



REVIEW BY

Sandeep Kumar Singh,
GLBITM Greater Noida

*CORRESPONDENCE

Vikas Kumar

✉ vikasksr@hotmail.com

0009-0008-1425-5457

RECEIVED 16 July 2026

ACCEPTED 11 Aug 2026

PUBLISHED 11 Sept 2026

CITATION

Kumar, V. (2026). A Framework for Multi-Layered Data Encryption and Data Compression to Optimize Cloud Security. *Nimbus Journal of Academic Research*, 1(1), 13–23.

COPYRIGHT

© 2026 Kumar, V. This is an open-access article distributed under the terms of the [Creative Commons Attribution License \(CC BY\)](#). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

A Framework for Multi-Layered Data Encryption and Data Compression to Optimize Cloud Security

Vikas Kumar

Research Scholar, Department of Computer Science, Jamia Millia Islamia, New Delhi

Abstract

Cloud Computing is the revolution in digital infrastructure, wherein computing resources are made available on demand and scale. Even with the move to the cloud, obstacles to adoption remain, including security breaches or security vulnerabilities on the way to the cloud. To overcome these problems, this research work proposes a new multiplying encrypted and compressed data scheme. Due to this our way increases the integrity of the data and their privacy from outside threats, as well as improve its performance – reduce transmission delays and error rates. The results of simulation indicate the proposed model is far superior than the conventional secure measures, and is also an efficient and robust solution for secure management of data in a cloud environment. This study offers a practical route to the secure and smooth exploitation of the potential of cloud computing, closing the gap between cutting-edge security and operational effectiveness.

Keywords: *Cloud security, Data integrity, Data Breach, Encryption, Privacy.*

Introduction

The study of cloud computing has been rapidly advancing for the past decade. It is based on the concept of service deployment. Users are allowed to use all of the resources freely. It has a greater selection of services, all of which come from different suppliers. The services can be used at any time when needed, only paying for what is actually used. But it is just a baby. It offers a huge array of excellent web-based materials for businesses. This way, we can effectively do our best to utilize the resources without taking ownership. It has increased the organization's accessibility and have decreased the computational and management costs.

Cloud Computing

Cloud computing system is an extensive collection of services. Cloud Computing is being used for computer services. Examples range from virtual machine hosting, database hosting, software hosting,

all the way to even network services. Cloud providers are companies that offer access to resources in the cloud. These vendors charge fees similar to how residential power is charged, based on usage. Cloud computing is easier and more available for any configuration of devices and networks. The term "cloud computing" refers to the utilization of remote servers to do common Internet-based tasks including sending email, updating files, watching videos, listening to music, and storing large picture collections. Numerous studies have been performed to ensure that Cloud services are secured when working with big data. Some of them are not included here. In this study, an effort has been made to address the issue of the perception of IDS method. It provides protection according to your needs. The length of the network lifetime becomes more important. This is possible due to a reduction in the amount of energy used by the nodes. The network is split into smaller networks for best use of each node. The value of regional controllers is recognised too. The controller learns all of the details of the local

business ledgers. Practical controller has accurately collected the hop information with extreme efficiency, satisfying the requirement in effective routing.

In the Clouds It's a model used in computer programmes. This is a large set of systems which are linked together in known and predictable ways. It created a basis for applications that can be quickly expanded, and it can be used to store data and records. The dramatic drop in compute cost with the spread of application hosting has been a major driver. The availability of application hosting has contributed significantly in bringing the compute cost down. Cloud is used to describe a network of networks. With cloud computing, strategies can be deployed that go beyond a few nodes. With cloud computing, a new paradigm has been established. It's a first step towards the emergence of offline applications. It allows you to browse, create, arrange and adjust cloud-based software. It can be used to enable users to access information from database resources online, anytime, anywhere. The repair and/or arrangement of a rare resource is no longer an issue. The initial idea behind cloud computing was devised around a "recycling rule" for IT skills. It becomes clear when it comes to computer systems, or automated processes, or more traditional distributed data processing methods, that the former can reach beyond the organisations boundary when compared to the later. Forrester provides the missing piece to the puzzle. It can be customized to address the needs of the user, it has a structured management of computing resources, it is very flexible and it is compensated by the quantity of the service used by the user.

Advantages of cloud computing

There are several advantages to doing so. The following are examples of these:

- a) Useful tools that can be accessed remotely can be found on the internet.
- b) Cloud computing provides access to a suite of hosted programming resources.
- c) The executer always has access to the application's web backend where it may be updated and reorganised
- d) The platform has enabled operators the possibility of autonomous cloud resource availability over the internet.

- e) The cloud facilitates the provision of services at the user's discretion. There is no need to have any kind of communication with the cloud service provider.
- f) Cloud services are often very effective in their intended tasks. Since it won't be used to its full potential, it's been deemed cheap.
- g) Load Balancing is one reason why cloud computing is more dependable.

Disadvantages of cloud computing

Some of the more common disadvantages of Cloud Computing include the following:

1. Inadequate protection against unauthorized access to cloud-stored data and resources is a persistent threat.
2. One's internet connection quality is crucial. If you don't have access to the internet, you can't use a cloud service.
3. Lack of privacy and security is a major problem with cloud computing.
4. The data centres hosting the cloud services are situated in countries with lax consumer protection regulations. This leads to lower levels of compliance.
5. Continuous connectivity makes clouds an attractive target for cybercriminals. Users' information is constantly at risk. In the case of a user problem, it is not always possible to provide support at all hours of the day.

Role of Security in Cloud computing

The accelerated advancements in cloud computing have made it one of the most sought-after topics today. It provides an affordable way for companies to access computing and storage resources, to name a few. As more and more companies move into cloud computing, their concerns around the security of such applications are increasing as well. There is apprehension among many customers about data security issues when it comes to moving to the cloud. Loss of data control, multi-tenancy risk, data security and privacy concerns, and dependability problems are just a few of the hazards connected with cloud computing. With the many cloud computing services available, many businesses are currently storing their extensive data on the cloud. It highlights the need of having trustworthy and reliable data stored in the cloud. Unauthorized users accessing sensitive information is a major security risk.

With cloud storage the user has no control over the data that is held, stored and processed by the cloud provider's servers. All security rules and procedures (including identity management) are enforced by the service provider. Whether the supplier has access to and can ensure the safety of the customer's information and resources is dependent on the supplier. It's a very serious security and privacy danger. Cloud computing's multi-tenancy feature, in which users share an infrastructure, is very advantageous. This renter's computer may be used by others, and he might be a victim of a crime. It is inappropriate to leave sensitive data unattended and open for easy access by malicious individuals. The security of stored data is essential to the security of cloud. The data breach has become a serious problem in recent years. The cloud is as secure as all the data that's stored on it. The cloud infrastructure relies on data as its lifeblood. Since 2016 (Subramanian and Jeyaraj, 2018), CSA has considered data breaches to be the greatest security risk.

With the advent of cloud computing, data is crucial and its safety must be ensured. This information is housed off-site. It could be in a different city, country or continent. There's more than one-way data can be leaked in the quest for multi-tenancy. Data goes through a progression from creation to transfer to use to sharing to documentation to deletion. The information has to be safeguarded on all fronts. There are two types of protection for data that is sensitive. The data is moving at the first level and at rest at the last level. There is a distinctive security problem with data stored. Data transfer is safer, as TLS is employed. Threats lurk the longer time remains unused. On both levels there are security problems with the data. Answers to the problems are required. The security of data can be accomplished in various ways, but usually it comes with a smaller storage space, faster data transfer or some extra CPU. When fixing security holes, this causes unexpected expenditures. Good, flexible and secure encryption is required with granular permissions. It will provide an extra level of safety, at not much additional cost.

Literature Review

A. Jabbar et al. (2020) highlighted important areas on the security and reliability of cloud computing. The cloud paradigm was a new one that could revolutionize the delivery of computer resources. A critical part of the concept of "cloud computing" was sharing computer resources among several users. The

security of cloud computing is meant to protect data, applications, infrastructure deployed in the cloud, as well as align with compliance standards for applicable regulations. But data integrity guarantees that digital data has not been altered in any way and that no one else but the authorized user can view or alter it. In this article, you will get an overview of cloud computing and how many applications it has and ways how data can be protected on the Cloud.

Y. S. Abdulsalam et al. (2022) analysed the privacy & data protection on the cloud. In this research, they take into consideration the literature's adaptability in protecting against recurrent threats and demonstrate how cloud security conflicts have rendered their offered models useless. The security issues of cloud computing are then conveyed in the user's perspective using the methodology called STRIDE. It also reviews literature and a lot of the ineffective solutions proposed, and provides guidance on how to design a safe and flexible cloud infrastructure.

S. Aldossary et al. took the focus on the data integrity, privacy and its future and the availability of cloud computing. They discuss the problems that have prevented cloud adoption so far, and provide an overview of the work that has been done to address these concerns. For example, cloud-based information needs to be secure, but still be available and meet integrity requirements. Furthermore, the service providers' unreliability in handling authentication and authorization is still a reason for not extending the use of cloud storage. This book is focused on specifically data in the cloud and potential issues that may emerge as a consequence; as opposed to being more general with the cloud as the topic.

Alenizi et al. (2021) performed a review on security and privacy issues of Cloud Computing. There has been a plethora of researchers who have attempted to resolve the problems of security and privacy, but the problem has not gone away. Having confidence in the cloud's security was a key factor in people making the decision to use it. The article firstly gives a detailed review of basic cloud privacy and security issues and concerns and then presents the countermeasures to address the security challenges faced by cloud systems and the solutions for cloud privacy issues. Furthermore, as a research contribution, we have given a framework to deal with privacy and security issues in CC. The proposed architecture in the paper ensures the safety of the CC by employing an hybrid authentication technique.

This paper is valuable for researchers and practitioners to learn more about CC, the related security and privacy issues, and a new approach to CC that can be implemented to address these challenges.

H. Dey et al. (2019) looked the security for cloud authentication and multi-tenancy used a unified model. One way to enhance the security of Cloud in terms of Authentication and multi-tenancy is to integrate a paradigm. A single instance of the server supporting multiple customers via multi-tenancy. Many tenants could use the same server at the same time, thus increasing the risk of sensitive information being in the hands of the wrong people. To enhance the security of authentication, our architecture utilises the Kerberos authentication protocol.

The method proposed by Elsayed, M. et al. (2019) is a brand-new technique in the area of security diagnostics for SaaS. It endures software as a service programmes. The framework discovers weak points and minimizes risk during the initial stages of app development. Ensures that all communication is data correct. A comprehensive report is published based on the proposed framework. Possible threats which are highlighted in the paper. If the framework's static analysis is its own limitation, then it is a good one. It is possible to explore the context of the code's run.

I. Gupta et al. (2022) examined the methods that can be used for the protected information when storing and sharing files in the cloud. This article assesses and contrasts the most common ways of keeping data secure and private in the cloud. For each approach in the area, data protection functions, prospective and innovative solutions, core and appropriate information (including workflow, successes, scope, gaps, future directions, etc.) are explained in detail. In addition, a thorough comparison of the various methods was provided. The usefulness of the approaches was then discussed taking into account the need and possible future developments and research gaps within the area were presented. The authors hope that the work presented in this paper will be used as a catalyst for additional research in the field.

J. Hassan et al. (2022) introduced the data security, privacy, and emerging research opportunities in the era of cloud computing. In this paper they perform an SLR to identify how to provide protection of the data both while it is stored in the cloud and while

retrieved. Thus, this study aimed to summarize, categorize and identify relevant research, with the primary purpose of the study being to do this. Therefore, this research makes use of an evidence-based methodology. Four research questions have been answered, and these preliminary answers lead to the following findings. Of all those papers (493), the following 52 papers were selected for the following reasons: Fifty-two publications are presented that use various methods of data security, and they can be grouped into two categories: cryptography and no cryptography. Data splitting, data anonymization, and steganographic methods are examples of noncryptographic methods, whereas encryption, searchable encryption, and signcryption were examples of cryptographic methods. They compare the overhead, accuracy and usability of various approaches to data masking in this study. The book concludes with a discussion of the research challenges to be addressed before these approaches can be generally applied.

D. V. S. Kaja1 et al. (2022) looked threats to cloud-based data integrity. Cloud services are increasingly popular in past few years. Since cloud computing was inexpensive and can be paid for on an as-needed basis, many businesses were making the move from their previous computer strategy. With data integrity and security concerns a top priority for any CSP, you can be confident that your data is safe with them. There were however, several issues with data integrity that needed to be addressed. Issues of data integrity are particularly very relevant in the Cloud. They have summarised the existing literature concerning cloud data storage security, considering issues such as data theft, server downtime, and data breaches. They also identified the different threats to data integrity, and how to protect against them.

J. Kollu et al. (2022) did researched on cases for cloud computing to improve privacy-safe data analysis. The aim of the research was to identify safe cloud file downloading practices. They have reviewed in depth the most modern approaches and methodologies that are today applied to trying to solve this important problem. They categorize privacy-protection strategies into four classes: cryptographic methods, probabilistic methods, anonymizing techniques and ranking systems. Our team also has developed a taxonomy of methods to protect private administrative data. They also provide an in-depth analysis of the privacy-preserving techniques in terms of how well they measure up to

industry norms. Hence, there was a strong need for providing opportunities of implementing effective auditing and accountability measures which can trace the source of data and track the use of data records in an anonymous manner.

A group of researchers presented their work with information in the cloud in 2017 (T. Lakum et al.). In this research, the security concerns of cloud storage are discussed. Here's a way to address one of the biggest issues in cloud data security. Then, these inquiries were divided into three groups: Data security issues can be broken down into three categories: (1) those that arise when integrating traditional infrastructures with a cloud's worth of features; (2) those that arise in cloud storage at every stage of the application life cycle (data processing, use, and transfer); and (3) those that are directly related to data security qualities like privacy, usability, and confidentiality. Each subgroup was urged to take an own path towards cloud data security.

Y. Ping et al. (2020) investigated into safe and public cloud data integrity verification system. They propose firstly a public data integrity verification method using elliptic curve cryptography and algebraic signature. This technique supports security from malicious attacks such as replay attack, replacement attack, and forgery attack and also allows a third-party authority to act as a substitute for users to verify the integrity of outsourced data. The best way to ensure data is kept private is to use symmetric encryption. They also construct an exclusive Hash List named "Divide and Conquer" which is helpful to carry out different operations such as insertion, deletion or modification of data in the list quickly and easily. The proposed method is proved to be superior to the available methods presented in the literature with respect to integrity verification and dynamic updating using security analysis and performance evaluation.

B.S. Rawal et al.(2018) studied the deconstruction of user data in a cloud storage system by employing disintegration protocol. Providers in the cloud provide servers, networks, and apps for use via the Internet. Users get access to the cloud services located in a data centre by way of an internet connection. This highlights the need of safeguarding cloud resources. Most security tools had only limited success and as intruders become increasingly sophisticated, security breaches are becoming

common. To reduce privacy issues from the start to some extent, as well as in the cloud, we propose to use a SDP in this work. The discussed architecture in this paper can be used in cloud storage along with our new concept of data compression and encoding. Through a probabilistic analysis, the SDP's tolerance for intrusion was determined.

R. P. Romansky et al. (2020) did researched on the privacy and data security in the digital age: new frontiers. This article aimed to establish some of the distinguishing features of the data and information security and define the main risks to user privacy and security in the digital age. They first sum up the main laws that play a role in the field of privacy and personal data protection and then go on to discuss other literature. Reviewed Information security against Assaults and key concepts in administration of Data Privacy. At the same time, they outline the principles that need to be followed to safeguard users' personal information in the light of the General Data Protection Regulation (GDPR) and they summarise the basic challenges that are arising with the digital world due to the use of technologies as new as social computing, cloud services, the Internet of Things, Big Data and Big Data Analytics which are threatening users' privacy by using innovative technologies.

R. K. Sadavarte et al. (2020) have published a study on the significance of protected data in the cloud. Data integrity and security in the cloud were the focus of this study. It is a study projects that deal with Data safety issues. Here, they explore in detail some of the data-protection approaches adopted across the world to ensure the most secure information possible. Later the study examines the different approaches to cloud security of data.

S. D. M. Satar et al., (2018) discussed issues of cloud data privacy and integrity architecture. When it comes to mainstream use of cloud computing, concerns about security are a major roadblock. Hesitation was also among several businesses and academic institutions regarding their move to totally cloud services to store their digital assets. The point of this, therefore, was to lay out the threats to users' privacy and data in the cloud. A random sampling of 20 articles was selected for this study on the approach used for the anonymity and security of data. The challenges that are involved in the method were presented.

In 2018, N. Singh et al. have proposed safeguards for confidential cloud data. They have developed a classification of the different techniques employed to secure vulnerable governmental data. Besides, they comprehensively analyzed the privacy-protective methods from the aspect of the privacy-protective standards. So, the creation and application of methods that monitored the use of data records in an anonymous way and were also able to trace their origin was greatly desired.

A Subhadra et al. (2020) studied the effects of cloud computing on privacy and security of data. When comparing various cloud services, security features are more important. While the benefits associated with cloud computing services are significant, users were right to worry about the security of any data they access via the cloud. In this article, the following aspects of cloud computing were discussed: data security, confidentiality regarding the data kept on the cloud, availability and integrity of data. How will hackers be stopped from gaining access to the data that is stored on the cloud? Cloud data risk management is another area of difficulty. Businesses

need to evaluate the risks of moving data and services to the Cloud before doing so. They talk through a few of the challenges of cloud adoption and offer strategies to conquer these challenges.

Suganya M et al. (2021) looked at how different heterogeneous multi-cloud storage and retrieval methods affect users' privacy. The research presented in this work analyzes the present best practices on data storage and retrieval in multi-cloud environments with heterogeneous clouds. It was looked into what the goals, method, implementation data and assessment parameters were for the approaches studied. In addition, the examined models' performance was compared in a small sample. Finally, a discussion of the research problem and future directions were given to allow the readers to narrow in on the research problem.

A comparative table has been prepared based on the literature research done above, which will help in better understanding of the different techniques as presented in Table 1.

Table 1 Literature Review

Sr. no.	Author/Year	Objective	Methodology	Limitation
1	Abdul-Jabbar /2020	The Importance of Data Integrity and Security in the Cloud	Cloud Computing, Security	Scope of work is limited
2	Abdulsalam, Y. S., /2022	Concerns about cloud computing security and privacy	Security, privacy, cloud computing	Did not considered Real life solution
3	Aldossary, S/ 2016	Data Integrity, Privacy, Availability, and the Future of Cloud Computing.	Security, Cloud Computing	There is not performed in future
4	Dey, H /2019	Improve the safety of cloud authentication and multi-tenancy with this unified paradigm.	Cloud, Secure	Lack of efficiency
5	Elsayed, M. / 2019	Providing cloud-based security evaluation for software as a service	Security, cloud	Need to improve the performance and accuracy
6	Gupta, I., /2022	Methods of Protecting Information When Storing It on the Cloud	Secure, Cloud	There is lack of performance
7	Hassan, J / 2022	Issues in Cloud Computing Security, Privacy, and Open Science	Cloud Computing	Research is limited to traffic flow
8	Kaja, D. V. S / 2022	Data Integrity Attacks in Cloud Computing	Data Integrity, Cloud Computing	There is less technical work
9	Kollu, J. / 2022	Applications of Cloud Data Storage for The Enhancement Of Privacy	Cloud Data Storage	Lack of security and accuracy
10	Kumar, V /2017	Data security in cloud computing.	Data security, cloud computing	There is lack of performance
11	Ping, Y /2020	Public data integrity verification scheme for secure cloud storage.	Data integrity, Secure	Lack of technical work
12	Rawal, B. S	Secure disintegration protocol for privacy preserving cloud storage.	Secure, Cloud storage	Performance of this research is very low

Problem Statement

It was clear from the literature that data security is important when reviewing it. There have already

been studies that demonstrate a higher risk of cyber-attacks than had previously been believed. Moreover, it was critical to ensure improved cloud data transfer performance. The simulation demonstrates that data

security is enhanced, using a multi-layer encryption approach. The suggested method can be used to enhance the security of clouds and provide a safer and better way to do so. Data packets are shrunk and compressed before sending to prevent delay that might occur if they were large because of congestion in the cloud. Such investigation is very relevant to cloud computing. The data in cloud apps would be encrypted and able to traverse greater distances without degradation in quality.

Proposed Work

Research methodology" refers to the entire process of designing, conducting, analyzing and interpreting a research. It involves choosing the method, tools and strategies to complete the study. The study utilizes the following approach as depicted in Figure 1 below.

1. With the goal of pinpointing where the current safeguards in the Cloud need improvement, a thorough literature assessment of relevant works will be conducted.
2. The different security factors in relation to Cloud computing will be identified.
3. The optimum security approach for this study will be determined by a comparison of the available options.
4. The collected data will be used to inform the design of a mechanism, which will then be implemented in a cloud model either in a simulator or with.NET.
5. There will be an assessment of how well the planned job really turns out.

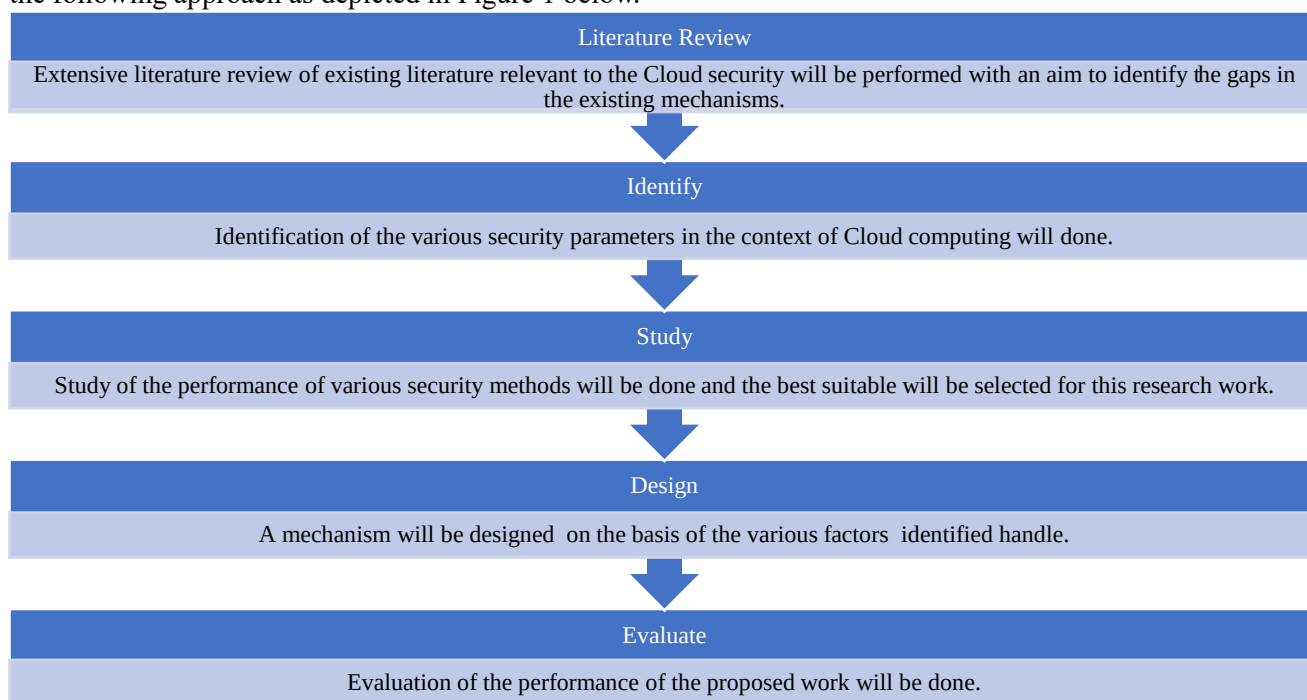


Figure 1 Research Methodology

Result and Discussion

Comparative analysis of performance

In this section, you'll see a simulation of the time it takes for processing. It has been shown that the time required to process a data set is much less than the time required by traditional processing methods. When comparing the two, this is the case. If you are keeping track of a data packet, then divide the total by 10 at regular intervals. The results of a study

comparing the planned work processing times to the typical work processing durations are shown in Table 2.

Table 2 Comparative analysis of performance

Data Packets	Conventional time taken	Proposed time taken
10	1.6546498	0.9317915
20	2.8705754	0.7065519
30	3.7942401	1.5133642
40	4.654424	2.2282392

50	5.3923387	3.1791161
60	6.4838232	4.2476274
70	7.6005827	5.5958466
80	8.4623807	6.7812614
90	9.8057716	7.2305574
100	10.212334	8.8522545

Taking table 2 into account, the following figure provides a comparative analysis of the performance of the recommended design as well as the conventional layout.

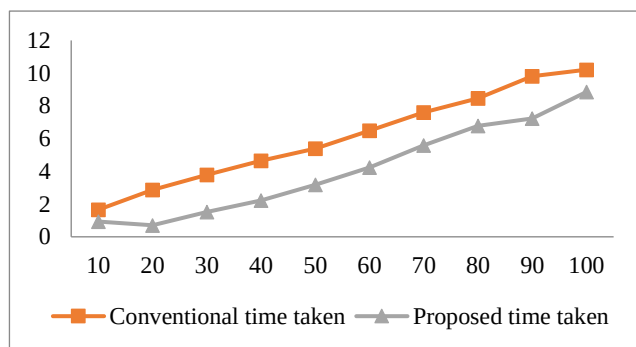


Fig 2 Comparative analysis of performance

Comparative analysis of error rate

In this section there is a model of how likely errors might be when data is processed. It was found that if the quantity of Data Packets is calculated every 10, the quantity of error that occurs is much smaller, compared to the traditional way. The researchers came to this conclusion. The comparison results on the error rate of the standard task processing time and the proposed task processing time are shown in table 3.

Table 3 Comparative analysis of error rate

Data Packets	Conventional Scheme	Proposed scheme
10	6	4
20	8	6
30	9	8
40	11	9
50	13	11
60	15	12
70	17	14
80	18	16
90	21	17
100	23	19

Figure 3 presents a comparative analysis of the error rate for both the old technique and the recommended scheme when table 3 is taken into account.

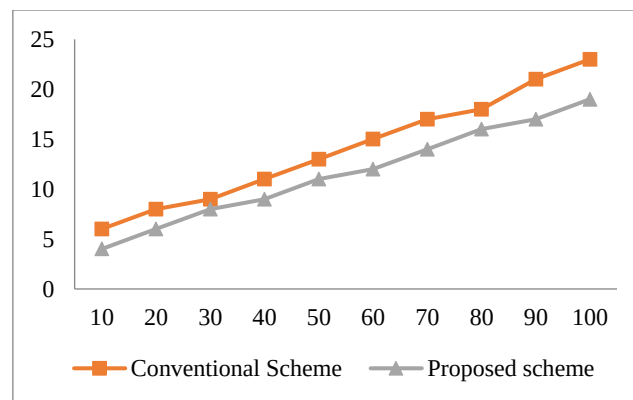


Fig 3 Comparative analysis of error rate

Comparative analysis of data affected by external attacks

This section of the paper models the results of data attacks from the outside. Examining Data Packets in packs of 10 showed that there were significantly fewer Data Packets contaminated by external attacks than with more traditional methods. The number of compromised Data Packets was compared to the overall number of Data Packets to get this conclusion. The findings of a comparison study of the compromised data are shown in Table 4. This study analyses the differences between the typical and suggested job processing times.

Table 4 Comparative analyses of data affected by external attacks

Data Packets	Conventional Scheme	Proposed scheme
10	7	5
20	9	6
30	10	8
40	13	10
50	13	10
60	17	13
70	17	14
80	19	16
90	21	17
100	24	19

When table 4 is taken into account, the following figure provides a comparative analysis of the data that have been affected by external attacks in the

circumstances of both the existing system and the recommended scheme.

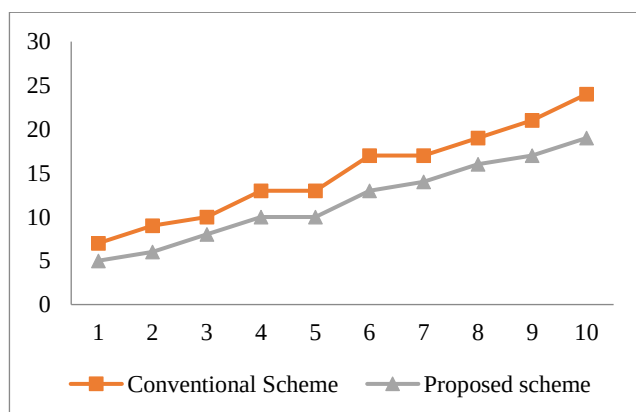


Fig 4 A comparative investigation of the data that have been subjected to external assaults

Conclusion

During review of literature, an issue of concern was data security. Based on the research available, cyber-attacks are not as uncommon as they used to be. It was also necessary to improve the performance of the clouds as data was being sent. The simulation has demonstrated that the data is safe and secure when it is well-protected using multiple layers. The proposed effort has been found to be more secure and better to help achieve safety and strengthening in the cloud security area. In order to avoid congestion when sending data through the cloud, packets are shrunk and compressed. This study would be of great importance in cloud computing. The information stored in the clouds will be encrypted and will be capable of traveling further without degradation.

Future Scope

The healthcare industry has started to adopt cloud computing networks to protect patient privacy and to transfer and share the data between medical institutions, labs, pharmaceutical companies and doctors. This is to maintain the patient's confidentiality. When used to the medical profession, optimization-based cloud computing apps may reliably detect serious, perhaps life-threatening errors. Because of its decentralized nature, data encryption is also a great option for companies and groups that deal with sensitive data, protecting its confidentiality. Another major and troublesome security concern for cloud computing-based systems is the potential weakness of the technology's

endpoints. At the end of the cloud computing network, any cloud computing action is possible, such as on a computer or mobile phone. Hackers would be able to monitor the user and attack only specific devices to obtain their key.

Declarations

Author Contributions

Vikas Kumar contributed to the conceptualization and design of the study, literature review, development of the proposed framework, methodology, analysis and interpretation of the results, and preparation and revision of the manuscript. The author has read and approved the final version of the manuscript.

Funding

The author received no financial support, grants, or other funding for the research, authorship, or publication of this article.

Acknowledgments

The author would like to thank the academic and research community whose published work contributed to the literature review and development of the proposed framework. The author also acknowledges the support of the institution and colleagues, where applicable, in facilitating the completion of this research.

Conflict of Interest

The author declares that there is no conflict of interest associated with this research, its authorship, or publication.

Generative AI Statement

The author declares that no generative artificial intelligence (AI) tools were used to generate, analyze, or interpret the research results or to develop the scientific content of this manuscript. The author takes full responsibility for the content, accuracy, and integrity of the work.

Data Availability Statement

The data generated or analyzed during the current study are available from the corresponding author upon reasonable request.

References

- Abdul-Jabbar, S. S., Aldujaili, A., Mohammed, S. G., & Saeed, H. S. (2020). Integrity and Security in Cloud Computing Environment: A Review. *Journal of Southwest Jiaotong University*, 55(1), 1–15. <https://doi.org/10.35741/issn.0258-2724.55.1.11>
- Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. *Future Internet*, 14(1). <https://doi.org/10.3390/fi14010011>
- Aldossary, S., & Allen, W. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions. *International Journal of Advanced Computer Science and Applications*, 7(4). <https://doi.org/10.14569/ijacsa.2016.070464>
- Alenizi, B. A., Humayun, M., & Jhanjhi, N. Z. (2021). Security and Privacy Issues in Cloud Computing. *Journal of Physics: Conference Series*, 1979(1). <https://doi.org/10.1088/1742-6596/1979/1/012038>
- Dey, H., Islam, R. and Arif, H., 2019, January. An integrated model to make cloud authentication and multi-tenancy more secure. In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)* (pp. 502-506). IEEE.
- Elsayed, M. and Zulkernine, M., 2019. Offering security diagnosis as a service for cloud SaaS applications. *Journal of information security and applications*, 44, pp.32-48.
- Gupta, I., Singh, A. K., Lee, C. N., & Buyya, R. (2022). Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions. *IEEE Access*, 10(June), 71247–71277. <https://doi.org/10.1109/ACCESS.2022.3188110>
- Hassan, J., Shehzad, D., Habib, U., Aftab, M. U., Ahmad, M., Kuleev, R., & Mazzara, M. (2022). The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges - A Systematic Literature Review (SLR). *Computational Intelligence and Neuroscience*, 2022(5). <https://doi.org/10.1155/2022/8303504>
- Kaja, D. V. S., Fatima, Y., & Mailewa, A. B. (2022). Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques. *International Journal of Research Publication and Reviews*, 3(2), 713–720. <https://doi.org/10.55248/gengpi.2022.3.2.8>
- Kollu, J., & Engineering, E. (2022). APPLICATIONS OF CLOUD DATA STORAGE FOR THE ENHANCEMENT OF PRIVACY-. 10(10), 151–159.
- Kumar, V., Chaisiri, S., & Ko, R. (2017). Data security in cloud computing. *Data Security in Cloud Computing*, 1–308. <https://doi.org/10.1049/PBSE007E>
- Ping, Y., Zhan, Y., Lu, K., & Wang, B. (2020). Public data integrity verification scheme for secure cloud storage. *Information (Switzerland)*, 11(9), 1–16. <https://doi.org/10.3390/INFO11090409>
- Rawal, B.S., Vijayakumar, V., Manogaran, G., Varatharajan, R. and Chilamkurti, N., 2018. Secure disintegration protocol for privacy preserving cloud storage. *Wireless personal communications*, 103(2), pp.1161-1177.
- Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17(5), 5288–5303. <https://doi.org/10.3934/MBE.2020286>
- Sadavarte, R. K., & Kurundkar, G. D. (2020). Data security and integrity in cloud computing: Threats and Solutions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3307, 356–363. <https://doi.org/10.32628/cseit206667>
- Satar, S. D. M., Hussin, M., Hanapi, Z. M., & Mohamed, M. A. (2018). Data privacy and integrity issues scheme in cloud computing: A survey. *International Journal of Engineering and*

- Technology(UAE), 7(3.28SpecialIssue 28), 102–105. <https://doi.org/10.14419/ijet.v7i3.28.20978>
- Singh, N., & Singh, A. K. (2018). Data Privacy Protection Mechanisms in Cloud. *Data Science and Engineering*, 3(1), 24–39. <https://doi.org/10.1007/s41019-017-0046-0>
- Subhadra, A. (2020). An Analysis of Data Security and Privacy for Cloud Computing. *Asian Journal of Computer Science and Technology*, 9(1), 27–39. <https://doi.org/10.51983/ajcst-2020.9.1.2153>
- Suganya, M., & Sasipraba, T. (2021). An analysis of privacy preserving data storage and retrieval approaches in heterogeneous multi-cloud architectures. *Indian Journal of Computer Science and Engineering*, 12(4), 878–884. <https://doi.org/10.21817/indjcse/2021/v12i4/211204074>
- Subramanian, N. and Jeyaraj, A., 2018. Recent security challenges in cloud computing. *Computers & Electrical Engineering*, 71, pp.28-42.
- Sun, P.J., 2019. Privacy protection and data security in cloud computing: a survey, challenges, and solutions. *IEEE Access*, 7, pp.147420-147452.
- Yan, Z., Deng, R.H. and Varadharajan, V., 2017. Cryptography and data security in cloud computing.
- Yassin, M., Talhi, C. and Boucheneb, H., 2019. ITADP: an inter-tenant attack detection and prevention framework for multi-tenant SaaS. *Journal of Information Security and Applications*, 49, p.102395.
- Zulifqar, I., Anayat, S., & Kharal, I. (2021). A Review of Data Security Challenges and their Solutions in Cloud Computing. *International Journal of Information Engineering and Electronic Business*, 13(3), 30–38. <https://doi.org/10.5815/ijieeb.2021.03.04>

Publisher's Note: *The Nimbus Journal and the editorial team remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The content presented reflects the authors' research and perspectives, and does not imply endorsement or dispute of territorial boundaries or institutional status by the publisher.*