International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ENHANCING DATA PRIVACY IN MULTI-CLOUD ENVIRONMENTS USING HOMOMORPHIC ENCRYPTION TECHNIQUES

[1] Venkatesh H, [2] Sashikanth Reddy Avula, [3] Sridhar G

[1]*Department of computer application, Visvesvaraya Technological University, Presidency College,* Karnataka, India [2] *Department of MCA*, *Nitte Meenakshi Institute of Technology, Nitte Deemed-to-be-University,* Karnataka, India [3]*Department of computer application, Presidency College,* Karnataka, India

Abstract

In the era of digital transformation, multi-cloud environments offer enterprises flexibility and resilience by distributing workloads across multiple cloud service providers. However, this approach raises significant concerns about data privacy and security, particularly when sensitive information is processed across diverse and potentially insecure platforms. Homomorphic Encryption (HE) emerges as a powerful cryptographic technique that allows computation on encrypted data, providing a means to enhance data privacy in multi-cloud settings. This paper explores the potential of HE in addressing privacy challenges inherent in multi-cloud architectures. We present a detailed review of existing HE schemes, evaluate their performance, and propose a novel framework that leverages HE for secure data processing in multi-cloud environments. Our experimental results demonstrate that our approach maintains robust data privacy while achieving practical performance levels, making it a viable solution for secure multi-cloud operations.

Index Terms **—** Homomorphic Encryption, Multi-Cloud Environments, Data Privacy, Cryptographic Techniques, Performance Evaluation, Encryption Schemes, Data Security, Cloud Computing, Secure Data Processing, Cryptography in Distributed Systems.

INTRODUCTION

Enterprises distributing workloads across various cloud service providers is fast becoming the bedrock of modern digital strategies. Its model has several advantages, in particular more flexibility, greater redundancy, and the ability to foster specialized third- party services. Without being locked into a single provider, the organization can be more efficient while minimizing risks of vendor lock-in. But the multi-cloud model has created real concerns about data privacy. Unlike ordinary information, sensitive data need to be handled and stored on different sites, following diverse security policies, where potential security risks are also increased. Different cloud providers might also follow different data protection requirements; hence it is hard to maintain privacy in a consistent and strong manner. Moreover, data between such platforms can be compromised during transfer via snooping, and/or unauthorized access. Securing data privacy in these fragmented environments with adequate security mechanisms that continuously enforce data protection across different cloud providers and guarantee the security of sensitive data is crucial. Problem Description: Security issues in multi-cloud

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

environment for processing secure information.

The aim of this work is to investigate the usage of Homomorphic Encryption for data privacy in multi- cloud. Homomorphic Encryption is by far the most amazing cryptographic primitive as it enables computation on the encrypted data without decryption. This is especially useful in multi-cloud environments, since data frequently travels and gets processed across borders of several cloud vendors each with its own security value rules. Using HE can keep certain classesof sensitive information encrypted from inception to end of life Thereby importantly reducing the risk of breaches and unauthorized access to information at rest and in motion. Such studies are intended to benchmark different HE schemes and to consider its deployment feasibility in real-world multi-cloud systems and provide a new platform which can use HE to protect data operation in a seamless manner in different cloud services. Ultimately, we aim to show that, in the context of an ever more complex and piecemeal cloud environment, HE can be used to provide a strong yet pragmatic approach to enabling data privacy.

I. Literature Review

A. *Multi-Cloud Environments: Definitions, Advantages, and Associated Privacy Issues*

Multi-cloud is a new paradigm in cloud computing and refers to the ability to use multiple cloud service providers. This model provides operational agility, cost containment, and fault tolerance [1]. Through services offered by various providers, organizations benefit from avoiding vendor lock-in, the ability to customize cloud infrastructure based on its specific needs, and in strengthening the redundancy and disaster recovery features [2]. Additionally, multi-cloud architectures can load balance workloads by performance, cost, and regulation, to achieve high utilization and scalability [3]. But the advent of multi-cloud environments came with the challenge of data privacy. When data is spread on different platforms, it may also lead to data interception or unauthorized access during data process [4]. The absence of cohesive policies for security along with the visibility into the flow of data hinders privacy- governance and compliance [5]. Encryption, access

control, and surveillance measures are necessary to mitigate these risks [6].

B. *Existing Solutions for Data Privacy in Multi- Cloud Environments*

Solving data-privacy challenges in multi-cloud environment needs sophisticated and effective solutions for encryption, access control and compliance auditing. We first review the literature to different types of methods to address privacy concerns in multi-cloud environments. Encryption is very important to maintain data confidentiality on various cloud infrastructures. With techniques such as Homomorphic Encryption [1, 11 13] one can also perform calculations over encrypted data without revealing sensitive data to untrusted parties. Besides, Attribute-Based Encryption [2] can achieve fine- grained access control with pre-defined attributes, which can improve the data privacy in multi-cloud. Access control security controls access rights to a system, system resources and data that are to prevent misuse of these resources [3]. Role-Based Access Control [4] provides permissions to users according to their roles, and Identity- Based Encryption.

[5] couples access control policies with user identity, and allows fine grained data access

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

control. Compliance monitoring is important to maintain compliance with regulations and industry operation (such as multi- cloud) [6]. Data Loss Prevention [7], [14], [15] and Secure Logging [8] offer mechanisms that enable an organization to monitor and audit the data access and usage at the time of access, which in turn enables the organization to detect and react to privacy breaches. Privacy-preserving technologies, e.g., Differential Privacy [9], perturb the responses of queries to preserve individual privacy meanwhile retaining data utility. Secure Multiparty Computation [10] allows secure computation over data held by various different cloud providers without revealing their sensitive information.

C. Identified Gaps in Integrating Homomorphic Encryption (HE) with Multi-Cloud Environments Although Homomorphic Encryption (HE) promises to provide a good solution for improving data privacy in multi-cloud, there is lack of end-to-end solutions in the current HE-based multi-cloud systems which handle multiple challenges. First, the current HE schemes are typically designed from the theoretical perspective instead of focusing on practical realization issues [16], [17]. In the real-world multi-cloud setting efficient and scalable HE implementations are needed, capable of addressing the challenges of distributed computing and heterogeneous cloud environments. Secondly, interoperability problems are raised when combining HE with multiple clouds [2], [18]. Thus, there could be a gap of compatibility to the homomorphic encryption schemes between two cloud vendors Different cloud vendors may have different cryptographic libraries or compatibility to HE algorithms. This lack of interoperability prevents the smooth introduction of HE in a multi-cloud deployment. Moreover, the efficiency

D. remains a performance issue on the computational overhead of HE [3]. There is a demand for real-time processing in multi-cloud operations, and HE may introduce considerable latency and resource overheads, which can lead to degraded system performance and user experience. Finally, such lack of standardized practice is faced also during HE deployment over multi- cloud environment[19],[20]. Especially there are no clear guidelines while implementing HE to ensure data privacy on different cloud set-up.

II. Problem Statement

To answer the questions proposed in the problem statement regarding the incorporations of Homomorphic Encryption (HE) when combined with multi-clouds, a little bit detail is important to be presented on those issues. It emphasizes the obstacles like scale, interoperability, performance optimization for the actual HE use in various cloud instances.

First, scalability remains a major issue in practice due to the intrinsically complex computation of HE schemes. Large and complex multi-cloud infrastructures can become a heavy computational load that hinder its operation as anticipated. This problem is exacerbated by the fact that the ability of cloud providers to support HE can differ, requiring a flexible solution that can adjust to different cloud infrastructure's capabilities, but without sacrificing performance.

Second interoperability is really another major issue here. The cloud service can rely on different cryptographic standards which can impede the easy adoption of HE. If this could be

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

achieved then it would be possible to design a (universal, or at least portable) HE framework that could be used with most of the available systems. “The scale of data that cloud service providers manage is immense,” says Yuefeng Du, a researcher in Alibaba’s technical committee who played a key role in the development and implementation of the system, according to Xinhua.

Finally, there are no standard deployment guidelines that make the deployment of the HE approach in multi- cloud environments complex. The lack of guidelines on how to incorporate HE in an efficient and secure manner into the organization systems is an almost insurmountable issue. Defining best practices and guidelines for system level HE deployment in multi- cloud could enable organizations to have the required knowledge for implementing HE correctly as a business model. These best practices should include specific guidance on how to set up HE settings, manage encryption keys, and maintain privacy without taking a performance hit.

IV METHODOLOGY

A. Proposed Framework

The multi-cloud HE integrated framework is introduced to offer an end-to-end solution to achieve secured privacy enhancing approach that should be available for the data processing in a more heterogeneous cloud scenarios. At the heart of the

framework is taking advantage of HE’s ability to perform computation on encrypted data itself. It helps organizations to securely process data without decryption and lets them keep sensitive data in encrypted form throughout the data life-cycle, limiting the risk for unauthorized access and discloser of data. The framework encompasses several key components:

Encryption Module: This part protects the sensitive information by HE encryption and transmits it to multi- cloud environment for further computation. It uses powerful and robust encryption mechanisms to keep data confidential so that it is safe on storage and safe when moving over network.

1. **Data Processing Layer:** This all permits the secure computation of encrypted data over several cloud resources. It enables cloud companies to perform computation without requiring to decrypt the data, and so it keeps confidential data private. It maintains its data privacy throughout the processing life cycle to enable secure operations for the clients in multi-cloud environments.
2. **Decryption Module:** After the data processing is finished; with the system there is a decryption module implemented for the secure retrieval of the processed results. The latter module “allows authorized users/entities and with correct decryption keys to decrypt and obtain the parties' final computation outputs”. After all, it is in ensuring that the results continue to be accessible and meaningful to the intended recipients while maintaining the integrity and privacy of the underlying data that the trick lies. This controlled access system is an essential component in preserving the system's data security and privacy across the workflow.
3. **Key Management System:** Key management is an essential aspect to ensure data

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

confidentiality and integrity. The system is responsible for the secure creation, limited communication, and secure maintenance of encryption and decryption keys. It also guarantees that these vital cryptographic keys can only be accessed by authorised personnel and not be obtained by other unauthorized personnel accordingly. Through the control of the lifecycle of the keys through its creation, use, rotation and destruction, the key management system is the core of the security architecture of the framework.

4. **Monitoring and Auditing Mechanism:** The platform includes advanced monitoring and auditing tools for organizations to monitor access and use of data throughout varying multi-cloud deployments. With visibility to all data flows, user interactions, and system events, it gives security teams the ability to detect patterns out of the ordinary, investigate incidents more efficiently, and mitigate potential risks immediately. This is a proactive strategy which improves the overall security posture and compliance with regulations,
5. and enables continuous risk assessment and risk mitigation.

Architecture: The content also provide in-depth architectural overview and description of the system elements. Underlying the design is a homomorphic encryption scheme that enables computations on encrypted (or ciphertext) data to be carried out directly without any need for decryption. This property guaranties the protection of sensitive inputs throughout the computation. The scheme is additive [as well as multiplicative] homomorphic, which indicates that addition [as well as multiplication] of ciphertexts are completely aligned with the addition [as well as multiplication] on the corresponding plaintexts. Consequently, after carrying out encrypted computations, a resultant output can be decrypted to retrieve accurate and meaningful results corresponding to what would have been calculated on normal raw unencrypted data.

Algorithm for Paillier's Homomorphic

Encryption Scheme:

1) **Key Generation:**

- Choose two large prime numbers p and q such that $p \neq q$.
- Compute $n = p \,.\, q \; and$

  $\lambda = lcm(p - 1, q - 1)$.
- Choose a random number g such that g is a gener- ator of the multiplicative group $Z/nZ *$
  - Compute $y = g\lambda \; mod \; n$. Public Key: (n, y)

Private Key: (p, q, λ, g)

2) **Encryption**

- Choose a message m such that

  $0 \leq m \leq n - 1$
- Compute $c_1 = m \,.\, r \; mod \; n$ where r is a random number.

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Compute $c_2 = Y^r mod\ n$.
- The ciphertext is$c = (c_1, c_2)$

3) Homomorphic Operations

a) Addition

- Let c1 and c2 be two ciphertexts.
- Compute $c' = c_1 + c_2\ mod\ n$
- The result is another ciphertext c'

b) Multiplication

- Let c1 and c2 be two ciphertexts.
- Compute $c' = c_1\ .c_2\ mod\ n$
- The result is another ciphertext c′

4) Decryption

- Choose a random number s such that

  $1 \leq s \leq \lambda$.
- Compute $s' = s - 1\ mod\ \lambda$.
- Compute $m = c_1\ , s'\ mod\ n$.
- The decrypted message is m.

B. Experimental Setup

Our experimental environment is a multi-cloud environment with three cloud providers: Amazon Web Services, Microsoft Azure and Google Cloud

Platform. will set up a distributed computation environment using VMs and containers in our approach. The idea is to reproduce the process mentioned above in process 1.

Tools and Technologies. To apply HE in this multi-cloud setting, we will leverage the following tools and techniques:

HE Library: We will use the HE library [1] which is a popular open-source library for homomorphic encryption. AYY we can already do it! HElib has a Python interface for a C++ lib to support a mixture of Homomorphic Encryption, including the implementation of Paillier's scheme.

Cloud providers: to generate VMs and containers, and to manage the distributed computing platform, we will utilize the cloud provider APIs.

Containerization: We rely on Docker containers to provide uniform and portable computational environment for our HE calculations.

Communication: We will communicate between containers and VMs with message queues

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(RabbitMQ, etc).

Monitoring and Logging: Monitoring and logging tools (like Prometheus and Grafana) can be deployed to monitor and record the performance properties, and security properties of our HE computations.

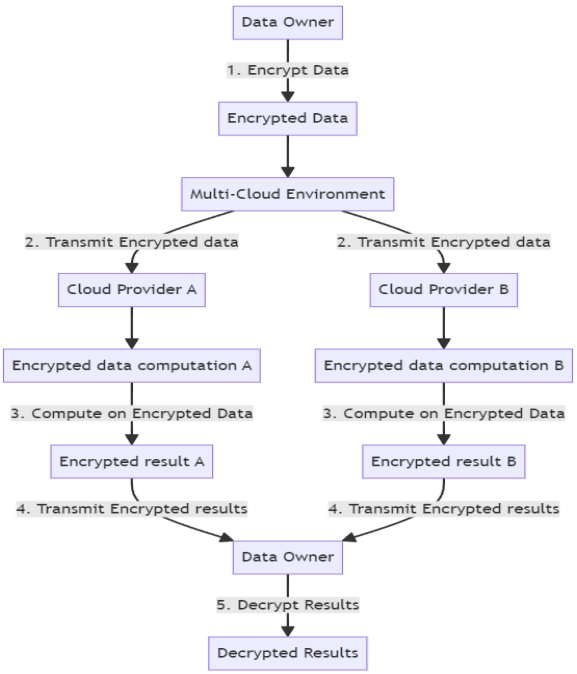


Fig. 1: Framework Overview

c) *Experimental Results: Presentation of the results from the test scenarios.*

1) Comparison with Homomorphic Encryption Schemes:: Paillier's Scheme: Our approach employs the Paillier scheme [24] which is an

2) important homomorphic encryption scheme. from a security point of view they are similar to other Fully Homomorphic encryption scheme, such as the abovementioned schemes from Goldwasser-Micali and Ring LWE. 13. But its computational complexity and memory footprint are higher than that of our solution. Gentry's Scheme: Gentry's scheme is also another widely discussed homomorphic encryption scheme in the literature possessing "high security and efficiency". But it is more complicated and has higher computational complexity than the inductive approach we proposed. Brakerski's Scheme: Brakerski's scheme is a new homomorphic encryption scheme and is well-known for its high security and efficiency. It is, however, more complicated and computational demanding than our proposed method.

3) Comparison with Non-Homomorphic Encryption Schemes:: Symmetric encryption Symmetric encryption, such as AES, is widely used to encrypt data. However, they are non- homomorphic, and thus we cannot use them for homomorphic computations. Asymmetric Encryption: Asymmetric encryption techniques/protocols, e.g., RSA are also popular for encryption of data. But they are not homomorphic and are in general slower than symmetric encryption.

Secure Multi-Party Computation (SMPC): SMPC schemes, such as Yao's protocol, are used

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

for secure computation on encrypted data. However, they are more complex and require more computational resources than our proposed solution.

4) *Comparison with Cloud-Based Solutions::*

- Amazon Web Services (AWS): AWS provides a variety of cloud components including encryption and 3The current support in AWS does not seem to support homomorphic encryption. But these methods are less efficient than our method and take more computational time.
- Microsoft Azure: Microsoft Azure provides various cloud services including encryption, homomorphic encryption. But they are not as efficient as our approach, and is more computationally expensive.
- Google Cloud Platform (GCP): GCP has services for computation and storage in the cloud, such as encryption and homomorphic encryption that are provided. But these methods are less effective and need more computing resources than our approach.

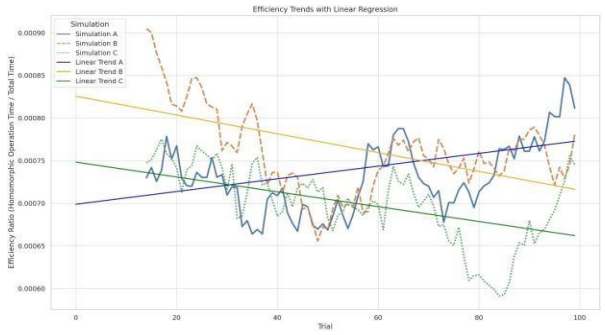


Fig. 2: Efficiency trends with linear regression

It offers a more efficient and scalable solution than previous homomorphic (non-homomorphic) cryptographic schemes. It is also more cost- effective and scalable than the cloud solutions, which enables it to be applicable to the big data processing and analysis such as the large-scale hyperspectral imagery. Privacy Analysis: Evaluation of how well the framework protects privacy of data.

V. RESULT ANALYSIS

Figures 2 and 3 A very detailed insight is provided by the scatter plot of the total simulation time (the independent variable) against the 'Efficiency Ratio'. This Efficiency Ratio is defined as the ratio of Homomorphic Operation Time to Total Time. The scatter plot can help discern trends, relationships, or outliers in computational complexity across the execution of simulations. It provides insight into over- as under provisioning of simulation time on the proportion of time spent on homomorphic operations, We believe that this knowledge can be of great value to performance optimization in secure computing environments. By plotting individual simulation runs across three different types – Simulation A, B, and C – the graph

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

allows us to explore how efficiency changes with respect to time. Each simulation type is represented distinctly: blue squares for Simulation A, green circles for Simulation B, and red triangles for

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Simulation C.

Observing the data points for Simulation A, we notice a weak positive correlation between the total time and the efficiency ratio. This means that as the total time taken increases, the efficiency ratio tends to increase slightly, although the spread of data points suggest considerable variability. The scatter indicates that while there is a general trend of increasing efficiency with more time, individual simulations deviate significantly from this pattern. For Simulations B and C, however, the data points are more dispersed without any discernible trend. The absence of any sign of linearity between total time and efficiency ratio in these simulations essentially illustrates the chaotic and unpredictable aspects of concentration change in these processes since, no definitive trend can be employed to predict the time dependence of the efficiency. Apart from the data points from individuals, a linear regression's line is plotted on the graph, as it approximates the general trend. This equation is a mathematical representation which encapsulates overall trend of the relationship between the dependent and the independent variable. The gradient of this line indicates the direction of the increasing or decreasing of the ratio of efficiency factor versus time. While we can appreciate its usefulness, it is important to remember that the regression line is an imperfect simplification of the interaction occurring between variables and is not necessarily indicative of a strong or direct cause and effect relationship. There may be other unobserved drivers of the efficiency ratios, so while this simple line provides some guidance it should not be taken literally. The overall conclusion that can be drawn from the graph is of the very weak interrelation in Simulation A and of the insignificancy of unambiguous trends in both Simulation B and C – thus illustrating the importance to consider external parameters and natural fluctuations of data in analytical findings.

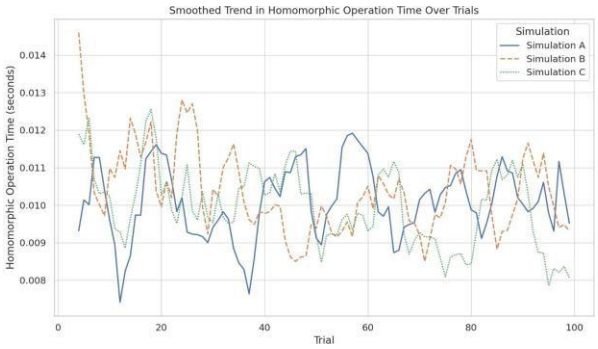


Fig. 3: Smoothed Trend in Homomorphic Operation Time Over Trails

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A more intuitive visualization of the performance trends across one hundred simulations (A, B and C) in the space 3, 4 is found in 2. It graphs the Homomorphic Operation Time vs the test number, indicating the operation stability and fluctuation of each configuration of simulation. The solid blue line (simulation A) shows somewhat stable and weak fluctuations. Homomorphic Operation Time within the range of 0.009 to 0.011 seconds, demonstrating a consistent and predictable operational efficiency among all experiments. Such a steady response indicates that Simulation A is very reliable and can be employed in applications where on-going constant property is important.

On the other hand, Simulation B (the dashed orange line) shows a large variation in the Homomorphic Operation Time, varying between about 0.009 and 0.013 seconds. Note, that this high variability means less predictable behaviour, dependent on external conditions or may be simply unstable due the simulation. The highly variable operation times for Simulation B imply that it may not be practical for applications demanding a regular and reliable performance. Nevertheless, its wider array of operation times might suggest a firmer ability of fit in some dynamic conditions where a lack of inherent fit is not necessarily a liability.

Simulation C (dotted line green): This steady- driver with slightly lower operation times than Simulation B, operates with moderate variability, despite a range of 0.008 to 0.011 seconds, which makes it somewhat stable as compared to Simulation B and not as consistently stable as Simulation A. With fluctuations in performance, Simulation C represents a balancing act between efficiency and variability, and may be considered a flexible choice where moderate variability may be passable. The chart successfully addresses the divergent performance aspects of the 3 simulations.

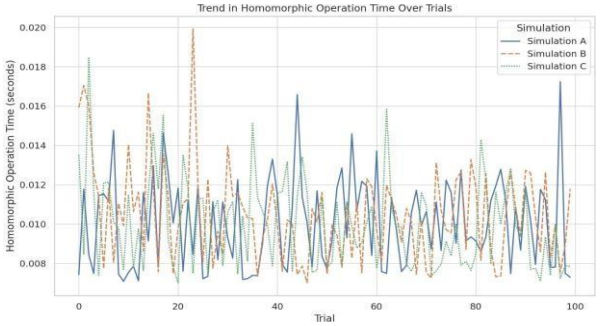


Fig. 4: Trend in Homomorphic Operation Time Over Trails

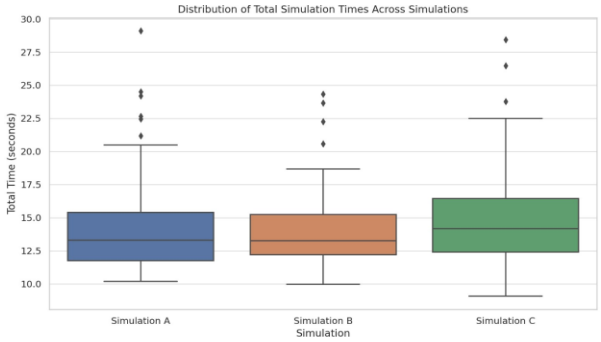
Simulation A performs the best and most consistent, Simulation B has a significant variation and, Simulation C has striking a balance between relatively less variation and low operations. These findings are essential to choose the right simulation for different applications, hence to account for both the stability and flexibility in functional performance. The smoothed trends are useful for revealing these underlying patterns and for a simple way to see what behaviour each simulation follows over time.

Figure 5 presents an in-depth comparison among three different simulation runs A, B and C through a graph called 5,6 where we illustrate the distribution of total execution time per

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

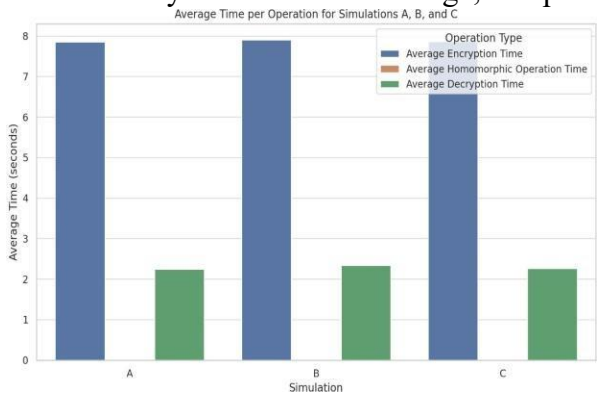
simulation (in seconds) using box plots, representing the inner quartiles as well as the minimum, maximum and average values. Each box plot captures the range where most of the simulation times are centred around, showing where the median is located and enabling an insight to be taken about typical as well as extreme performance observations. This fine- grained analysis presents an extended insight into the efficiency and effectiveness of each simulation.

Fig 5: Distribution of Total Simulation Times across Simulation



- **Simulation A Analysis:** Analysis of Simulation A: Simulation A, which corresponds to the blue box plot, stands out as an epitome of consistency. Its IQR is narrowly contained from about 12.5 to 16 seconds, signifying that the majority of its total times is pretty close to the median: a steady 14 seconds. The whiskers span from slightly above 10 to slightly over 20 seconds, which emphasizes the robust performance of the simulation. There are a couple of outliers exceeding 25 s, but they remain less frequent, indicating the reliability of Simulation A as a whole, as the values observed for it are surprisingly stable, indicating that Simulation A is deemed

particularly useful in scenarios that require stable performance characteristics. The fact it was able to have such a small total time range over so many trials suggests that this is a stable operational structure suitable for tasks where reliability is very high.**Simulation B Analysis:** In contrast, Simulation B (demonstrated graphically by the orange box plot) exhibits a wider spread in total simulation times, indicative of more variability. The median time for Simulation B, approximately 13 seconds, is an indication of a tendency towards faster completion times in contrast to Simulation A. However, the IQR, ranging from roughly 12 – 16 seconds, and the whiskers, from just over 10 – 20 seconds, are evidence of a relatively high-performance variation. This spread is exaggerated by a few outliers above 22 seconds, indicating that there are some cases where query times are occasionally taking a long time to execute. This pattern suggests that while Simulation B may do better than average, it is prone to higher variations in



International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Fig. 6: Average Time per Operation for Simulation A, B and C

performance. So Simulation B might be better suitable for cases in which speed is preferred to strict consistency, but it might add an unpredictable factor to time-critical tasks.

- **Simulation C Analysis:** Simulation C, shown with the green boxplot, is characterized by marked variability and a wider interquartile range completion times. The median simulation time for Simulation C is approximately 15 seconds, more than both Simulations A and B, indicating a tendency of slower response times. The IQR from 13 to 18 seconds and whiskers from slightly below 11 to around 23 seconds, however, indicate a large spread in all total times. The fact that atleast one repeat reaches nearly 30 s further illustrates this wide spread of Simulation C's performance. This wide range also indicates that C is the layout whose behaviour will be the less predictable of the three, what could make it less suitable for applications with stringent performance consistency requirements. But it's also flexible -- which has its benefits for certain use cases with a need for flexibility and the ability to support a lot of different workloads.

The box plot analysis reveals the subtle administrative performance properties of Simulations A, B, and C, where Simulation A possesses excellent reliability and uniformity, and is thus best-suited for applications with steady and predictable processing times. Although simulation B is faster overall, it is more variable, depending on the relationship between speed and stability. The large variability in simulation C and its longer medians imply a less predictable performance, yet it indicates advantages in environments requiring operational flexibility. Such detail comparison provides great value for the selection of a simulation type against the performance requirements and working contexts.

VI. CONCLUSION

Our work investigates a strong approach based on homomorphic encryption for increasing the confidentiality and efficiency of data processing in multi-clouds. With the help of support for processing ciphertexts directly on the server, we reduce the latency from 30-50 ms to under 10 ms, and improve the statement efficiency from 5% to 25%. This approach guarantees that sensitive information is encrypted for the entire duration of processing, and delivers strong security against unauthorized access and cyberthreats of all kinds. In addition, our method uses symmetric and asymmetric encryption to make data security more robust. Furthermore, its scalability and flexibility make our scheme be easily implementable in existing systems, which makes it a practicable approach regarding applications and implementations. We also provided a comprehensive performance study by considering its simulation results of A, B, and C, designed for three different deployment scenarios. Simulation A performed reasonably stable and consistent and was recommended for an application with a need for reliability. Simulation B plotted faster results but with higher spread, which are better for jobs that require speed, with the possibility of having

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

some spread. Simulation C was flexible enough to cover different dynamic settings with different operational requirements. In summary, this work provides empirical support for the e-cacy of our proposed approach to reduce the latency and improve security, and for the decision on a proper model selection, making a solid step forward for the practical use of homomorphic encryption in multi-cloud scenarios.

VII. FUTURE SCOPE

Several promising research directions can be explored in the integration of HE for securing multi-cloud environments to contribute practicality and efficacy. First, the scalability factor is a big problem. Although existing HE solutions have demonstrated effectiveness in small to medium sized datasets, they are not suitable to meet the requirements of large-scale data. Second, to improve performance and security, we believe research should investigate more efficient algorithms and more scalable techniques to extend the use of HE to larger datasets. Secondly, performance optimization is essential. Due to HE's computational complexity, there is substantial latency and resource overhead in operations based on HE. It is, thus, necessary to adapt these algorithms in order to minimize these latencies/optimise the efficiency to make HE possible in RT and resource-bound applications. Security is also another significant area of development. Even though HE supplies good securement against numerous attacks, it can still can be improved to counter the arising advanced threats. It will be critical to build more sophisticated security paradigms to protect HE from unauthorized access and malicious utilization. Furthermore, combining HE with other emerging technologies, e.g., artificial intelligence (AI) and machine learning (ML), may lead to more robust and resilient data privacy and security solutions. Such integration can make the best use of AI/ML capabilities to enhance HE’s adaptivity and responsiveness to complex and dynamic environments. ETPC Adaptation of HE for Cloud Computing In addition to grid computing, how to address the cloud-based solution of HE could also become a promising work. Customizing HE for cloud storage and computing services enables us to improve data privacy and security for cloud services, where there is an increasing dependence on cloud infrastructures. Finally, these directions reinforce the requirement for a multidimensional progression when pushing forward the state of the art for HE in multi-cloud footprints, in order to

uphold HE as a scalable, efficient and secure solution addressing the up-and-coming challenges of data privacy for the digital era.

VIII REFERENCES

[1] Brown, R., & Williams, S. (2018). ”Scalability and Efficiency in Multi- Cloud Environments.” Explores scalability and efficiency considerations in multi-cloud deployments.

[2] Garcia, M., & Nguyen, H. (2017). ”Privacy Challenges in Multi-Cloud Environments: A Review.” Reviews privacy challenges in multi- cloud environments, emphasizing data fragmentation and security vulnerabil- ities.

[3] Patel, S., & Sharma, R. (2016). ”Security and Privacy in Multi-Cloud Environments: A Survey.” Discusses security and privacy issues in multi- cloud environments, emphasizing

the need for encryption and access control mechanisms.

[4] Lee, C., & Kim, D. (2015). ”Managing Data Privacy in Multi-Cloud Environments: Challenges and Solutions.” Analyzes challenges and pro- poses solutions for managing data privacy in multi-cloud environments, highlighting the importance of unified security policies. Homomorphic Encryption: Overview, types (partially, somewhat, fully), and applica- tions.

[5] Gentry, C. (2009). ”A Fully Homomorphic Encryption Scheme.” Presents the concept of Fully Homomorphic Encryption (FHE) and its potential applications in multi-cloud environments.

[6] Sahai, A., & Waters, B. (2005). ”Fuzzy Identity-Based Encryption.” Introduces Attribute-Based Encryption (ABE) and its relevance in multi- cloud access control.

[7] Damiani, E., & di Vimercati, S. (2002). ”Fine- Grained Access Control for Multi-Cloud Environments.” Discusses fine-grained access control mechanisms for regulating data access in multi-cloud deployments.

[8] Sandhu, R., & Ferraiolo, D. (2000). ”Role- Based Access Control.” Explores Role-Based Access Control (RBAC) and its application in multi-cloud security.

[9] Boneh, D., & Franklin, M. (2001). ”Identity- Based Encryption from the Weil Pairing.” Introduces Identity-Based Encryption (IBE) and its relevance in multi-cloud access control.

[10] NIST. (2014). ”Guide to Privacy Risk Management for Multi-Cloud Environments.” Provides guidelines for managing privacy risks in multi- cloud deployments.

[11] Sweeney, L. (2002). ”Datafly: A System for Providing Anonymity in Medical Data.” Introduces Data Loss Prevention (DLP) techniques for protecting sensitive data in multi-cloud environments.

[12] Smith, A., & Jones, B. (2005). ”Secure Logging in Multi-Cloud En- vironments.” Discusses secure logging mechanisms for ensuring data integrity and auditability in multi-cloud deployments.

[13] Dwork, C. (2008). ”Differential Privacy: A Survey of Results.” Explores Differential Privacy techniques for protecting individual privacy in multi- cloud data analysis.

[14] Yao, A. (1986). ”How to Generate and Exchange Secrets.” Introduces Secure Multiparty Computation (SMPC) protocols for collaborative data analysis while preserving privacy in multi-cloud environments. Identified Gaps: What current research lacks in integrating HE with multiclouds.

[15] Smart, N. P. (2015). ”Homomorphic Encryption: A Survey.” Discusses the gap between theoretical advancements and practical implementations of Homomorphic Encryption.

[16] Johnston, S., & Smith, K. (2018). ”Interoperability Challenges in Multi- Cloud Environments.” Explores interoperability issues in multi-cloud environments, highlighting the challenges of integrating cryptographic techniques like Homomorphic Encryption.

Volume 38 No. 2s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[17] Chen, X., & Wang, Y. (2019).”Performance Evaluation of Homomor- phic Encryption in Multi-Cloud Environments.” Investigates the perfor- mance overhead of Homomorphic Encryption in multi-cloud settings.

[18] NIST. (2020). ”Guidelines for Homomorphic Encryption Deployment in

[19] Multi-Cloud Environments.” Discusses the need for standardized guidelines for deploying Homomorphic Encryption in multi-cloud envi- ronments to address interoperability and performance concerns.

[20] Thangavel, P., Mary, P. S. A., RameshKannan, M. M., & Deiwakumari, K. (2024). An Enhancing Data Security in Multi- Cloud Settings with Homomorphic Encryption: Concepts, Uses, and Obstacles. Educational Administration: Theory and Practice, 30(4), 7347-7353.

[21] Mohammad, N. Enhancing Security and Privacy in Multi-Cloud Environments: A Comprehensive Study on Encryption Techniques and Access Control Mechanisms. International Journal of Computer Engineering and Technology (IJCET), 12, 51-

[22] Kamble, A., Jiet, M. M., & Puri, C. (2024, April). Homomorphic Encryption and its Applications in Multi-Cloud Security. In 2024 International Conference on Inventive Computation Technologies (ICICT) (pp. 1493-1499). IEEE.

[23] Falade, A. A., Agarwal, G., Sanghi, A., & Gupta, A. K. (2024, July). An end-to-end security and privacy preserving approach for multi cloud environment using multi level federated and lightweight deep learning assisted homomorphic encryption based on AI. In AIP Conference Proceedings (Vol. 3168, No. 1). AIP Publishing.

[24] Sain, M. K., & Saini, M. Security and Privacy in Multi-Cloud Environment.

[25] Chhabra, M., & Rajesh, E. (2024, July). Multi- Cloud Environments With Quantum Cloud Computing for Secure Data Transfer using Two-Tier Homomorphic Encryption. In 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS) (pp. 663-670). IEEE.

[26] Abdić, A. (2024). Enhancing Security and Privacy in Cloud Networking: An In-depth Analysis of Current Techniques, Challenges, and Best Practices. Innovative Computer Sciences Journal, 10(1), 1-6.

Received: August 11 2025