International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Accuracy Enhancement in Machine Learning Approach for Cloud Application

Aarti Sharma[1], Vikas Malik[2]

[1]Scholar, Bhagat Phool Singh Mahila Vishwavidyalaya
[2]Professor, Bhagat Phool Singh Mahila Vishwavidyalaya

Abstract
The emphasis of the current research is on improving accuracy during cloud machine learning operations. Conversations or networks may use machine learning instead of building and maintaining their own computer systems. A long-term ecosystem where social network members may exchange resources is presently being built by AI and social. Data storage, machine learning, and social media are all possible applications for deep learning. Businesses may improve their analytics by using this method. Because of the openness of social media, people may freely and intelligently share their personal information utilizing machine learning. Peer-to-peer is a better term. Using social networks and other forms of peer-to-peer communication, the identities of users are verified. The accuracy and performance of past studies have been shown to be problematic, thus the suggested study will present a fresh way to providing a better answer.

Keyword: Machine Learning, Cloud Computing, Accuracy and Precision.

[1] Introduction

Machine learning might be utilized by social conversations or networks instead of constructing and maintaining their own computer systems. "Artificial intelligence" and "social" now work together to produce a sustainable environment for social network members to exchange resources with one other deep learning may also be used for social media, machine learning in addition to data storage. An effective alternative for organizations to increase their analytics is by employing this strategy. With machine learning, users may freely disclose their personal information on social media because of the openness that social media allows and wisely. Peer-to-peer is a more appropriate word. It is a sort of social artificial intelligence where users' identities have been validated using social networks or other peer-to-peer verification systems.

1.1 Machine Learning

A software application's ability to accurately forecast its output is enabled by this approach, which requires no coding on the user's part. Machine learning algorithms employ prior data as an input for predicting new output values.

Detection of fraud, waste filtering, detection of cyber threats, BPA, and predictive maintenance are all feasible uses for machine learning at this time.

1.1.1 WORKING

Algorithms in classical machine learning are often judged on how effectively they predict the future. Learners may use either unsupervised or supervised learning, which are the most frequent approaches. Algorithm selection may be predicted using data, according to scientists.

1.1.2 WORKING OF SUPERVISED MACHINE LEARNING

The data scientist must use supervised machine learning and train the system using inputs and outputs that are clearly labelled. supervised learning algorithms are best suited for the following tasks:

1. Binary classification – Use this method to divide data into two groups.
2. Multi-class classification – For making a choice amongst more than two possible solutions. 3. Regression modeling – For the prediction of continuous values.

1.1.3 WORKING OF UNSUPERVISED MACHINE LEARNING

Unsupervised machine learning techniques do not need the use of data labels. The goal of data sifting is to discover patterns that may be used to further segment the data. To do the following tasks, unsupervised learning algorithms are ideal:

Clustering --In order to divide the dataset into distinct subsets.

Anomaly detection - For spotting outliers and anomalies in data sets.

Association mining - For determining the most often occurring sets of objects in a dataset.

1.1.4 USES OF MACHINE LEARNING

A broad variety of industries are currently using machine learning. For example, it is used in Facebook's News Feed algorithm. Recommendation engines prioritise a member's activity if they routinely read the posts in a certain group. The engine is working behind the scenes to reinforce the user's online habits that it has observed.. Changes in the member's reading habits, such as not reading posts from the group for many weeks, will be reflected in their news feed.

1.1.5 OTHER USES OF MACHINE LEARNING INCLUDE THE FOLLOWING:

It is possible for HRIS systems to apply ML models for resume sorting and to identify the best candidates for a job position.

It is possible for even semi-autonomous vehicles to employ ML algorithms to identify a partially visible object and alert the driver. Virtual assistants - In order to analyze spoken speech and provide context, smart assistants often use a combination of supervised and unsupervised ML models.

Choosing the right mensionality Reduction – As a result, a dataset's number of variables drops.

1.2 Cloud Computing

Data storage and processing power are made accessible on demand without the user needing to actively manage them, making it easier for businesses to operate. Large cloud services are often distributed over many data centres. Cloud computing's "pay-as-you-go" model may help users save money up front, but it may also lead to unexpected long-term charges for those who don't keep an eye on the fine print. The demand for cloud computing services is increasing on a daily basis. There are a lot of uses for it. All of

this suggests that data protection is now a need. Significant data delivery in a secure way to the service provider is tough. An attempt was made to improve security for cloud computing and large data by this researcher. In order to accomplish this goal, cryptography was used. It's common practise in cloud computing for data to be transferred often.

The Internet is used to disseminate this information. Because of this, cloud computing necessitates the consideration of data security in the background. There has been a lot of study done so far to ensure the safety of cloud services in the presence of large amounts of data. Some of them are the subjects of this article. Research on how people perceive the IDS method is given here. Based on the requirements, it delivers security. The overall length of the network is increased. To do this, the node might reduce its power usage. The network has been partitioned into smaller areas so that local nodes may be more effectively used. There is also a place for practical area controllers here. Controllers are entrusted with complete access to the financial records of their jurisdiction. This effective collection of hops was done by the practical controller in accordance with the need for routing efficiency.

Cloud computing It's possible that the term refers to an internet or a network. It provides services across a public or private network. A faraway place may access the cloud. Both wide area and local area networks have used them. Virtual private networks may also benefit from it. Email and online conferencing are popular examples of cloud-based apps. Thanks to cloud computing, it is now feasible to be platform independent. It is possible since no special computer software is required to be installed on the computer. It's no secret that most government applications these days are available on mobile devices. Cloud computing has access to these resources. Cloud computing is becoming more widely accessible and user-friendly thanks to a slew of new services.

1.3 Accuracy

As the most straightforward performance indicator, precision is the proportion of correctly predicted observations to the total number of observations. The degree to which a set of measures comes close or far to accurately representing the true value of the data it contains is known as the accuracy of the set. As a measure of statistical bias, it describes only systematic mistakes, a measure of the difference between a result and its real value, which ISO refers to as "truth." High accuracy requires both high precision and high trueness in order to describe the combination of the two categories of observational mistake.

For binary classification tests, accuracy is employed as a statistical measure of how successfully they identify or exclude conditions. In other words, the accuracy is the percentage of right predictions among the total number of instances studied.. Thus, it compares probabilities predicted before and after a test. The "Rand accuracy" or "Rand index" is often referred to to make the context obvious via semantics.

[2] Literature Review

In 2020, T. N. Yogi [1] provided for sentiment-labeled phrases utilized three separate datasets of varying sizes, to test and compare the performance of three classification algorithms, MNB, KNN, and SVM, for sentiment labeled sentences. All three classification techniques for sentiment analysis were evaluated, and SVM is determined to be a superior approach in every area for the detection of sentiment polarity in all three datasets for sentiment labeled sentences.

In 2019, Ananthi [2] looked faculty, employees, and students at educational institutions were polled to learn about the benefits and challenges of using cloud computing. Security and risk divisions were also

addressed. There are several ways cloud computing may impact the education sector, according to an assessment of the literature. Researchers will be able to concentrate their efforts on finding relevant topics by reading this article, which also discusses security management and the obstacles encountered by the education sector in underdeveloped nations.

In 2017, Jathanna [3] reviewed emphasizes cloud computing-related concerns. Cloud computing expansion has been hindered by security concerns, one of the most pressing difficulties. Privacy and data security issues remain a concern for businesses.

In 2011, A. Huth [4] introduced used the cloud, you may access your data from any location at any time. The cloud removes the requirement for you to be in the same location as the data storage device, unlike a normal computer configuration. Because you don't have to physically be near the hardware that keeps your data, you can use the cloud. To operate your home or business apps, your cloud service provider may both store and own the hardware and software required.

In 2011, M. T. Khorshed [5] presented cloud computing was vulnerable to cyber assaults because of concerns with trust. There was a lot of work done on cloud system security there.

In 2019, A. P. Achilleos et al [6] reviewed study into the modelling of cloud-based applications In their investigation, they also examined the language used to carry out their task.

In 2019, R. Moreno-Vozmediano [7] expressed efforts to improve the supply of resources. For Cloud services, they conducted this study. ML methods were used by researchers to enhance the intelligence of the system.In 2017, D. Kwon [8] reviewed a DL network survey is underway. Anomaly detection was the goal of this study.

In 2015, Y. Lecun [9] presented Deep learning research is used to suggest a machine learning method.

In 2020, H. Tabrizchi and M. Kuchaki Rafsanjani [10] introduced cloud computed security problems survey During their study, they evaluated concerns, dangers, and remedies.

In 2017, I. Avdagic and K. Hajdarevic [11] expressed completed a survey on algorithmic learning for machines. During the course of their investigation, they concentrated on cloud service for CIDPS.

In 2016, G. Nenvani and H. Gupta [12] looked a study on cloud-based attack detection In order to reach these goals, researchers looked into supervised learning methods.

In 2015, M. Eskandari [13] provided used to determine the location of virtual machines in cloud computing environments.

In 2017, E. Hesamifard [14] expressed thought about privacy-preserving cloud-based machine learning.

In 2017, Z. He, T. Zhang [15] proposed detection of DDoS attacks based on machine learning. These measurements were taken from the cloud's source side.

In 2018, M. Marwan [16] proposed medical cloud security research is being carried out. The author used machine learning to accomplish their goals.

Table1: literature Survey

SNO.	AUTHOR/YEAR	TITLE	METHODOLOGY	LIMITATION
[1]	Yogi /2020	Comparative study of sentiment analysis classifiers based on machine learning algorithms.	Machine Learning, Sentiment Analysis	Lack of technical work

[2]	Ananthi Claral Mary /2019	Cloud Computing in the Academic Field: Implications, Risks, and Challenges	Cloud Computing	There is no implication in future
[3]	R. Jathanna /2017	Problems with cloud computing safety	Cloud Computing	Performance of this research is very low
[4]	A. Huth /2011	The fundamentals of cloud computing are covered here.	Cloud Computing	Scope of this research is very less
[5]	M. T. Khorshed /2011	Cloud computing has trust difficulties, which makes it vulnerable to cyber assaults.	Cloud Computing	There is no security in this system.
[6]	A. P. Achilleos /2019	Modeling and execution language for cloud computing applications.	Cloud Computing	There is lack of performance
[7]	R. Moreno-Vozmediano /2019	Machine learning-based resource provisioning for elastic Cloud services	Cloud Computing, Machine Learning	Lack of accuracy
[8]	D. Kwon /2017	Network anomaly detection with deep learning	Deep learning	Lack of security
[9]	Y. Lecun /2015	Deep learning	Deep learning	Lack of accuracy
[10]	H. Tabrizchi /2020	Cloud computing security concerns, threats, and solutions are examined in this report.	Cloud computing	There is lack of performance
[11]	I. Avdagic /2018	An investigation of cloud-based machine learning techniques for CIDPS.	Machine learning	Lack of technical work
[12]	G. Nenvani /2016	An investigation on the use of supervised learning methods to identify attacks on the cloud	Cloud computing	Performance of this research is very low

[13]	M. Eskandari/2017	Method for verifying the location of a virtual machine in the cloud using VLOC	Cloud computing	Lack of technical work
[14]	E. Hesamifard/2017	Machine learning in the cloud that respects privacy	Cloud computing, Machine learning	Scope of this research is very less
[15]	Z. He/2017	Detection of DDoS Attacks from the Source in the Cloud Using Machine Learning	Machine learning	There is lack of performance
[16]	M. Marwan/2018	Machine learning is being used to improve cloud healthcare security.	Machine learning , Cloud computing	Performance of this research is very low

Table 2: feature of comparison chart

Citation	Machine learning	Cloud computing	Deep learning	Security
[1]	Yes	No	No	No
[2]	No	Yes	No	No
[3]	No	Yes	No	Yes
[4]	No	Yes	No	No
[5]	No	Yes	No	No
[6]	No	Yes	No	No
[7]	Yes	Yes	No	No
[8]	No	No	Yes	No
[9]	No	No	Yes	No
[10]	No	Yes	No	Yes
[11]	Yes	Yes	No	No
[12]	No	Yes	No	No
[13]	Yes	Yes	No	No
[14]	No	Yes	No	Yes
[15]	Yes	Yes	No	Yes
[16]	Yes	No	No	Yes

[3] Problem Statement

In the subject of machine learning and cloud computing, a lot of research has been done recently. However, it has been shown that these studies had problems with performance and accuracy. Performance and cost need to be improved. The accuracy and scalability of the system must also be

enhanced. A more effective machine learning system for cloud applications is anticipated to be provided by the proposed work's hybrid methodology.

[4] Need of Research

The purpose of the current study is to boost the accuracy of cloud-based machine learning procedures. Instead of constructing and maintaining their own computer systems, social interactions or networks may apply machine learning. Using artificial intelligence with social media to establish a long-term ecosystem in which users of social media networks may trade resources is now achievable. Social networking, machine learning, and data storage are just a few of the applications for which deep learning may be employed. Analytical skills may be strengthened by the use of this approach. It is feasible to divulge personal information on social media using machine learning because social media is so accessible. The term "peer-to-peer" is a better one. Social networks or other peer-to-peer systems are used to authenticate the identification of users in this form of social AI. Past research has had difficulties with accuracy and performance, hence the suggested study would present a new technique to acquire a more accurate outcome.

[5] Scope of Research

The goal of the present research is to increase the accuracy of cloud-based machine learning processes. Instead of developing and maintaining their own computer systems, social conversations or networks may employ machine learning. Using artificial intelligence with social media to create a long-term ecosystem in which members of social media networks may swap resources is now possible. Social networking, machine learning, and data storage are just a few of the applications for which deep learning may be used. Analytical capabilities may be enhanced by the use of this technique. It is possible to disclose personal information on social media using machine learning since social media is so accessible. The phrase "peer-to-peer" is a better one. Social networks or other peer-to-peer systems are used to verify the identity of users in this kind of social AI. Past research has had concerns with accuracy and performance, therefore the proposed study would provide a new approach to get a more accurate result.

References

1. Yogi, T. N., and Paudel, N. (2020). Comparative Analysis of Machine Learning Based Classification Algorithms for Sentiment Analysis. International Journal of Innovative Science, Engineering & Technology, 7(6),1-9.
2. 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
3. R. Jathanna and D. Jagli, “Cloud computing and security issues,” Int. J. Eng. Res. Appl., vol. 7, no. 6, pp. 31–38, 2017.
4. A. Huth and J. Cebula, “The basics of cloud computing,” United States Comput., 2011.
5. M. T. Khorshed, A. B. M. Shawkat Ali, and S. A. Wasimi, “Trust issues that create threats for cyber attacks in cloud computing,” in Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS, 2011, doi: 10.1109/ICPADS.2011.156.

6. A. P. Achilleos et al., "The cloud application modelling and execution language," J. Cloud Comput., 2019, doi: 10.1186/s13677-019-0138-7.
7. R. Moreno-Vozmediano, R. S. Montero, E. Huedo, and I. M. Llorente, "Efficient resource provisioning for elastic Cloud services based on machine learning techniques," J. Cloud Comput., 2019, doi: 10.1186/s13677-019-0128-9.
8. D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," Cluster Comput., pp. 1–13, 2017, doi: 10.1007/s10586-017-1117-8.
9. Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.
10. H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," J. Supercomput., vol. 76, no. 12, pp. 9493–9532, 2020, doi: 10.1007/s11227-020-03213-1.
11. I. Avdagic and K. Hajdarevic, "Survey on machine learning algorithms as cloud service for CIDPS," in 2017 25th Telecommunications Forum, TELFOR 2017 - Proceedings, 2018, doi: 10.1109/TELFOR.2017.8249467.
12. G. Nenvani and H. Gupta, "A survey on attack detection on cloud using supervised learning techniques," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570872.
13. M. Eskandari, A. S. De Oliveira, and B. Crispo, "VLOC: An approach to verify the physical location of a virtual machine in cloud," in Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, 2015, doi: 10.1109/CloudCom.2014.47.
14. E. Hesamifard, H. Takabi, M. Ghasemi, and C. Jones, "Privacy-preserving machine learning in cloud," in CCSW 2017 - Proceedings of the 2017 Cloud Computing Security Workshop, co-located with CCS 2017, 2017, pp. 39–43, doi: 10.1145/3140649.3140655.
15. Z. He, T. Zhang, and R. B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," in Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, 2017, doi: 10.1109/CSCloud.2017.58.
16. M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," Procedia Comput. Sci., vol. 127, pp. 388–397, 2018, doi: 10.1016/j.procs.2018.01.136.
17. U. A. Butt et al., "A Review of Machine Learning Algorithms for Cloud Computing Security," Electronics, vol. 9, no. 9, p. 1379, Aug. 2020, doi: 10.3390/electronics9091379.
18. T. Kim et al., "Monitoring and detecting abnormal behavior in mobile cloud infrastructure," in Proceedings of the 2012 IEEE Network Operations and Management Symposium, NOMS 2012, 2012, doi: 10.1109/NOMS.2012.6212067.
19. F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Comput., vol. 20, pp. 343–357, 2016, doi: 10.1007/s00500-014-1511-6.
20. B. Amos, H. Turner, and J. White, "Applying machine learning classifiers to dynamic android malware detection at scale," in 2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013, 2013, pp. 1666–1671, doi: 10.1109/IWCMC.2013.6583806.

21. B. Gulmezoglu, T. Eisenbarth, and B. Sunar, “Cache-based application detection in the cloud using machine learning,” in ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, 2017, pp. 288–300, doi: 10.1145/3052973.3053036.
22. K. Borisenko, A. Smirnov, E. Novikova, and A. Shorov, “DDoS attacks detection in cloud computing using data mining techniques,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, vol. 9728, pp. 197–211, doi: 10.1007/978-3-319-41561-1_15.
23. Z. Chkirbene, A. Erbad, and R. Hamila, “A Combined Decision for Secure Cloud Computing Based on Machine Learning and Past Information,” in IEEE Wireless Communications and Networking Conference, WCNC, 2019, doi: 10.1109/WCNC.2019.8885566.
24. V. Sharma, V. Verma, and A. Sharma, “Detection of DDoS Attacks Using Machine Learning in Cloud Computing,” in International Conference on Advanced Informatics for Computing Research, 2019, vol. 1076, pp. 260–273, doi: 10.1007/978-981-15-0111-1_24.
25. A. Inani, C. Verma, and S. Jain, “A machine learning algorithm TSF k-Nn based on automated data classification for securing mobile cloud computing model,” in 2019 IEEE 4th International Conference on Computer and Communication Systems, ICCCS 2019, 2019, pp. 9–13, doi: 10.1109/CCOMS.2019.8821756.