RESEARCH
www.commprac.com
ISSN 1462 2815

IMPLEMENTATION OF SYSTEMATIC SECURITY TECHNIQUE FOR DATA STORAGE IN CLOUD COMPUTING USING MACHINE LEARNING

Shalini Singh [1]*, Dev Baloni [2] and Manash Sarkar [3]

[1] PhD Scholar, Quantum University, Roorkee, India.
*Corresponding Author Email: shalini027.singh@gmail.com
[2] Associate Professor, Quantum University, Roorkee, India.
Email: devbaloni1982@gmail.com
[3] Associate Professor, Atria Institute of Technology, Bangalore, India.
Email: manash.sarkar26@gmail.com

DOI: 10.5281/zenodo.11076419

Abstract

Cloud computing (CC) is providing on-demand network resources that is used for data storage without concern of processing ability and physical hardware capabilities. A data contribution in the CC is a strategy to permit clients to promisingly give a correction of passage to data or an information in excess of the cloud. Lately, some public and private platforms are provided to the clients through the Internet. Because it built the cloud on a per- user subscription model, retrieving the required document will take longer, increasing the financial burden and lowering cloud users' satisfaction. There are different approaches to support user seclusion and protect the data in CC. Security should be provided to store any kind of data and storing that data in a cost-effective manner. The data holder revaluates their information in the cloud because of cost diminishing and the tremendous assets given by cloud administrations. For a secure cloud storage system, the suggested work combines a multi-layered neural network architecture together with encryption and DSA and AES encryption algorithm with Cosine similarity. Cloudsim simulator is used to perform and implement a secure cloud platform with real-time scenarios. To test the suggested work's recall and accuracy, we experimented on 700 text pieces. The average accuracy was 93.57 percent. According to simulation results, the suggested method provides high level of security for data storage in cloud computing.

Keywords: Cloud Security, Encryption and Decryption, Machine learning, Cloudsim.

1. INTRODUCTION

A technological advancement known as cloud computing (CC) provides information technology infrastructure, platforms, and software as internet services. Cloud registration is becoming more common and is being used more frequently. A small number of organisations are making investments in this field, either for their own needs or to help others. Due to the least upfront capital investment, greatest scalability, and other advantages of the cloud environment, a significant number of academic institutions, government agencies, and business companies are adopting it. The cloud environment supports a variety of advantages, but it also has a number of drawbacks. In the context of information security and cloud computing, data protection is of utmost importance [1].

One effect of the innovation in cloud computing is the rise of new security issues for both consumers and businesses. As security threats are a growing concern today, providing data protection is crucial for preserving any organization's data. The main goal is to give freedom to the customers to pay according to the use and what they require while promising benefits for their product or framework requirements upon request.

It is the realisation of a long-held desire known as Computing for the emergence of new security concerns for both business and consumers are one of the results of cloud computing innovation. There are always dangers involved when keeping sensitive data on third-party service providers, despite the highest industry certifications and security criteria put in place by cloud service providers. When talking about data security, especially when handling sensitive data, security and privacy must be given substantial consideration. To address this issue, many solutions have been developed. There is a lack of analysis in the available solutions, so it is essential to find, categorise, and analyse the significant previous work. [2]

Without a direct special arrangement by the client, cloud computing is providing the resources to the end-users that is particularly used for data storage and information analytics. A phrase that is frequently used but might mean different things to different people is distributed computing. However, CC faces several security issues that prevent the computing model from being quickly adopted, such as client and association vulnerability.

This paradigm's distributed idea forces a change in the security strategies employed in distributed computing. Additionally, as information may pass via several distributed hubs connected to the Web before reaching the cloud, it is important to adopt special encryption mechanisms. Edge hubs may also be asset-obligated devices, which would limit the options for security measures. It is plausible to shift ownership of information from service providers to end users by keeping information at the edges.

Threats to confidentiality, integrity, and availability encompass the main security issues in CC. Cloud services range from information storage to software service management, with needs for indefinite availability. As an impermeable environment that can provide architecture, services, and computing power at request, CC is frequently built [3]. Large uses of infrastructure and hardware assets are encouraged and made possible by the cloud model (to supply the supported service) [4]. CC is a new computer model, therefore despite its benefits, it still has drawbacks. Not every service, every provider customer, or every party involved will benefit from every cloud deployment approach [5]. This study discusses the security concerns and difficulties in CC as well as related machine learning (ML) algorithmic solutions.

Artificial intelligence known as machine learning enables software programmes to get better at making predictions and generating the patterns based on the history. It will generate outputs for new inputs using the trained model generated from the past outcomes. There are numerous approaches to employ machine learning for cloud attack detection. It recognises when an attack occurs, targets users, and stops the attack in its tracks by scanning the security system for flaws.

Machine learning techniques, which include several algorithms that can recognise patterns in data and make predictions based on those patterns, are highly useful for spotting threats. Machine learning algorithms are currently the most common for evaluating data that has been heavily used in the education sector. The AES encryption method has been used to secure data, helping to shield it from malevolent users. When storing items close to home that are recognisable in cloud climate, security requirements significantly increase. The data is then stored to cloud since it is easier to operate and cost-effective.

The contribution of this article is as follows:

- To study how to store data with high security using encryption methods in Machine Learning.
- To implement advanced concepts of ML to segregate and classify data.
- To execute capable data security.
- AES and DES algorithms are used for securing the data.
- To store information in Cloud which is cost proficient.
- To design the efficient and secure system which is cost effective.

Rest of the paper is organized in distinguished sections such as section II explain the researches have been conducted by the researchers. Section III proposed a methodology through which the setup is prepared and implemented. In section IV, results analysis is done in terms of distinguished parameters based on ANN algorithm. Finally, paper is concluded in the last section with future work.

2. LITERATURE SURVEY

The Cloud computing (CC) [6] is a developing pattern in numerous fields like IT areas, clinics, finance on account of the compelling use of assets through the arrangements. Each advancing execution in the cloud faces numerous difficulties like protection and security of client's information. In a unified climate, the information can be adjusted without the information on proprietor by unapproved clients (i.e., security break is unavoidable). The research team's [7] focus is on the development and enhancement of the C3ISP Framework and an API Gateway that provides an extension between end users and their information sources. It streamlines end users' access to their CTI data and controls data sharing contracts to sanitise the information. The results of these tests will demonstrate the effectiveness of our entryway design as well as the benefits it will provide to end users who use it to access the C3ISP substructure [8].

The author suggests CloudDLP, a transparent and scalable method that enables businesses to use various cloud apps that are browser-based to automatically sanitise sensitive data in photos and documents. An enterprise deploys CloudDLP as an internet gateway to sanitise sensitive premise data using JavaScript injection techniques and deep learning techniques. In browser-based cloud storage services, it has no discernible impact on application functionality or user experience. a number of real-world cloud apps were used to assess CloudDLP. The experimental findings demonstrate that automatic data sanitization is possible with cloud storage services while maintaining the majority of cloud application functions. [9]

Author officially defines, identifies potential violations of, and introduces a new method that demonstrably upholds data consistency in multi-cloud storage systems. The suggested technique can preserve data consistency with a delay in data uploading, according to the implementation and trials, and it is scalable in terms of both the number of clouds used and the number of users. The usefulness and dependability of multi-cloud storage systems will be improved by incorporating this technique. [10]

The regular operation of the network security defence systems is ensured by model's prediction of the security state and detection of attacks based on recent malicious attacks. Simulation studies confirm the viability of the cloud trust model and Deep

Belief Networks (DBN) models. Comparing the DBN algorithm to the Support Vector Machine (SVM) algorithm, the DBN algorithm increases the correct identification rate of unknown samples by 4.05%. [11]

The author offers a feature-engineered, cloud-based intrusion detection model based on random forest (RF). To improve accuracy (ACC) of the suggested detection model, the RF classifier is specifically obtained and integrated. The suggested model technique has been assessed and verified on two datasets and, when using the Bot-IoT and NSL-KDD datasets, respectively, yields 98.3% ACC and 99.99% ACC. As a result, when compared to current relevant efforts, the acquired findings exhibit good ACC, precision, and recall performances [12].

The author discussed various ways to protect data secrecy in cloud environments; one of them is encryption, which is a popular way to do so. This study makes an effort to review the encryption methods used to protect the confidentiality of the data. The type of approach and the type of validation employed to support the approach are used to categorise the review outcomes [13]

With machine and deep learning approaches for attack detection, the emphasis is on highlighting various security attacks in the cloud. Review various Machine Learning (ML) techniques to address cloud security issues [14].

The best machine learning method has been identified by the author for analysing cloud network data for anomaly detection. In order to conduct a systematic review, this research study used academic articles released between 2017 and 2023. This review study has discussed numerous methods and techniques for finding anomalies in the cloud. [15]

The development of numerous frameworks nowadays enables customers for the handling of cloud data. They are typically constructed utilising distributed networks, cryptosystems, or a combination of the two. The primary security measures for practically all current implementations include Secure Multi-Party Computation (SMC), homomorphic cryptosystems, Secret Share Schemes (SSS), and Service-Oriented Architecture (SOA). The biggest issue with applying these techniques for massive data analysis on the cloud is the computational expense of image processing operations. The biggest difficulty is preventing unauthorised access to medical records and private health information. A novel method for safeguarding data processing in a cloud environment was developed by the authors of [16] based on machine learning techniques. To better classify picture pixels (FCM), we frequently employ Support Vector Machines (SVM) and Fuzzy C-means Clustering. The CloudSec module, a third level, is added to the traditional two-tiered architecture to reduce the risk of medical data leakage. To evaluate the suggested method, they run two sets of tests. Support Vector Machines (SVM) are a good choice for concurrent image segmentation and data preservation, as shown by the simulation results. In fact, they come up with some positive results that offer fresh perspectives on how to advance cloud computing in the healthcare industry [17].

Cross-VM assaults have grown to be a serious concern for commercial clouds. On shared physical servers, these attacks frequently take use of hardware level leakages. These attacks frequently make use of leaks at the hardware level on shared physical servers [18]. Performance degradation caused by competition for shared resources on a co-located system makes it possible to identify the presence of a co-located instance with a high computational load. The last level cache (LLC), a shared cache

design, is becoming a major leakage source for cross-VM attacks. As a result, it is crucial to test sensitive data implementations across all target platforms and versions, which is a difficult, expensive, and error-prone operation for humans to complete. According on their cache access profiles, the authors of [19] suggested a machine learning-based technique to categorise programmes. They show how support vector machine models may be trained using feature vectors to properly categorise applications with the least amount of human processing. The training and profiling processes are fully automated and do not require reading or studying the classification-required code. They can categorise 40 benchmark apps from the Phoronix suite at a rate of up to 98% (L1 cache) and 78% (LLC) in native execution with only a small amount of training [20]. For a group of 25 applications, the cross-VM success rate drops to 60% in the noisy Amazon EC2 scenario. With this initial work, we demonstrate that it is possible to train useful models to accurately forecast applications running in co-located instances [21].

Through the web, clients can access cloud administrations in distributed computing. Disappointment is a grave problem with today's advanced registering and cloud frameworks. As large-scale frameworks continue to grow in scope and complexity, mitigating the effects of bad luck and developing reliable hypotheses with excellent lead times remain onerous exploration challenges. Elite figure frameworks are becoming increasingly unpredictable, making it difficult for the present internal failure processes to be adequately adapted, such as successive registration and replication. It emphasises the value of having a practical and effective method for dealing with disappointment that the executives have set up to lessen its effects within the framework. With the use of AI approaches, it is now possible to predict prospective framework failure even more precisely thanks to the ability to learn from the past to predict future personal conduct standards. In [22], the authors examine the foresight capabilities of AI by applying a few computations to increase the accuracy of disappointment projection. We've prepared ourselves for disappointment. the core analysis that considers Random Forests (RF), SVM, Classification and Regression Trees (CART), etc. Exploratory findings reveal that, in comparison to other calculations, their paradigm's typical expectation precision using SVM while predicting breakdown is 92% exact and beneficial. According to this finding, all likely future device and application failures can be successfully predicted by their cycle inside [23].

By offering a forward-protected ID-based ring signature mechanism with a higher level of security [24]. If a user's secret key is compromised, all previously produced signatures are included, and the user's validity is not affected. Asking all data owners to reauthenticate their data is not possible if a user's secret key has been hacked. The security level of ring signatures was raised by offering forward secure ID-based methods [25]. If a user's secret key is compromised, all previously produced signatures are included, and the user's validity is not affected. If a user's secret key has been compromised, it is not viable to request that all data owners reauthenticate their data. A cloud computing attribute-based, secure data exchange approach with EABDS was suggested by the authors [26]. This system encrypts data using DEK and a symmetric encryption method, followed by CP-ABE encryption, in order to implement fine-grained access control and safeguard data security. By utilizing a key server and attribute authority to generate attribute secret keys for users, homomorphic encryption is used to circumvent the problem of key escrow. The EABDS conspiracy achieves rapid

characteristic renunciation by verifying forward and backward security and easing client burden. This tactic has the advantages of being effective and safe.

A typical authority-based insurance saving approval show address security issues for a conveyed stockpiling [27]. This encourages cloud applications with several users working together. Verification is essentially at the core of security solutions. The SAPA shared access authority is obtained through an anonymous access request matching mechanism, offers attribute-based Ciphertext-policy access control to provide clients with dependable access to their own information fields, and employs intermediary re-encryption to distribute data among many clients. This achieves data access control, access authority sharing, and privacy continuity shielding while addressing the user's sensitive access-related privacy during data sharing in a cloud environment. Protecting private customer data does not affect SAPA convention, verification, or approval.

Predicting the Student Academic Performance in Knowledge, Skills, and Abilities (KSA) using Data Mining Techniques and by using Machine Learning Techniques [27]. The main goal of this paper is to be implemented in institutions of higher education, such as schools and colleges, in order to give its students a quality education. Finding out what influences academic execution and then attempting to pinpoint where these fundamentals are falling short is one way to achieve the highest level of value. The algorithm used here is classifying and segregating the data successfully in to two clusters by using the features mentioned above that will confirms the appropriateness of the selected attributes for a forecasting cause.

3. PROPOSED METHODOLOGY

The proposed work is used to create a database if it is not present in the directory with tables which is generated by the end-user. One table is for the data and IP address of the user which is sent and another table is about user details with credentials of user. The verification of the user is done by the credentials and user details stored in the table. The whole work can be divided into two different parts such as authentication of user and encryption of data shown in Figure 1.

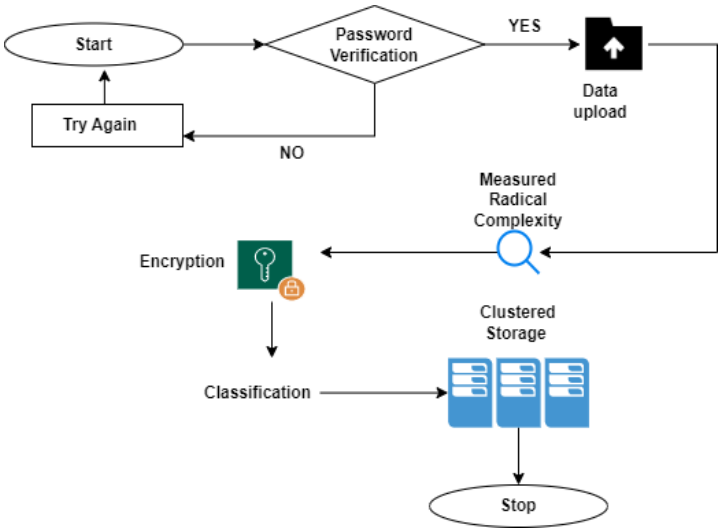

Fig 1: Proposed Framework of the System

The proposed system starts with the credential verification process, if yes then move forward otherwise re-initiate the process. The login panel has verification code for login on the system such as credentials of user, which are used to authenticate the correct user. There are some conditions applied on the password length (8 character) and verification process shown in the algorithm given below.

Authentication Algorithm 1: UserAuth (UserID, pass)

Input: Raw data which is required to measure the similarity

Output: Cosine is used to evaluate the similarity

```
UserID = Input (Interface)
Pass = Input (Interface)
Cap = Random.Input (8,1)
Count =0
Start loop: for i  → 1 to len (input)
Instance_input = input (i)
Start loop: for j  →i+1 to len (input)
A =Cosine (Instance_input) – Cosine (Input (j))
Cosine (Count, 1) = Instance_data
Cosine (Count, 2) = Input (j)
Cosine (Count, 2) = A
Count = Count +1
End both loops here
Return Cosine
End
```

After choosing an encryption scheme, radical complexity can be the next step is to evaluate the radical difficulty of the messages based on how similar they are to one another. The use of radical complexity finder during the transfer of the document to the encryption block resulted in a sizable reduction in execution time. The selection of an appropriate algorithm is used to save the time of execution and loss of data during transmission. The evaluation of radical complexity can be done by using the algorithm described below:

Encryption Algorithm 2: Encrypt (complexity)

```
Apply AES, if Examined_complexity > Theortical_complexity
Apply DSA, if Examined_complexity <= Theortical_complexity
Probability = evaluate_Probability (Doc)
Com_probability = (len (Stored_doc) / len (uploaded_doc))
Com_probability = Com_probability * 100;
Return Com_probability
End
```

After being authentication on the encrypted data, the neural network is applied to classifies it and determines where on the cloud server the cloud provider should keep the data. The architecture of ANN is shown in Figure 2 which consists of input layer, activation function, and output layer.

Before the activation function, there may be several hidden layers. The hidden layers are processed with either Advanced Encryption Standard or AES is used to encrypt the data with a symmetric key using 128-bit blocks or DSA algorithm which is providing the secure key that is shared between the client and server.

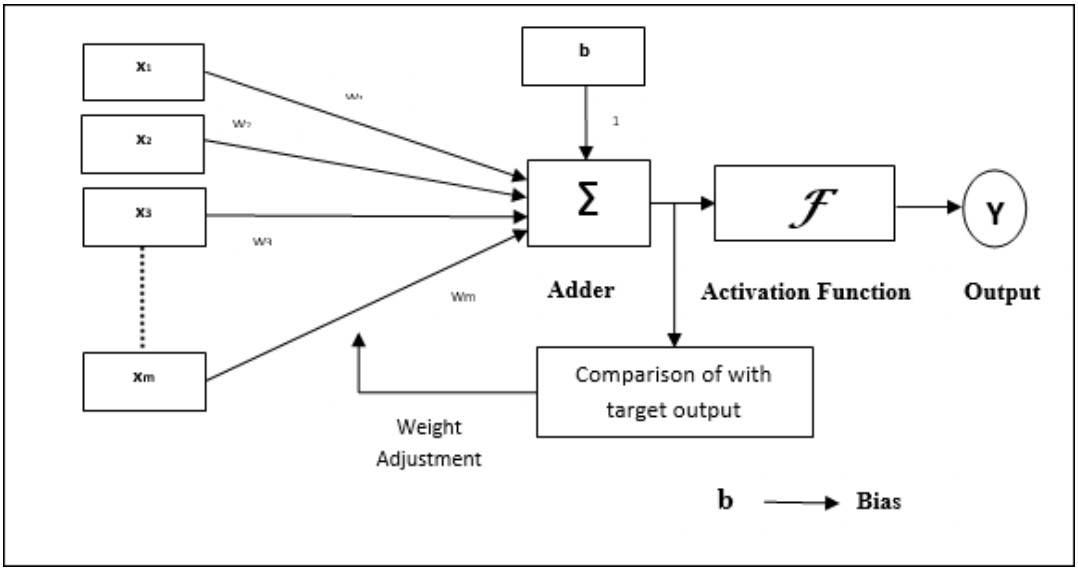

Fig 2: General Structure of ANN

After gathering the data, machine learning techniques are implemented to predict the data pattern and information flow (Shown in Figure 3). In this process, we have applied several steps to process the data:

- Gathering information from data sources.
- Labelling the data rows after pre-processing the data to create a normalised dataset [18].
- The Machine Learning Algorithm is responsible for handling the outcome of the future advancement, the preparation and testing dataset.
- The trained model or trained classifier created by the ML method may predict the label of a new data row when it is input.
- Utilizing AES encryption calculation, the gathered information is ensured and gotten that is protected and secured.
- The Secured data is stored in a cloud.

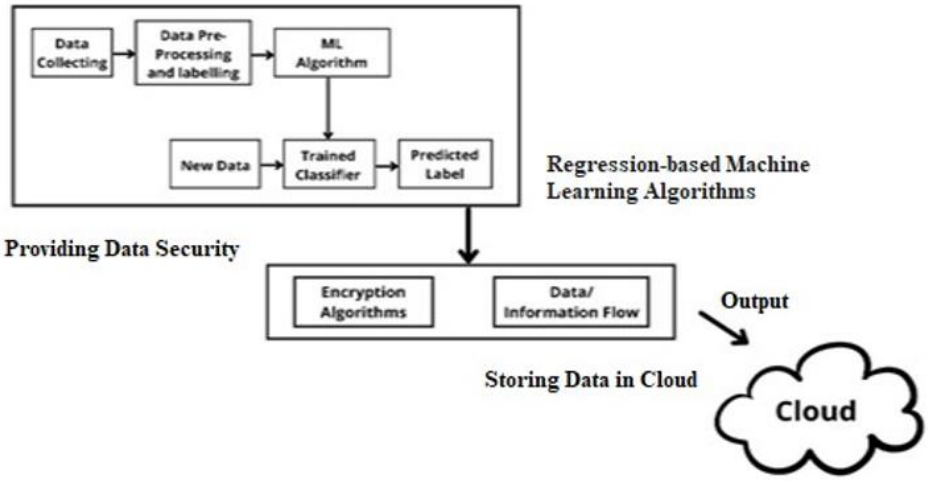

Fig 3: Information flow and Pattern prediction

System Framework

The major aim of this work is to build a privacy-aware framework to secure private data and make the user aware of what data is being shared (Figure 4). The model is deployed on the windows 10 system which is having i7 core 7 model, 8GB RAM, Jupyter notebook, and Anaconda software. The data is pulled from file using get API and post API where a token is generated and the data is obtained in json format. We used the TCP/UDP protocol to send the data from the phone to the server. The information is sent in word reference design i.e., dictionaryformat. And now user data will be collected from the clients' server and a prompt will pop up by questioning to store the data in the database or not and asks the user toset expiry of data. If we click yes, on the off chance that we click indeed, the information will be shipped off the data setin an AES encoded design or on the other hand in case no ischosen by the client it will consequently kill the interaction.

Result Analysis

The simulation has been done by using Cloudsim simulator and generates the real-time scenario. Recall and accuracy parameters were determined the outcomes of the proposed secure cloud model. The confusion matrix is used to determine the relation among the false and true results as shown in Figure 4. Table 1 and Figure 5 demonstrated the recall results and graphical representation of recall based on uploaded documents using ANN. The graph shows that the recall rate of the ANN technique is lie below than the cosine index.

		Actual Values	
		1	0
Predicted Values	1	540	150
	0	110	200

Fig 4: Confusion Matrix

Table 1: Results based on document uploaded using ANN

Total uploads	Similarity with Cosine	Recall
90	0.640	0.618
180	0.630	0.610
270	0.617	0.589
360	0.612	0.580
450	0.585	0.569
540	0.578	0.559
650	0.572	0.550

This is done due to encryption algorithm is integrated with ANN, and similarity approaches worked well to compare uploaded text documents for similarity, and because the classifier uses the same features that were used during training, reducing the number of false positives.

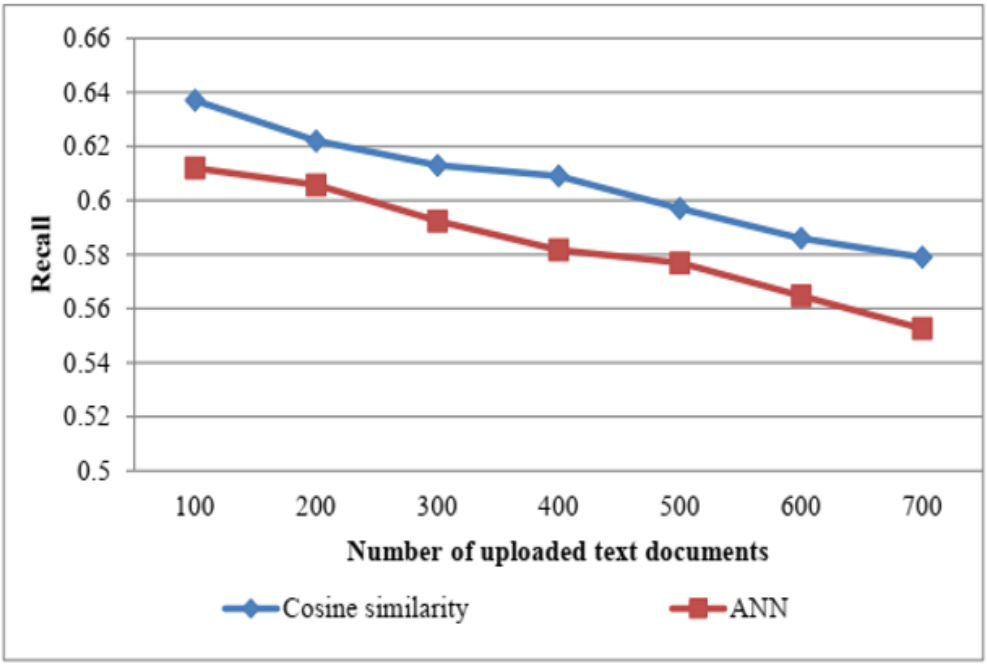

Fig 5: Result analysis of recall using ANN

Table 2: Results based on document uploaded using ANN

Total uploads	Similarity with Cosine	Accuracy
90	66.6	94.5
180	65.7	93.7
270	64.8	92.6
360	63.9	92.4
450	63.2	88.5
540	62.9	82.8
650	62.7	79.5

Table 2 and Figure 6 display the design's secure cloud system's accuracy. The graph shows that the accuracy of the designed system declines as the quantity of uploaded text documents increases.

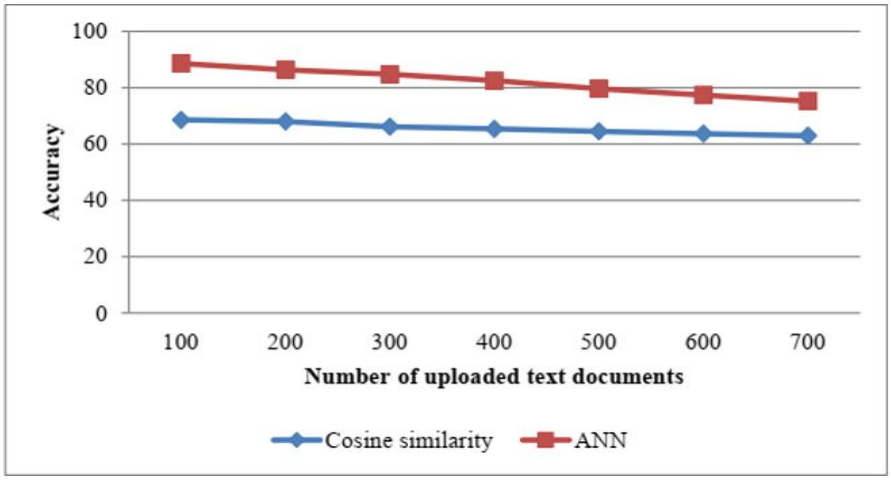

Fig 6: Result analysis of Accuracy using ANN

This is since when the numbers of text documents grow, the likelihood of both relevant and irrelevant features also grows, which lowers detection accuracy. The socket is created and then the port is reserved for a service and then host will bind. After the above process the connection is made with the client and after sending the data from the client to the data is decrypted by fetching the IP data and loads to the set of information. Data sharing in traditional storage requires physical drives and the establishment of a network between them (Figure 6). In this paradigm, the organization's speed affects how quickly documents may be accessed. Comparing this approach to distributed cloud storage, it has a short access time. Because cloud storage connects with security systems, it is more secure. This system will ensure that all the data is securely preserved.

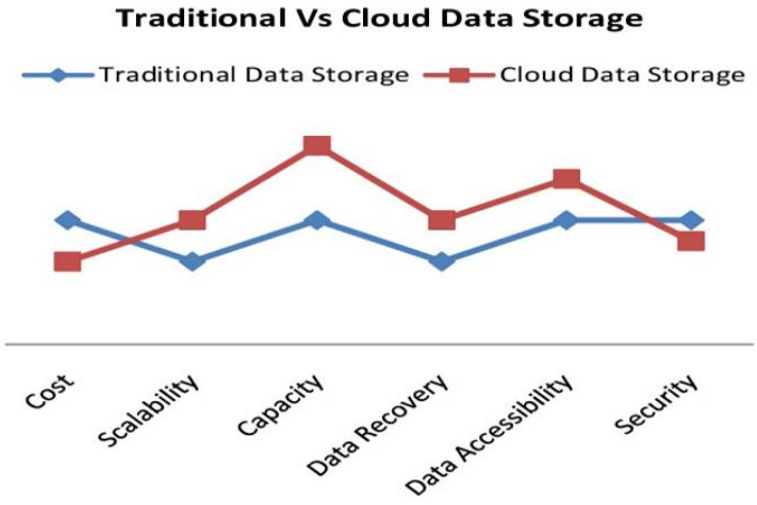

Fig 6: Storage Comparison

4. CONCLUSION AND FUTURE WORK

The main objective is to securely store and access data that is not in the owner's control but rather resides in the cloud. We use the encryption method to safeguard cloud-based data files. The encryption algorithms employed here will enhance both the encryption and decryption processes' performance. This approach of storing and

accessing information is far better. Here, using a variety of machine learning methods, the is examined and divided. The algorithms for classification are frequently utilized. Decision tree, Logical Regression algorithms are used here for these purposes.

This paper deployed an encryption-decryption and cosine-similarity-based neural network-based secure cloud storage architecture. According to multiple text documents ranging from 90 to 650, the model provides high security in terms of accuracy and recall parameter for data storage. AES and DSA were used to encrypt the document, while Cloudsim was used as a simulator to compute the findings. A comparison study comparing neural architecture with and without ANN architecture was conducted to demonstrate the significance of the proposed system. Further, the findings with the simulator demonstrate that the average accuracy of 93.57%, the suggested work was successful in providing a secure data storage platform for cloud customers.

References

1) Ne Gupta, Ishu, Ashutosh Kumar Singh, Chung-Nan Lee, and Rajkumar Buyya. "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions." IEEE Access (2022).

2) Kandi, P., Tarapatla, S. R., Kumar, S., Kadiyam, H., Chowdary, D., & Moparthi, N. R. (2022, December). A Review: Data Security in Cloud Computing Using Machine Learning. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 1447-1451). IEEE.

3) Brijesh Kumar Baradwaj, and Saurabh Pal, " Mining instructive information or a data to investigate under studies' exhibition".International Journal of Advanced Computer Science and Applications Vol. 2,No.6.

4) Shovon, M. H. I., & Haque, M. (2012). An Approach of Improving Students Academic Performance by using k means clustering algorithm and Decision tree. arXiv preprint arXiv:1211.6340.

5) Márquez-Vera, C., Cano, A., Romero, C., & Ventura, S. (2013). Predicting student failure at school using genetic programming and different data mining approaches with high dimensional and imbalanced data. Applied intelligence, 38, 315-330

6) Ogwoka, T. M., Cheruiyot, W., & Okeyo, G. (2015). A model for predicting students' academic performance using a hybrid of K-means and decision tree algorithms. International Journal of Computer Applications Technology and Research, 4(9), 693-697.

7) Sen, J. (2011). A secure and efficient searching scheme for trusted nodes in a peer-to-peer network. In Computational Intelligence in Security for Information Systems: 4th International Conference, CISIS 2011, Held at IWANN 2011, Torremolinos-Málaga, Spain, June 8-10, 2011. Proceedings (pp. 100-108). Springer Berlin Heidelberg.

8) Nawal Ali Yassein, Rasha Gaffer M Helali and Somia B Mohomad(2020) , "Predicting Academic Performance of students in KSA using Data Mining Techniques", Journal of Information Technology & Software Engineering., Vol.7, No. 5.

9) Han, P., Liu, C., Cao, J., Duan, S., Pan, H., Cao, Z., & Fang, B. (2020). CloudDLP: Transparent and scalable data sanitization for browser-based cloud storage. IEEE Access, 8, 68449-68459.

10) Mhaisen, N., & Malluhi, Q. M. (2020). Data consistency in multi-cloud storage systems with passive servers and non-communicating clients. IEEE Access, 8, 164977-164986.

11) Lv, Z., Chen, D., Cao, B., Song, H., & Lv, H. (2023). Secure deep learning in defense in deep-learning-as-a-service computing systems in digital twins. IEEE Transactions on Computers.

12) Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques. Big Data Mining and Analytics, 6(3), 311-320.

13) RAFI, S. M., PVENKATASUBRAMANYAM, Y., & SWATHI, A. Deep Learning for Encryption-Decryption Techniques for Cloud Data Confidentiality.

14) Mishra, J. K., & Janarthanan, M. (2023, February). Cloud Computing Security: Machine and Deep Learning Models Analysis. In Macromolecular Symposia (Vol. 407, No. 1, p. 2100521).

15) Jayaweera, M. P. G. K., Kithulwatta, W. M. C. J. T., & Rathnayaka, R. M. K. T. (2023). Detect anomalies in cloud platforms by using network data: a review. Cluster Computing, 1-11.

16) Chavan, S. S., & Jayaseeli, J. D. (2021, February). A Review on Outsourced Attribute-based Encryption Technique for Secure Data Storage. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 81-88). IEEE.doi: 10.1109/icicv50876.2021.9388386

17) Ahuja, R., Mohanty, S. K., & Sakurai, K. (2017). A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing. Computers & Electrical Engineering, 57, 241-256. doi: 10.1016/j.compeleceng.2016.11.028

18) Zhou, J., Duan, H., Liang, K., Yan, Q., Chen, F., Yu, F. R., ... & Chen, J. (2017). Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation. The Computer Journal, 60(8), 1210-1222. doi: 10.1093/comjnl/bxx017.

19) Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2011). Privacy-preserving public auditing for secure cloud storage. IEEE transactions on computers, 62(2), 362-375. doi: 10.1109/tc.2011.245.

20) Xu, Q., Tan, C., Fan, Z., Zhu, W., Xiao, Y., & Cheng, F. (2018). Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption. IEEE Access, 6, 34051-34074. doi: 10.1109/access.2018.2844829.

21) Palumbo, F., Aceto, G., Botta, A., Ciuonzo, D., Persico, V., & Pescapé, A. (2019, December). Characterizing Cloud-to-user Latency as perceived by AWS and Azure Users spread over the Globe. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE. doi: 10.1109/globecom38437.2019.9013343.

22) Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532. doi: 10.1007/s11227-020-03213-1.

23) Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. Archives of Computational Methods in Engineering, 29(6), 3587-3608. doi: 10.1007/s11831-022-09708-9.

24) Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. N., & Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. IEEE Transactions on Industrial Informatics, 18(11), 8065-8073. doi: 10.1109/tii.2022.3161631.

25) Gnanavel, S., Narayana, K. E., Jayashree, K., Nancy, P., & Teressa, D. M. (2022). Implementation of Block-Level Double Encryption Based on Machine Learning Techniques for Attack Detection and Prevention. Wireless Communications and Mobile Computing, 2022. doi: 10.1155/2022/4255220.

26) Silva, F. S. D., Schneider, L. M., Rosário, D., & Neto, A. V. (2022, May). Network slicing mobility aware control to assist handover decisions on e-health 5g use cases. In 2022 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1034-1039). IEEE. doi: 10.1109/iwcmc55113.2022.9825010.

27) S. Singh, R. Yash, A. Tarang, “Cloud -Fog Computing Dataset”, by Optimal Resource Management in Cloud-Fog Computing, https://www.kaggle.com/datasets/sachin26240/vehicular fogcomputing, (Accessed on 04-10-2022).