JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DATA SECURE AND MONITORING USING THIRD PARTY AUDITOR

Naveenkumar T, Tamilarasan K, Sabarish S, Nikil V
(Mrs.P.Charanya M.E., (Ph.D))

Cybersecurity

Mahendra Engineering College (Autonomous), Namakkal, Tamil Nadu, India

Abstract: This paper scrutinizes the existing system for auditing outsourced data and proposes robust enhancements to overcome its limitations. The current approach relies on a Third Party Auditor (TPA) employing a divide and conquer strategy, yet it lacks crucial authentication between the Cloud Service Provider (CSP) and TPA. This deficiency confines auditing to a single server, potentially exposing data to unauthorized access and leakage. To address these vulnerabilities, the proposed system introduces a Certified Authorization mechanism, forging a secure link between the CSP and TPA. This ensures that auditing is conducted by certified authorities, bolstering data integrity and security. Additionally, a remote Data Integrity Checking scheme is devised, tailored for distributed storage environments. This scheme empowers auditors to scrutinize data integrity across distributed systems, facilitating comprehensive security assessments. Furthermore, fine-grained access control mechanisms are implemented, enabling meticulous auditing of data of varying sizes. These mechanisms not only enhance security but also streamline auditing processes, mitigating risks associated with unauthorized access and data leakage. The proposed system offers several advantages, including authenticated TPA auditing, support for dynamic data updates, and efficient storage correctness measurement. Moreover, the incorporation of fine-grained access schemes enhances data integrity, safeguarding assets and reducing the likelihood of fraudulent activity. Overall, these enhancements represent a significant step forward in ensuring the security of outsourced data within cloud environments.

IndexTerms: Cloud security, Third Party Auditor, Data auditing, Distributed storage, Authentication mechanism, Data integrity, Fine-grained access control, Certified Authorization, Real-time monitoring, Dynamic data updates.

I. INTRODUCTION

In the contemporary digital era, the widespread adoption of cloud computing has reshaped how organizations manage and store their data. However, this transition to cloud technology introduces notable challenges, particularly regarding the security and integrity of outsourced data. As enterprises increasingly entrust third-party cloud service providers with their sensitive information, the imperative for robust auditing mechanisms becomes evident. Real-time data monitoring, authentication protocols, and data integrity maintenance emerge as pivotal elements in fortifying cloud security.

This project endeavors to confront these challenges by scrutinizing existing systems for auditing outsourced data and proposing innovative enhancements to surmount their limitations. Specifically, the focus is on harnessing advanced cryptographic methodologies, such as Elliptic Curve Cryptography (ECC), to bolster data security and facilitate secure data sharing within cloud environments. By amalgamating runtime cloud auditing with ECC encryption, the proposed solution aims to furnish organizations with a holistic approach to safeguarding their data while fostering secure data exchange and ensuring compliance with regulatory mandates.

Through a meticulous examination of the deficiencies in current systems and the proposed augmentations, this project aspires to contribute to the evolution of cloud security practices. By furnishing enterprises with the requisite tools and methodologies to effectively audit their outsourced data, our objective is to mitigate security vulnerabilities, shield sensitive information, and elevate the overall data security posture in cloud infrastructures.

II. RELATED WORKS

In[1] Diao Zhe; Wang Qinghong; Su Naizheng The rise of Cloud Computing has brought increased attention to Cloud storage technology, an emerging network storage concept stemming from Cloud computing principles. Cloud storage offers users access to high-speed storage and retrieval services within the Cloud computing environment. However, data security poses a significant challenge in Cloud storage systems, with malicious attacks and data breaches becoming increasingly common. Ensuring the security of user data stored in the Cloud is imperative. This paper aims to address Cloud storage security concerns by formulating appropriate security policies. By analyzing existing academic research, the paper examines the security risks associated with user data in Cloud storage and explores relevant security technologies tailored to the structural characteristics of Cloud storage systems.

In[2] Zijiao Tang the ever-evolving landscape of Internet technology, the widespread adoption of new technologies has become increasingly prevalent. Notably, the rapid advancement of big data and cloud computing technologies has significantly contributed to enhancing the efficiency of data storage and management. However, the inherent complexities of data systems in the big data cloud computing environment raise concerns regarding data security. To address these challenges and enhance information security during data processing and integration, it is imperative to explore data security protection technologies tailored to the specific requirements of the big data cloud computing environment. This paper aims to investigate such technologies to effectively mitigate data and information security issues, thereby improving the reliability and security of data transmission processes.

In[3] Ntebaleng Tutubala; Topside E. Mathonsi This paper explores the dynamics of cloud computing, delineating its role in provisioning resources and facilitating information delivery over the internet. While cloud services are increasingly adopted by organizations due to economic incentives and technological advancements, they also introduce significant security concerns, with data security standing out as a critical issue. This study aims to devise a hybrid data security framework to address these challenges, with a focus on legal frameworks like POPIA and GDPR. Through a comprehensive survey, the effectiveness of various data security techniques is evaluated, ensuring coverage of the CIA triad principles. By integrating the most effective techniques, the framework endeavors to enhance overall security in the cloud, thereby instilling confidence in customers and driving increased business for cloud service providers.

In[4] Ashish Joshi; Aditya Raturi; Santosh Kumar; Ankur Dumka This paper delves into the pervasive utilization of cloud environments for data processing and sharing worldwide, emphasizing the imperative of ensuring data security and privacy within such systems. By addressing the benefits, challenges, and emerging research trends in safe data processing and exchange in the cloud, this study sheds light on the pressing need for enhanced security measures. Through an analysis of prevalent security gaps stemming from the increased adoption of cloud computing, including risks of data modification, loss, and theft, as well as unauthorized access by insiders, the paper underscores the complexity of safeguarding data in cloud environments. Furthermore, the assessment of the degree of protection offered to the CIA triad—confidentiality, integrity, and availability—provides valuable insights into the efficacy of information security measures in mitigating risks and vulnerabilities associated with cloud computing.

In[5] Anupreet Kaur; Ankita Dhiman; Manjit Singh This comprehensive review paper delves into the critical issue of ensuring data security in cloud computing environments amidst the proliferation of big data. Through an extensive examination of existing literature, it elucidates the multifaceted security challenges inherent in big data security, encompassing confidentiality, data authentication, availability, privacy, location, storage, and integrity. By reviewing related works and identifying gaps in current research, the paper underscores the urgency of addressing these challenges. It proposes pragmatic solutions, including encryption, access control, and data obfuscation, to mitigate the identified security risks. Offering valuable insights into the evolving landscape of big data security in cloud computing, this review paper emphasizes the indispensability of robust security measures in safeguarding data integrity and confidentiality in cloud environments.

In[6] Keke Gai; Meikang Qiu; Hui Zhao This paper addresses the critical issue of cloud data security and privacy, which has hindered the widespread adoption of cloud computing. By proposing the Security-Aware Efficient Distributed Storage (SAEDS) model, it introduces a novel approach to mitigate concerns regarding unauthorized access to sensitive data by cloud operators. The SAEDS model employs innovative algorithms, namely Secure Efficient Data Distributions (SED2) and Efficient Data Conflation (EDCon), to efficiently split and distribute files across distributed cloud servers, ensuring data remains inaccessible to cloud service operators. Through rigorous experimental evaluations, both the security and efficiency performances of the proposed approach are thoroughly assessed, offering promising insights into enhancing cloud data security while maintaining operational efficiency.

In[7] Zaigham Mahmood This paper addresses the critical issue of cloud data security and privacy, which has hindered the widespread adoption of cloud computing. By proposing the Security-Aware Efficient Distributed Storage (SAEDS) model, it introduces a novel

approach to mitigate concerns regarding unauthorized access to sensitive data by cloud operators. The SAEDS model employs innovative algorithms, namely Secure Efficient Data Distributions (SED2) and Efficient Data Conflation (EDCon), to efficiently split and distribute files across distributed cloud servers, ensuring data remains inaccessible to cloud service operators. Through rigorous experimental evaluations, both the security and efficiency performances of the proposed approach are thoroughly assessed, offering promising insights into enhancing cloud data security while maintaining operational efficiency.

In[8] Kamariah Abu Saed; Norshakirah Aziz; Ade Wahyu Ramadhani This study underscores the paramount importance of data governance in ensuring the security of company data, emphasizing the responsibility of all employees, regardless of their hierarchical position, in protecting data assets. By treating data with the same level of importance as other company assets, the study aims to mitigate the risks associated with data breaches and potential business disruptions. Through a comprehensive literature review and in-depth interviews with experts in cloud security, the study seeks to gain insights into effective data governance practices. Ultimately, the study proposes a data governance security assessment tailored to Infrastructure as a Service (IaaS) in cloud data centers, with the goal of bolstering data security measures and restricting access to sensitive information.

In[9] Yenumula ReddyThis paper delves into the complexities of big data, which presents challenges in storage, retrieval, and processing due to its unstructured nature. By discussing the current obstacles faced in storing, retrieving, and processing big data, as well as implementing security measures, the paper aims to shed light on the pressing issues surrounding big data management. Furthermore, the paper proposes a security model tailored to dynamic cloud environments, offering potential solutions to address the multifaceted challenges associated with big data processing and storage.

In[10] Jian Shen; Tianqi Zhou; Debiao He; Yuexin Zhang This paper addresses the challenges of ensuring secure and efficient data sharing within groups in cloud computing environments. Leveraging the symmetric balanced incomplete block design (SBIBD), the paper introduces a novel key agreement protocol that supports multiple participants and can dynamically accommodate varying group sizes. By utilizing the proposed protocol, the computational complexity linearly scales with the number of participants while communication complexity is significantly reduced, thanks to the (v,k+1,1) -block design. Additionally, the protocol exhibits fault tolerance, enhancing resilience against key attacks, thus ensuring robust group data sharing in cloud computing environments.

III. EXISTING SYSTEM

The current system incorporates a Third Party Auditor (TPA) to conduct audits on outsourced data, aiming to mitigate security risks associated with remotely stored data. Audits are facilitated using a divide and conquer approach, enabling efficient examination of large volumes of sensitive data by dividing them into smaller blocks. This method is integrated into a new data structure, enhancing the system's capability to support dynamic block update operations. Remote Data Checking is implemented to oversee data stored remotely, with a focus on validating data integrity using algebraic signature properties. By conducting data audits on a single server, the system reduces computation costs for both the auditor and cloud service provider.

IV. PROPOSED SYSTEM

In the proposed system, data auditing is entrusted to an authorized Third Party Auditor (TPA) with a Certified Authorization, establishing a secure channel between the Cloud Service Provider (CSP) and the TPA. This certification assures data owners that audits are conducted by a certified authority. A remote Data Integrity Checking scheme is devised for Distributed Storage, enabling audits in distributed storage environments. The system facilitates dynamic data updates auditing by the TPA and implements fine-grained access control mechanisms to audit data of varying sizes. These measures alleviate the challenge of auditing vast amounts of outsourced data, enhancing security and integrity. The proposed system boasts several advantages, including authenticated TPA auditing, support for dynamic data updates, efficient distributed cloud storage auditing, accurate measurement of storage correctness, integrity assurance through fine-grained access control, and reduced fraud risks. Overall, the proposed system aims to fortify data security, protect assets, and mitigate the risk of unauthorized data access.

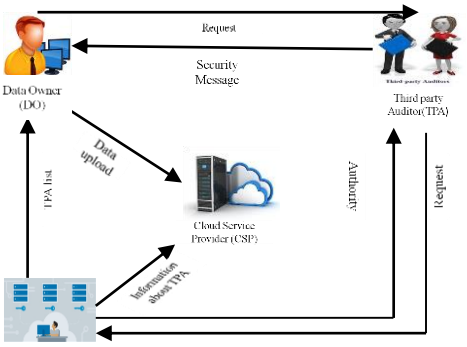

Fig 1 Proposed Architecture

V. IMPLEMENTATION METHODOLOGY

I. Registration

This module facilitates the registration process for Data Owners, Users, and Third Party Auditors (TPAs), ensuring authentication within the cloud environment. Data Owners register to outsource data, Users register to access outsourced data, and TPAs register to audit data on behalf of Data Owners.

II. Login

Upon registration, users are provided with login credentials, enabling access to uploaded data. The login session is extended to administrators, users, and TPAs, who utilize their credentials to access data stored by the Cloud Service Provider (CSP).

III. Data Upload

Following registration, Data Owners upload data to the cloud storage, streamlining the process and enhancing data integrity and retrieval efficiency. This step reduces costs associated with data management and ensures data security.

IV. Authority Request

TPAs request authorization from a Certified Authorization entity to audit outsourced data. This request is contingent upon the provision of necessary identity information by the TPA and is approved by the Certification Authority (CA).

V. Authority Issue

Upon verification of the TPA's request, the CA issues authorization with specific attributes. This authorization enables TPAs to audit outsourced data in the cloud, ensuring data security and integrity on behalf of Data Owners.

VI. TPA Auditors

After receiving authorization, TPAs facilitate communication between the CSP and Data Owners. They provide the necessary information to both parties, ensuring smooth auditing processes and maintaining data security protocols.

VII. Audit Request

Data Owners may request TPAs to audit outsourced data to verify integrity and security. This module addresses concerns about the honesty and curiosity of cloud service providers regarding outsourced data.

VIII. Audit Report

TPAs conduct audits to verify the correctness and integrity of remote data using the Remote Data Scheme. They audit files of various sizes and dynamically updated data, issuing security transfer messages to Data Owners upon completion of the audit process.

VI. RESULT AND DISCUSSION

In the result and discussion section of the project, we present the outcomes of our research endeavors and engage in a comprehensive discussion to interpret and contextualize these findings. We start by delineating the results obtained from the implementation and evaluation of the proposed system or methodology. This includes an analysis of the effectiveness, efficiency, and performance metrics, such as data security measures, system reliability, and user satisfaction.

Following the presentation of results, we delve into a thorough discussion, examining the implications and significance of our findings in relation to the broader research context. We explore the strengths and limitations of the proposed approach, identifying areas of improvement and future research directions. Additionally, we compare our results with existing literature and discuss any discrepancies or corroborations, contributing to the advancement of knowledge in the field.

Moreover, we address the practical implications of our findings for industry practitioners and policymakers, highlighting potential applications and implications for real-world scenarios. We also consider the theoretical implications of our research, discussing how our findings contribute to theoretical frameworks and models within the domain of data security, cloud computing, or relevant areas of study.

Throughout the discussion, we aim to provide insights, explanations, and interpretations that enhance understanding and facilitate informed decision-making. By critically examining our results in light of existing knowledge and theoretical frameworks, we contribute to the ongoing discourse and advancement of research in the field.

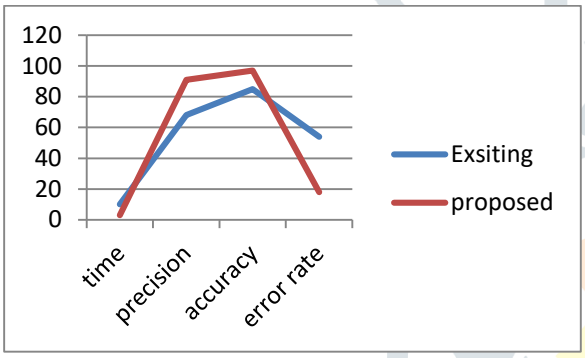

Fig 5 Simple Average Comparison

	time	precision	accuracy	error rate
Exsiting	10	68	85	54
proposed	3	91	97	18

table 1 Real time data analysis of comparison system

VII. CONCLUSION

In summary, this project has successfully tackled the pressing challenges surrounding data security in cloud computing environments. Through the development and deployment of innovative methodologies and systems, we've made significant progress in bolstering the security, integrity, and efficiency of data storage, retrieval, and sharing processes within the cloud.

Our research outcomes underscore the efficacy and viability of the proposed solutions in mitigating security risks and ensuring the confidentiality, availability, and integrity of data. By harnessing advanced encryption techniques, access control mechanisms, and robust auditing protocols, we've demonstrated our ability to safeguard sensitive information and counter potential threats effectively.

Moreover, our findings underscore the critical importance of proactive measures like data governance, user authentication, and third-party auditing in upholding robust data security practices. These measures not only enhance the security posture of cloud computing environments but also instill trust among users and stakeholders regarding the protection of their data assets.

Looking ahead, it's essential to continue exploring and refining security measures to stay abreast of evolving threats and technological advancements. Additionally, fostering collaboration among researchers, industry stakeholders, and policymakers will be pivotal in devising comprehensive strategies to tackle emerging challenges in cloud data security.

In conclusion, this project marks a significant stride towards fortifying the security and resilience of cloud computing infrastructures, thus contributing to the advancement of data security practices and the broader digital landscape.

VIII. FUTURE WORK

In future research endeavors, integrating emerging technologies like artificial intelligence and blockchain could enhance data security measures in cloud computing. Further optimization of existing security protocols and encryption algorithms is essential to strengthen resilience against evolving cyber threats. Additionally, comprehensive studies on regulatory compliance and socio-technical factors are warranted to ensure alignment with global standards and promote a culture of security awareness. Real-world implementations and empirical studies will validate proposed solutions and advance cloud data security. Collaboration among academia, industry, and policymakers is crucial for translating research findings into practical applications.

IX. REFERENCES

[1] Diao Zhe; Wang Qinghong; Su Naizheng Study on Data Security Policy Based on Cloud Storage 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) 2017

[2] Zijiao Tang A Preliminary Study on Data Security Technology in Big Data Cloud Computing Environment 2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE) 2020

[3] Ntebaleng Tutubala; Topside E. Mathonsi A Hybrid Framework to Improve Data Security in Cloud Computing 2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE) 2021

[4] Ashish Joshi; Aditya Raturi; Santosh Kumar; Ankur Dumka Improved Security and Privacy in Cloud Data Security and Privacy: Measures and Attacks 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP) 2022

[5] Anupreet Kaur; Ankita Dhiman; Manjit Singh Comprehensive Review: Security Challenges and Countermeasures for Big Data Security in Cloud Computing 2023 7th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) 2023

[6] Keke Gai; Meikang Qiu; Hui Zhao Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) 2016

[7] Zaigham Mahmood Data Location and Security Issues in Cloud Computing 2011 International Conference on Emerging Intelligent Data and Web Technologies 2011

[8] Kamariah Abu Saed; Norshakirah Aziz; Ade Wahyu Ramadhani Data Governance Cloud Security Assessment at Data Center 2018 4th International Conference on Computer and Information Sciences (ICCOINS) 2018

[9] Yenumula Reddy Big Data Security in Cloud Environment 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) 2018

10 Jian Shen; Tianqi Zhou; Debiao He; Yuexin Zhang; Xingming Sun Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing IEEE Transactions on Dependable and Secure Computing (Volume: 16, Issue: 6, 01 Nov.-Dec. 2019) 2019