "Comparative Analysis of Security Algorithms used in Cloud Computing," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 875–880.

[2]. Ibrahim I. A. and Bassiouni M., “Improvement of job completion time in data-intensive cloud computing applications,” Journal of Cloud Computing, vol. 9, no. 1, Feb. 2020, doi: 10.1186/s13677-019-0139-6 [DOI] [Google Scholar]

[3]. Seth B. et al. , “Secure Cloud Data Storage System using Hybrid Paillier-Blowfish Algorithm,” Computers, Materials & Continua, vol. 67, no. 1, pp. 779–798, 2021, doi: 10.32604/cmc.2021.014466 [DOI] [Google Scholar]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 06 June 2025
Page No: 2771 - 2778
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0409

[4]. Maeser R., "Analyzing CSP Trustworthiness and Predicting Cloud Service Performance," IEEE Open Journal of the Computer Society, vol. 1, pp. 73–85, 2020, doi: 10.1109/OJCS.2020.2994095 [DOI] [PubMed] [Google Scholar]

[5]. Hassan J. et al., "The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR)," Computational intelligence and neuroscience, vol. 2022, p. 8303504, Jun. 2022, doi: 10.1155/2022/8303504 [DOI] [PMC free article] [PubMed] [Google Scholar] [Retracted]

[6]. Kim Y.-K., Kim H.-J., Lee H., and Chang J.-W., "Privacy-preserving parallel kNN classification algorithm using index-based filtering in cloud computing," PLOS ONE, vol. 17, no. 5, p. e0267908, May 2022, doi: 10.1371/journal.pone.0267908 [DOI] [PMC free article] [PubMed] [Google Scholar]

[7]. Mustafa M., Alshare M., Bhargava D., Neware R., Singh B., and Ngulube P., "Perceived Security Risk Based on Moderating Factors for Blockchain Technology Applications in Cloud Storage to Achieve Secure Healthcare Systems," Computational and Mathematical Methods in Medicine, vol. 2022, pp. 1–10, Jan. 2022, doi: 10.1155/2022/6112815 [DOI] [PMC free article] [PubMed] [Google Scholar] [Retracted]

[8]. Al-Issa Y., Ottom M. A., and Tamrawi A., "eHealth Cloud Security Challenges: A Survey," Journal of Healthcare Engineering, vol. 2019, pp. 1–15, Sep. 2019, doi: 10.1155/2019/7516035 [DOI] [PMC free article] [PubMed] [Google Scholar]

[9]. Hussein M., Mousa M., and Alqarni M., "A placement architecture for a container as a service (CaaS) in a cloud environment", Journal of Cloud Computing, vol. 8, no. 1, 2019. Available: doi: 10.1186/s13677-019-0131-1 [DOI] [Google Scholar]

[10]. P. Kulkarni, R. Khanai, and G. Bindagi, "A Comparative Analysis of Hybrid Encryption Technique for Images in the Cloud Environment," 2020 International Conference on Communication and Signal Processing (ICCSP), Jul. 2