International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimizing AI/ML Workloads in Cloud Environments: A Scalable Approach

Srinivasa Subramanyam Katreddy

Submitted: 14/09/2023 **Revised:** 25/10/2023 **Accepted:** 08/11/2023

Abstract: AI/ML workloads present unique challenges in resource-intensive cloud environments, necessitating innovative optimization techniques. This paper introduces a scalable framework for optimizing AI/ML workloads in multi-cloud and hybrid cloud infrastructures. The approach leverages dynamic resource allocation, auto-scaling mechanisms, and workload scheduling algorithms to enhance performance and cost efficiency. Experimental results demonstrate reduced latency, improved throughput, and significant cost savings across diverse AI/ML applications. This work provides actionable insights for organizations aiming to optimize cloud usage for complex AI workloads.

Keywords: *AI/ML Workloads, Cloud Optimization, Scalable Infrastructure, Resource Allocation, Multi-Cloud Strategies.*

I. Introduction

Models of artificial intelligence (AI) are at the forefront of technical breakthroughs, propelling improvements across a wide range of industries, including healthcare, finance, automotive, and many more. These models, which are driven by intricate algorithms and enormous datasets, can imitate human intellect, automate operations, and extract insights from data on a scale that has never been seen before. Despite this, artificial intelligence models are facing severe scalability issues as they continue to grow in complexity and scale. Within the scope of this discussion, the term "scalability" refers to the capability of artificial intelligence models to manage larger datasets, handle rising workloads, and either maintain or increase performance with the addition of resources. Scalability presents a number of challenges from a variety of angles, including processing resources, data handling capabilities, and the complexity of the model [1].

When it comes to addressing these objectives, traditional computer systems frequently fall short due to constraints in processor power, storage capacity, and customisation versatility. Researchers and developers are increasingly looking to cloud infrastructure as a feasible answer to these scalability difficulties. This is because cloud infrastructure offers a number of advantages. Cloud infrastructure, with its distributed computing environments, provides scalable resources, such as computing power and data storage, which can be dynamically altered to match the requirements of artificial intelligence models. The transition to cloud infrastructure represents a significant change in the way artificial intelligence models are generated, trained, and deployed. It enables models to access essentially unlimited computational resources [2], makes it easier to manage large-scale datasets, and helps the deployment of artificial intelligence applications to a wide user base without requiring major upfront expenditures in hardware.

New paradigms in artificial intelligence research and development are introduced as a result of this transition, which places an emphasis on adaptability, cost-effectiveness, and accessibility. This transition not only tackles the technical demands of scaling AI models. Nevertheless, utilising cloud infrastructure for scalable artificial intelligence models presents its own unique set of challenges and factors to take into consideration. Concerns regarding the privacy of data, the security of data, the interoperability of data [3], and the financial ramifications of cloud services are of the utmost importance. In addition, there are ethical and societal problems that need to be carefully considered, such as the influence that large-scale computing has on the environment and algorithmic bias.

AI Solutions Architect,
328 Camelot Dr, City: Pittsburgh State: Pennsylvania, USA - 15028
srinivasa.katreddy@gmail.com

The purpose of this research is to investigate the impact that cloud infrastructure plays in improving the scalability of artificial intelligence models. This project intends to provide complete examination of how cloud computing makes it easier to design and deploy scalable artificial intelligence models [4]. Additionally, it will address the obstacles that are involved with this endeavour, including those that are technological, ethical, and cost-related. This article will shed light on the synergistic link between cloud infrastructure and artificial intelligence scalability by conducting a deep assessment of existing practices, case studies, and developing trends.

Additionally, this research will offer insights into future directions and breakthroughs in the field. The purpose of this research is to add to the continuing conversation about the development of artificial intelligence technologies by bridging the gap between the constraints of AI scalability and the solutions offered by cloud computing. It also highlights the crucial role that cloud infrastructure plays in enabling the next generation of AI applications.

II. Literature Survey

As the field of artificial intelligence (AI) continues to undergo rapid development, scalability has emerged as an essential quality of AI models. The ever-increasing complexity of these models, as well as the exponential development in the amount of data that they handle, both demonstrate the importance of this demand. Scalability is the capacity of an artificial intelligence system to effectively manage increasing amounts of work or to accommodate expansion. Scalability can also be defined as growth capacity. The purpose of this section is to investigate the imperatives that are driving the demand for scalable artificial intelligence models, to emphasise the significance of scalability through a variety of applications, and to evaluate the influence that scalability has on performance and impliedness [5].

A considerable movement towards models that are characterised by sophisticated architectures and an expanded parameter space has arisen as a result of the trajectory of the development of artificial intelligence. As an illustration of this pattern, consider the progression from the earliest neural networks to more complex frameworks like as GPT-3 and BERT (Devlin et al., 2019). The fact that these models contain billions of parameters makes it necessary to have a significant amount of processing capacity for training and inference. This highlights the fact that scalability is an essential prerequisite for the efficient utilisation of these models. According to [6], the growing number of datasets, which is occurring concurrently with the increase in the complexity of models, also emphasises the requirement for scalable solutions.

Applications of Artificial Intelligence That Need to Be Scalable Not only does the utility of scalability extend beyond the technical realm, but it also has a substantial impact on the effectiveness and implementation of artificial intelligence across a variety of applications. In the field of natural language processing (NLP) [7 – 9], scalable models are of the utmost importance for a wide variety of tasks, including machine translation and sentiment analysis. These models enable sophisticated interpretation and the production of text. The ability to collect and analyse large amounts of visual data in real time is essential for applications such as automated medical diagnostics and autonomous vehicle navigation. This is also true in the field of computer vision and image recognition. Scalability is also critical to the performance of recommender systems and predictive analytics, both of which require the management of enormous datasets in order to produce outputs that are accurate and personalised [10].

Impact of Scalability on the Performance and Applicability of Artificial Intelligence Models The scalability of artificial intelligence models has a direct impact on both their performance and the scope of their applications. Scalable models can effectively utilise larger datasets, which can result in greater accuracy, enhanced generalisation capabilities, and a deeper understanding of intricate patterns. Scalable models are also capable of exploiting larger datasets. Not only is this scalability [11] essential for the development of artificial intelligence research, but it is also the key to the successful implementation of AI solutions across a wide range of industries. At the other end of the spectrum, models that are not scalable may suffer from decreased performance as a result of bottlenecks in computational and data processing, which limits their application to tasks that require a significant amount of data or are performed on a big scale. Furthermore, the scalability of AI models is essential to the democratisation of artificial intelligence, which refers to the process of making advanced AI technologies available to a wider audience, which may include individuals and smaller businesses.

According to [12], cloud-based solutions make it possible to dynamically allocate computational resources in line with demand. This democratisation is made possible by cloud-based solutions. In conclusion, the increasing complexity of these models, the vast datasets that they use, and the wide variety of applications that they serve are the driving forces behind the impetus for the development of scalable artificial intelligence models. Not only is it essential to address the scalability challenge in order to improve model performance and widen the practical uses of these models, but it is also essential in order to further the democratisation of artificial intelligence technology [13].

For the purpose of maintaining the expansion and utilisation of artificial intelligence technologies, it will be necessary for future developments in AI development to continue concentrating on scalable solutions, most likely by utilising cloud infrastructure [14].

III. Cloud Infrastructure

A paradigm change in computing has occurred with the introduction of cloud infrastructure, which has fundamentally altered the ways in which data is stored, processed, and accessed. This section provides an overview of the fundamental components of cloud infrastructure, presents an explanation of the many types of cloud services, and highlights the advantages of utilising cloud solutions for the development of artificial intelligence, with a particular emphasis on scalability. As opposed to local servers or personal computers, cloud infrastructure is made up of a network of remote servers [15] that are hosted on the Internet. These servers allow for the storage, management, and processing of data. The cloud allows for the distribution of computing services such as servers, storage, databases, networking, software, analytics, and intelligence. This infrastructure enables the delivery of these services. Cloud infrastructure is characterised by a number of key qualities, including on-demand self-service, extensive network access, resource pooling, quick flexibility, and measured service. According to [16], these characteristics guarantee that cloud services are adaptable, scalable, and administered in an effective manner.

III.1. Types of Cloud Services:

Cloud services can be broken down intoA three basic models, each of which caters to a particular set of requirements during the process of application development and deployment, including projects involving artificial intelligence and machine learning: IaaS, which stands for "Infrastructure as a Service," is a service that offers virtualised computing resources through the internet. Users are able to rent virtual machines, storage, and networks on a pay-as-you-go basis through the usage of infrastructure as a service (IaaS), which provides the fundamental components of cloud computing. Because it provides the greatest amount of flexibility and control over computing resources, this approach is perfect for projects that have requirements that are either one of a kind or that are subject to quick change. PaaS, which stands for "platform as a service," provides a cloud-based environment for software development and deployment, complete with tools for the creation, testing, deployment, management, and updating of software applications [17 -19].

The purpose of platform as a service (PaaS) is to provide developers with a framework that they can use to build upon and customise apps in a more effective manner. PaaS is designed to support the entire lifecycle of web applications. Software as a Service (SaaS) is a model that provides software programs to users [20] on a subscription basis and is delivered over the internet. As part of their service, software as a service (SaaS) providers host and maintain applications, which includes taking care of maintenance duties like software upgrades and security patches. The software can be accessed by users from any device, which makes software as a service (SaaS) very useful for applications that require extensive access.

The Advantages for the Development of AI The infrastructure of the cloud provides a number of benefits for the development of artificial intelligence, addressing many of the scaling difficulties that are faced by AI model [21] Cloud services may be scaled up or down fast to suit the computing demands of artificial intelligence projects. This ensures that resources are utilised effectively and expenses are kept under control. [22] Organisations are able to avoid the considerable upfront expenditures that are associated with setting up and maintaining physical servers by utilising the pay-as-you-go model. Because of this, complex artificial intelligence projects are now more accessible to a wider variety of entities, ranging from small businesses to huge corporations [23].

Cloud platforms provide access to powerful computational capabilities, such as graphics processing units (GPUs) and teraflops (TPUs), which are a vital component for the training of complicated artificial intelligence models. Access to high-performance computing resources is democratised as a result of this, making it possible for smaller teams to conduct large artificial intelligence projects. The modern computational environment is supported by cloud infrastructure, which provides a platform that is durable, adaptable, and cost-effective for hosting advanced artificial intelligence models that are scalable [24]. Cloud infrastructure has the ability to enable artificial intelligence practitioners to concentrate on research and development without being hampered by the constraints of hardware. This is accomplished by offering on-demand access to computational resources. As artificial intelligence models continue to increase in both complexity and applicability, the essential role that cloud infrastructure plays in supporting these developments is becoming increasingly significant.

IV. Proposed Methodology

Financial fraud fraud is a serious ethical problem in the business world. The research primary goal is to detect financial fraud fraud and offer a workable solution to this problem. Financial fraud fraud has resulted in billions of dollars in losses worldwide for victims and financial institutions. Even though there are many security measures in place to prevent fraud, attackers are always devising new techniques to deceive unsuspecting victims. The banking industry and other financial institutions place a premium on fraud detection. The proposed model use historical fraud data to improve its ability to identify future instances of fraud. While fraud detection algorithms based on mining data had been tried, they had not shown any promising results. The research makes use of supervised learning methods applied to a highly skewed and imbalanced dataset considered from Kaggle.

Feature selection is a crucial part of data preparation to avoid over fitting due to the curse of dimensionality reduction. Through the process of feature selection, superfluous or unimportant details are eliminated. Filter and wrapper are the two most well-known approaches, and both have their advantages and drawbacks. The wrapper method has some drawbacks, such as the high processing cost and reliance on the algorithm as an evaluation function to select the features. On the other hand, the filter approach has the drawback of only searching for features independently, therefore features that are highly dependent on one another will be missed.

A ML based feature selection strategy that combines filter and wrapper approaches is an alternate solution that is less exhaustive and has less drawbacks. In order to determine the degree of similarity between the numerical characteristics, a correlation-based filter was employed. Positive features that were highly associated were omitted from the prediction model to prevent over fitting and to conserve computational resources. This research presents a Related Feature Subset Model for Financial fraud Fault Detection for accurate detection of financial fraud frauds. The proposed model architecture is shown in Figure 1.

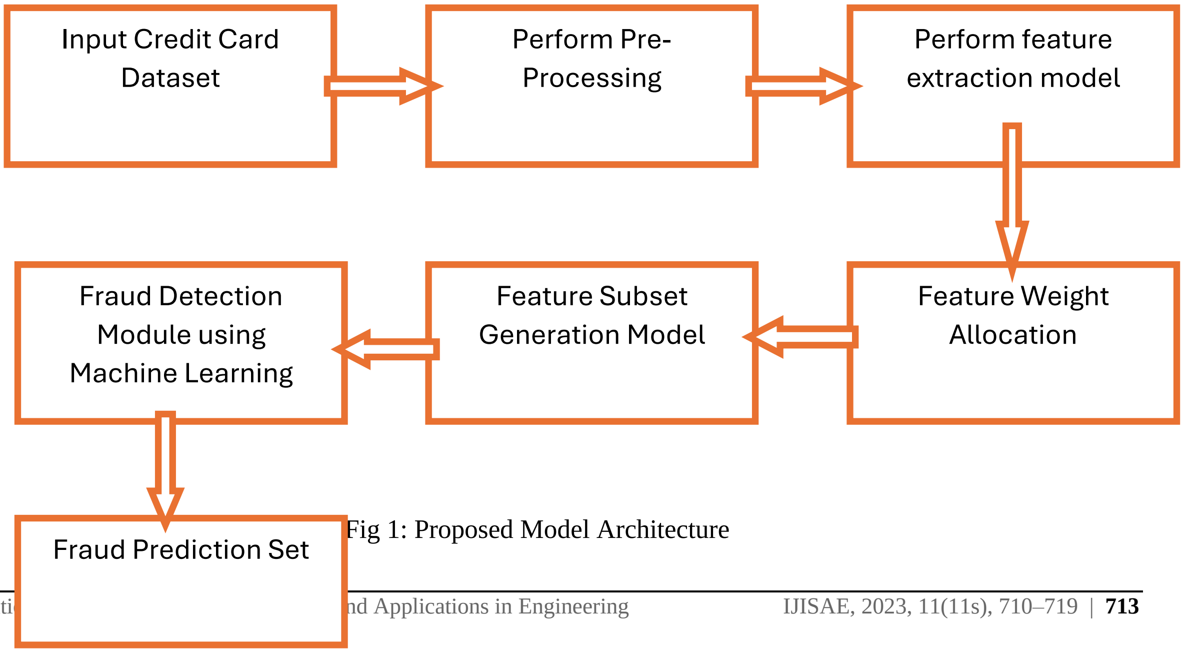

Input Credit Card Dataset
Perform Pre-Processing
Perform feature extraction model
Feature Weight Allocation
Feature Subset Generation Model
Fraud Detection Module using Machine Learning
Fraud Prediction Set

Fig 1: Proposed Model Architecture

Algorithm RF-CFD

{

Input: Financial fraud Fraud Dataset {CCFDSET}

Output: Fraud Prediction Set {FPSET}

Step-1: Load the dataset and then analyze the records to perform pre processing on the dataset. The pre processing cleans the data from the available ones. The pre processing is performed as

Step-2: As a method of dimensionality reduction, feature extraction organises large amounts of raw data into more manageable parts. In order to process these massive data sets, a great deal of computational power is needed because of the sheer amount of variables involved. To reduce the amount of data that needs to be processed while still providing an accurate and complete description of the original data set, a number of techniques have been developed under the feature extraction process. The feature extraction process is performed as

Step-3: The parameters employed in each layer of the model are reflected in the model's weights. The weights are allocated based on the correlation factor and the highly correlated features are removed and most useful features are considered.

Step-4: From the features extracted, the feature subset is generated which considers the most useful features that is used for financial fraud fraud detection.

Step-5: The financial fraud fraud detection is performed by training the model using the feature subset.

Machine learning algorithms can identify suspicious activity on a financial fraud and prevent further losses. The first step in using a model to predict potential instances of fraud is to collect and organize raw data for use in training that model. Machine learning provides solutions for detecting financial fraud fraud, including the use of learning algorithms to classify transactions as authentic or fraudulent, financial fraud profiling to predict whether legitimate cardholders or malicious actors are using the cards, and outlier detection methods to identify records of transactions that are significantly different from the norm.

Financial fraud fraud is a big problem in today's interconnected global economy. Worldwide, fraud results in massive financial losses. As a result, many banks have invested in studying the problem and creating tools to help identify and stop financial fraud fraud. The major goal of this research is to develop a ML model that efficiently and accurately identify fraudulent transactions for financial fraud issuers. Computer software that may rapidly construct a prediction system for detecting financial fraud fraud by automatically picks suitable Machine Learning algorithms, adjusting their hyper-parameter variables, and evaluating performance on a highly skewed dataset.

There is zero overhead in terms of user setting of method parameters during model training. It also requires little work to apply the model, retrain this whenever new data becomes available, produce visualizations of the findings, and communicate them across the many levels of management in the organization.

A. Source of information and tools for analysis:

The proposed model is implemented in python and executed in Google Colab. The proposed model is compared with the traditional Enhanced financial fraud fraud detection based on attention mechanism and LSTM deep model (FDAM-LSTM) model.

Data preprocessing, or the manipulation or removal of data before to its usage, is a crucial part of the data mining process, as it ensures or improves performance. Any action taken on raw data in order to get it ready for further processing is referred to as data preprocessing, and it is part of the larger data preparation process. It is a crucial first stage in the data mining process and has been for a long time.

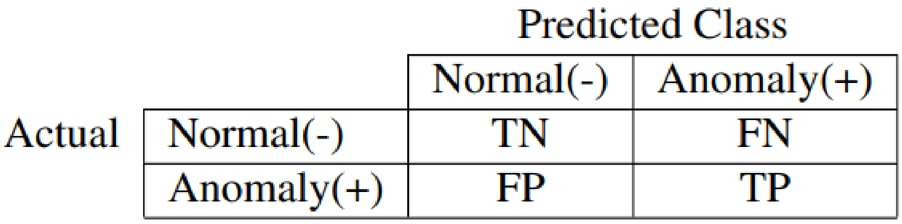
1. The data preprocessing secure accuracy levels of the existing and proposed models.
2. The feature extraction time levels of the existing and proposed models
3. The feature weight allocation secure accuracy levels of the traditional and proposed models
4. The feature subset generation time levels of the proposed and the traditional method.
5. The feature subset generation secure accuracy levels of the traditional and proposed models
6. The proposed model fraud detection time levels is less than the existing models
7. The fraud detection secure accuracy levels of the proposed model is high than the existing models

V. Performance Analysis

Criminals are more likely to resort to online payment fraud in an attempt to circumvent payment providers' security measures, as the popularity of such transactions has grown. With the ultimate goal of preventing fraud in an online payment system and devising countermeasures against attacks, there is a lot of pressure to investigate any security vulnerabilities that could be exploited. Detecting potentially fraudulent financial transactions as early as possible is an important aspect of this research. The development of online payment systems has led to an increase in demand for automated detection technologies that can detect and stop fraudulent transactions in real-time.

With the spread of smartphones, there is an increase in the usage of mobile payment methods, which piques the interest of scammers. Numerous fraud detection algorithms that employ supervised machine learning have been developed in response to the aforementioned body of literature. Nonetheless, suitable labelled data are scarce, and the considerable class imbalance in financial fraud data reduces detection performance. Given the monetary ramifications of fraud detection systems, this study seeks to propose an improved logistic regression framework for detecting fraudulent behaviour. The system was validated using a massive dataset of over 3 million Internet transactions. This study presents a Linked Feature Set with Enhanced Logistic Regression (LFS-ELR) Model for accurately detecting online payment fraud. Results from a comparison with the standard Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services (FGCO-BFD-OPS) show that the proposed model delivers respectable results. The fraud prediction set is calculated using the formulas shown below.

Evaluation Metrices



		Predicted Class	
		Normal(-)	Anomaly(+)
Actual	Normal(-)	TN	FN
	Anomaly(+)	FP	TP

Based on above table, different performance parameters are calculated in evaluation of model.

True positive Rate OR Recall:

$$TPR = \frac{TP}{TP + FN}$$

Accuracy:

$$Accuracy = \frac{TP + TN}{TN + FP + FN + TP}$$

Precision:

$$Precision = \frac{TP}{FP + TP}$$

F1 score:

$$F1score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

Feature extraction is a form of dimensionality reduction that involves partitioning an initial set of raw data into more manageable subsets. One of the characteristics of these massive data sets is the large number of variables that must be processed, which requires a significant amount of computational power. The process of selecting and/or combining variables to create features is known as feature extraction. This effectively reduces the amount of data that must be handled while accurately and thoroughly characterizing the initial data set. Table 1 shows the feature extraction time levels of the proposed and traditional models.

Table. 1: Feature Extraction Time Levels

Size of the Dataset	FDAM-LSTM	Proposed RF-CFD
5	12.0	6.0
10	14.0	7.8
15	15.9	9.3
20	17.7	11.2
25	21.4	13.5
30	21.4	14.6

The feature extraction accuracy levels of the suggested and current models are displayed in Table 2.

Table 2: Feature Extraction Accuracy Levels

Size of the Dataset	FDAM-LSTM	Proposed RF-CFD
5	78.2	82.7
10	80.9	84.5
15	82.1	86.4
20	84.5	88.2
25	86.7	90.2
30	88.3	92.6

Feature selection is the process of using only the data that is relevant to the model and removing noise from it to limit the number of variables that are fed into the model. It is the technique of automatically identifying appropriate features for a machine-learning model based on the type of problem being addressed. This can be accomplished by selectively including or removing significant features while leaving them unchanged. Thus, data noise and size can be reduced. Table 3 shows the Feature Selection Accuracy Levels of the existing and proposed models.

Table 3: Feature Selection Accuracy Levels

Size of the Dataset	FDAM-LSTM	Proposed RF-CFD

5	82.1	88.1
10	82.6	90.5
15	84.7	92.1
20	87.4	94.8
25	89.4	96.2
30	90.7	97.8

The detection of modern payment fraud makes use of machine learning based ELR model and statistical analysis to continually monitor transactions and evaluate the level of risk that is connected with each transaction. This may require comparing lacks of different pieces of transactional data to various models of fraud that are already known to exist. Scammers take advantage of the payment request option that is available in apps that support the UPI in order to obtain the PIN or OTP that is required to authorize a transaction. They start the process of requesting payment and then contact the person in question to inquire about the OTP or PIN, claiming that this information is necessary on their end in order to finalize a transaction. The Figure 2 represents the Online Payment Fraud Detection Accuracy Levels of the proposed and existing models.

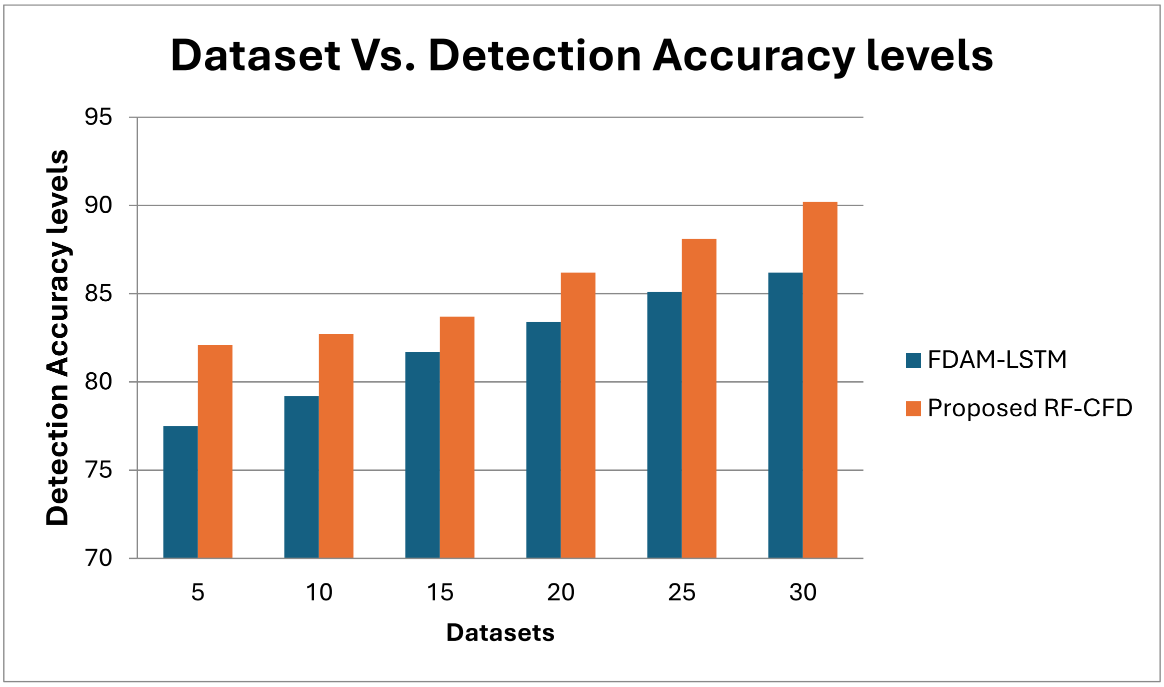


Figure. 2 Dataset Vs. Detection Accuracy levels

VI. Conclusion

Providing the processing power, storage capacity, and deployment flexibility that are necessary to address the rising complexity and data-intensive nature of contemporary AI systems, cloud infrastructure is emerging as a major enabler for scalable artificial intelligence models. Researchers and practitioners are able to devote their attention to innovation rather than infrastructure management because to the specialised tools and services that cloud providers have developed. These tools and services ease the process of implementation and deployment. The significant advancements that have been made in the field of artificial intelligence are demonstrated by the incorporation of scalable AI models with cloud infrastructure. The fact that it symbolises a convergence of technological developments that are not only driving the next wave of innovation in artificial intelligence but also solving some of the most important concerns of our day is a significant achievement. When we consider the future, it is without a doubt that the ongoing investigation and development of this field will unquestionably play a significant part in determining the course that artificial intelligence research will take and how it will be applied in the actual world. The process of fully realising the potential of scalable artificial intelligence models is a continuing journey, and cloud infrastructure will surely continue to be at the forefront of this endeavour intended to alter the industry.

References:

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58. https://dl.acm.org/doi/10.1145/1721654.1721672

[2] Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and Abstraction in Sociotechnical Systems. *ACM Conference on Fairness, Accountability, and Transparency*, 59-68. https://dl.acm.org/doi/10.1145/3287560.3287598

[3] Covington, P., Adams, J., & Sargin, E. (2016). Deep neural networks for YouTube recommendations. *Proceedings of the 10th ACM conference on Recommender Systems*, 191-198. https://dl.acm.org/doi/10.1145/2959100.2959190

[4] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. https://doi.org/10.48550/arXiv.1810.04805

[5] Halevy, A., Norvig, P., & Pereira, F. (2009). The unreasonable effectiveness of data. IEEE Intelligent Systems, 24(2), 8-12. https://doi.org/10.1109/MIS.2009.36

[6] Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and Policy Considerations for Deep Learning in NLP. 57th Annual Meeting of the Association for Computational Linguistics (pp. 3645-3650). https://doi.org/10.48550/arXiv.1906.02243

[7] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). https://dl.acm.org/doi/10.5555/3152676

[8] Doctor, A. (2023). Manufacturing of Medical Devices Using Artificial Intelligence-Based Troubleshooters. In: Paunwala, C., et al. Biomedical Signal and Image Processing with Artificial Intelligence. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-15816-2_11

[9] Preyaa Atri, "Design and Implementation of High-Throughput Data Streams using Apache Kafka for Real-Time Data Pipelines", International Journal of Science and Research (IJSR), Volume 7 Issue 11, November 2018, pp. 1988-1991, https://www.ijsr.net/getabstract.php?paperid=SR24422184316 and Research

[10] Preyaa Atri, "Enhancing Big Data Interoperability: Automating Schema Expansion from Parquet to BigQuery", International Journal of Science (IJSR), Volume https://www.ijsr.net/getabstract.php?paperid=SR24522144712 8 Issue 4, April 2019, pp. 2000-2002,

[11] Atri P. Enabling AI Work flows: A Python Library for Seamless Data Transfer between Elasticsearch and Google Cloud Storage. J Artif Intell Mach Learn & Data Sci 2022, 1(1), 489-491. DOI: doi.org/10.51219/JAIMLD/preyaa-atri/132

[12] M.A., Ferrag "The performance evaluation of blockchain-based security and privacy systems for the internet of things: a tutorial." IEEE Internet of Things Journal 8.24 (2021): 17236-17260.

[13] S., Bauk "Blockchain implementation barriers in maritime: a case study based on ism and micmac techniques." Journal of Maritime Research 20.3 (2023): 72-80.

[14] V.S., Rao "Energy exchange process for smart grid based on integrating blockchain with gcn-lstm." Journal of Theoretical and Applied Information Technology 101.24 (2023): 8430-8446.

[15] X., Lin "Making knowledge tradable in edge-ai enabled iot: a consortium blockchain-based efficient and incentive approach." IEEE Transactions on Industrial Informatics 15.12 (2019): 6367-6378.

[16] D., Folkinshteyn "Braving bitcoin: a technology acceptance model (tam) analysis." Journal of Information Technology Case and Application Research 18.4 (2016): 220-249.

[17] H., Wu "Blockchain-based onsite activity management for smart construction process quality

traceability." IEEE Internet of Things Journal 10.24 (2023): 21554- 21565.

[18] R., Pise "A survey on smart contract vulnerabilities and safeguards in blockchain." International Journal of Intelligent Systems and Applications in Engineering 10.3s (2022): 1-16.

[19] J.G., Allen "Wrapped and stacked: 'smart contracts' and the interaction of natural and formal language." European Review of Contract Law 14.4 (2018): 307- 343.

[20] K., Werbach "Contracts ex machina." Duke Law Journal 67.2 (2017): 313-382.

[21] W., Lee "A robust identity recovery scheme for the ethereum blockchain platform." Information (Japan) 20.11 (2017): 8133-8141.

[22] X., Feng "Cobc: a blockchain-based collaborative inference system for internet of things." IEEE Internet of Things Journal 10.24 (2023): 21389-21400.

[23] W.A., Kaal "Crypto transaction dispute resolution." Business Lawyer 73.1 (2017): 109-151.

[24] Y. Jani, A. Jani, and K. Prajapati, “Leveraging multimodal ai in edge computing for real time decisionmaking,”computing, vol. 7, no. 8, pp. 41– 51, 2023.

[25] Rahul Kalva. Revolutionizing healthcare cybersecurity a generative AI-Driven MLOps framework for proactive threat detection and mitigation, World Journal of Advanced Research and Reviews, v. 13, n. 3, p. 577-582, 2022.