Developing the Security for Cloud Information Via Alexnet Learning Model versus the accuracy of Artificial Neural Network

Thriveni. E[1], Mahaveerakannan R[2,*]

[1]Research Scholar, [2]Project Guide & Corresponding Author,
Department of Computer Science and Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences,
Saveetha University, Chennai, Tamil Nadu. India. Pincode: 602105

ABSTRACT : The main objective of the study is to protect cloud from different types of attacks by using AlexNet classifier compared accuracy with Artificial Neural Network and user's data to be stored in the cloud safely by Advanced Encryption Standard. Materials and Methods: This research examines two groups AlexNet withArtificial Neural Network. Statistical study used 1300 training and 403 testing datasets from UNSW-NB15 dataset. ClinCalc programme utilised N=10, 0.05 is alpha value, 0.8% is G-Power, and 95% confidence interval.Result and Discussion: Novel Alexnet (91.081%) has an increased precision over ANN (90.075%) with the P value is 0.012($p<0.05$) from the results of Independent samples t-test. There is a statistical significant difference between these two algorithms.Conclusion: This study concludes that the Novel AlexNet classifier algorithm seems fundamentally better than the ANN in terms of increasing the accuracy of secure cloud data and holding sensitive data with the dataset of UNSW-NB15.

Keywords: Advanced Encryption Standard, Artificial Neural Network, Authentication, Cloud, Equality, Novel Alexnet,Security.

INTRODUCTION

Users find it incredibly challenging to store the enormous volume of data locally because of the data explosion. As a result, many businesses and people prefer to store their data in the cloud. Furthermore, the data kept in the cloud may be deleted or destroyed due to inevitable software bugs, hardware issues, and human errors (S et al. 2022). The US government encrypted sensitive data with Advanced Encryption Standard, a symmetric block cipher (AES). Advanced Encryption Standard-encrypted hardware and software worldwide protect sensitive data (Koshy,2021). Indistinguishability requires that the attacker cannot extract the secret key, which would simplify any challenge. Quantum computing will test Advanced Encryption Standard key lengths of 128, 192, and 256 bits in the coming years (Mouha 2021). This study gives private cloud users a two-phase server design. First, protect the cloud and find data that looks suspicious. Second, sort and protect cloud-stored client

* Corresponding Author Mail:mahassecse@gmail.com

data (C. Zhao et al. 2019). IoT, big data, and cloud computing are current information and communication systems. It is applicable to all social systems—commerce, banking, industry, manufacturing, management, personal data, and ICT. So, keeping aware of new findings, applications, concerns, and challenges is essential and several applications in various fields like business, data storage, entertainment, management, social networking, education, art, GPS (Gupta and Agrawal 2019).

Data security in the cloud using identity-based integrity auditing has been studied extensively, with 599 publications covering the topic in IEEE Xplore and 10 covering it in ScienceDirect. One key symmetric encryption. Huge datasets need symmetric key encryption. 3 AES key lengths (128, 192, or 256 bits). Advanced Encryption Standard supports 256-bit keys. Symmetric encryption increases client/server data encryption. Asymmetric encryption protects the slower symmetric key (Pohl 1990). Identity-based dynamic data auditing addresses enormous data storage security issues. The service business can extract the authorizer's private key from preserved information in a private key disclosure attack (X. Li et al. 2021). The study proposes a two-stage server design for users of private cloud. The initial stage involves safeguarding the cloud and detecting anomalous data, while the subsequent stage entails organizing and securing the clients' valuable data stored in the cloud (Y. Li and Zhang 2022). Based on these two considerations, an authentication technique was designed to enhance cloud data safety. This system relies on the cloud infrastructure to function. Two pieces of information are required for decryption when a sender uses the cloud to transmit a message to a receiver. The first component is a one-of-a-kind security gadget that is attached to the computer separately. A password is the second layer of security. The findings confirm that cloud-based information is secure and that revocability services are functional (Sethy et al. 2022). It has been suggested that a unique attacking technique and Intrusion Detection System (IDS) be developed for use with the network using the cloudstack equality environment. Machine learning methods like k-means, decision tree, Random Forest, Naive Bayes, Support Vector Machine, and C4.5 were used to analyse the dataset. Analysis of network performance and accuracy with intrusion detection reveal that C4.5 and SVM algorithms perform well (Kumar, Zindani, and Paulo Davim 2021). Nanotech news "ANNs" are improving. Nanotechnology researchers should examine neural networks for authentication. Neuroscientists, experimentalists, and statisticians must collaborate. Nanotechnologists like ANNs because they manage nonlinear processes without affecting experimental data (Amani and Mohammadyani 2011). In order to show the DCNNs' information extraction pattern, we evaluated the DCNNs with significant face features covered using the reverse correlation equality approach in the second phase of the experiment (disrupted inputs) (Y.-F. Li and Ying 2022).

The cloud storage still has many research gaps that have not been fully addressed, and new issues are continually appearing. In an effort to better understand how Novel Alexnet stacks up against ANN, a comparison between the two has been conducted. To further protect cloud-based information, the proposed approach employs identity-based integrity auditing.

MATERIAL AND METHOD

All of the research work was done in the Cloud Computing Lab at the Computer Science Department of the Saveetha School of Engineering at the Saveetha Institute of Medical and Technological Sciences in Chennai. ANN as well as Novel AlexNet are being used throughout this project. The results of 10 examples utilizing different 80% training and

20% assessment iterations with different numbers of entries in the dataset are compared between the Novel AlexNet as and SGD learning algorithms. A comparison is made between the two groups that were selected to serve as the foundation for the comparison, and the outcome is found. In this study, 10 iterations are obtained from each of the two groups that are being investigated. We use specialized analysis of Clincalc software to implement Novel Alexnet as Group 1 and ANN as Group 2 Each group, calculated using the clincalc software (g-power setting parameters: alpha value=0.05 and power = 0.80) (Y. Zhao et al. 2019).
The data utilized in this research came from the publicly available Kaggle dataset in the form of csv file. The dataset called UNSW-NB15 was used to train the classifier. The UNSW-NB15 dataset contains 1753 samples used for statistical analysis, split into a training set (1300) and a testing set (453) (Banachewicz, Massaron, and Goldbloom 2022). Another dataset is used for encrypting data and that dataset contains data on symptoms connected to the British Job employment agency, including duplicate, null, and missing values. It has 10 columns and 105 rows. Using the capabilities that Microsoft Excel offers, pre-processing is done on the datasets to get rid of duplicate and null entries. There is no need to convert the data because the dataset is entirely composed of numerical forms.("AMA-TV: TOMS, Online Identities, and Stakeholders" 2012).

The recommended work is created and carried out using the Python OpenCV programme. The effectiveness of deep learning was evaluated on the Windows 10 platform. The machine included an Intel Core i7 processor and 4GB of Memory. Data was sorted using a 64-bit computer processor. The code was written in Python, a popular programming language. The code was executed in the Jupyter notebook environment. As the application is running, the dataset is being updated to ensure reliable results(S et al. 2022).

AlexNet

The novel AlexNet is a multi-layer convolutional neural network. The ImagNet collection already includes a system with more than a thousand images. The network has been trained to recognize many different types of items, including animals, a mouse, a keyboard, and a pencil. Alex Krizhevsky is largely responsible for the creation of Novel AlexNet. Ilya Sutskever and Krizhevsky's dissertation advisor, Geoffrey Hinton, collaborated on the paper's publication. This network is a CNN, or convolutional neural network.The flowchart of this algorithm is described below.

Procedure:
Step 1:Import the necessary libraries and modules.
Step 2: Load the dataset you want to classify.
Step 3: Preprocess the data by normalizing.
Step 4: The architecture should also include activation functions, such as ReLU, and dropout layers to prevent overfitting.
Step 5: Compile the model.
Step 6: Train the model using the training data.
Step 7: Evaluate the model's performance on the test data.
Step 8: Save the trained model for future use or deployment.

ANN Algorithm:

Artificial neurons, which are a group of connected nodes or units that approximately

resemble the neurons in a real brain, are the foundation of an artificial neural network (ANN). Like terminals in the human mind, each link may send a signal to surrounding neurons. No specific piece of information is contained in a single neuron; rather, the collective action of the neurons defines the cell's capacity for computation.

Procedure:

Step1: Create input database

Step2: Train Artificial neural network.

Step3: Storage save highest test R

Step4: Save best predicting ANN depending on inputs

Step5: End.

Statistical Analysis

SPSS version 26, a tool developed by Novel Alexnet and ANN, is used for statistical analysis. Independent parameters are decrypted text.. Dependent parameters are encrypted text and key length(“Table 11: Precision, Recall and F1-Score of AlexNet and AlexNet with DBAP Layer Using Softmax Classifier,”2006). A separate T-test analysis is performed to assess the accuracy of both methods.

RESULTS

The suggested Novel Alexnet and ANN were run in Anaconda Navigator with a sample size of 10 at various time intervals. Table 1 displays a comparison between the Novel AlexNet and ANN learning algorithms based on the outcomes of 10 instances using 80% training and 20% evaluation iterations with varying amounts of entries in the dataset. There are 105 rows in the dataset, and 10 random iterations are utilized to compare the performance of the Novel AlexNet and ANN methods. Compared to the ANN algorithm, the novel AlexNet method performs significantly better. The data is cleaned up in the preparation phase so that the machine learning algorithm can utilize it effectively. This was done because of the higher error and null value rates in the original dataset. The dataset has been shrunk to a manageable size as much as the network will allow.
Table 1 displays the estimated accuracy of Novel Alexnet. Tabulated one provides the accuracy with which ANN predictions were made. With these 10 evidence iterations, we can calculate statistically distinct loss values for each method. Novel Alexnet's average accuracy was 91.081 percent, whereas ANN's was 90.075 percent.

Table 1. Accuracy Analysis of Alexnet and ANN

Iterations	AlexNet Accuracy (%)	ANN Accuracy (%)
1	86.90	85.21
2	87.40	86.59
3	88.70	87.48
4	89.10	88.77
5	90.80	89.69
6	91.70	90.58
7	92.90	91.40
8	93.40	92.80
9	94.30	93.50
10	95.61	94.73

Table 2. Group Statistical Analysis of Alexnet and ANN. Mean, Standard Deviation and Standard Error Mean are obtained for 10 samples. Alexnet has higher mean accuracy and when compared to ANN.

	Group	N	Mean	Std. Deviation	Std. Error Mean
Accuracy	Alexnet	10	91.0810	2.99345	.94661
	ANN	10	90.0750	3.11332	.98452

Table 3. Independent Sample T-test: Alexnet is significantly better than ANN with the P value is 0.012 ($p<0.05$) for there is a statistical significant difference between these two algorithms.

		Levene's test for equality of variances		T-test for equality means with 95% confidence interval						
		f	**Sig.**	**t**	**df**	**Sig. (two-tailed)**	**Mean difference**	**Std. Error difference**	**Lower**	**Upper**
Accuracy	**Equal variances assumed**	.001	0.97	.737	18	0.012	1.00600	1.36578	-1.86339	3.87539
	Equal Variances not assumed			.737	17.972	0.012	1.00600	1.36578	-1.86371	3.87571

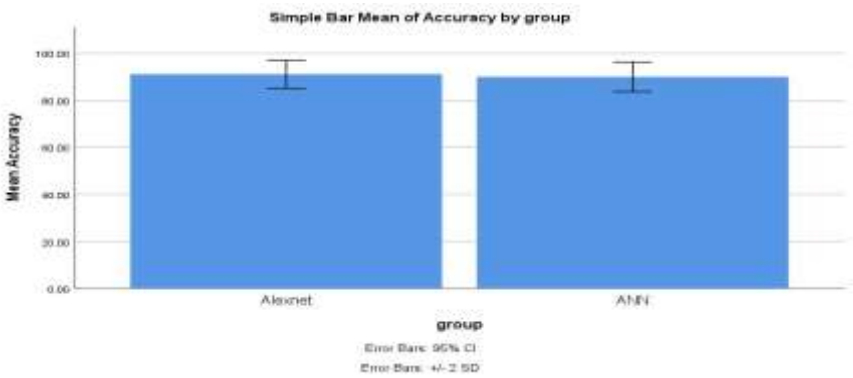

Fig. 1. Comparison of Alexnet and ANN. Classifier in terms of mean accuracy and loss. The mean accuracy of Alexnet is better than ANN. Classifier; Standard deviation of Alexnet is slightly better than ANN. X

Axis: Alexnet Vs ANN Classifier and Y Axis: Mean accuracy of detection with +/- 2 SD

The mean accuracy values for Novel Alexnet and ANN are given in Table 2. Novel Alexnet's(91.0810) average value is greater than the ANN's(90.075), with SD(standard deviations) of 2.99345 and 3.11332 respectively.
The data from the Novel Alexnet and ANN, Table 3 displays the Independent Sample T-test results with the P value is 0.012($p<0.05$) for there is a statistical significance difference between these two algorithms.
Figure 1 shows the mean accuracy comparison between Novel Alexnet and ANN. This graph demonstrates that the AlexNet classifier is more accurate than the ANN. Novel Alexnet has a Average, standard deviation(SD), and standard error mean of 91.0810, 2.99345, and.94661, respectively. Similarly, the mean, standard deviation, and standard error mean for the ANNt are 90.0750,3.11332 and .98452, respectively.Novel Alexnet's loss values for mean, standard deviation and standard error mean, on the other hand, are 8.9190, 2.99345, and.94661, respectively. The mean, standard deviation, and standard error mean loss values for random forest are 9.9250,3.11332 and .98452, respectively.
The group statistics value is also given with the mean, standard deviation, and standard error mean for the two approaches. The categorization of loss mechanisms and graphical comparison of Novel Alexnet and ANN This demonstrates that Novel Alexnet's classified accuracy of 91.081% is significantly inferior to ANN's accuracy of 90.075% with an significant value of 0.012.

DISCUSSION

The significance value for this research is 0.012 ($p<0.05$), which suggests that Novel Alexnet would be preferable than ANN. While Novel Alexnet's accuracy is 91.081%, the accuracy of the Novel Alexnet is examined as 90.075% and it is statistically significant. Two well known algorithms which Alexnet and ANN are used as third party between user and cloud.The Novel AlexNet classifier shows some differences when compared to ANN, There is a distinction in terms of accuracy and statically significant.

To support this work, the performance of each algorithm's accuracy was evaluated in order to aid in this endeavor, and it was found that CNN classifier is used in comparative dementia research to quickly and accurately detect dementia. Instruments and methods MRI brain data sets from CNN and ANN40 are used to train algorithms for dementia detection. Results: The MATLAB results show that the accuracy and detection rate for CNN classifiers is 96.3%, while the accuracy ratio for authentication for ANN is statistically significant (0.012) (Y.-F. Li and Ying 2022). In the test data sets for dementia diagnosis, this research found that the CNN strategy performed better than the ANN methodology for authentication (Rahul and Jagadeesh 2022). The author challenges this approach by addressing data variance. CNN struggles to comprehend concealed items. The network also has trouble identifying rotated or captioned pictures. CNN cannot encode object orientation and position or analyse spatially invariant data (Gupta and Agrawal 2019). To oppose this work, in this study, the AlexNet framework was used since it has been trained to recognise C-scans exhibiting ancient architectural styles. The effectiveness of the ANN and the Adaptive Moments Estimation are compared and contrasted (Adam). The two optimizing compilers were used to train models using data from a GPR dataset collected at several archaeological sites (Bengacemi et al. 2021). AlexNet has several advantages over traditional ANNs for image recognition tasks. One major advantage is the use of convolutional layers, which allow the network to learn spatially invariant features that are robust to translations and rotations. This is important for image recognition tasks, as images

can be taken from different angles or orientations. In addition, AlexNet's use of ReLU activation functions and dropout regularization helped to reduce overfitting and improve generalization performance (Y. Li and Zhang 2022).
In the study, the proposed framework limitation is that Particularly when training on huge datasets, novel Alexnet takes a while. According to the future aims of the study, the system should be enhanced to include more items while needing less time to gather the data collection

CONCLUSION

This investigation concludes that the Novel AlexNet classifier algorithm appears to be fundamentally superior to the ANN in terms of boosting the accuracy of sharing the cloud file that stores sensitive data by detecting malicious behavior from user request. In comparison, the accuracy rate for ANN is 90.075% with the dataset of UNSW-NB15 , whereas the accuracy rating for the Novel Alexnet is 91.081%.

DECLARATION

Conflicts of Interest
No conflicts of interest in this manuscript.
Author Contributions
Author NV was responsible for all data collection, data analysis, and manuscript preparation. Author RS was responsible for all conceptualization, data validation, and critical evaluation of papers..
Funding
We thank the following organizations for providing financial support that enabled us to complete the study.

1. DreamsPlus Consulting Pvt Ltd,Chennai.
2. Saveetha School of Engineering
3. Saveetha University
4. Saveetha Institute of Medical and Technical Science

REFERENCE

1. Amani, Amir, and Dariush Mohammadyani. 2011. “Artificial Neural Networks: Applications in Nanotechnology.” Artificial Neural Networks - Application. https://doi.org/10.5772/15551.
2. “AMA-TV: TOMS, Online Identities, and Stakeholders.” 2012. https://doi.org/10.4135/9781473986190.
3. Bengacemi, Hichem, Abdenour Hacine-Gharbi, Philippe Ravier, Karim Abed-Meraim, and Olivier Buttelli. 2021. “Surface EMG Signal Classification for Parkinson’s Disease Using WCC Descriptor and ANN Classifier.” Proceedings of the 10th International Conference on Pattern Recognition Applications and Methods. https://doi.org/10.5220/0010254402870294.
4. Gupta, B. B., and Dharma P. Agrawal. 2019. Handbook of Research on Cloud Computing and Big Data Applications in IoT. IGI Global.
5. Koshy, Joel Mathew.2004 “Introduction Advanced Encryption Standard (AES).” https://doi.org/10.14293/s2199-1006.1.sor-.ppbwb9z.v1.
6. Kumar, Kaushik, Divya Zindani, and J. Paulo Davim. 2021. “Artificial Intelligence in Mechanical and Industrial Engineering.”

https://doi.org/10.1201/9781003011248.

7. Li, Xiong, Shanpeng Liu, Rongxing Lu, and Xiaosong Zhang. 2021. "On Security of an Identity-Based Dynamic Data Auditing Protocol for Big Data Storage." IEEE Transactions on Big Data 7 (6): 975–77.
8. Li, Yi-Fan, and Haojiang Ying. 2022. "Disrupted Visual Input Unveils the Computational Details of Artificial Neural Networks for Face Perception." Frontiers in Computational Neuroscience 16 (November): 1054421.
9. Li, Yumei, and Futai Zhang. 2022. "An Efficient Certificate-Based Data Integrity Auditing Protocol for Cloud-Assisted WBANs." IEEE Internet of Things Journal 9 (13): 11513–23.
10. Mouha, Nicky. 2021. "Review of the Advanced Encryption Standard." https://doi.org/10.6028/nist.ir.8319.
11. Pohl, L. R. 1990. "Drug-Induced Allergic Hepatitis." Seminars in Liver Disease 10 (4): 305–15.
12. Rahul, P., and P. Jagadeesh. 2022. "Detection of Dementia Disease Using CNN Classifier by Comparing with ANN Classifier." 2022 International Conference on Business Analytics for Technology and Security (ICBATS). https://doi.org/10.1109/icbats54253.2022.9759085.
13. S, Asha, S. Asha, K. Punitha, and Tanmay Joshi. 2022. "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage." 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT). https://doi.org/10.1109/icicict54557.2022.9917653.
14. Sethy, Prabira Kumar, A. Geetha Devi, Bikash Padhan, Santi Kumari Behera, Surampudi Sreedhar, and Kalyan Das. 2022. "Lung Cancer Histopathological Image Classification Using Wavelets and AlexNet." Journal of X-Ray Science and Technology, November. https://doi.org/10.3233/XST-221301.
15. "Table 11: Precision, Recall and F1-Score of AlexNet and AlexNet with DBAP Layer Using Softmax Classifier."2009 https://doi.org/10.7717/peerj-cs.497/table-11.
16. Zhao, Chenbin, Li Xu, Jiguo Li, Feng Wang, and He Fang. 2019. "Fuzzy Identity-Based Dynamic Auditing of Big Data on Cloud Storage." IEEE Access 7: 160459–71.
17. Zhao, Yao, Nick Barnes, Baoquan Chen, Rüdiger Westermann, Xiangwei Kong, and Chunyu Lin. 2019. Image and Graphics: 10th International Conference, ICIG 2019, Beijing, China, August 23–25, 2019, Proceedings, Part III. Springer Nature..