Journal of Science and Technology

ISSN: 2456-5660 Volume 6, Issue 6 (December -2021)
www.jst.org.in

DOI: https://doi.org/10.46243/jst.2021.v6.i6.pp231-243

Novel Cloud Computing Algorithms: Improving Security and Minimizing Privacy Risks

Himabindu Chetlapalli,
QA Architect, So Cast Inc, Toronto.
Email ID: chetlapallibindu@gmail.com

ABSTRACT

Cloud computing provides both opportunities and challenges for maintaining user privacy and security. This study addresses these issues by proposing unique ways for boosting security and reducing privacy threats in multi-cloud systems. A significant priority is the creation of the Global Authentication Register System (GARS), a comprehensive strategy for mitigating the danger of material outflow in cloud environments while prioritizing privacy safeguards. The study addresses the specific security and privacy concerns faced by multi-cloud systems and presents the GARS as a pioneering solution based on a thorough review of the literature. System simulations are used to examine the effectiveness of GARS, including performance, security, and availability. Furthermore, user-centric privacy-preserving strategies are created based on insights gleaned from user research, guaranteeing that privacy concerns are effectively addressed across various cloud platforms. The report also looks at advanced threats and upcoming technologies, which can help strengthen the security framework's resilience against sophisticated cyberattacks. Regulatory compliance and data sovereignty are prioritized, with the security architecture built to meet legal criteria while efficiently managing data sovereignty concerns. The methodology takes a multidisciplinary approach, combining several analytical tools to deliver practical recommendations for enhancing cloud computing systems' security posture. Overall, the goal of this research is to help create a more secure and reliable computing environment for enterprises and individual users functioning in multi-cloud environments.

Keywords: Global Authentication Register System (GARS), Deployment Security, Privacy Preservation, Authentication, Authorization, Token Management, User-Centric Privacy, User Studies, Regulatory Compliance, Data Sovereignty, Analytical Techniques.

1. INTRODUCTION

Safeguarding user privacy and implementing strong security measures are critical in the ever-changing world of cloud computing. But the complexity of managing material security has increased due to the quick uptake of cloud services, especially in multi-cloud setups. To effectively overcome these obstacles, inventive solutions are necessary. This work introduces novel approaches to cloud computing to tackle these issues. It suggests a thorough strategy to reduce the possibility of material outflow in cloud environments by creating the Global Authentication Register System (GARS). In order to improve cloud computing systems' security posture, this study prioritizes privacy preservation measures. The goal of implementing GARS is to provide more dependable and secure methods for exchanging and storing information. The ultimate goal of this research is to improve cloud computing security and provide a more dependable and safe computing environment for both businesses and individual users.

Software system deployment has been transformed by cloud computing, which has made large-scale distribution easier for vendors. But as cloud services have proliferated, material security management has gotten harder, especially in multi-cloud setups. Businesses are more concerned about security than individual users are about privacy violations. This study explores different cloud computing architectures and how deployment security is affected by them, emphasizing the difficulties caused by improper settings. To reduce the risk of material outflow in cloud environments, it suggests the Global Authentication Register System (GARS), an improved deployment architecture and material protection method. The effectiveness of GARS is assessed in terms of performance, security, and availability using system simulations. The results highlight how well this strategy works to protect user privacy and improve cloud information security. This report also provides actionable suggestions for strengthening cloud computing security procedures, promoting a more secure and dependable computing environment for all parties involved.

The goal of this research is to fully handle the complex issues related to privacy and security in multi-cloud systems. Through an exhaustive examination of diverse cloud computing architectures and their effects on deployment security, the research aims to detect possible weaknesses stemming from inaccurate setups. The main goal is to present the Global Authentication Register System (GARS) as a cutting-edge countermeasure to the danger of material outflow in cloud computing settings. The research attempts to assess the performance, security, and availability of GARS using comprehensive system simulations. The ultimate goal of this study is to improve the security posture of cloud computing systems while lowering privacy concerns by addressing current research gaps and offering useful insights.

Using a multidisciplinary approach, this research aims to address the crucial issues of security and privacy in cloud computing systems. Through an analysis of various cloud computing designs and their effects on deployment security, the study seeks to identify potential weaknesses that may result from incorrect setups. In order to reduce the risk of material outflow in cloud settings, the research presents the Global Authentication Register System (GARS) as a ground-breaking solution. The performance, security, and availability of GARS are thoroughly assessed by extensive system simulations. The ultimate goal is to provide practical advice aimed at strengthening cloud computing security procedures, thus cultivating a more robust and reliable computing environment that meets the requirements of both business and individual users.

The intricate relationship between security standards and privacy concerns in multi-cloud setups is still poorly understood, despite the advances in cloud computing security. While previous research has looked at different cloud computing architectures and suggested creative ways to reduce material outflow risks—like the Global Authentication Register System (GARS)—very few have thoroughly assessed the usefulness and practical implications of these approaches in a range of deployment scenarios. Furthermore, there is disagreement on the best ways to prioritize privacy protection while guaranteeing strong security protocols. By carefully analyzing various cloud computing designs, evaluating their effect on deployment security, and closely examining the effectiveness of cutting-edge techniques like GARS, this research aims to close these gaps. The goal of this study is to close these research gaps and offer insightful advice for improving cloud computing systems' security posture and successfully reducing privacy threats.

The swift growth of cloud computing services has given rise to intricate security and privacy challenges, especially in multi-cloud settings. Businesses continue to emphasize security concerns, while individual users are still concerned about possible privacy violations. Innovative approaches to reducing material outflow concerns in cloud environments have been suggested by current research, such as the Global Authentication Register System (GARS). On the other hand, the complex interplay between security protocols and privacy-preserving techniques in multi-cloud architectures is not well understood. Moreover, not enough research has been done on the usefulness and practical consequences of these suggested solutions in various deployment circumstances. By carefully examining different cloud computing designs, gauging their effect on deployment security, and testing the effectiveness of cutting-edge techniques like GARS, this study seeks to close these gaps. The objective of this study is to offer practical recommendations for improving the security posture of cloud computing systems and efficiently reducing privacy concerns for businesses and individuals.

2. LITERATURE REVIEW

Wang et al. (2019) investigate sensor clouds, which combine wireless sensor networks and cloud computing to increase processing power and storage capacity. Despite these developments, sensor clouds confront constraints such as limited communication and energy, high latency, and security and privacy concerns. Mobile edge computing emerges as a promising option since it moves computer chores closer to the data source, potentially alleviating these difficulties. The study evaluates the current state of sensor clouds, explains their properties, and introduces a trust evaluation technique as well as reliable data gathering methods based on mobile edge computing. Future research directions in this area are also discussed.

Ismagilova et al. (2022) present a thorough examination of the security, privacy, and associated concerns of smart cities. The article covers the significant problems and hazards associated with security and privacy in smart city environments, emphasizing the importance of understanding smart city infrastructure and its impact on personal data management. To overcome these difficulties, the authors propose a smart city interaction framework. Furthermore, the article investigates the possible use of future technologies like blockchain and social media to improve security and privacy. Key avenues for future research are also suggested, making the findings a useful resource for both academics and practitioners.

Mohammed Yakubu and Chen et al. (2020) explore the privacy and security concerns that come with the increased usage of genomic data in biomedical research and healthcare. The low cost of

DNA sequencing has resulted in a wealth of genomic data, yet the sensitive nature of the human genome raises serious privacy and security concerns. The study examines a variety of privacy attacks, including identity tracing and attribute disclosure, that endanger individual privacy. It analyzes existing cutting-edge technologies for protecting genetic privacy, as well as current concerns and future research directions in this field.

Qayyum et al. (2020) undertake a systematic study of the security of cloud-based machine learning services, revealing an increasing interest in both attacking and defending these services. The popularity of Machine Learning as a Service (MLaaS) cloud platforms has grown due to cloud computing's efficiency and cost-effectiveness. However, the growing use of cloud-hosted ML/DL systems opens up possible attack vectors for adversaries. The report underlines the necessity for additional research into establishing strong security mechanisms to defend these services from diverse threats.

Suárez-Albela et al. (2017) analyze the usage of RSA and ECC for protecting IoT gateways in fog computing situations, concluding that ECC is a better option, saving up to 50% on energy consumption and double data throughput compared to RSA. Fog computing enables new IoT applications and services, but the security and privacy of essential data remain significant challenges. IoT gateways, which are critical for data security and processing, frequently have limited computational resources and power supplies. The article concludes that ECC is a more efficient and feasible alternative for safeguarding IoT gateway communications. Furthermore, the study evaluates data compression algorithms in IoT contexts and concludes that they do not significantly improve data throughput or power consumption for tiny payloads.

Sareen et al. (2016) propose a mobile-based architecture for automatically predicting epileptic seizures using wireless sensor technology and the cloud. This system extracts significant features from EEG recordings using the fast Walsh-Hadamard transform (FWHT) and Higher Order Spectral Analysis (HOSA). The k-means classifier then diagnoses seizure states with 94.6% accuracy. Tested on the Amazon EC2 cloud, the model yields encouraging results in terms of execution time and accuracy, demonstrating the promise of merging cloud computing and wireless sensors for effective seizure prediction.

Balasubramaniam and Kavitha et al. (2015) present a unique approach for managing personal health record transactions in cloud computing based on geometric data perturbation, solving concerns about information security and key management. Cloud computing, a rapidly growing delivery mechanism for IT services, provides scalable and virtualized resources via the Internet. Personal health records, which are critical for health information sharing, are rapidly being outsourced to third-party providers, such as cloud services. However, present encryption approaches for personal health records frequently encounter unresolved key management concerns. To address these issues, the proposed technique entails perturbing the personal health record database geometrically and outsourcing it to the Amazon EC2 cloud, giving a promising route for improving security and privacy in healthcare data management in cloud contexts.

Al Ayubi et al. (2016) provide a study report on the creation of a mobile app guideline specifically for hospitals functioning in a BYOD (bring-your-own-device) environment. The guideline's goal is to help people use personal gadgets more effectively while also reducing security threats. The project entailed the development of an in-house mobile app, TaskList, which was refined following a pilot implementation at Boston Children's Hospital. During this procedure, fourteen practical recommendations were developed and classified into four categories: authentication and authorization, data management, app environment protection, and remote enforcement. These efforts culminated in the establishment of the BCH Mobile Application Development Guideline. This guideline is intended to help developers ensure compliance with regulatory frameworks such as HIPAA regulations, as well as to facilitate seamless integration with hospital information systems, ultimately improving the overall security and functionality of mobile applications in healthcare settings.

Alnajrani et al. (2020) undertook a thorough mapping study on privacy and data protection in mobile cloud computing (MCC), with the goal of identifying current trends and unresolved challenges in the area. The study collected and analyzed a total of 1711 studies published between 2009 and 2019, of which 74 primary studies were chosen for investigation. During this procedure, the researchers identified data privacy concerns, assaults, remedies, and numerous research kinds pertinent to MCC. The findings provide unique insights into the present state of privacy and data protection in MCC, making them a useful resource for both researchers and practitioners.

Liao et al. (2016) investigate the use of the analytical hierarchy approach to evaluate cloud computing service systems in the healthcare industry. The study concludes that cost-effectiveness is the most important aspect in building and executing optimal systems, followed by practical considerations like software design and system architecture. Volatility, health insurance policies, and the standing of healthcare professionals all provide substantial issues. However, cloud computing serves as both a challenge and an opportunity for healthcare companies, allowing them to strike a delicate balance between quality and affordability. Notably, the study emphasizes that cost-effectiveness is the major determinant impacting the design and implementation of ideal cloud computing healthcare service systems, with practical concerns serving as secondary variables.

Carter (2019) investigate the challenges and techniques involved in maintaining genomic data in the cloud, with an emphasis on next-generation sequencing (NGS). With NGS producing massive amounts of data, laboratories are increasingly relying on cloud technologies for effective data management. The research focuses on the use of public cloud repositories for crowdsourcing contributions of human genetic variation data. The study also dives into ways for assuring compliance with regulatory standards in the United States, specifically in the context of genetic information, addressing the intricacies of the regulatory environment surrounding genomic data management.

Wu (2019) provide a study report on the creation of a secure and efficient digital-data-sharing system designed for cloud environments, with a particular emphasis on educational settings. The study emphasizes the importance of such a system in educational settings, underlining the crucial relevance of appropriate security methods in protecting the confidentiality and integrity of cloud computing environments. Recognizing the significance of encryption in reducing the danger of privacy breaches, the study underlines the necessity for strong encryption mechanisms for digital resources, data, and educational materials. Furthermore, the study describes the creation of a cloud-based, learner-centered access control mechanism designed to handle issues related with multi-user access requests and dynamic updating in digital-sharing systems. By combining these components, the proposed system aims to provide comprehensive data access and security features that promote effective digital data sharing inside educational cloud environments.

3. METHODOLOGY

3.1. Literature Review and Analysis

Objective: In order to comprehend the present state of cloud computing security and privacy, with an emphasis on multi-cloud systems, the first step entails a thorough reading of the literature.

Activities: In order to identify the distinct features and difficulties that differentiate single-cloud and multi-cloud configurations, the first stage is a thorough examination of academic journals, industry studies, and white papers on cloud computing security. To determine the main security and privacy issues related to each configuration, this requires methodically going through the literature. To illustrate the shortcomings and unresolved problems in the existing research, a comprehensive gap analysis will also be carried out. This will focus on issues related to interoperability, multi-cloud interactions, and the integration of security measures across various cloud platforms. To provide a comprehensive picture of the current situation and guide future research endeavors, this foundational study attempts to.

3.2. Problem Identification

Objective: Determine the particular privacy and security issues that are particular to multi-cloud systems and demonstrate the need for creative solutions such as the Global Authentication Register System (GARS).

Activities: Surveys and interviews with a wide range of stakeholders, including cloud security specialists, IT professionals, and end users, will be undertaken in order to obtain thorough insights into the issues and viewpoints surrounding cloud security. By eliciting firsthand experiences, worries, and opinions on a range of cloud security-related topics, these exchanges hope to identify important problems and possible answers.

Thorough documentation of the issues brought up by stakeholders with respect to crucial elements like data sovereignty, regulatory compliance, and cross-cloud data flows will be maintained throughout the documentation stage. The ramifications of these issues for security and privacy in multi-cloud settings will be fully examined through in-depth analysis. Furthermore, in order to formulate effective ways for resolving these problems, relevant factors—such as local laws and data residency requirements—will be closely investigated.

3.3. Framework Development

Objective: Create a thorough security strategy and risk assessment specifically for multi-cloud settings.

Activities: The creation of an extensive multi-cloud security architecture will be a component of the security framework design. This architecture will provide strong protection across many cloud platforms by integrating current security policies and fixing gaps found. To effectively reduce potential dangers, crucial elements including threat detection systems, encryption methods, and access control mechanisms will be thoughtfully planned and put into place. In order to handle the dynamic nature of multi-cloud settings, the framework will also place a high priority on interoperability and scalability, all the while offering uniform security measures across all interconnected cloud services.

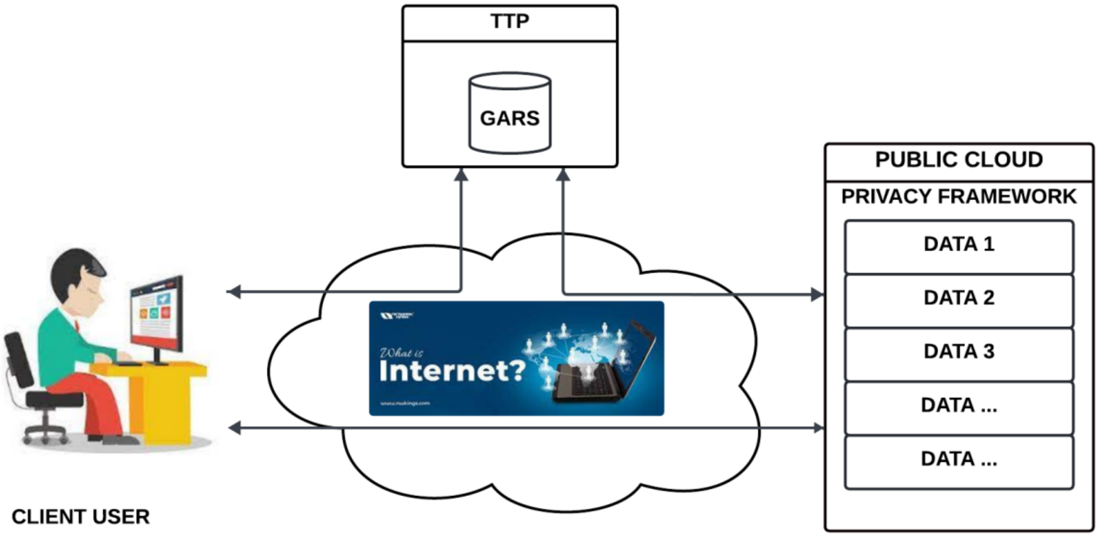

Figure 1: Optimization model of cloud computing.

A cloud computing optimization model for security and privacy protection is put out in this study. It recommends creating a trusted third-party cloud's Global Authentication Register System (GARS) (TTP). Clouds and subscribers go through distinct certification processes for disposable registration. The public cloud establishes a framework and methodology for privacy, processing and safeguarding private information and security through encryption based on the GARS technique.

Integrating the Global Authentication Register System (GARS) into the multi-cloud security framework includes creating and implementing a centralized authentication and permission system. GARS will be a key component for maintaining user identities, access privileges, and authentication tokens across numerous cloud platforms. GARS will provide users with seamless and secure access to a variety of cloud services, while administrators will be able to centrally administer and monitor access controls. Furthermore, GARS will enable interoperability between multiple cloud environments, ensuring that security rules and user authentication methods are consistent across the entire multicloud infrastructure.

On this phase, the Global Authentication Register System (GARS) components will be thoroughly described and modeled. This involves explaining fundamental capabilities like user authentication, access control, and token management, as well as describing how these components interact with various cloud services to enable seamless and safe integration.

3.4. System Simulation and Implementation

Objective: To evaluate the effectiveness of the proposed framework and GARS system, test them in a controlled, simulated environment.

Activities: To simulate real-world scenarios, a multi-cloud infrastructure will be built. This environment will contain a wide set of cloud platforms, including AWS, Azure, and Google Cloud. Each platform will be built to emulate normal usage patterns and interactions, enabling for full testing of the security framework and the Global Authentication Register System (GARS).

The GARS algorithm will be implemented in a simulated multi-cloud scenario. This includes implementing and integrating GARS functionalities such as user authentication, authorization management, and token handling. The algorithm will be modified to ensure compliance with the simulation's many cloud platforms, allowing for precise testing and evaluation of its effectiveness in handling authentication and access across several clouds.

A complete series of tests will be carried out to determine the effectiveness of the GARS system in the simulated multi-cloud scenario. These tests will assess the system's availability, security measures, and performance across a variety of scenarios, assuring its dependability and suitability for real-world deployment across many cloud platforms.

During the testing phase, experimental data will be rigorously collected in order to capture various metrics about the GARS system's performance, security, and usability within the simulated multi-cloud context. This information will be rigorously examined to determine GARS' success in managing authentication and access across numerous cloud platforms.

3.5. Evaluation and Analysis

Objective: Evaluate the proposed security framework and GARS system rigorously to determine their effectiveness.

Activities: After the data gathering phase, a thorough performance study will be carried out in order to assess the efficacy of the GARS system in a variety of scenarios inside the simulated multi-cloud environment. Metrics including response times, throughput, and resource usage will be examined in this research to evaluate the effectiveness and scalability of the system under different workload conditions.

An extensive analysis of the security improvements resulting from the deployment of GARS in the multi-cloud environment will be part of the security assessment. This assessment will look at things like data encryption, access control, and authentication systems to see how well GARS strengthens cloud security protocols.

The efficacy of the suggested framework—specifically, the Global Authentication Register System (GARS)—will be compared to that of other security measures through a comparison study. To ascertain which of the two frameworks is better at improving multi-cloud security, this comparison will assess performance, security features, and scalability.

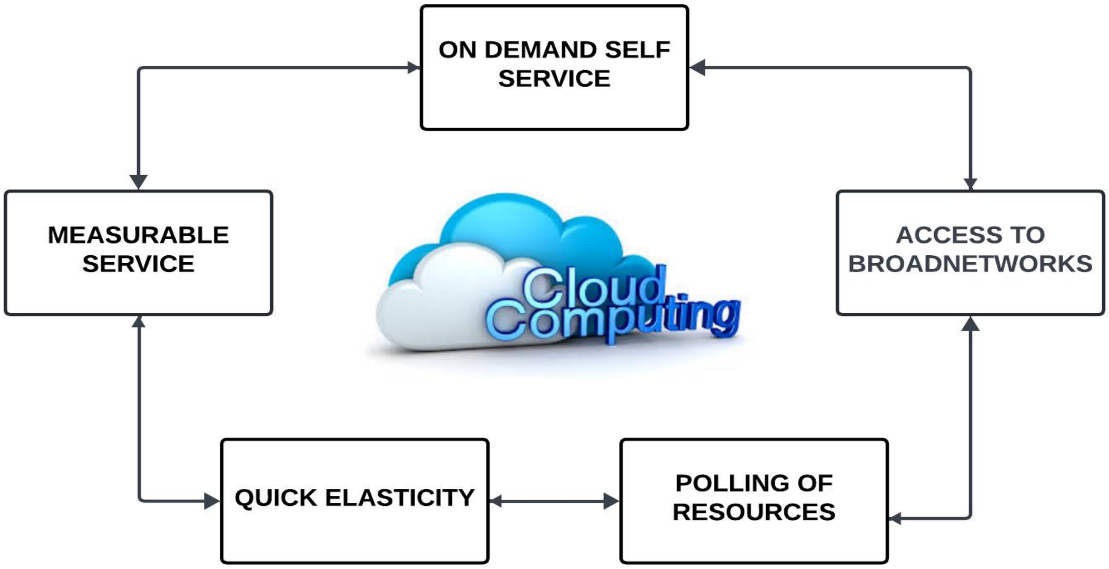

Figure 2: Cloud Computing Characteristics.

The National Institute of Standards and Technology (NIST) has defined two fundamental aspects of cloud computing: Broad Network Access (BNA), which enables services to be accessed across various platforms using standardized mechanisms, and On-Demand Self-Service, where resources are provisioned automatically without human interaction. While Quick Elasticity allows services to be quickly scaled up or down as needed, giving the impression of boundless resources, Pooling of Resource combines physical and virtual provider resources and distributes them to consumers at abstract levels. With the use of metering capabilities, measured services monitor resource usage, including processing, bandwidth, and storage, ensuring transparency and optimization that is advantageous to both providers and customers.

3.6. User-Centric Privacy and Security

Objective: To create user-centric privacy-preserving techniques, it is important to comprehend user attitudes and behaviors about privacy in multi-cloud systems.

ISSN: 2456-5660 Volume 6, Issue 6 (December -2021)
www.jst.org.in
DOI: https://doi.org/10.46243/jst.2021.v6.i6.pp231-243

Activities: Data on preferences, activities, and privacy concerns from various user groups will be collected through user studies. Privacy-preserving techniques will be developed based on the gathered insights. User privacy will subsequently be given top priority and be adequately safeguarded across a range of cloud platforms thanks to the integration of these techniques into the suggested multi-cloud security framework. Using this method would increase user satisfaction and general trust in cloud computing services by ensuring that the security architecture is not only technically sound but also meets user expectations and needs.

Table 1: Use Rates of Different Application Cloud Services Among Internet Users.

Cloud Application Service	**Internet Users as a Percentage**
Webmail (such as Yahoo! Mail, Gmail, Hotmail, etc.)	56%
Online picture storage for private images	34%
Programs for online applications (such as Adobe Photoshop Express and Google Documents)	29%
Online video storage for private videos	7%
Online file storage and payment	5%
Hard drive online backup	5%

3.7. Advanced Threats and Emerging Technologies

Objective: Assess the effects of emerging technologies such as edge computing and make sure the security framework is resilient to sophisticated cyberattacks.

Activities: Threat analysis will entail a thorough examination of cutting-edge cyberthreats and how they might affect environments with multiple clouds. This analysis will help assess how new technologies, such as edge computing, are affecting multi-cloud security. The security framework will be modified to efficiently handle new technologies and advanced threats in light of these findings. By taking this approach, the security posture of multi-cloud systems is eventually improved since the framework is guaranteed to stay resilient and adaptable in the face of growing cyber threats and technological breakthroughs.

3.8. Regulatory Compliance and Data Sovereignty

Objective: Make that the security architecture complies with legal standards and adequately handles concerns related to data sovereignty.

Activities: Identification of rules entails determining relevant laws and standards of compliance in different areas. The security architecture will then be created with regulatory compliance and efficient data sovereignty management in mind. By putting auditing methods in place, compliance across multi-cloud environments can be tracked and audited. By ensuring that the security framework complies with legal and regulatory requirements, this strategy reduces the risk of non-compliance and boosts confidence in cloud services.

Data Collection and Analysis

Data Sources: To acquire thorough information, consult a variety of sources including scholarly journals, industry reports, expert interviews, user surveys, and experimental outcomes.

Analytical Techniques: Use comparative analysis for benchmarking, quantitative analysis for surveys and experimental data, and qualitative analysis for literature reviews and interviews.

Expected Outcomes

The research paper's methodology includes creating a solid framework for risk assessment that is adapted to multi-cloud settings. The Global Authentication Register System (GARS), which acts as a central mechanism for safe data interchange and access management across several clouds, is implemented in conjunction with this architecture. Moreover, user-centric approaches are improved by taking into account perceptions of user attitudes and privacy-related actions, guaranteeing efficient privacy protection. Furthermore, the security framework is strengthened to resist sophisticated cyberattacks and adjust to new technological advancements, guaranteeing resilience against changing threats. Moreover, regulatory compliance is given top priority. The framework is made to guarantee compliance with rules and efficiently handle issues related to data sovereignty, promoting compliance and confidence in multi-cloud settings.

The research intends to solve the crucial concerns of security and privacy in multi-cloud environments by using this thorough methodology and by providing cutting-edge solutions like GARS to improve the security posture of cloud computing systems.

4. EXISTING RESULT AND DISCUSSION

This work presents novel ways for improving security and reducing privacy threats in multi-cloud systems, particularly in the context of cloud computing issues. It introduces the Global Authentication Register System (GARS) to mitigate material outflow concerns while prioritizing privacy protection. Through a detailed literature study, specific security and privacy challenges in multi-cloud scenarios are identified, laying the groundwork for innovative solutions. Stakeholder surveys and interviews are used to create a customized security framework that incorporates GARS for centralized authentication and access management across several cloud platforms. Simulation and implementation enable framework evaluation using measures such as response times and resource utilization. User-centric privacy-preserving techniques are created based on user research, addressing privacy concerns across several platforms. Regulatory compliance and data sovereignty are prioritized, with tracking and auditing procedures in place. A strong risk assessment framework, GARS implementation, and improved privacy protections are all expected to improve cloud system security in the long run.

5. CONCLUSION

The significance of tackling security and privacy issues in the dynamic field of cloud computing, especially in multi-cloud setups, is emphasized by this study. This project intends to improve cloud system security posture while reducing privacy concerns by using a multidisciplinary approach and creative solutions such as the Global Authentication Register System (GARS). This work establishes the foundation for a more reliable and safe computing environment by methodically evaluating different cloud computing architectures, finding vulnerabilities, and suggesting thorough security frameworks. In the end, GARS implementation combined with user-centric privacy-preserving strategies presents viable ways to strengthen cloud security and boost confidence in both organizations and consumers.

6. FUTURE SCOPE

In order to improve threat detection and response mechanisms in multi-cloud systems, future research may investigate the integration of artificial intelligence and machine learning approaches. Additionally, researching how quantum computing affects privacy and cloud security may offer insightful information for creating strong defenses against new threats.

7. REFERENCE

1. Wang, T., Lu, Y., Cao, Z., Shu, L., Zheng, X., Liu, A., & Xie, M. (2019). When sensor-cloud meets mobile edge computing. Sensors, 19(23), 5324.
2. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22.
3. Mohammed Yakubu, A., & Chen, Y. P. P. (2020). Ensuring privacy and security of genomic data and functionalities. Briefings in bioinformatics, 21(2), 511-526.
4. Qayyum, A., Ijaz, A., Usama, M., Iqbal, W., Qadir, J., Elkhatib, Y., & Al-Fuqaha, A. (2020). Securing machine learning in the cloud: A systematic review of cloud machine learning security. Frontiers in big Data, 3, 587139.
5. Suárez-Albela, M., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2017). A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications. Sensors, 17(9), 1978.
6. Sareen, S., Sood, S. K., & Gupta, S. K. (2016). An automatic prediction of epileptic seizures using cloud computing and wireless sensor networks. Journal of medical systems, 40, 1-18.
7. Balasubramaniam, S., & Kavitha, V. (2015). Geometric data perturbation-based personal health record transactions in cloud computing. The Scientific World Journal, 2015.
8. Al Ayubi, S. U., Pelletier, A., Sunthara, G., Gujral, N., Mittal, V., & Bourgeois, F. C. (2016). A mobile app development guideline for hospital settings: Maximizing the use of

and minimizing the security risks of" bring your own devices" policies. JMIR mHealth and uHealth, 4(2), e4424.

9. Alnajrani, H. M., Norman, A. A., & Ahmed, B. H. (2020). Privacy and data protection in mobile cloud computing: A systematic mapping study. Plos one, 15(6), e0234312.
10. Liao, W. H., & Qiu, W. L. (2016). Applying analytic hierarchy process to assess healthcare-oriented cloud computing service systems. SpringerPlus, 5, 1-9.
11. Carter, A. B. (2019). Considerations for genomic data privacy and security when working in the cloud. The Journal of Molecular Diagnostics, 21(4), 542-552.
12. Wu, Z. Y. (2019). A secure and efficient digital-data-sharing system for cloud environments. Sensors, 19(12), 2817.