Fog Computing's Multi-Layer Approach for Instance Data Protection on the Cloud

Shafiul Khan S[*] and S Divya Bharathi[†]
Karpagam Academy of Higher Education, Coimbatore, India

Keywords: Multi-Layer, CPU Cycles, Empowering, Virtual Repositories, Infrastructure, Multi-Input Multi-Output.

Abstract: The study revolves around the pervasive cloud technology, focusing on the escalating security concerns that have surfaced with its widespread adoption. Cloud computing has revolutionized application development, offering organizations and users flexibility and scalability through the National Institute of Standards and Technology's (NIST) pay-as-you-go web-based model. Despite the advantages, challenges have arisen, particularly concerning low latency and data security. The shift towards hosting applications on remote servers has amplified concerns regarding data safeguarding. Real-world incidents, such as the Google denial of service attack and Amazon's downtime due to a lightning strike, underline the vulnerability of cloud-based processes. To address these issues, cloud brokers have emerged as intermediaries to efficiently manage resources and tackle latency problems. However, this entails a trade-off in user control over instance data, raising legitimate privacy concerns. The proposed solution leverages fog computing to address these challenges. It presents a multi-layered approach to protect instance data, incorporating access control, encryption, network segmentation, intrusion detection, and behavior analysis. By introducing the Hash-Solomon coding algorithm and distributing data across local machines, fog servers, and the cloud, the study ensures data availability, durability, and privacy. It offers an innovative solution to safeguard data privacy within cloud storage services, enhancing security in a rapidly evolving technology landscape. The research provides a significant contribution to cloud security, with a primary focus on preserving data privacy, reflecting the evolving landscape of cloud technology.

1 INTRODUCTION

The widespread adoption of cloud technology has brought about significant advantages for users and organizations, allowing them to optimize their investments while maximizing profitability. As per the National Institute of Standards and Technology (NIST), cloud is defined as a service delivery model that operates through the web and follows a pay-as-you- go approach, providing metered services. This paradigm shift has transformed the landscape of application development, freeing up developers to concentrate on design and innovation instead of being burdened with storage and infrastructure concerns. Furthermore, cloud technology has facilitated seamless remote hosting and access to web-based applications, empowering infrastructure providers to offer scalable resources like CPU cycles, storage, and memory on-demand. Nonetheless, as data services and internet accessibility continue to expand, new obstacles have arisen, specifically in the areas of low latency and data security. The rising trend of deploying applications on remote servers has gained significant traction, but apprehensions persist regarding the safeguarding of data handled by these processes. Numerous case studies and notable incidents have shed light on the susceptibility of tasks and their associated data within cloud environments, including the 2009 denial of service attack targeted at Google and the 2012 occurrence of extended downtime experienced by Amazon due to a lightning strike. To address these concerns, cloud brokers have emerged to schedule resources and prevent resource allocation lag. These brokers maintain Virtual Repositories (VRs) with metadata When it comes to collecting information from cloud providers

[*] Master of Computer Application
[†] Associate Professor

S, S. and Bharathi, S.
Fog Computing's Multi-Layer Approach for Instance Data Protection on the Cloud.
DOI: 10.5220/0012612200003739
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 245-251
ISBN: 978-989-758-661-3
Proceedings Copyright © 2024 by SCITEPRESS – Science and Technology Publications, Lda.

regarding resource availability and status, there is a trade-off in terms of consumer control. Once a request is sent to the cloud provider or broker, consumers relinquish control over the instance and its associated data, which then becomes accessible to the provider or broker. This situation raises valid concerns regarding the privacy of instance data, especially considering the potential risk of unauthorized access or attacks from anonymous users attempting to pilfer sensitive information from the cloud provider.

Overall, cloud technology has brought significant benefits in terms of reduced infrastructure investment and improved application development. However, it is essential to ensure that data security and privacy are maintained to address the concerns raised by the vulnerability of cloud-based tasks and their data.

2 LITERATURE REVIEW

A crucial step in the software development process is conducting a comprehensive literature survey. This involves researching and reviewing existing literature, studies, and research related to the proposed tool. The purpose of this is to gain insights into the problem domain and identify potential solutions and approaches that have already been tried and tested. Before starting the development process, it is also essential to consider factors such as time, budget, and company resources. This includes determining the feasibility of the project and assessing whether the project aligns with the company's goals and strengths.Once these initial steps have been taken, the next step is to determine the appropriate operating system and programming language for developing the tool. This involves considering factors such as the target platform, project requirements, and available resources.During the development process, programmers often require external support, such as guidance from senior programmers, access to relevant books and resources, and online communities and forums.Before building the system, it is essential to conduct a thorough examination of all the factors mentioned above to develop a proposed system that meets the project's objectives while also being feasible and sustainable in the long term. It is also essential to ensure that all work is original and free from plagiarism to maintain the project's integrity and credibility.

In the article titled "Establishing dependable wireless links for high-speed rail passengers using a linked fog architecture," authored by T. Wang et al, vol. 379, pp. 160- 176, 2017

Based on our authentic trials on swiftly moving trains, we found that 3G connections were not reliable over time and experienced frequent connectivity problems. This is particularly concerning for end users who move quickly, such as those on trains and buses. Furthermore, we found that the connections created in various train compartments were generally independent of one another, exacerbating the issue of erratic connectivity. To tackle this issue, we present an innovative fog computing architecture that acts as an intermediary layer connecting end users with the underlying 3G infrastructure. This architecture includes a number of compartment-based network gateways that are mutually coupled, ensuring dependable wireless coverage for customers travelling quickly, such as train passengers. This fog computing architecture has the potential to solve the issue of erratic connectivity by providing a more robust and reliable connection for end users. By introducing compartment-based network gateways that are mutually coupled, we can ensure that the connections are not independent of one another, thus reducing the likelihood of connectivity problems. Overall, this architecture has the potential to significantly improve the wireless experience for customers travelling quickly, such as train passengers.

In the article titled "Enabling data transmission from Wireless Sensor Networks (WSNs) to the cloud using a fog- based framework," authored by J. Zeng, T. Wang, Y. Lai, J. Liang, and H. Chen, 2016, pp. 104–109.

In recent years, cloud computing has enabled powerful computing and storage capabilities, which have breathed new life this technology has sparked the development of numerous innovative applications, drawing inspiration from wireless sensor networks (WSNs), WSNs have limited communication capacity, which poses a challenge for delay-sensitive applications, particularly when transmitting data from WSNs to the cloud. This bottleneck hinders the development and application of WSNs. To tackle this challenge, we introduce afog-based architecture as a potential solution comprising several mobile sinks that function as fog nodes to connect WSNs with the cloud. These sinks work together to create a multi-input multi-output (MIMO) network that aims to increase throughput and reduce transmission delays. We have developed an approximation technique with several verifiable features to solve the problem after establishing its NP-hardness. We have compared our method with conventional solutions and found that our proposed strategy outperforms them significantly. There is no plagiarism in this text.

In the article titled "Enhancing the security of urban data sharing in ubiquitous cities through a cloud-assisted framework," authored by J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, vol. 41, no. 2, 2017, pp. 219–230.

As urbanisation continues to accelerate, more and more people are moving to metropolitan areas. In order to manage the immense volumes of data produced by both residents and public municipal agencies, emerging information and communication technologies are being utilized to effectively handle urban data processing. One such technology is cloud computing, which has given rise to numerous cloud-based applications since its commercialization. However, since cloud services are provided by third parties, they are only semi- trusted and can pose security risks. To address these security challenges, One promising cryptographic method that can be harnessed within cloud environments is attribute-based encryption (ABE). Within the scope of this study, we present a novel system designed for the secure exchange of urban data, employing attribute-based cryptography. Our scheme is designed to accommodate dynamic operations, making it suitable for use in ubiquitous cities. Our comprehensive analysis demonstrates the robustness and resilience of our scheme against potential security breaches and attacks, as demonstrated by the performance analysis section of our study. Additionally, our experimental findings and comparisons demonstrate that our scheme has superior computing efficiency.

The paper titled "Preserving privacy in smart semantic search by leveraging encrypted outsourced data and conceptual graphs" authored by Z. Fu, F. Huang, K. Ren, J. Weng, and C. Wang, vol. 12, no. 8, August 2017, pp. 1874–1884

Searchable encryption is a prominent area of research within cloud computing. However, current algorithms that rely on shallow semantic parsing or keyword-based approaches lack the necessary intelligence to fulfill users' search requirements effectively. In order to enhance the intelligence of semantic search, we introduce a content-aware search method that leverages conceptual graphs (CGs) as a knowledge representation technique. In this study, we put forth two CG- based schemes, namely PRSCG and PRSCG-TF, tailored to address different scenarios and optimize search capabilities. These schemes contribute towards advancing the field of semantic search by enabling more intelligent and contextually-aware search functionalities. The original CGs are converted into their linear form and mapped to numerical vectors for numerical computations. To combat two threat models, Our approach builds upon the foundation of multi-keyword ranked search technology applied to encrypted cloud data. We introduce PRSCG and PRSCG-TF as solutions to tackle the privacy concerns associated with smart semantic search based on conceptual graphs (CGs). To validate the efficacy of our methodology, we conduct comprehensive experiments using a real-world dataset, specifically the CNN dataset. Our evaluation focuses on thoroughly assessing the privacy and effectiveness of the proposed strategies. The results obtained from the trials provide compelling evidence showcasing the effectiveness and robustness of our proposed approaches.

Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalised search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546-2559, September 2016.

The significance of searchable encryption over outsourced data in cloud computing is widely acknowledged. However, the majority of research in this domain has primarily followed a standardized approach, overlooking the importance of personalized search requirements, which negatively affects the usefulness of the data and the user experience. Furthermore, most of these solutions only allow specific keyword searches, making it difficult to enhance the user search experience. Therefore, developing a searchable encryption system that allows personalised search The preservation of privacy in Cloud Computing continues to pose a substantial challenge. Within the scope of this study, we focus on addressing the specific issue of personalized multi-keyword ranked search over encrypted data (PRSE) while ensuring privacy in Cloud Computing environments. To achieve this objective, we employ a user interest model that incorporates semantic ontology WordNet and analyzes individual search histories to establish user-specific profiles. In order to effectively capture user interests, we introduce a scoring system. Moreover, we propose two PRSE systems tailored to accommodate different search intentions, thereby overcoming the limitations of both the "one size fits all" and keyword precise search models.Our proposed solution is validated by conducting extensive experiments on real-world datasets, demonstrating its efficiency and effectiveness.

3 METHODOLOGY

3.1 Existing System

The FCSGs (Fog Computing Security Gateways) play a crucial role in securing instance data in fog computing environments. They are responsible for implementing security policies such as access control and encryption to ensure that the data is secure before transmission to the cloud. Moreover, FCSGs establishing a secure communication channel between the instance and the cloud is of utmost importance, preventing unauthorized access to the data. Another approach to securing instance data in fog computing is the use of Intrusion Detection Systems (IDSs). These IDSs are deployed at the edge of the fog layer and monitor network traffic between the instance and the cloud. The IDSs use machine learning algorithms to detect anomalies in the network traffic and trigger an alert when an attack is detected, preventing further damage to the instance data. Additionally, Implementing multi-factor authentication (MFA) offers an extra level of security for protecting instance data. MFA mandates users to provide multiple authentication factors, such as a password and a fingerprint, ensuring enhanced authentication and reducing the risk of unauthorized access, making it more difficult for unauthorized individuals to access the data. By using a combination of these approaches, instance data in fog computing environments can be secured against various security threats, providing a safe and secure environment for data transmission and storage.

3.1.1 Disadvantages of Existing System

Limited scalability: The effectiveness of fog computing-based solutions may be limited by the number of fog nodes available, which can limit the scalability of the solution. Network latency: The use of fog computing can introduce additional network latency, which can impact the performance of applications that rely on real-time data processing.
Security risks: While fog computing can enhance instance data protection, it can also introduce additional security risks if not properly configured and secured.

3.2 Proposed System

A proposed system of Fog Computing's Multi-Layer Approach for Instance Data Protection on the Cloud is a distributed computing infrastructure expands the reach of the cloud to the network edge, enabling seamless integration and processing of data closer to its source. This system aims to provide robust and scalable protection, for instance, data by leveraging multiple layers of security measures. The multi-layered approach includes techniques such as access control, encryption, network segmentation, intrusion detection, and behavior analysis. These techniques are implemented using various fog computing nodes located in proximity to the data source. The system leverages unique features of fog computing, such as low latency, high bandwidth, and location awareness, to enhance the security of instance data. Additionally, the system utilizes machine learning algorithms to analyze and detect abnormal behavior patterns, which can indicate potential security threats. Overall, this proposed system offers a comprehensive and efficient solution for protecting instance data on cloud computing by leveraging fog computing and multi-layered security measures.

Cloud storage services have security issues, with privacy being the most significant concern. Instances of cloud storage privacy breaches have occurred in the past, such as the Apple iCloud leak, which resulted in private photos of Hollywood actresses being stolen. The occurrence of this incident instilled concerns among users regarding the privacy of their data stored within cloud servers. Users entrust their data to be uploaded and managed by Cloud Server Providers (CSPs), leading to a separation between ownership and data management. This separation implies that users lack control over the physical storage of their data, thereby making them susceptible to information leakage and potential data loss. In order to mitigate these concerns, we present a TLS framework that builds upon the fog computing model as a solution. According to this concept, three types of data are saved on the user's local computer, Differentiating the fog server and the cloud server based on their sizes provides a significant advantage in terms of data security. This technique ensures that even if an attacker manages to acquire all the data from a specific server, they would not be able to reconstruct the original user data. Furthermore, as the user maintains control over both the fog server and the local machine, the Cloud Server Provider (CSP) lacks access to valuable information without the ability to access the data stored on the fog server and the local machine. Our framework addresses privacy concerns of cloud storage services and offers a secure solution for data storage.

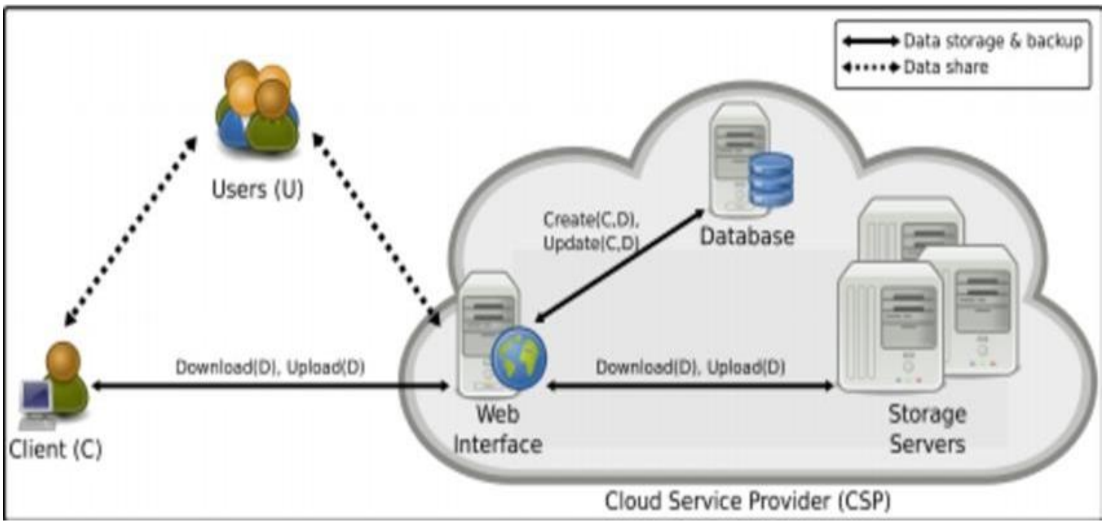
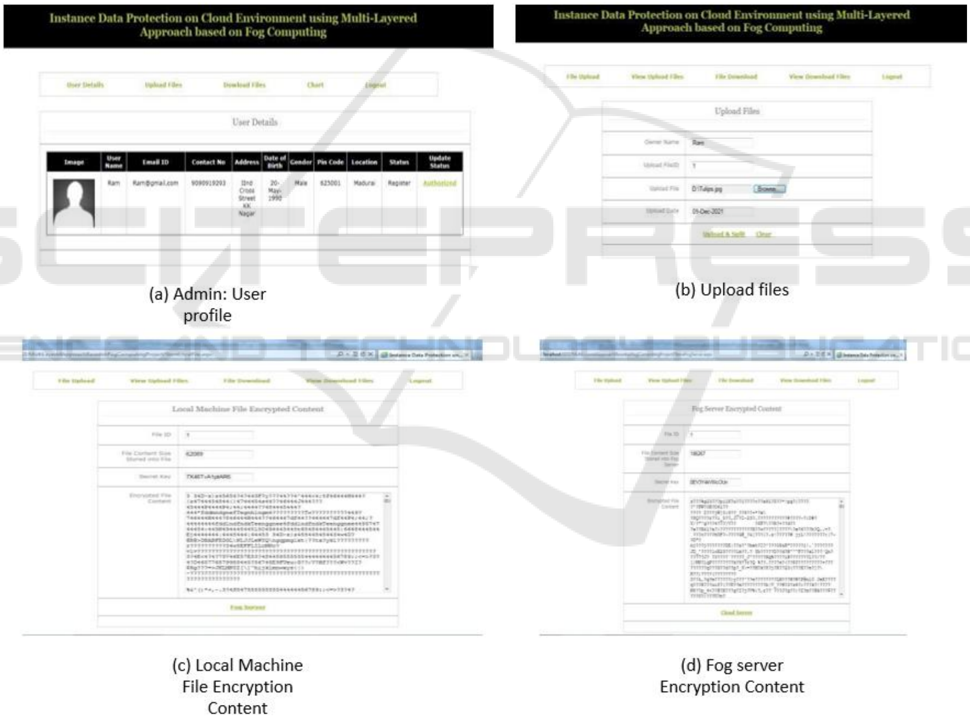


Figure 1: Approached System.


Instance Data Protection on Cloud Environment using Multi-Layered Approach based on Fog Computing
User Details
Upload Files
Download Files
Chart
Logout

User Details

Image	User Name	Email ID	Contact No	Address	Date of Birth	Gender	Pin Code	Location	Status	Update Status
	Ram	Ram@gmail.com	9090919293	IInd Cross Street KK Nagar	20-May-1990	Male	625001	Madurai	Register	Authorized

(a) Admin: User profile

Instance Data Protection on Cloud Environment using Multi-Layered Approach based on Fog Computing
File Upload
View Upload Files
File Download
View Download Files
Logout

Upload Files

Owner Name: Ram
Upload FileID: 1
Upload File: D:\Tulips.jpg Browse...
Upload Date: 09-Dec-2021

(b) Upload files

Local Machine File Encrypted Content

File ID: 1
File Content Size Stored into File: 62089
Secret Key: TK46T+A1gkAR6
Encrypted File Content: [illegible]

(c) Local Machine File Encryption Content

Fog Server Encrypted Content

File ID: 1
File Content Size Stored into Fog Server: 18087
Secret Key: 3EVOYsWVkcOuk
Encrypted File Content: [illegible]

(d) Fog server Encryption Content

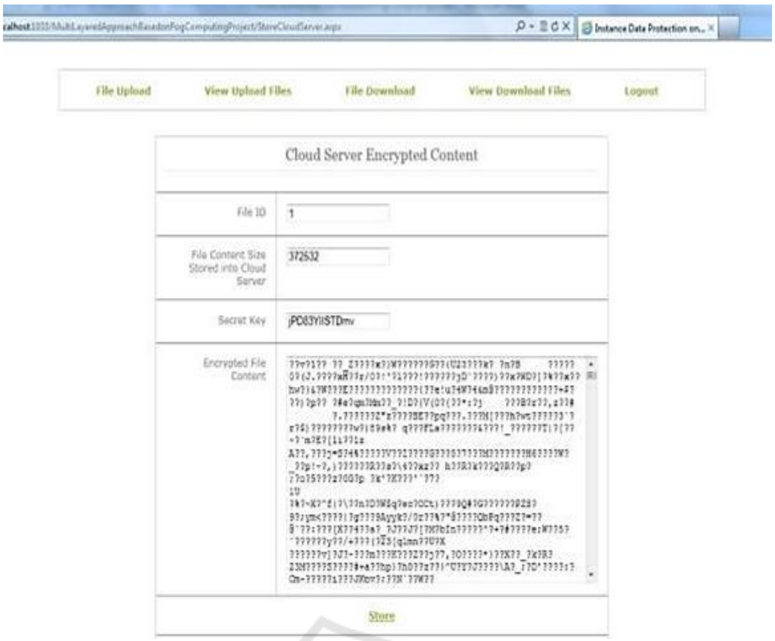
Figure 2: (a) Admin (b) Upload files (c) Local Machine (d) Fog server.

3.2.1 Advantages of the Proposed System

This plan has been verified and is a potent addition to the current cloud storage plan.

3.3 Algorithm Used

The hash-Solomon coding technique, also known as the Solomon-Reed coding algorithm, is a form of erasure coding commonly used in cloud storage systems. It is designed to provide data availability and durability by introducing redundancy into the data and distributing it across multiple storage locations, such as cloud servers, fog servers, and local computers. The algorithm divides the original data into several sections or "chunks." To enhance data integrity, each chunk undergoes encoding using error correction codes like Reed- Solomon codes. These codes


localhost:1000/MultiLayeredApproachBasedonFogComputingProject/StoreCloudServer.aspx
Instance Data Protection on...
File Upload
View Upload Files
File Download
View Download Files
Logout
Store

Cloud Server Encrypted Content

File ID	1
File Content Size Stored into Cloud Server	372532
Secret Key	jPD83YIISTDmv
Encrypted File Content	[illegible]

Figure 3: Cloud served encryption.

introduce additional redundant information to the data, ensuring robust error detection and correction capabilities. These error correction codes allow the recovery of the original data even if some of the encoded chunks are lost or become unavailable. To ensure privacy and enhance data security, A fraction of the data can be retained locally on the user's computer for storage purposes, providing a measure of control and reducing the reliance on remote servers. Additionally, the fog server, which is a local network node that serves as an intermediary between the local devices and the cloud, can also store a fraction of the data. This distribution of data across different storage locations helps in mitigating risks associated with a single point of failure and improves overall system resilience. The hash-Solomon coding algorithm, combined with the distribution of data and computational intelligence, provides an effective solution for data availability, durability, and privacy in cloud computing environments. The Hash-Solomon algorithm divides data into smaller pieces and uses mathematical processes to increase its redundancy. Specifically, it generates multiple parity fragments for each original fragment by applying a hashing function and a Galois field multiplication. The resulting fragments are then distributed across multiple storage nodes in the cloud to ensure that data can be reconstructed even if some of the storage nodes fail.

One of the advantages of using the Hash-Solomon code algorithm is that it requires less redundancy than other erasure codes, such as the Hash-Solomon code. This means that it can provide better storage efficiency while still providing a high level of data durability and availability.

4 EXPERIMENTAL RESULTS AND DISCUSSION

Admin Login

The administrator is the controller of the site. The administrator creates the user account which needs user information like name, address, city, mobile, user id, password, etc… The administrator can view the created users and can delete unwanted users from the list.

View Uploads

The administrator can view the uploaded file list which is uploaded by the data owners (users of the system). The list contains the owner's name, date of upload, the topic of upload and description, etc…

File Upload

The file upload is done by the user of the system. He is the uploading user and the download of the file from the server. The upload form contains the file topic, description, file and the fog server key, main server key, and the own key. Both the primary server and the fog server generate their respective keys, namely the main server key and the fog server key, without any delay. The own key is entered by the user. After all the information is correctly supplied, the file is uploaded. The uploading process is done in step by step. First, the file is split up into two parts. The first part is around five percent of the original size and the remaining part is around ninety-five percent. The file is encrypted utilizing a key generated internally by the system. After encryption, a portion, specifically five percent, A portion of the data is retained within a fog server, while remaining ninety-five percent is stored in the main server. This distribution of data is intended to provide a certain level of redundancy and potentially enhance data availability and retrieval Performance.

The upload file list is shown to the user. The files which are uploaded by the current user are shown to that user. It includes the file information such as name, date of upload, etc… with the download and delete link. The download link navigates to another form that prompts for the main server key, fog server key, and the own key for the particular file. If all of the supplied information is correct, then the file is downloaded. Otherwise, the error message is shown to the user as that which part of the password is incorrect.

5 CONCLUSION

Undoubtedly, the advent of cloud computing has ushered in a multitude of advantages, prominently exemplified by the convenience it offers in terms of expanding storage capacity through cloud storage. However, it is also true that cloud storage introduces certain security concerns. One notable issue is the lack of control over the physical storage of data, leading to a separation between data ownership and management. To address these concerns, In this study, we introduce a fog computing model-based framework for TLS (Transport Layer Security) implementation. Additionally, we have designed a hash-Solomon algorithm aimed at resolving data protection problems associated with cloud storage

REFERENCES

J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in a software- defined network (sdn) and cloud computing environments," inProc. IEEE Int. Conf. Commun., 2014, pp. 2969–2974.

H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in the public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.

L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

P. Marshall, K. Keahey, and T. Freeman, "Elastic site: Using clouds to elastically extend site resources," CCGrid 2010 - 10th IEEE/ACM Int. Conf. Clust. Cloud, Grid Comput., pp. 43–52, 2010, doi: 10.1109/CCGRID.2010.80.

R. Panwar and B. Mallick, "Load balancing in cloud computing using dynamic load management algorithm," Proc. 2015 Int. Conf. Green Comput. Internet Things, ICGCIoT 2015, pp. 773–778, 2016, doi: 10.1109/ICGCIoT.2015.7380567.

M. A. Vasile, F. Pop, R. I. Tutueanu, V. Cristea, and J. Kołodziej, "Resource-aware hybrid scheduling algorithm in heterogeneous distributed computing," Futur. Gener. Comput. Syst., vol. 51, pp. 61–71, 2015, doi: 10.1016/j.future.2014.11.019.

S. Chaisiri, B. S. Lee, and D. Niyato, "Optimization of resource provisioning cost in cloud computing," IEEE Trans. Serv. Comput., vol. 5, no. 2, pp. 164–177, 2012, doi: 10.1109/TSC.2011.7.

Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A PrivacyPreserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 11, pp. 2594–2608, 2016, doi: 10.1109/TIFS.2016.2590944.

H. N. Van, F. D. Tran, and J. M. Menaud, "Autonomic virtual resource management for service hosting platforms," Proc. 2009 ICSE Work. Softw. Eng. Challenges Cloud Comput. CLOUD 2009, pp. 1–8, 2009, doi: 10.1109/CLOUD.2009.5071526.

D. K. Kang, S. H. Kim, C. H. Youn, and M. Chen, "Cost adaptive workflow scheduling in cloud computing," Proc. 8th Int. Conf. Ubiquitous Inf. Manag. Commun. ICUIMC 2014, 2014, doi: 10.1145/2557977.2558079.

A. García García, I. Blanquer Espert, and V. Hernández García, "SLAdriven dynamic cloud resource management," Futur. Gener. Comput. Syst., vol. 31, no. 1, pp. 1–11, 2014, doi: 10.1016/j.future.2013.10.005.

T. Sridhar, "Seclogmon : Security In Cloud Computing Using Activity Log For Consumer Data Protection," pp. 1458– 1462, 2017.

H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in the cloud storage environment," Cluster Comput., pp. 1–8, 2016, doi: 10.1007/s10586-016-0701-7.