Educational Administration: Theory and Practice
2024, 30(5), 9709-9720
ISSN: 2148-2403
https://kuey.net/

Research Article

Performance Enhancement Techniques In Hybrid Cloud Computing

Manesh[1*], Dr. Kamal[2]

[1*]Phd.Scholar, Computer Science and Engineering Department, OM Sterling Global University (Hisar)- 250011mjangra9717@gmail.com
[2]Associate Professor, Computer Science and Engineering Department, OM Sterling Global University (Hisar)-125001;kamaldhanda05@gmail.com

Citation: Manesh et al. (2024), Performance Enhancement Techniques In Hybrid Cloud Computing, *Educational Administration: Theory and Practice*, *30* (5), 9709-9720
Doi: 10.53555/kuey.v30i5.4632

ARTICLE INFO

ABSTRACT

The security concerns that are associated with cloud computing are investigated in this paper. The usage of data encryption and firewall security technologies has been used in a number of research projects in order to enhance protection. There is a possibility that performance may suffer if security is emphasized more, which is one of the issues that has been seen. As a consequence of this, a solution is needed that has the potential to either hold or improve performance while simultaneously providing better security features. In addition, machine learning has been used to differentiate between methods of data transportation that are safe and those that are not secure. When it comes to the hybrid approach, the combination of encryption and machine learning ultimately produces the desired outcomes, which are enhanced security without compromising efficiency. Combining a number of different strategies, such as AES encryption, replacement-based compression, and an LSTM machine learning model, is what the hybrid technique does.

Keywords: Data Security, Cloud Computing, Performance, Encryption, Machine learning.

1. INTRODUCTION

In today's rapidly evolving digital world, one of the most important things to focus on is enhancing the speed and security of various systems and applications. As our reliance on digital platforms continues to grow, we are finding ourselves confronted with more complex challenges in terms of ensuring efficiency and safeguarding ourselves against potential threats. In the beginning, we will investigate the reasons why performance enhancements are required. In practically every industry, including e-commerce platforms, scientific simulations, mobile applications, and enterprise-level software, there is a persistent need for systems that are both faster and more responsive. A lag-free experience is something that people expect whether they are using a website, a mobile app, or when they are processing huge datasets. In order for businesses and organizations to meet these expectations, they need to make consistent efforts to improve the efficiency of their processes. Among them are the enhancement of performance via the implementation of effective algorithms, the simplification of procedures, and the configuration of technology to optimize its capabilities. Cloud computing systems have been improved in terms of both security and efficiency thanks to the efforts of researchers. In an effort to reduce the amount of data, we used a content replacement method, which included exchanging big words for smaller ones using a substitution technique. Utilizing cryptography has resulted in an increase in the level of security. By using cloud computing technology, it is possible to transmit data on a consistent basis. The spread of this information may be found on the internet. As a result, customers should give consideration to the safety of their data while employing cloud services. The usage of education solutions that are hosted on the cloud is becoming more common among professionals, students, and educators. By enhancing the security and effectiveness of cloud-based remote education systems, this research project sets the standard for the quality of the service that is provided [1-4]. On the other hand, the establishment of robust security measures has emerged as a primary priority in parallel with the pursuit of performance advancements. Given the growing number of cyber threats, such as data breaches, identity theft, malware, and ransom ware attacks, the need to secure sensitive information and ensure system integrity has never been stronger. This is because the number of cyber threats is expanding. It is important for companies to establish stringent security

protocols, encryption technologies, and access limits in order to protect themselves from potential dangers and protect themselves from behaviors that are damaging or unlawful. In addition, there is a multifaceted and mutually advantageous link that exists between performance and security systems. When adopting modifications to boost speed, it is essential to keep security in mind in order to prevent unwanted effects. Some examples of these repercussions are the optimization of code, the elevation of system throughput, and the use of parallel computing technologies [5-7]. Although stringent security measures are essential for the protection of data and resources, they may sometimes result in performance concerns for the system owing to the overhead they produce. It is essential to maximize performance while simultaneously applying security measures in order to maintain the efficiency of systems and ensure that they are resistant to new threats. Due to the fact that user expectations are continually shifting and cyber threats are always there, there is an ongoing need to constantly enhance both performance and security. Organizations are required to continuously develop and modify their operating systems in order to guarantee the highest possible level of performance and to increase their defenses against potential vulnerabilities and attacks [9-11].

1.1 Background

Digitally recorded data is quickly becoming more valuable, says the author. Researchers in the fields of data processing, transmission, and storage employ the redundant residue number approach to find and fix mistakes efficiently. In order to include a wide range of ideas in the field of computing, the author suggested the term "cloud computing". Machine learning and optimization techniques are becoming more popular among manufacturing companies as a result of digitalization breakthroughs in the sector, the author claims. New computer resources and approaches, along with massive datasets, have changed several academic disciplines and promise enormously beneficial technological advances in the future. Governments are reportedly taking steps to make cities smarter in general, which will increase their intellect [12]. An plethora of pseudogenes due to redundancy induced by whole-genome duplication or the integration and transfer of gene segments by transposable elements makes the proper annotation of plant genomes a challenging process, as highlighted by the author. With an emphasis on cloud computing, this article surveys the current landscape of online learning, teaching, and education. As far as is currently understood, "cloud computing" is shorthand for a highly scalable model for providing various services over the internet. The use of cloud computing to the field of online education is the primary emphasis of this study. This study's findings show that having a streamlined system to preserve and retrieve important course materials and resources is very important to both students and teachers. Examining the pros and cons of cloud computing is the main goal of this research. The essay goes on to discuss risk and security divisions as well [13-16]. In this paper, we define cloud computing and show how to build a cloud computing platform that incorporates E-Learning.

1.2 Role of security in cloud computing

Cloud computing may deliver services over either a public or private network, depending on the needs of the user as determined by the situation. There is the possibility of accessing the cloud from a remote place. It is possible to utilize this device for wide area networks as well as local area networks. There is a possibility that cloud computing and virtual private networks (VPNs) interact with one another [17]. Only two of the numerous cloud-based applications that are available to users are Internet-based conference calling and electronic mail. Computing on the cloud has made platform independence more accessible than ever before. As there is no need for the client system to be set up, it is feasible. Over the course of the last several years, mobile apps have grown more commonplace in the corporate sector. Utilizing cloud computing, these programs might be shared with other users [18-20].

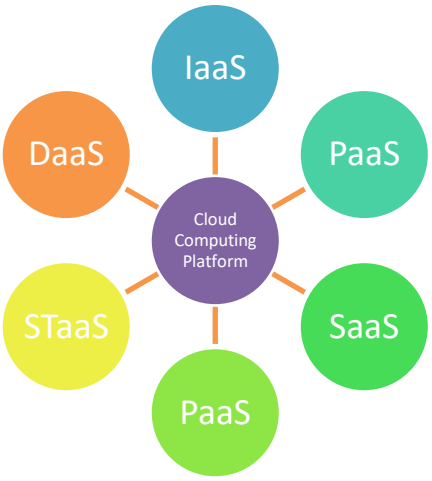

Fig 1 The cloud computing platform

The cloud computing platform is undergoing a number of infrastructure improvements in order to make it more user-friendly and accessible. One possible explanation for the growing demand for cloud services is that cloud applications are becoming more popular. The security of data is unquestionably a must in the modern day. It is not a simple process to receive big data sets from an external service provider in a secure manner. Customers have access to resources such as processing power and data storage inside computer systems thanks to cloud computing, which allows for on-demand access to these resources [21-23]. Large clouds often make use of a large number of data centers in order to provide their services. On the other side, if the concept of "pay as you go" is not well understood beforehand, cloud computing might result in expenses that are far higher than intended.

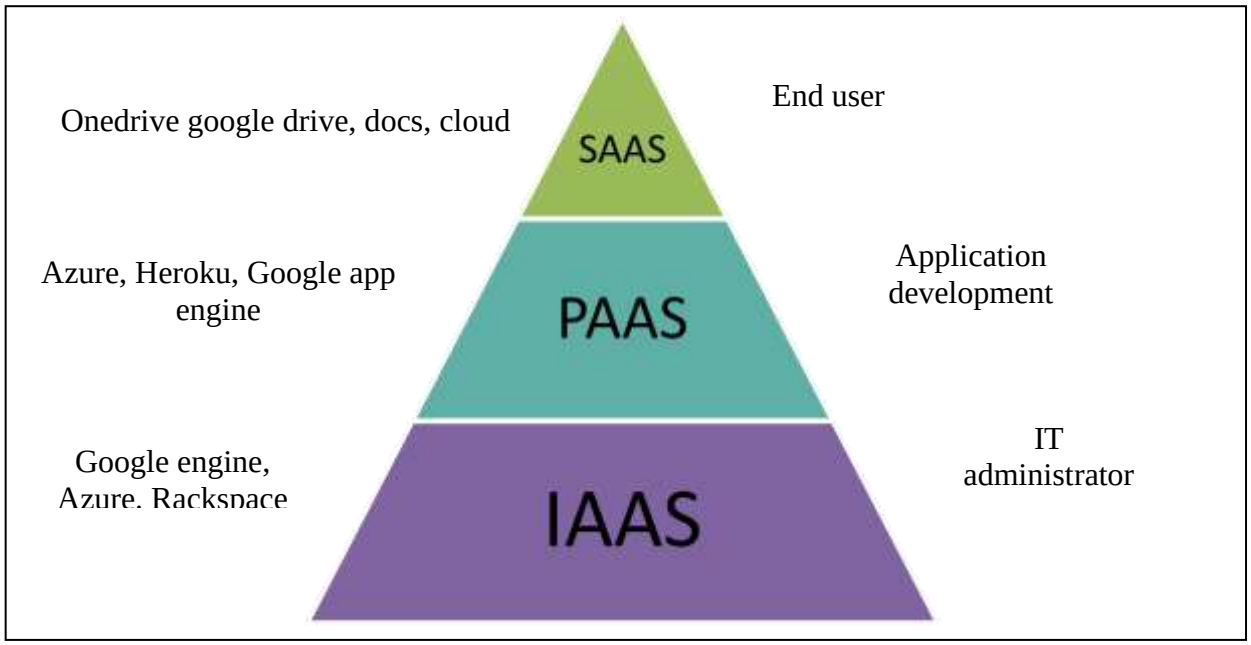

Fig 2 Cloud Service Level

On a daily basis, there is a rising need for cloud services. Users often make use of its applications. As a result of this, the protection of data is becoming more critical. Sensitive information cannot be sent to a service provider in a secure manner without additional effort. For the purpose of this study, researchers attempted to improve the security of cloud computing while working within the context of big data. This goal was accomplished via the use of cryptography. In cloud computing, data is sent on a regular basis. The spread of this information may be found on the internet. As a result, customers should give consideration to the safety of their data while employing cloud services [24].

Fig 3 Cloud Computing Security

A significant amount of research and development has been done on the topic of ensuring the security of cloud services while simultaneously managing enormous amounts of data. A number of them will be discussed in this section. The way in which individuals understand the IDS method is taken into consideration in this study. The user's requirements are taken into account, and the system offers protection [25-27]. Increases are made to the overall length of the network. It is possible to reduce the amount of power that the node consumes. The ability to split networks into smaller, more manageable chunks has been made feasible by local nodes, which has resulted in a significant improvement in the overall performance of the networks. Also, we acknowledge the existence of a realistic area controller in this scenario.

1.3 Predicted Observations

One of the most basic performance indicators is accuracy, which is simply the fraction of predicted observations that were actually observed divided by the total number of observations. When we speak about the accuracy of a set of measurements, we are referring to the extent to which they are representative of the actual value of the thing being measured. As a result of inadequate accuracy, which is quantified by this statistic for a particular measure of central tendency, the gap that exists between a result and a true value is referred to as trueness by the International Organization for Standardization (ISO). In order to achieve high accuracy, which in turn requires high precision and trueness, it is necessary to combine the two kinds of observational mistakes that were discussed before. It is also feasible to examine the validity of binary classification tests by examining the degree to which they are able to identify or exclude a certain condition. When seen from a different perspective, accuracy might be understood as the percentage of total occurrences in which the predictions were accurate. The result of this is a comparison of the likelihood before and after the test was carried out [28].

1.4 Challenges faced by Research

The challenges that cloud computing presents in educational environments have been the focus of study done in the past. It has also been investigated by researchers that security and risk divides exist. There is consideration given to the potential impacts that cloud computing might have on the academic community here. One of the most important goals for emerging nations is to strengthen their security measures. Hacking and cracking are actions that attackers engage in, and they represent a danger to the security of the system [29]. Cloud services are advantageous for a number of reasons, one of which is that they are always available to users. Cloud storage is essential for today's students since it allows them to access their data from any location and at any time. A portion of the investigation was focused on determining strategies to reduce the cost of receiving an education over the internet. The appropriate application of the most recent findings has also been the subject of previous research. Educating children and students in countries that are not yet developed via the use of online courses that are housed on the cloud is a difficult endeavor [30-34].

2. PROBLEM STATEMENT

In the realm of cloud computing and data security, there are many different kinds of research that may be conducted. On the other hand, it has been observed that there has been a dearth of research in the subject of data security. In addition to this, it is essential to design a hybrid model that is capable of efficiently controlling and addressing a variety of different types of attacks. This proposal would include the use of a machine-learning approach and would also involve the encryption of data. In the realm of cloud computing and data security, there are many different kinds of research that may be conducted. On the other hand, it has been observed that there has been a dearth of research in the subject of data security. In addition to this, it is essential to design a hybrid model that is capable of efficiently controlling and addressing a variety of different types of attacks. This proposal would include the use of a machine-learning approach and would also involve the encryption of data.

3. NEED OF RESEARCH

Modern studies employ cloud-based threat detection and security solutions increasingly. Compressing and encrypting data before transmitting it to cloud servers is a good practice. Thus, machine learning models like Long Short-Term Memory (LSTM) networks may improve security by detecting threats. Data compression reduces data size before transmission. Researchers and organizations can better optimize their bandwidth and reduce time delays, particularly when working with large volumes of data. Compression may effectively reduce data without compromising integrity. Encrypting data during transmission protects its privacy and integrity. This reduces unauthorised access and interception. AES or RSA may protect data before it is transferred from the originating place. RNNs like LSTM are good at sequential data analysis. It works in natural language processing, time series forecasting, and anomaly detection. Historical data may be used to train anomaly detection to detect anomalies. This helps identify and prevent security threats including unauthorized network access, malicious behaviors, and system anomalies. Before being delivered to cloud servers, data is compressed and encrypted to keep it private. Decryption and decompression are done on cloud servers. After processing, the LSTM model analyzes this data to detect dangers. Real-Time Monitoring and Response We provide alerts, prohibit suspicious activities, or start incident response when threats or irregularities are discovered. Data compression, encryption, and LSTM-based threat detection protect data during transmission and identify threats. Scalable and flexible cloud solutions allow enterprises to adapt to changing security needs and effectively handle enormous amounts of data. Cloud-based processing optimizes resource usage for threat detection without straining local infrastructure. Compliance with privacy and compliance laws is crucial when managing sensitive data. Data protection rules are met via strong encryption. Integrating cloud-based research approaches is a comprehensive strategy for boosting security while leveraging cloud computing infrastructure's scalability and flexibility. These methods include data compression, encryption, and LSTM threat detection. This holistic strategy helps organizations identify and minimize security threats, secure sensitive data, and meet legal requirements.

4 Proposed works

To achieve these objectives, research is considering the proposed research methodology that involved a systematic review of existing literature, an analysis of the challenges, and proposed model along with the evolution of comparison. Present research work has considered research related to cloud computing and security challenges and focus has been made on the factors that are influencing security. In this way proposed work would be capable to enhance security mechanism by LSTM in cloud. Finally comparison of the performance and security of conventional and proposed work would be made.

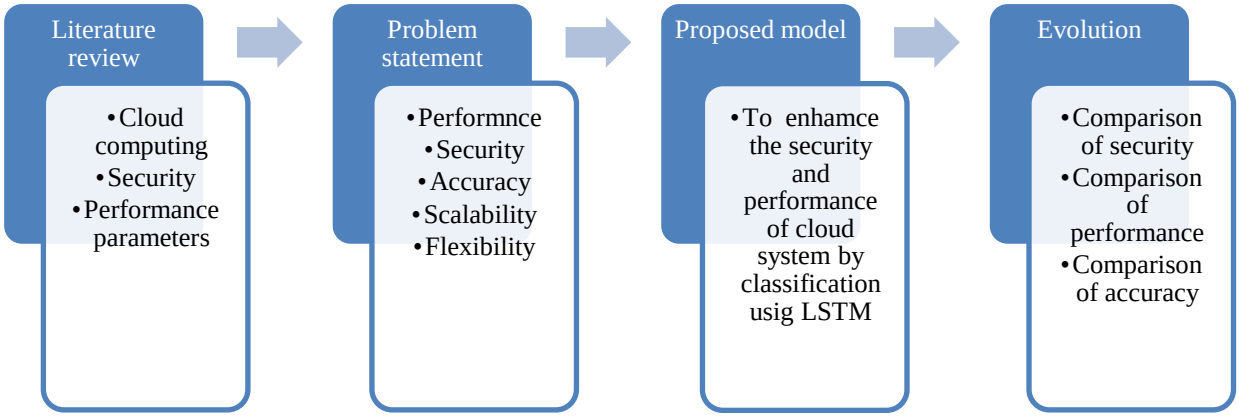

Fig Proposed Research Methodology

4.4 Proposed Work

To ensure the safety of cloud-based networks, the theoretical underpinnings for using polynomial encryption are laid forth in the current research. Incorporating novel hybrid cryptography algorithms into existing data encryption standards is the focus of this study, with the end goal of bolstering the security of polynomial-encrypted cloud server infrastructure. With so many companies using cloud services, it's important to evaluate your company's vulnerabilities.

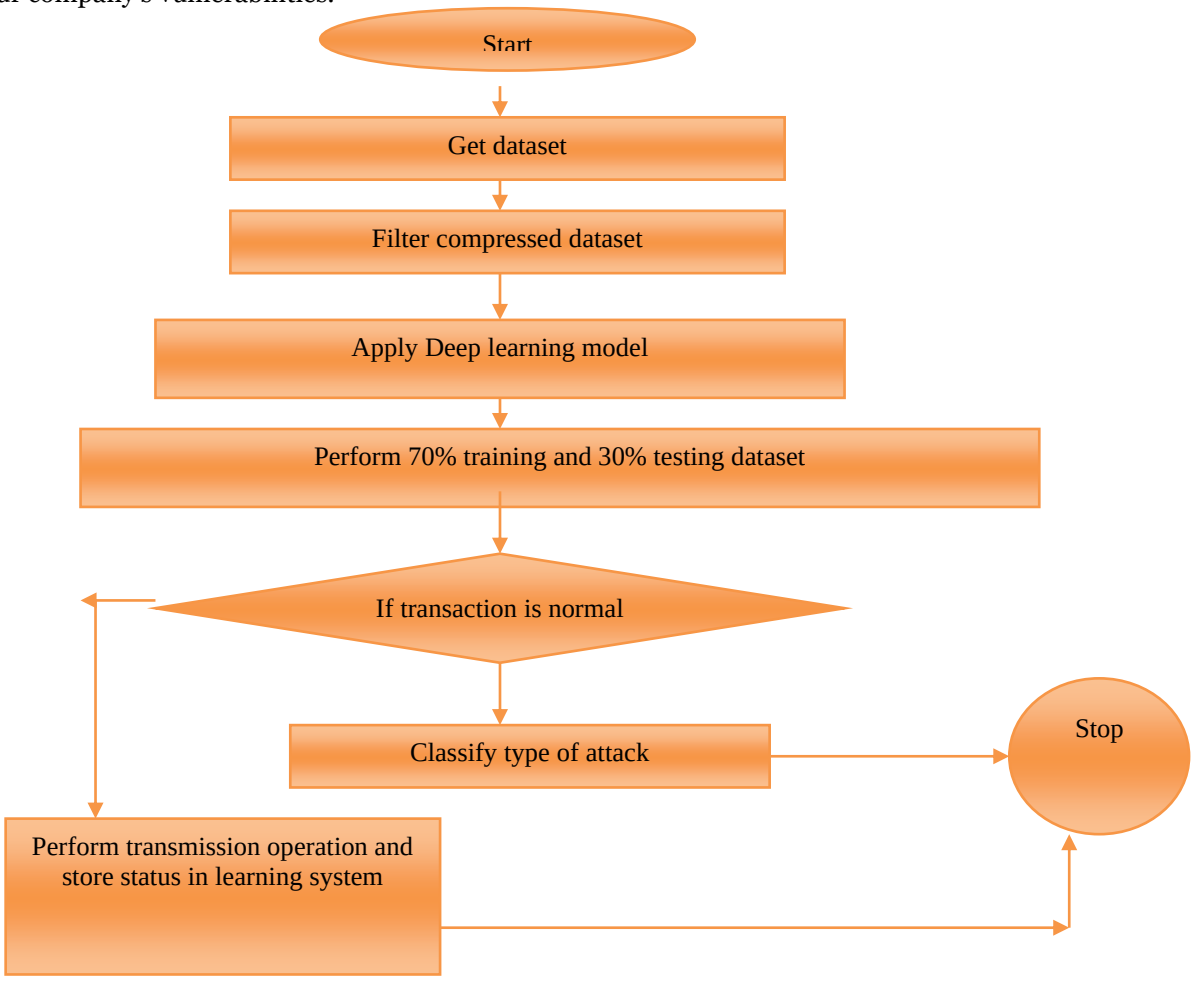

Fig 3 Process Flow of Proposed work

The rapid pace of innovation enabled by cloud computing has helped both the public and private sectors. This caused previously unforeseen concerns for people's safety. Because of the cloud service model's emergence as a means of offering technical redundancy for businesses, the computing landscape has undergone a profound transformation. Using deep learning, we were able to categorise the various forms of assault.

5. Result and discussion

To build an LSTM model for the classification of attacks, you'd start by preparing a dataset containing sequences of features representing network traffic data along with their corresponding attack labels. This dataset would be divided into training, validation, and testing sets. After preprocessing the data by tokenization, padding sequences, and encoding labels, you would design the architecture of the LSTM model. This architecture typically includes one or more LSTM layers followed by a dense layer for classification. Dropout layers may also be added for regularization to prevent overfitting. The model would be compiled with an appropriate loss function such as categorical cross-entropy and an optimizer like Adam. Training the model involves feeding the training data into the LSTM network and adjusting the model's parameters to minimize the loss. Hyperparameters such as learning rate, batch size, and number of epochs would be tuned to optimize performance. After training, the model's performance is evaluated on the validation set using metrics like accuracy, precision, recall, and F1 score to assess its effectiveness in classifying attacks. Finally, the trained LSTM model can be deployed to classify attacks in real-time scenarios, providing valuable insights into network security threats. Throughout this process, continuous refinement and iteration are essential to improve the model's accuracy and robustness in detecting and classifying different types of attacks effectively.
To implement an LSTM model for the classification of attacks, you would typically follow these steps:

1. Data Preparation: Prepare your dataset containing samples of attacks and their corresponding labels. Each sample should consist of input data (e.g., sequences of features representing network traffic data) and the corresponding attack label (e.g., indicating whether the sequence represents a normal or malicious activity).
2. Data Preprocessing: Preprocess your data by converting it into a format suitable for input into the LSTM model. This may involve tasks such as tokenization, padding sequences to ensure uniform length, and encoding labels into numerical format (e.g., one-hot encoding).
3. Model Architecture Design: Design the architecture of your LSTM model. This typically involves defining the number of LSTM layers, the number of units in each layer, the activation functions, and any additional layers such as dropout or dense layers for regularization and classification.
4. Model Compilation: Compile your LSTM model by specifying the loss function, optimizer, and evaluation metrics. For classification tasks, common loss functions include categorical cross-entropy, and popular optimizers include Adam or RMSprop.
5. Model Training: Train your LSTM model on the prepared dataset. During training, the model learns to extract features from the input sequences and predict the corresponding attack labels. Adjust the hyperparameters (e.g., learning rate, batch size, number of epochs) as needed to optimize performance and prevent overfitting.
6. Model Evaluation: Evaluate the performance of your trained LSTM model using metrics such as accuracy, precision, recall, and F1 score. You can also visualize the training and validation curves to assess model convergence and identify potential issues such as overfitting or underfitting.
7. Model Deployment: Once satisfied with the performance of your LSTM model, deploy it to classify attacks in real-world scenarios. This may involve integrating the model into an application or system capable of processing incoming data streams and making real-time predictions.

Throughout this process, it's important to iterate and refine your model based on the performance metrics and domain-specific considerations. Additionally, consider techniques such as hyperparameter tuning, data augmentation, and ensembling to further improve the performance of your LSTM model for attack classification.

Confusion matrix during attack classification on unfiltered dataset

Table 2 Confusion matrix during attack classification on unfiltered dataset

	Class 1	Class 2	Class 3	Normal
Class 1	2233	197	381	189
Class 2	168	2242	191	399
Class 3	196	353	2303	148
Normal	369	194	197	2240

Result

TP: 9018
Overall Accuracy: 75%

Table 3 Accuracy For Unfiltered

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	2966	3000	87.5%	0.74	0.75	0.75
2	2986	3000	87.48%	0.75	0.75	0.75
3	3072	3000	87.78%	0.77	0.75	0.76
4	2976	3000	87.53%	0.75	0.75	0.75

5.3 Confusion matrix during attack classification on filtered dataset

Table 4 Confusion matrix during attack classification on filtered dataset

	Class 1	Class 2	Class 3	Normal
Class 1	2491	112	299	98
Class 2	97	2586	102	215
Class 3	109	241	2557	93
Normal	198	59	97	2646

Result

TP: 10280
Overall Accuracy: 85%

Table 5 Accuracy For Filtered

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	2895	3000	92.39%	0.83	0.86	0.85
2	2998	3000	93.12%	0.86	0.86	0.86
3	3055	3000	92.16%	0.85	0.84	0.84
4	3052	3000	93.67%	0.88	0.87	0.87

5.3 Comparison Analysis of Parameters

1. ACCURACY

Table 6 shows the outcomes of each class's inventory of the quality of finished work and the priority of future assignments (1, 2, 3, and 4). Data that has been filtered has been proved to be more accurate than the original data that has not been filtered.

Table 6 comparison of accuracy

Class	Unfiltered dataset	Filtered dataset
1	87.5%	92.39%
2	87.48%	93.12%
3	87.78%	92.16%
4	87.53%	93.67%

Using the information in table 6, we can now compare the filtered and unfiltered datasets to demonstrate the improved accuracy of the filtered version in figure 4.

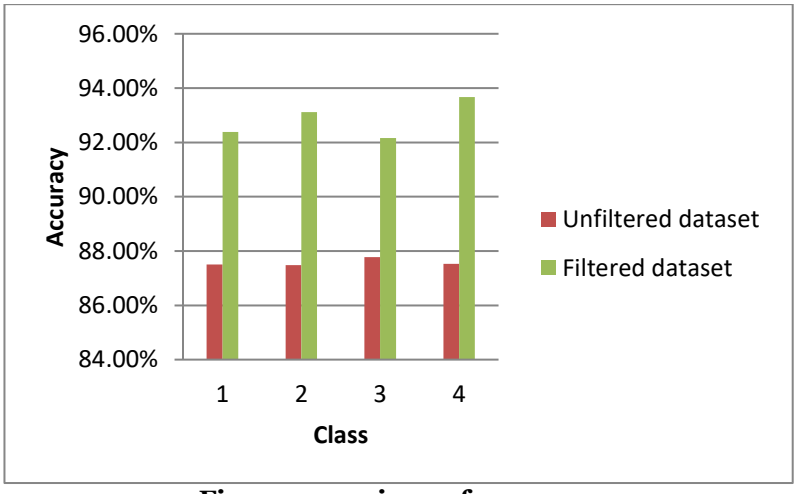

Fig 4 comparison of accuracy

2. PRECISION

Table 7 displays the results of taking into account the accuracy of past and projected work for classes 1, 2, 3, and 4. In comparison to the unfiltered dataset, the precision of the filtered one is much higher.

Table 7 comparison of precision

Class	Unfiltered dataset	Filtered dataset
1	0.74	0.83
2	0.75	0.86
3	0.77	0.85
4	0.75	0.88

When comparing the filtered and unfiltered data sets, recall in the filtered dataset is seen in figure 5.

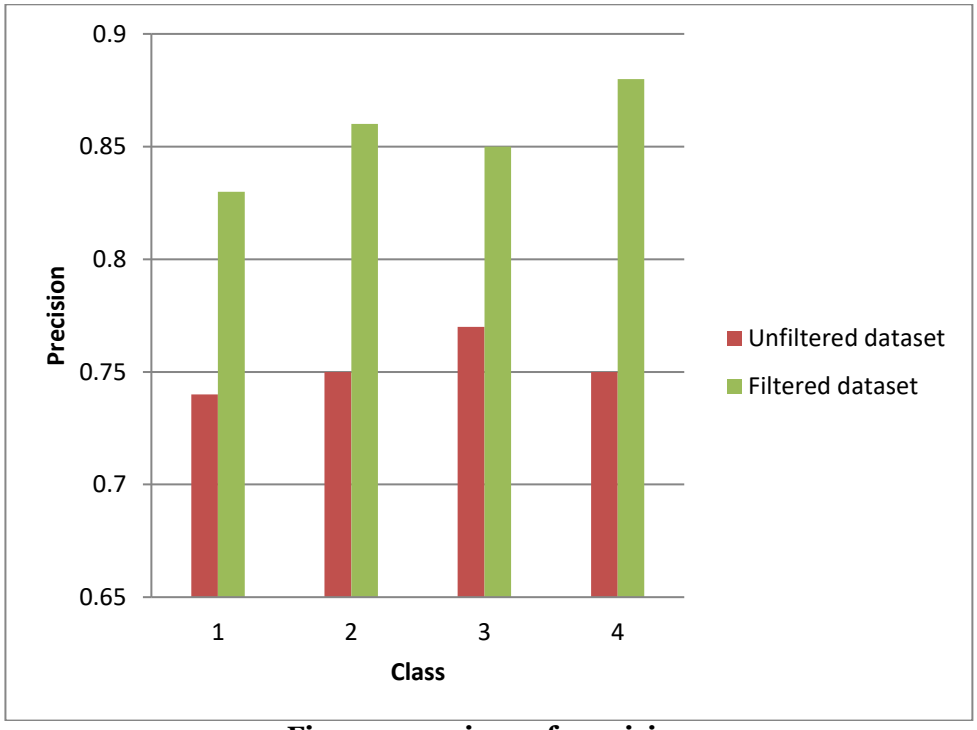

Fig 5 comparison of precision

3. RECALL VALUE

Table 8 displays the results of comparing the recall values of the existing work with the proposed work for classes 1, 2, 3, and 4. One difference between the filtered and unfiltered datasets is shown in the Recall value.

Table 8 comparison of Recall value

Class	Unfiltered dataset	Filtered dataset
1	0.75	0.86
2	0.75	0.86
3	0.75	0.84
4	0.75	0.87

Taking into account the data in table 8, we can see how the filtered dataset performs in terms of recall by comparing it to the unfiltered dataset in picture 6.

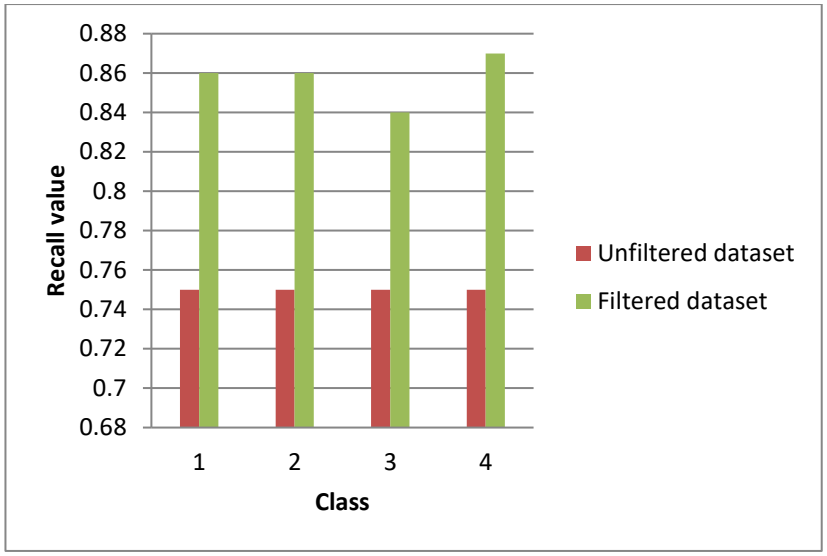

Fig 6 comparison of recall value

Table 9 displays the F1-scores of completed and planned projects in each of the four classes. The F1-Score of the filtered dataset improves over the unfiltered one.

4. F1- SCORE

Table 9 comparison of f1-score

Class	Unfiltered dataset	Filtered dataset
1	0.75	0.85
2	0.75	0.86
3	0.76	0.84
4	0.75	0.87

Figure 7 was created based on data in table 9 to demonstrate the difference between the filtered and unfiltered F1-scores.

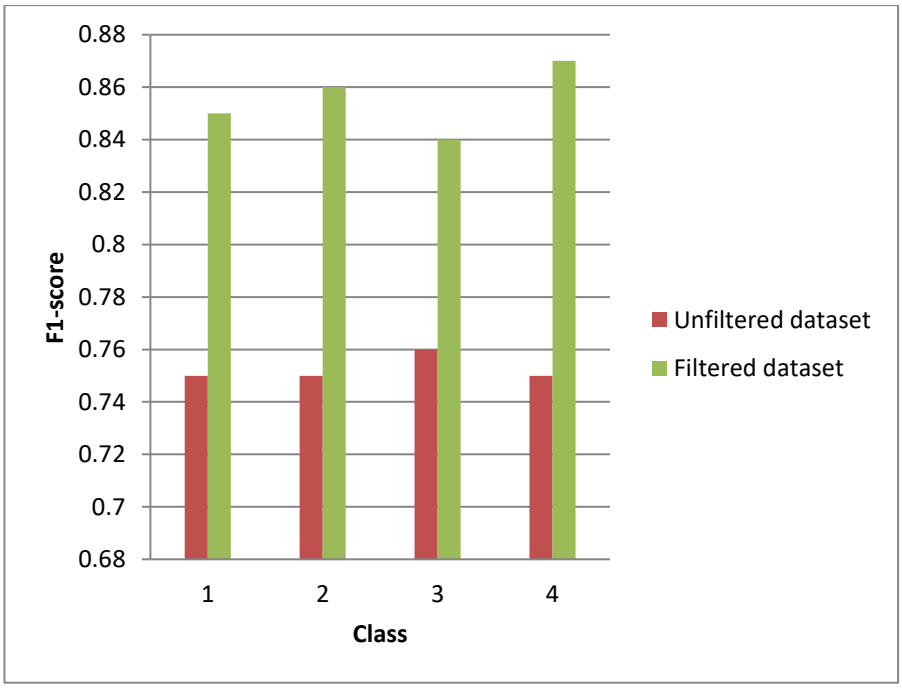

Fig 7 comparison of f1-score

4. DISCUSSION

It has been finished with the effort that was advised, which has resulted in a reduction in the amount of time that the LSTM model takes to process. This is an example of a technique that may be used to simulate the passage of time. In order to diagnose cancer using the LSTM module, it is necessary to get a standard sample

for cloud. In order to demonstrate the time difference, you need develop a simulation module in Python. The proposed research effort focuses on enhancing the efficiency, accuracy, and security of cancer diagnosis using LSTM models within cloud-based environments. The optimization techniques employed aim to reduce processing time, space utilization, and vulnerability to security threats. In the context of time simulation, efforts have led to significant reductions in the processing time of the LSTM model, showcasing the efficacy of the applied techniques. This reduction is crucial for timely diagnosis and treatment planning in cancer detection scenarios. Through python simulations, the comparative analysis of time differences underscores the efficiency gains achieved. Similarly, the optimization work extends to size simulation, where the space occupied by the LSTM model is minimized.

By obtaining standard samples and calculating sample sizes, the disparity in dataset sizes is demonstrated through PYTHON simulations. This reduction in size is essential for efficient storage and processing within cloud environments. Furthermore, the research evaluates the impact of optimization techniques on accuracy and security. Simulation results illustrate improvements in accuracy metrics, enhancing the reliability of cancer diagnosis. Additionally, the comparative analysis of security measures, including the vulnerability to attacks, highlights the effectiveness of proposed adjustments. Specifically, the research suggests that compared to traditional encryption methods, the proposed techniques result in fewer impacted packets, thus reducing susceptibility to security breaches. The research endeavors to advance cancer diagnosis through LSTM models while addressing critical concerns related to time efficiency, data size, accuracy, and security within cloud-based environments. The simulations conducted using PYTHON serve as valuable tools for assessing the efficacy of proposed optimizations and their potential impact on improving healthcare outcomes while ensuring data integrity and security.

5. FUTURE SCOPE

The safety concerns that are associated with cloud computing are investigated in this research. Several different kinds of research have been conducted in the past that have used data encryption and firewall security techniques in order to improve protection. Security upgrades have been demonstrated to have a negative impact on system performance, according to research. As a result, a strategy is necessary in order to give improved performance in addition to higher security. Differentiating between secure and unsecure data transfers has been accomplished via the use of machine learning. Encryption and machine learning are both components of the hybrid approach, which aims to improve security without causing the process to become more sluggish. In the hybrid technique, an LSTM machine learning model, replacement-based compression, and encryption are all included. The performance and security of the cloud might be improved with the use of additional safeguards. In order to improve security, a number of different security methods might be used. The use of an optimization strategy might potentially improve performance if more study is conducted. In addition, in order to improve the reliability of cloud computing, future study should investigate the possibility of high availability and eliminating downtime. It is possible that more techniques exist that have the potential to enhance both the security and performance of the cloud. Additionally, for the purpose of enhancing security, a variety of security measures might be used. Through the use of an optimization technique, more study could be able to increase the performance. In addition, the next study may also take into account the high availability and zero downtime of cloud computing in order to enhance its dependability.

REFERENCE

1. K. Patel, "Performance analysis of AES, DES, and Blowfish cryptographic algorithms on small and large data files," Int. J. Inf. Technol., vol. 11, no. 4, pp. 813–819, 2019, doi: 10.1007/s41870-018-0271-4.
2. A. Tchernykh et al., “Performance evaluation of secret sharing schemes with data recovery in secured and reliable heterogeneous multi-cloud storage,” Cluster Comput., vol. 22, no. 4, pp. 1173–1185, 2019, doi: 10.1007/s10586-018-02896-9.
3. K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, “Enhancing the security of cloud data using hybrid encryption algorithm,” J. Ambient Intell. Humaniz. Comput., no. 2018, 2019, doi: 10.1007/s12652-019-01403-1.
4. D. Weichert, P. Link, A. Stoll, S. Rüping, S. Ihlenfeldt, and S. Wrobel, “A review of machine learning for the optimization of production processes,” Int. J. Adv. Manuf. Technol., vol. 104, no. 5–8, pp. 1889–1902, 2019, doi: 10.1007/s00170-019-03988-5.
5. G. Nguyen et al., “Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey,” Artif. Intell. Rev., vol. 52, no. 1, pp. 77–124, 2019, doi: 10.1007/s10462-018-09679-z.
6. I. S. Farahat, A. S. Tolba, M. Elhoseny, and W. Eladrosy, Data Security and Challenges in Smart Cities. Springer International Publishing, 2019. doi: 10.1007/978-3-030-01560-2_6.
7. R. C. Sartor, J. Noshay, N. M. Springer, and S. P. Briggs, “Identification of the expressome by machine learning on omics data,” Proc. Natl. Acad. Sci. U. S. A., vol. 116, no. 36, pp. 18119–18125, 2019, doi: 10.1073/pnas.1813645116.

8. Dr. Pranav Patil, “A Study of E-Learning in Distance Education using Cloud Computing“ International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 5, Issue. 8, August 2016, pg.110 – 113.
9. Asgarali Bouyer, Bahman Arasteh "The Necessity Of Using Cloud Computing In Educational System" CY-ICER 2014, 1877-0428 © 2014 Elsevier.
10. Agah Tugrul Korucu, Handan Atun "The Cloud Systems Used in Education: Properties and Overview " World Academy of Science, Engineering, and Technology International Journal of Educational and Pedagogical Sciences Vol:10, No:4, 2016
11. Ananthi Claral Mary.T, Dr.Arul Leena Rose. P.J "Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art" INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 12, DECEMBER 2019
12. Arshad Ali, Amit Bajpeye, Amit Kumar Srivastava" E-learning in Distance Education using Cloud Computing" International Journal of Computer Techniques -– Volume 2 Issue 3, May – June 2015
13. Sudhir Kumar Sharma, Nidhi Goyal, Monisha Singh" Distance Education Technologies: Using E-learning System and Cloud Computing" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1451-1454
14. Yinghui Shi , Harrison Hao Yang , Zongkai Yang and Di Wu” Trends of Cloud Computing in Education” S.K.S. Cheung et al. (Eds.): ICHL 2014, LNCS 8595, pp. 116–128, 2014. © Springer International Publishing Switzerland 2014
15. Sanjay Karak, Basudeb Adhikary "CLOUD COMPUTING AS A MODEL FOR DISTANCE LEARNING" International Journal of Information Sources and Services, Vol.2: July-aug 2015, issue 4
16. Jyoti Prakash Mishra, Snigdha Rani Panda, Bibudhendu Pati, Sambit Kumar Mishra” A Novel Observation on Cloud Computing in Education” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019
17. Awatef Balobaid, Debatosh Debnath” A Novel Proposal for a Cloud-Based Distance Education Model” International Journal for e-Learning Security (IJeLS), Volume 6, Issue 2, September 2016
18. Xu zhihong, Gu junhua, Dong yongfeng, Zhang Jun, Li-yan "Expand distance education connotation by the construction of a general education cloud "International Conference on Advanced Information and Communication Technology for Education (ICAICTE 2013)
19. G. P. Pandey, “Implementation of DNA Cryptography in Cloud Computing and Using Huffman Algorithm, Socket Programming and New Approach to Secure Cloud Data,” SSRN Electronic Journal. Elsevier BV, 2019. doi: 10.2139/ssrn.3501494
20. K. Singhal, “Secure Communication using RSA Algorithm for Cloud Environment,” pp. 143–148, 2016.
21. L. Hanupriya and S. Anto Ramya, “Data security in cloud computing using RSA Algorithm,” Data Anal. Artif. Intell., vol. 3, no. 2, pp. 95–98, 2023, doi: 10.46632/daai/3/2/18.
22. I. Bandara, F. Ioras, and K. Maher, “Cyber Security Concerns in E-Learning Education,” Proc. ICERI2014 Conf., no. November, pp. 728–734, 2014.
23. E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Data Security Model for Cloud Computing,” Unpublished, 2013, doi: 10.13140/2.1.2064.4489
24. S. Eldin Fattoh Osman, Mohammed Eltahir Abdelhag, and Saad Mamoun, “Performance Analysis of Cloud based Web Services for Virtual Learning Environment Systems Integration,” Int. J. Innov. Sci. Eng. Technol., vol. 3, no. 4, pp. 356–362, 2016.
25. I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” Journal of Big Data, vol. 7, no. 1. Springer Science and Business Media LLC, Jul. 01, 2020. doi: 10.1186/s40537-020-00318-5.
26. S. Namasudra, R. Chakraborty, S. Kadry, G. Manogaran, and B. S. Rawal, “FAST: Fast Accessing Scheme for data Transmission in cloud computing,” Peer-to-Peer Networking and Applications, vol. 14, no. 4. Springer Science and Business Media LLC, pp. 2430–2442, Aug. 28, 2020. doi: 10.1007/s12083-020-00959-6.
27. W. Li et al., “A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System,” Mobile Networks and Applications, vol. 26, no. 1. Springer Science and Business Media LLC, pp. 234–252, Jan. 06, 2021. doi: 10.1007/s11036-020-01700-6.
28. P. Karthika and P. Vidhya Saraswathi, “RETRACTED ARTICLE: IoT using machine learning security enhancement in video steganography allocation for Raspberry Pi,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 6. Springer Science and Business Media LLC, pp. 5835–5844, Jun. 04, 2020. doi: 10.1007/s12652-020-02126-4.
29. L. Liu, M. Gao, Y. Zhang, and Y. Wang, “Application of machine learning in intelligent encryption for digital information of real-time image text under big data,” EURASIP Journal on Wireless Communications and Networking, vol. 2022, no. 1. Springer Science and Business Media LLC, Mar. 21, 2022. doi: 10.1186/s13638-022-02111-9.
30. M. Verkerken, L. D’hooge, T. Wauters, B. Volckaert, and F. De Turck, “Towards Model Generalization for Intrusion Detection: Unsupervised Machine Learning Techniques,” Journal of Network and Systems Management, vol. 30, no. 1. Springer Science and Business Media LLC, Oct. 17, 2021. doi: 10.1007/s10922-021-09615-7..

31. W. Ma, T. Zhou, J. Qin, X. Xiang, Y. Tan, and Z. Cai, “A privacy-preserving content-based image retrieval method based on deep learning in cloud computing,” Expert Systems with Applications, vol. 203. Elsevier BV, p. 117508, Oct. 2022. doi: 10.1016/j.eswa.2022.117508.
32. V. Balamurugan, R. Karthikeyan, B. Sundaravadivazhagan, and R. Cyriac, “Enhanced Elman spike neural network based fractional order discrete Tchebyshev encryption fostered big data analytical method for enhancing cloud data security,” Wireless Networks, vol. 29, no. 2. Springer Science and Business Media LLC, pp. 523–537, Oct. 03, 2022. doi: 10.1007/s11276-022-03142-2.
33. R. Gupta, D. Saxena, and A. K. Singh, “Data Security and Privacy in Cloud Computing: Concepts and Emerging Trends.” arXiv, 2021. doi: 10.48550/ARXIV.2108.09508.
34. P. K. Bal, S. K. Mohapatra, T. K. Das, K. Srinivasan, and Y.-C. Hu, “A Joint Resource Allocation, Security with Efficient Task Scheduling in Cloud Computing Using Hybrid Machine Learning Techniques,” Sensors, vol. 22, no. 3. MDPI AG, p. 1242, Feb. 06, 2022. doi: 10.3390/s22031242.