Migration Letters

Volume: 21, No: S6 (2024), pp. 1608-1618

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Secure Document Sharing In Cloud By Providing Anonymity, Integrity And Privilege Depending On The Document Type

B.Angel Rubavathy[1] , Rebecca Jeyavadhanam Balasundaram[2] , S. Albert Antony Raj[3]

ABSTRACT

In the world of the technologies, cloud computing has made a great positive impact. The services offered by cloud are being used by the customers on a daily basis. Though cloud is a buzzword, the security issue has been one of the topmost concerns. The user stores his data or document in the cloud and retrieves it when needed. At many times, this data is attacked and is accessed by people who don't have access to it. This paper proposes a method, that ensures that a document is safely stored in the cloud and can only be accessed by the members who have access to it. The access rights are given to the members along with privilege constraints to access the document. The user also has the option to list out the data in the document that he wishes to share. The integrated cloud computing system comprises three key components: Cloud Service Provider (CSP), Sensitive Document Analyser, and User/Tenant Tracker. The CSP employs optimized job scheduling and a profit/loss calculator, adhering to a multi-tenancy framework for efficient resource utilization. The Sensitive Document Analyser categorizes user documents, employing encryption, OTP-based access, and a request handler for secure management. Meanwhile, the User/Tenant Tracker ensures system integrity through blockchain based verification and facilitates continuous improvement via feedback analysis. Together, these components form a robust and secure cloud infrastructure, providing advanced functionalities and safeguards for optimal user experience and data protection.

Keywords: *Cloud Computing, Security Concerns, Document Security, Multi-Tenancy Framework, Optimized Job Scheduling, Sensitive Document Analyser, User/Tenant Tracker, Blockchain Based Verification, Resource Utilization, Privilege Constraints.*

1. INTRODUCTION

The usage and applications of cloud is growing in a very rapid form. When compared to conventional and traditio[1]nal services in the field of IT, cloud computing has earned a market. Cloud computing has gained widespread popularity owing to its advantageous features such as high performance, primarily built on internet technology. Notably, the cloud proves to be economically viable, both in terms of initial setup and ongoing maintenance. Various services are offered to customers within the cloud framework, facilitated by Cloud Service Providers (CSPs). These essential services encompass Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Despite the ubiquity of the term "cloud," customers encounter several challenges in its implementation and utilization. In spite of the merits and benefits of found in the cloud technology some of the problems exist and they are under research. As the files are stored on an outsourced storage, the organizations or an individual need not update their storage capacity. There are a number of Cloud storage providers, like Amazon, Microsoft,

[1]Dept. of Comp Applications, CSH, SRMIST, Kattankulathur – 603403, INDIA.
[2]Dept. of Comp Science, York St John University London, UK.
[3]Dept. of Comp Applications, CSH, SRMIST, Kattankulathur – 603403, INDIA.

Google, Apple, etc. All these providers offer different storage services to customers. The customers can use this storage space to store documents, data or other information.

The storage cost for the storage is given to the customer and he pays for it. The cloud uses “pay-as-you-use” policy. The storage service and any other additional features that are provided to a customer will differ from one CSP to another. Mostly all the CSP’s usually provide a fixed bytes of space to the users. In general, the usual way of storage is to store the data or documents in Google drive, or in the Drop box, One drive, etc. by having a unique login credentials. Most Cloud Service Providers (CSPs) retain user files without encryption for the majority of cases.

Data stored in cloud can one of the most vital assets of an organization or for an individual. Each and every data stored may define the uniqueness of an enterprise. The data serves as the foundation for information, knowledge. Such a vital sensitive data can be used to make a decisions and act based on it. The data might cure a disease or increase an organization’s profit. The data might also be the backbone for building a business; at times this aids the customer in meeting their fixed targets, and also helps in improving the performance [1]. Apart from the vitality of the data, storing it and sharing the data is the vital services needed in the case of an organization, so as to enhance its performance [2].

Recent times the digital world has an explosive evolution of data, leading to the enterprises need to store such huge amount of data. This situation pressurised the enterprises for the need to be storing the enormous quantity of data locally [3]. The exploration of the data has also become a tiresome task due to availability of limited resources only [4]. As the cloud possess many advantages like on-demand service, scalability when more resources are added, and reliability while using cloud. Additionally, it incorporates attributes such as disaster recovery and accessibility, among others [5]. As a result, numerous organizations are transitioning to cloud computing, a technology distinguished by its extensive storage capacity and substantial computational capabilities at a notably reduced expense. Cloud users can seamlessly access a diverse array of services across various platforms, with the added benefit that the user's location and time do not affect the service provision [6].

It is possible to establish collaborations, save cost, enhance the productivity by migrating the local data management and other features of an organization to cloud by taking advantages of the cloud services offered [7]. Thus, there remain many benefits when an organization or an individual shift to cloud services [8]. In the near future there is a possibility where all the business transactions will be moved in to cloud [9]. The main hurdle to the CSPs is security. The challenges and issues of data security in cloud have attracted the attention of academicians [10, 11], the industry [12] and even the government [13]. One of the prevalent solutions has been to using cryptographic algorithms. This process uses encryption and decryption of the data for method proposed in this paper aims to provide a secure storage of data on the cloud and sharing of the same with protection measures.

2. RELATED WORKS

The organizations and individuals attracted towards the storage usage as service of cloud services. The cloud remains attractive to users, but they are not secure by nature. This is due to the reason that the store house provided for data storage is with the vendor control and the user has no control or power over it [14]. Historically, numerous surveys have been conducted on data breaches occurring at various service-oriented companies, including instances involving Apple's iCloud. Additionally, companies such as Trip Advisor and Sony Corp's online entertainment services have also experienced the impact of these breaches. Such kind of attack has made the users to think a lot before storing their data over the cloud.

Such kind of attacks was researched by a number of organizations like HPISecure [15], Twin Clouds [16], SecCSIE [17], and SecCloud [18] and they also proposed solutions. Sharing of the data in a controlled manner was made possible by the use of access control mechanisms in collaborative environments [19]. When the challenges started with sharing of data a lot of methods were proposed initially that used encryption techniques [20-25]. The fast growth of cloud could be stopped, if the security issues are not handled properly [26]. In a real time, scenario an organization may allow its employees in deploying cloud in data storage and data sharing. As far as the organization is considered the burden has been released from it when data are stored locally [27], [28]. At the same time, the organization might face many types of security threats, and this has been the leading problems of cloud users [29]. Since user data is housed in the Cloud Service Provider's (CSP) domain, the CSP becomes susceptible to targeted attacks, occasionally leading to the unauthorized disclosure of user data for financial gain [30], [31]. The prevalence of data breaches has escalated, witnessing a rise of $1.07 million attributed to the surge in remote work during the COVID-19 pandemic [32]. In response to these challenges, Kao et al. [33] introduced a model known as "uCloud," employing a user-centric key management approach to safeguard user data. Within this framework, user data is encrypted using the RSA algorithm.

3. OPTIMAL RESOURCE UTILIZATION, SECURE DOCUMENT MANAGEMENT, AND BLOCKCHAIN-ENHANCED INTEGRITY VERIFICATION

Cloud Service Providers (CSPs) are integral entities within cloud computing ecosystems, encompassing a range of sophisticated functionalities to ensure optimal resource utilization. An optimized job scheduling mechanism is implemented by the CSP, strategically allocating computational tasks across available resources. This meticulous scheduling approach aims to enhance overall system efficiency and responsiveness, mitigating potential bottlenecks in resource utilization. Furthermore, a profit/loss calculator is deployed within the CSP infrastructure. This tool facilitates financial assessments by computing the economic implications of resource allocation and service provision. This analytical capability empowers CSPs to make informed decisions, aligning their operational strategies with fiscal objectives. The integration of a profit/loss calculator adds a layer of financial intelligence to the CSP, fostering sustainable business practices within the dynamic cloud computing landscape.

Adhering to the tenant system concept, the CSP implements a multi-tenancy framework. This framework enables the concurrent hosting of multiple tenants on a shared infrastructure while ensuring logical isolation between them. By embracing the tenant system, the CSP optimizes resource utilization and provides a scalable and cost-effective solution for diverse user needs, fostering a collaborative and efficient cloud computing environment. The Sensitive Document Analyser plays a pivotal role in the secure management of user documents within cloud environments. Employing advanced categorization algorithms, the analyser differentiates between sensitive and normal documents stored over the cloud. This categorization serves as a foundation for implementing tailored security measures to protect sensitive information from unauthorized access and potential breaches.

Sensitive documents, identified through the categorization process, undergo encryption both during storage and retrieval processes. This encryption ensures that the information remains confidential and secure, mitigating the risk of data compromise. Moreover, the implementation of data privileges for each sensitive document establishes granular control over access, allowing for nuanced permission settings tailored to specific user roles. To reinforce document security, the Sensitive Document Analyser employs One-Time Password (OTP) code generation for both document owners and users seeking access.

This dual-factor authentication mechanism adds an additional layer of protection, requiring authentication from both parties before granting access or permissions. Simultaneously, a request handler facilitates communication between document owners and users, streamlining the process of access requests and permissions, ensuring a secure and seamless user experience.

The User/Tenant Tracker serves as a critical component responsible for feedback analysis and integrity verification within the cloud computing environment. Feedback analysis involves assessing user experiences and system performance, enabling the CSP to refine services based on user input. This iterative improvement loop contributes to the evolution of cloud services, aligning them with user expectations and industry standards. Integrity verification, a fundamental aspect of the User/Tenant Tracker, leverages blockchain technology. Blockchain ensures the immutability and integrity of data by creating a decentralized and tamper-resistant ledger. This approach enhances the trustworthiness of the cloud infrastructure, offering a transparent and verifiable record of activities. Through blockchain based integrity verification, the User/Tenant Tracker fosters a secure and accountable cloud computing environment, instilling confidence in users and stakeholders alike.

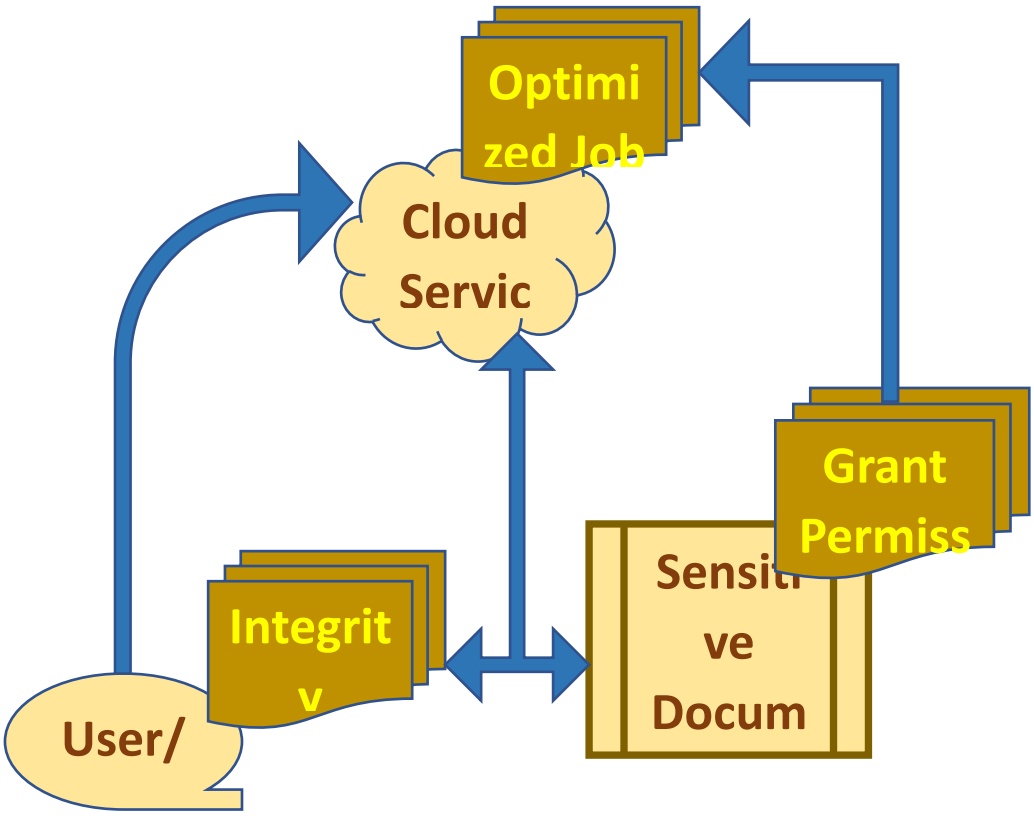


Figure 1 Architecture Diagram for Optimal Resource Utilization in Securing Document

The primary objective of the proposed approach is to enhance the security of documents stored in the cloud. The document owner has the capability to store files in the cloud and share them with other users. Consider a scenario, where the owner has stored a set of certificates over the cloud. The owner of those certificates wants to share the certificates for viewing purpose only. But the user may try to miss use the certificate. To prevent this, the proposed method tries to secure the document by maintaining and checking the integrity of the document. There are three main components present – (i) CSP, (ii) Sensitive

document analyser (3) User/ tenant tracker. The following section describes in detail about the working of the components.

3.1 OPTIMAL STORAGE

The user's document is stored on the cloud. The CSP is a third-party vendor where the user's documents are stored. The owner of the document uploads his/her document on to the cloud. The CSP has to allocate a free resource (storage space) for storing the document. The CSP uses an optimized scheduling policy to allocate a space for the storage. The CSP uses the multitenant concept for allocation. The pseudocode for the process followed is given in the pseudo code 1.

Pseudocode 1: CSP process

```
Step 1:
userDocument = uploadDocumentToCloud()
Step 2:
freeResource = allocateFreeResource()
Step 3:
allocateResourceWithSchedulingPolicy(freeResource)
Step 4:
storage = useMultitenantConcept(freeResource)
```

3.2 SECURED STORAGE

The document uploaded by the owner needs to be secured during its storage and transmission. For this a request handler is developed, it works as an automated software. The owner's document is taken for analyses by the request handler. Then the document is categorized as sensitive and non-sensitive document based on the keywords present in the document. For each sensitive document an extra security measure is carried out. These sensitive documents are encrypted and then stored over the cloud. As an extra measure, a set of data privileges are set. These data privileges lay restrictions on the document, which are set based on the person who will access the document.

The owner of the document will get the most privilege and others who use the document might get low privilege. If the user or the owner wants to access his/her document an OTP is sent. Based on the OTP authentication the owner/user can get access to the document. If another user wants to access another document, again an OTP is sent to both the owner and the current user of the document. This OTP will intimate the owner that another user is accessing his/her document. The pseudocode 2 gives the process that is executed by the request handler.

Pseudocode 2: Request handler process

```
function handleRequest(document):
if isSensitiveDocument(document):
encryptAndStore(document)
setDocumentPrivileges(document)
sendOTPToOwner(document)
sendOTPToCurrentUser(document)
else:
categorizeAsNonSensitive(document)
function isSensitiveDocument(document):
   // Perform analysis to determine if the document is sensitive
   // Return true if sensitive, false otherwise
```

```
function encryptAndStore(document):
   // Encrypt the sensitive document
   // Store the encrypted document

function setDocumentPrivileges(document):
   // Set data privileges for the sensitive document
   // Privileges may vary based on the user accessing the document

function sendOTPToOwner(document):
   // Generate and send OTP to the owner of the document
   // OTP is used for authentication to access the document

function sendOTToCurrentUser(document):
   // Generate and send OTP to the current user accessing the document
   // This OTP notifies the owner that another user is accessing the document
```

3.3 AUTOMATED TRACKER/AUDITOR

The automated tracker refers to a software designed for periodic audits of data stored in the cloud. Each document stored in the cloud receives a unique hash value, and a backup copy is created using blockchain technology to ensure document integrity. The primary objective is to safeguard and maintain the integrity of shared documents. To achieve this, a periodic audit is conducted on the document, comparing the hash value of the cloud-stored document with the backup copies stored using blockchain. Matching values confirm the document's authenticity and unaltered state, while differing values indicate document alteration. In the event of a mismatch, signaling potential tampering, the owner is promptly notified. Subsequently, a backup copy is utilized to ensure the availability of the original document. Additionally, a Machine Learning (ML) model is developed to identify documents facing constant malicious threats, particularly those containing highly sensitive data. These identified documents undergo more frequent audits as part of enhanced protection measures. The pseudocode outlining the tracker process is provided below.

Pseudocode 3: Automated tracker process

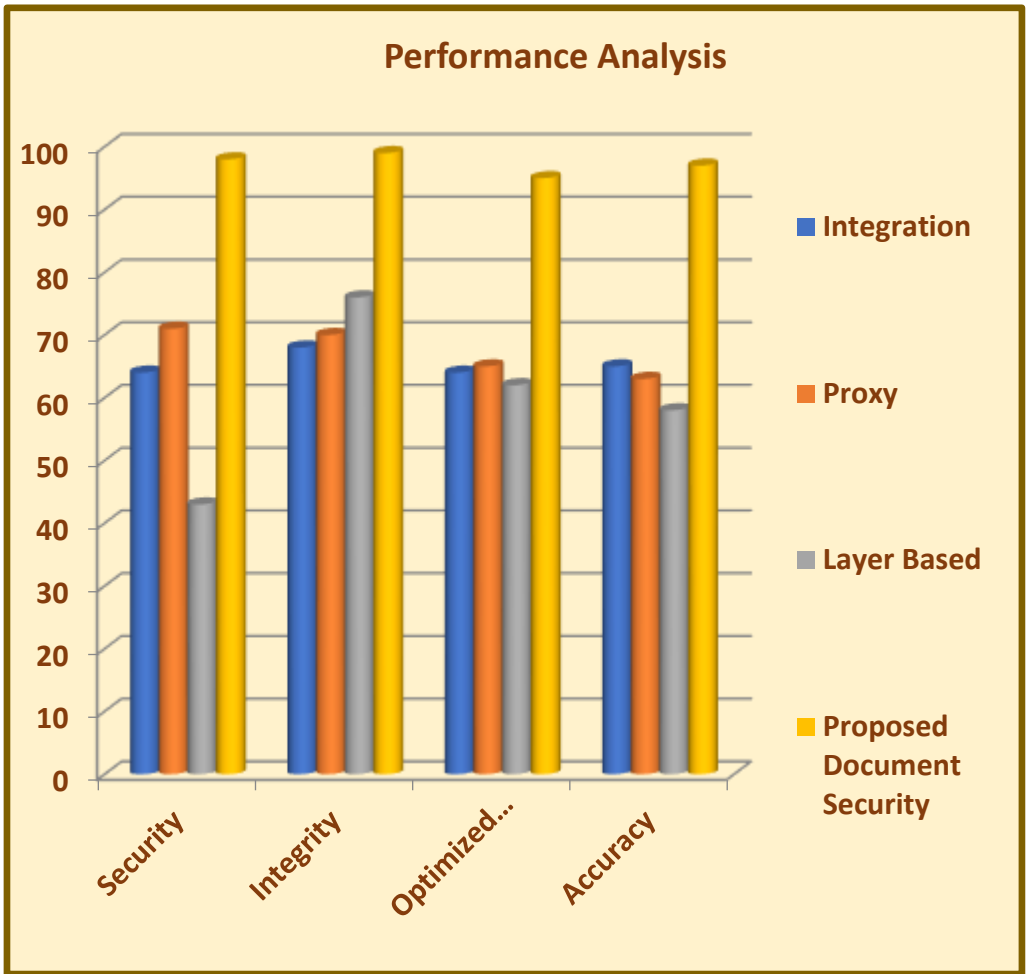
```
// Periodical audit using automated software
periodicalAudit() {
documents = getSensitiveDocuments() // Get all sensitive documents stored in the cloud

for each document in documents {
createBackup(document) // Create a backup copy for each sensitive document}
performPeriodicAudit(documents) // Perform a periodic audit over the documents stored in the cloud
for each document in documents {
validateBackup(document) // Check the hash value of the document stored in the cloud with the backup copies using blockchain }
maliciousDocuments= identifyMaliciousDocuments() // Identify documents with constant malicious threats using a machine learning model
for each maliciousDocument in maliciousDocuments {
if isSensitive(maliciousDocument) {
performMoreFrequentAudit(maliciousDocument) // Carry out the audit more often for sensitive documents with constant malicious threats  }
  }
performExternalAudit() // Perform an external audit with higher frequency}
createBackup(document) {
  // Create a backup copy using blockchain concept
```

```
  // Store the backup copy}

performPeriodicAudit(documents) {
  // Perform a periodic audit over the documents stored in the cloud
  // Check the integrity and security of the documents}
validateBackup(document) {
  // Retrieve the backup copies of the document using blockchain
  // Check the hash value of the document stored in the cloud with the backup copies}

identifyMaliciousDocuments() {
  // Use a machine learning model to identify documents with constant malicious threats
  // Return the identified malicious documents}
isSensitive(document) {
  // Check if the document is sensitive
  // Return true if the document is sensitive, false otherwise}
performMoreFrequentAudit(document) {
  // Carry out the audit more often for the sensitive document with constant malicious
threats}
performExternalAudit() {
  // Perform an external audit with higher frequency}
```

4. RESULT ANALYSIS

The performance of the proposed method is compared with other existing methods. The comparison graph is depicted in figure 1. As it can be derived from the graph, the performance is enhanced in the proposed method. Experimental results analysis and performance evaluation of the integrated cloud computing framework revealed commendable outcomes across various dimensions. In the realm of resource utilization, the optimized job scheduling implemented by the Cloud Service Provider (CSP) demonstrated a significant reduction in task completion times and improved overall system responsiveness.

The profit/loss calculator exhibited precise financial assessments, enabling the CSP to make informed decisions aligning with fiscal objectives. Moreover, the multi-tenancy framework contributed to efficient resource sharing among tenants, validating its efficacy in accommodating diverse user needs. The Sensitive Document Analyser's experimental results underscored its effectiveness in accurately categorizing documents, with minimal false positives or negatives. Encryption during storage and retrieval processes demonstrated robust security measures, and the implementation of OTP-based access and the request handler streamlined document management. Performance metrics, such as access latency and request processing times, indicated that the security measures did not compromise overall system efficiency.



Graph 1 Performance Analysis Graph

Performance Analysis	Integration	Proxy	Layer Based	Proposed Document Security
Security	64	71	43	98
Integrity	68	70	76	99
Optimized Scheduling	64	65	62	95
Accuracy	65	63	58	97

Table 1 Performance Analysis Table

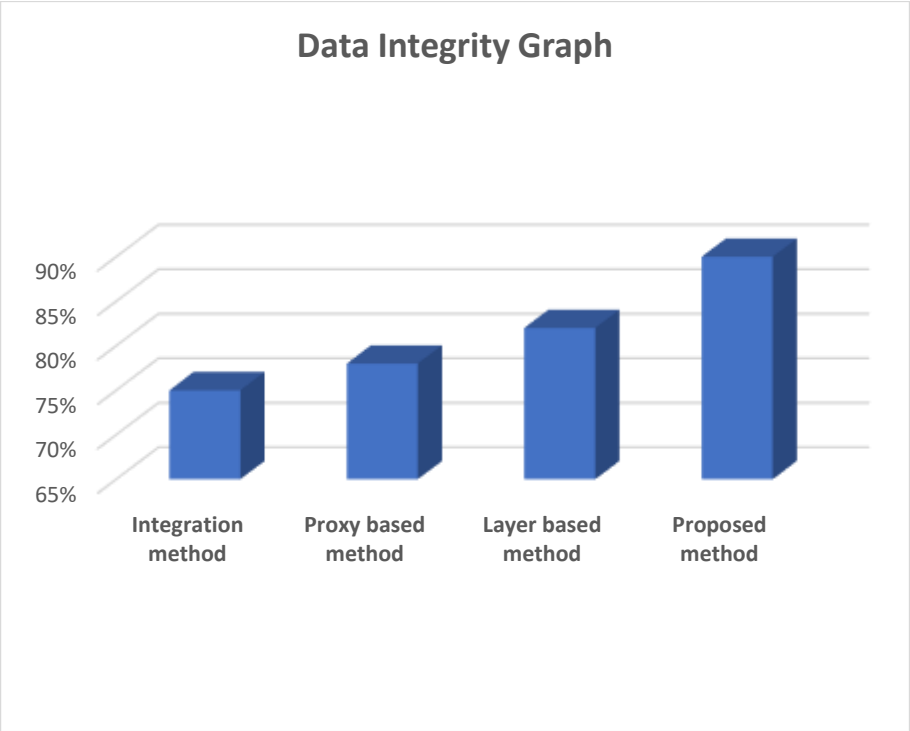


Figure 1 Comparison graph depicting the performance

The User/Tenant Tracker's feedback analysis revealed iterative improvements, incorporating user input to enhance service quality. Blockchain based integrity verification exhibited resilience against tampering, ensuring an unassailable record of activities. Performance analysis of this component highlighted negligible overhead in terms of verification times, emphasizing the seamless integration of blockchain technology without compromising system responsiveness. In exploring advanced algorithms for job scheduling, incorporating machine learning for more nuanced document categorization, and optimizing blockchain implementation for even faster integrity verification could further elevate the overall performance and capabilities of this integrated cloud computing framework.

5. CONCLUSION

In conclusion, the amalgamation of the Cloud Service Provider, Sensitive Document Analyser, and User/Tenant Tracker constitutes a comprehensive and robust cloud computing ecosystem. This integrated framework not only optimizes resource utilization and ensures the secure management of sensitive documents but also incorporates blockchain technology for integrity verification. The collaborative synergy of these components enhances the overall efficiency, security, and user experience within the cloud environment. Looking ahead, future enhancements could explore the integration of artificial intelligence for more sophisticated document categorization and predictive resource allocation, further advancing the capabilities of this integrated cloud computing framework.

6. REFERENCES

[1] A. K. Singh and I. Gupta, ``Online information leaker identificationscheme for secure data sharing," Multimedia Tools Appl., vol. 79, no. 41,pp. 31165_31182, Nov. 2020.
[2] E. Zaghloul, K. Zhou, and J. Ren, ``P-MOD: Secure privilege-based multilevelorganizational data-sharing in cloud computing," IEEE Trans. BigData, vol. 6, no. 4, pp. 804_815, Dec. 2020.

[3] I. Gupta and A. K. Singh, ``GUIM-SMD: Guilty user identification modelusing summation matrix-based distribution," IET Information. Security., vol. 14, no. 6,pp. 773_782, Nov. 2020.
[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ``Enabling identity-basedintegrity auditing and data sharing with sensitive information hiding forsecure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2,pp. 331_346, Feb. 2019.
[5] I. Gupta and A. K. Singh, ``An integrated approach for data leaker detectionin cloud environment," J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993_1005,Sep. 2020.
[6] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ``A lightweight securedata sharing scheme for mobile cloud computing," IEEE Trans. CloudComputing., vol. 6, no. 2, pp. 344_357, Apr. 2018.
[7] I. Gupta, N. Singh, and A. K. Singh, ``Layer-based privacy and securityarchitecture for cloud data sharing," J. Communication. Software. System., vol. 15, no. 2,pp. 173_185, Apr. 2019.
[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You,``An efficient attribute-based encryption scheme with policy update in cloud computing," IEEE Trans. Ind. Information., vol. 15, no. 12,pp. 6500_6509, Dec. 2019.
[9] C. Suisse. (2017). 2018 Data Center Market Drivers: Enablers BoostingEnterprise Cloud Growth. Accessed: May 19, 2019. [Online]. Available:https://cloudscene.com/news/2017/12/2018-data-center-predictions/
[10] Armbrust, M.. A. Fox, R. Griffith, A. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the Clouds: A BerkeleyView of Cloud Computing. Technical Report No UCB/EECS-2009-28, University ofCalifornia at Berkley, USA, 10 February, 2009.
[11]. Buyya, R., C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, “Cloud Computing andEmerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5thUtility”. – In: Future Generation Computer Systems. Amsterdam, The Netherlands, ElsevierScience, 2009.
[12]. Kaufman, L.M, “Data Security in the World of Cloud Computing”. – IEEE Security and Privacy,Vol. **7**, 2009, No 4, pp. 61-64.
[13]. Mell, P., T. Grance, “Effectively and Securely Using the Cloud Computing Paradigm”. NIST,Information Technology Laboratory, 2009.
[14] M. Lori, "Data security in the world of cloudcomputing," Co-published by the IEEE Computer Andreliability Societies, pp. 61-64, 2009.
[15] E. Saleh and C. Meinel, "HPISecure: Towards DataConfidentiality in Cloud Applications," in Cluster,Cloud and Grid Computing (CCGrid), 2013 13thIEEE/ACM International Symposium on, 2013, pp. 605-609.
[16] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider,"Twin clouds: An architecture for secure cloudcomputing," in Workshop on Cryptography and Securityin Clouds (WCSC 2011), 2011
[17] R. Seiger, S. Groß, and A. Schill, "SecCSIE: a securecloud storage integrator for enterprises," in Commerceand Enterprise Computing (CEC), 2011 IEEE 13thConference on, 2011, pp. 252-255
[18] L. Wei, H. Zhu, Z. Cao, W. Jia, and A. V. Vasilakos,"Seccloud: Bridging secure storage and computation incloud," in Distributed Computing Systems Workshops(ICDCSW), 2010 IEEE 30th International Conferenceon, 2010, pp. 52-61.
[19] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, "Accesscontrol in collaborative systems," ACM ComputingSurveys (CSUR), vol. 37, pp. 29-41, 2005
[20] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improved proxy re-encryption schemes withapplications to secure distributed storage," ACMTransactions on Information and System Security(TISSEC), vol. 9, pp. 1-30, 2006.
[21] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicyattribute-based encryption," in Security andPrivacy, 2007. SP'07. IEEE Symposium on, 2007, pp.321-334.
[22] R. Canetti and S. Hohenberger, "Chosen-ciphertextsecure proxy re-encryption," in Proceedings of the 14thACM conference on Computer and communicationssecurity, 2007, pp. 185-194.
[23] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, 2006, pp. 89-98.
[24] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, pp. 355-370, 2014.
[25] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology–EUROCRYPT 2005, ed: Springer, 2005, pp. 457-473.
[26] I. Gupta and A. K. Singh, ``A framework for malicious agent detectionin cloud computing environment," International Journal Advanced Science Technology., vol. 135,pp. 49_62, Feb. 2020.
[27] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, and K.-R. Choo, ``Fuzzyidentity-based data integrity auditing for reliable cloud storage systems,"IEEE Trans. Dependable Secure Computing., vol. 16, no. 1, pp. 72_83,Jan./Feb. 2019.

[28] I. Gupta and A. K. Singh, ``A probabilistic approach for guilty agentdetection using bigraph after distribution of sample data," Proc. Computing Sci., vol. 125, pp. 662_668, Jan. 2018.
[29] L. Zhang, Y. Cui, and Y. Mu, ``Improving security and privacy attributebased data sharing in cloud computing," IEEE Syst. J., vol. 14, no. 1,pp. 387_397, Mar. 2020.
[30] I. Gupta and A. K. Singh, ``Dynamic threshold based information leakeridentification scheme," Inf. Process. Lett., vol. 147, pp. 69_73, Jul. 2019.
[31] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, ``An efficient file hierarchy attribute-based encryption scheme in cloud computing,"IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1265_1277,Jun. 2016.
[32] Alarming Cyber Security Facts to Know for 2021 and Beyond.[Online]. Available: https://www.cybertalk.org/2021/12/02/alarmingcyber-security-facts-to-know-for-2021-and-beyond/
[33] Y. Kao, K. Huang, H. Gu, and S. Yuan, ``UCloud: A user-centric keymanagement scheme for cloud data protection," IET Inf. Secur., vol. 7,no. 2, pp. 144_154, Jun. 2013.