International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010

THE ROLE OF CLOUD COMPUTING IN MACHINE LEARNING APPROACHES

Abhishek Gautam, Sonika Jindal, Pashupati Kr. Baitha
Department of Computer Science
Shaheed Bhagat Singh State University, Ferozepur.

Aloukik Arora
IT & EE
University of Oulu, Finland

Ashish Gautam
Department of Computer Science
IKGPTU, Jalandhar

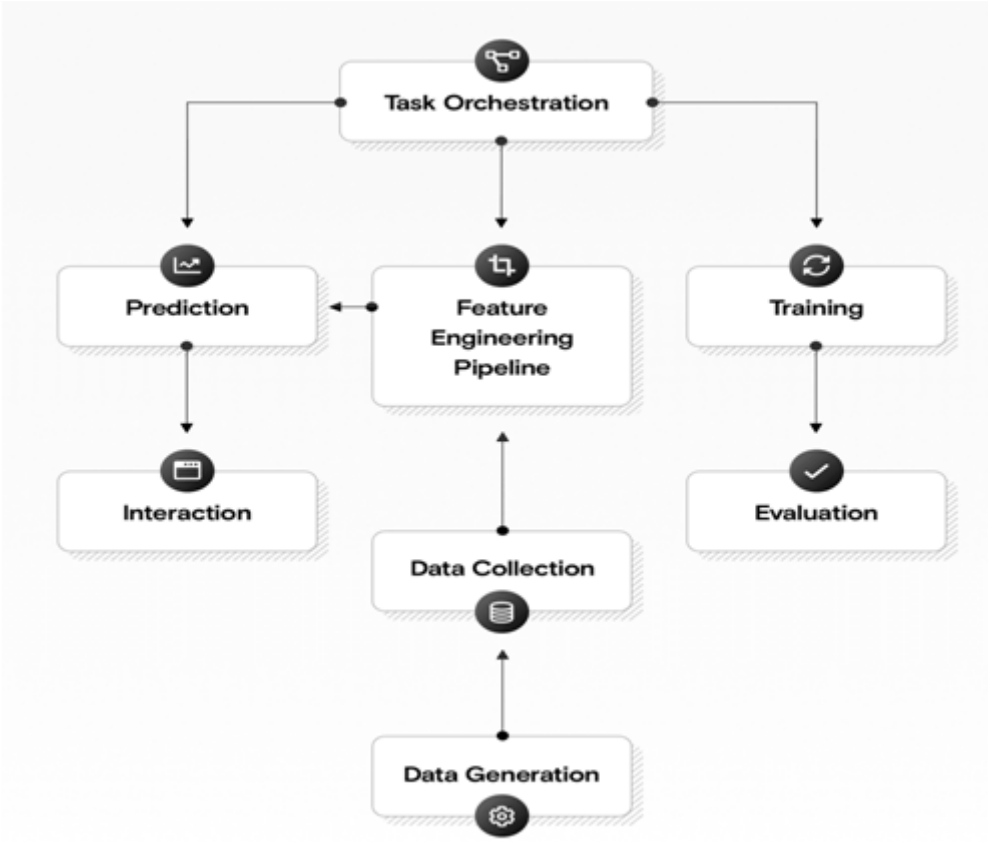
Abstract— **This paper is presented to explain the intersection of cloud computing (CC) and machine learning (ML), focusing on their synergies, challenges and solutions. It shows the changes in the Internet service area led by cloud computing (CC) and the economic impact of data collection and analysis. The document specifically addresses security issues in distributed models and introduces the concept of edge computing as a version of cloud computing (CC) for time-sensitive data.**
In this paper, we are discussing about data encryption, distribution of rights, and transfer of data responsibility from service providers to end users. The document breaks down Cloud computing into service and delivery models, addressing security issues related to integrity, availability, and identity threats.
It offers machine learning (ML) algorithms as a solution to security and data quality management.
With the help of this paper, we are highlights the challenges of integrating Cloud Computing (CC) and machine learning (ML), including data exchange latency, scalability optimization, resource management, data security, model deployment, and monitoring. A resource plan is provided to train organizations in the use of Cloud Computing (CC) and machine learning (ML). The summary ends by highlighting the evolution of Cloud Computing (CC) and machine learning (ML) integration to shape the future of computing and analytics and make organizations more competitive in the digital age.

Keywords— **Machine Learning, Haar Wavelet, DWT, PSNR**

I. INTRODUCTION

Cloud Computing (CC) has recently emerged as a new framework to facilitate and deliver Internet services [1]. A financial constraint and increased budget to store, analyse and present data have changed dramatically for today's cloud models [2,3]. Cloud computing is the need to access the end user, specifically data storage and operation, without the need for direct organization by the user. Distributed computing provides general and specific information to users on an Internet platform[4].

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010



Ref. figure - 01 [19]

However, CC has many security issues such as clients and related issues that delay using fast computing models[5,6]. Edge computing is a version of CC for processing time-sensitive data and provides application developers and service providers with distributed computing capabilities at the edge of the system [7]. The distribution strategy for this strategy introduces a change in the security method used in the distribution system.

In addition, a special encryption process must be used to encrypt data that can travel between distribution networks before it finally reaches the cloud. The end hub will also be the property's responsibility, limiting the decision regarding security requirements.

Data responsibility can be passed from the service provider to the end user by processing data at the edge.CC has service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and also discusses delivery models such as public cloud, community cloud, and hybrid cloud. The main security concerns in CC are devoted to integrity, availability, and privacy threats.

Cloud services range from data storage with unlimited resources to management software services. The Cloud model supports and supports the use of large-scale hardware (used to provide support services) and infrastructure [9]. Not all cloud deployments are suitable for all services, all service providers, or all participants [10]. This document describes security issues and challenges in CC and solutions using machine learning (ML) algorithms.

ML algorithms are used to solve security problems and better manage data[11]. The purpose of this article is to identify legal issues and security threats in distributed computing using machine learning algorithms. Increasing acceptance of Distribution products is the main driver behind their conversion into business offers to reduce real estate and labour costs.

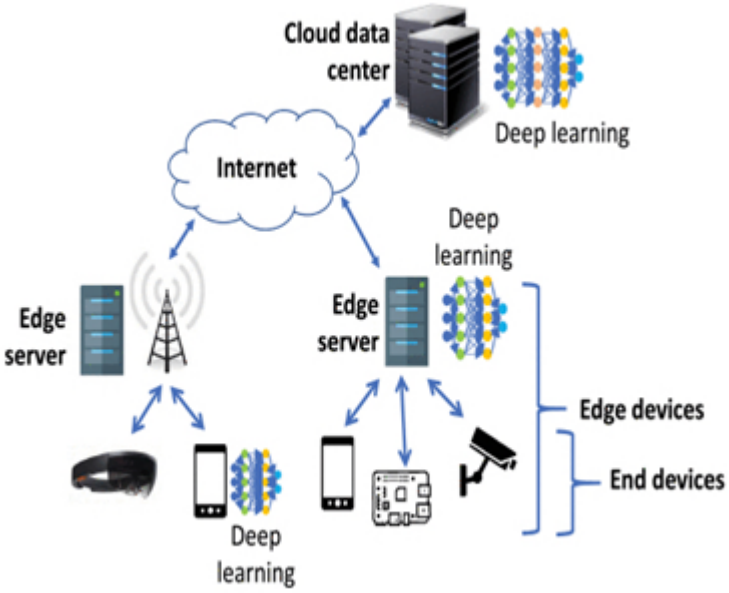
Therefore, management of security and privacy risks in a distributed environment is important because appropriate tools can resolve the problems associated with them[14]. Security issues and issues related to distributed computing using machine learning algorithms were reviewed and discussed, and practical steps were taken to address these issues. Many are inspired by the demand for efficient, effective and secure delivery services. We know that users who choose cloud service providers will not be able to pay for any deals on

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010

security and privacy risks that often place a heavy burden on cloud service providers. Using different algorithms, it is important to evaluate the security issues encountered and related to crime with the help of cloud providers [10].
The main issue we are examining is the security threat in distributed computing. We describe algorithms used to solve problems and improve performance. The security of the cloud environment is the most worrying issue of recent times. Even large cloud service providers with adequate security measures, such as Amazon and Google, are frequently reported by some cloud attacks. Machine Learning as a Service (MLaaS) is a service model used by cloud computing to develop defence strategies against multiple cloud attacks. With the help of machine learning algorithms, has developed several intrusion detection systems that increase the accuracy of intrusion detection and allow businesses to operate.

II. MACHINE LEARNING ARCHITECTURE:

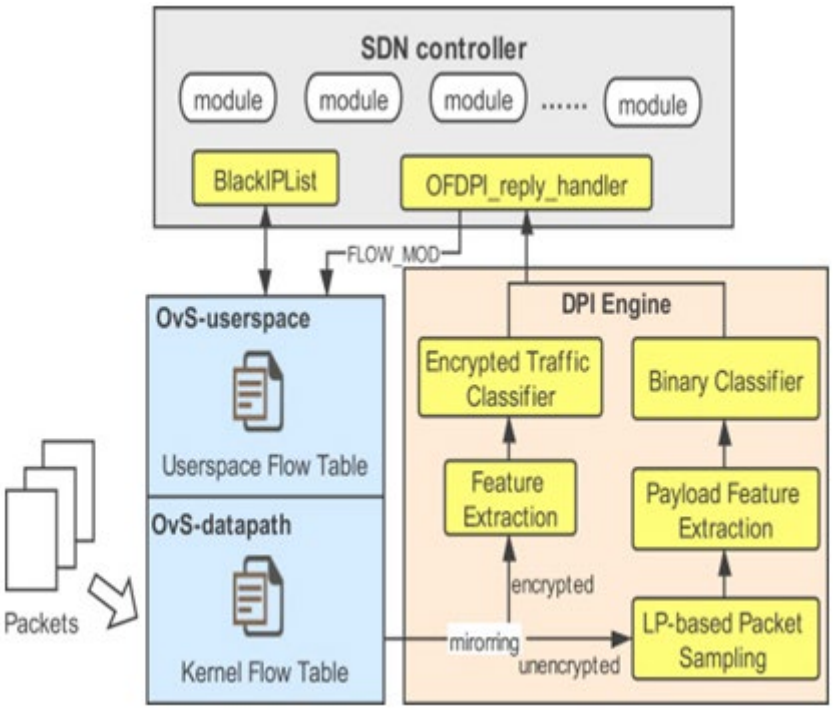
Inside the displaying system characterized over, we consider bland handling, preparing and distributing stage with specialized capacities valuable for the ML space, built on the beat of the essential semantic middleware foundation, so that it leverages its capabilities for interceding the association between conclusion nodes. It is essentially a platform offered as a bouquet of cloud-facilitated web administrations that make broad utilize of PaaS and SaaS highlights like workflows, enormous information administration, ML preparing models, etc. Leveraging the adaptability of the cloud assets it favors worldwide openness, tall accessibility, adaptability, execution, and tall security benchmarks [16].
Data and communication layers are versatile to diverse levels of reflection agreeing to the scope beneath thought. Such an instrument can serve to actualize reasonable ML scenarios with the least-taken toll and forthright venture. And it empowers us to contend on programs, strategies, operations & strategies, rules, and hones, but most vitally in terms of the effect on the lifecycle of the ML-enabled systems. A cloud-based micro-service transport design has been chosen to construct the system show and to typify the basic arrange subtle elements and controlling instruments. This is often satisfactory to oblige for the essential communication designs, changes, and interfacing of conveyed applications, including different parties with a wide range of complexity and separating qualities, concurring to their nature and target usefulness [17].



Ref. figure - 02 [15]

In such a system of widespread gathering of people, a protocol-agnostic approach is obligatory for the higher levels of administration, taking off to the fundamental framework the rudimentary administration of low-level conventions and middleware communication for information procurement or transfer. Other than being dependable for procuring, modelling, preparing and using the comes about either online or offline, it too gives mechanization instruments to associate assorted frameworks that will span the boundaries of the organization itself [18].

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010



Ref. figure - 03 [20]

Backed utilize cases are changing from a single source of information (e.g. a specialist that assesses a picture) that inquires for an ML appraisal through a web benefit, up to a 3rd party application server through an association with a total benefit with worldwide impression. Built on the beat of the commercially accessible PaaS and SaaS administrations, and taking after the most recent innovation advancements in a steady and overseen environment, bargains with trade handle necessities over an assortment of conveyed and heterogeneous systems with diverse possessions.

With clever innovations, counting occasion handling and information spilling strategies from the IoT space, Endeavour administration capture, total, and after that analyze real-time and authentic information of any assortment, volume, and speed. This permits us to plan layered APIs, actualize integration streams, and construct connectors with these low-friction advancement devices. APIs adaptability is the catalyst for this alter, unleashing data and killing the grinding of integration for uncommon speed and nimbleness. It makes it conceivable to make more channels for unused administrations and client encounters and engage the development at increasing speed through adjusted and uncovered usefulness in favour of the interoperability with other frameworks and wide differing qualities of neighborhood assets.

III. Challenges in Cloud Computing while using ML techniques:

There are various techniques of Machine Learning which play a significant role in optimizing and enhancing the aspects of cloud computing. The main significant challenge in cloud computing when using Machine Learning (ML) techniques is managing and optimizing the complex interplay between these domains.

- Information Exchange and Idleness: Machine learning models frequently require getting too expansive datasets for preparation and induction[21]. When these datasets are put away within the cloud and have to be exchanged to the ML environment, information exchange times and organize idleness can end up with critical bottlenecks. This could lead to expanded preparation times and slower demonstration predictions.

- Scalability: Cloud computing offers the advantage of flexible adaptability, permitting you to distribute assets as required. Be that as it may, adjusting ML calculations and models to use this versatility successfully can be challenging. Guaranteeing that the ML calculations and framework can take full advantage of the accessible cloud assets without relinquishing execution or causing superfluous costs requires cautious design.

- Resource Administration and Fetched: Whereas cloud computing gives adaptability, it can too lead to expanded costs

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010

in case assets are not overseen effectively.[21] ML workloads can be resource-intensive, and guaranteeing the ideal assignment of assets (e.g., virtual machines, GPUs) to prepare and deduction assignments is basic to control costs. Also, recognizing and disposing of asset wastage is crucial.

- Data Security and Security: Cloud-based ML involves transmitting and putting away touchy information in third-party situations. Guaranteeing the protection and security of this information could be a critical concern[20]. Procedures like information encryption, secure key administration, and compliance with important directions (e.g., GDPR) are basic to ensure touchy information.
- Model Arrangement and Integration: Sending ML models in a cloud environment and integrating them with existing applications or administrations can be complex. Compatibility issues, form control, and guaranteeing reliable execution between the preparation and induction stages are challenges that have to be addressed.
- Vendor Lock-In: Diverse cloud suppliers offer interesting administrations and APIs for ML. Whereas these differences can be profitable, they can too lead to merchant lock-in, making it troublesome to emigrate ML workloads between distinctive cloud platforms[21].
- Hybrid and Multi-Cloud Situations: Numerous organizations work in crossover situations, where a few components of the ML pipeline are facilitated on-premises while others are within the cloud. Planning and overseeing these half-breed setups proficiently can be challenging, as can guaranteeing steady execution and information astuteness over distinctive environments.
- Monitoring and Investigating: Following the execution and well-being of ML models and foundations in a cloud environment requires strong checking apparatuses and hones. Investigating issues related to disseminated computing, asset dispute, or information irregularities can be more complex in a cloud setting.

IV. RESOURCE SCHEDULING:

The goal is to solve the problems and challenges associated with the integration of cloud computing and machine learning. The following is a tentative appointment process:

- Cloud selection:

Select the appropriate cloud service model (IaaS, PaaS, SaaS) based on the calculation and storage of the machine learning algorithm. Choose a cloud deployment model (public, community, hybrid) based on data security and privacy considerations.

- Preparation and Export of Data:

Import and pre-generate required data from local or external sources to the chosen cloud platform. Optimizes data transfer strategies to reduce latency and network bottlenecks.

- Algorithm Implementation and Optimization:

Use selected machine learning algorithms using compatible frameworks with appropriate programming languages and cloud options. Optimizes algorithms for scalability, parallelism, and distributed computing using the computing power of the cloud.

- Resource Allocation and Scaling:

Dynamically allocate cloud resources (VMs, GPUs, storage) based on machine learning needs. The uses an autoscaling engine to manage different workloads and provide optimum performance.

- Data Security and Compliance:

Use encryption techniques to protect sensitive data when transmitted and stored in the cloud. Ensure compliance with data protection laws (eg., GDPR) and best air security.

- Model Deployment and Integration:

Deploy a trained machine learning model on cloud infrastructure for real-time prediction or analysis. Integrate templates with existing applications or services as needed.

- Performance Monitoring and Evaluation:

Install monitoring tools to monitor resource usage and measure performance and system health. The analysis of performance data to identify discrepancies and improve the allocation of funds for efficiency.

By following the planning process, we can effectively use cloud resources to apply and optimize the machine learning process while solving Problems.

V. CONCLUSION

In this paper, we explore the intersection of cloud computing (CC) and machine learning (ML) and understand the challenges and solutions associated with their integration. Cloud computing has changed the way we deliver and access services over the internet by providing powerful resources and supporting data storage, analysis and management. However, security concerns and the complexity of distributed computing and data transmission pose serious problems.

Machine learning algorithms are emerging as powerful tools to solve these problems by providing better security protection, better resource management and better performance in the cloud environment. We identified and discussed key issues including data exchange latency, scalability optimization, resource management, data security, distribution models, and cloud management.

With careful thinking and strategic planning, the integration of CC and ML can be fruitful. The proposed resource allocation map provides a way to address these issues. Organizations can leverage the full potential of CC and ML to drive innovation

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010

and performance by choosing the appropriate cloud service model, planning and optimizing data, implementing and evaluating processes, ensuring data security and compliance, enforcing standards and effectively monitoring performance.

As cloud computing continues to evolve and machine learning continues to advance, this document highlights the importance of addressing the challenges and taking advantage of the opportunities offered by its integration. The combination of CC and ML is ultimately shaping the future of computing and analytics, promising to improve security, resource efficiency, and performance.

By navigating the complex environment of cloud-based machine learning, organizations can position themselves at the forefront of technological advances and regain competitive advantage in the digital age.

VI. REFERENCE

[1] Lim, S.Y.; Kiah, M.M.; Ang, T.F. Security Issues and Future Challenges of Cloud Service Authentication. Polytech. Hung. 2017, 14, 69–89. [Google Scholar]

[2] Borylo , P.; Tornatore, M.; Jaglarz, P.; Shahriar, N.; Cholda, P.; Boutaba, R. Latency and energy-aware provisioning of network slices in cloud networks. Comput. Commun. 2020, 157, 1–19. [Google Scholar] [CrossRef]

[3] Carmo, M.; Dantas Silva, F.S.; Neto, A.V.; Corujo, D.; Aguiar, R. Network-Cloud Slicing Definitions for Wi-Fi Sharing Systems to Enhance 5G Ultra-Dense Network Capabilities. Wirel. Commun. Mob. Comput. 2019, 2019, 8015274. [Google Scholar] [CrossRef]

[4] Dang, L.M.; Piran, M.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 2019, 8, 768. [Google Scholar] [CrossRef][Green Version]

[5] Srinivasamurthy, S.; Liu, D. Survey on Cloud Computing Security. 2020. Available online: https://www.semanticscholar.org/ (accessed on 19 July 2020).

[6] Mathkunti, N. Cloud Computing: Security Issues. Int. J. Comput. Commun. Eng. 2014, 3, 259–263. [Google Scholar] [CrossRef][Green Version]

[7] Stefan, H.; Liakat, M. Cloud Computing Security Threats And Solutions. J. Cloud Comput. 2015, 4, 1. [Google Scholar] [CrossRef]

[8] Fauzi, C.; Azila, A.; Noraziah, A.; Tutut, H.; Noriyani, Z. On Cloud Computing Security Issues. Intell. Inf. Database Syst. Lect. Notes Comput. Sci. 2012, 7197, 560–569. [Google Scholar]

[9] Palumbo, F.; Aceto, G.; Botta, A.; Ciuonzo, D.; Persico, V.; Pescapé, A. Characterizing Cloud-to-user Latency as perceived by AWS and Azure Users spread over the Globe. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Taipei, Taiwan, 7–11 December 2019; pp. 1–6. [Google Scholar]

[10] Hussein, N.H.; Khalid, A. A survey of Cloud Computing Security challenges and solutions. Int. J. Comput. Sci. Inf. Secur. 2017, 1, 52–56. [Google Scholar]

[11] Le Duc, T.; Leiva, R.G.; Casari, P.; Östberg, P.O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. ACM Comput. Surv. 2019, 52, 1–39. [Google Scholar] [CrossRef][Green Version]

[12] Li, K.; Gibson, C.; Ho, D.; Zhou, Q.; Kim, J.; Buhisi, O.; Gerber, M. Assessment of machine learning algorithms in cloud computing frameworks. In Proceedings of the IEEE Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, 26 April 2013; pp. 98–103. [Google Scholar]

[13] Callara, M.; Wira, P. User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa, Algeria, 24–25 November 2018; pp. 1–6. [Google Scholar]

[14] Singh, S.; Jeong, Y.-S.; Park, J. A Survey on Cloud Computing Security: Issues, Threats, and Solutions. J. Netw. Comput. Appl. 2016, 75, 200–222. [Google Scholar] [CrossRef]

[15] Kyriakos N. Agavanakis, George. E. Karpetas, Michael Taylor, Evangelia Pappa, Christos M. Michail, John Filos, Varvara Trachana, Lamprini Kontopoulou; Practical machine learning based on cloud computing resources. AIP Conference Proceedings 17 July 2019; 2123 (1): 020096. https://doi.org/10.1063/1.5117023

[16] P. G. Papageorgas, K. Agavanakis, I. Dogas, and D. D. Piromalis, "IoT gateways, cloud and the last mile for energy efficiency and sustainability in the era of CPS expansion: 'A bot is irrigating my farm.. ,'" presented at the TECHNOLOGIES AND MATERIALS FOR RENEWABLE ENERGY, ENVIRONMENT AND SUSTAINABILITY: TMREES18, Beirut, Lebanon, 2018, p. 030075, doi: 10.1063/1.5039262.

[17] K. Agavanakis, K. Sakellarakis, and S. Koutroubinas, "Moving Intelligent Energy applications upwards: A customer oriented cloud solution," in The 1st IEEE Global Conference on Consumer Electronics 2012, Tokyo, Japan, 2012, pp. 607–611, doi: 10.1109/GCCE.2012.6379928.

[18] K. Thrampoulidis and K. Agavanakis, Wisdom of the Gurus, Editor: Charles Bowman. ch.7, "Object Interaction Diagram, a new technique in OO Analysis and Design",CAMBRIDGE-SIGS publications, reprinted from: Journal of Object -Oriented Programming, 1996.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 04, ISSN No. 2455-2143, Pages 73-79
Published Online August 2023 in IJEAST (http://www.ijeast.com)
DOI:10.33564/IJEAST.2023.v08i04.010

[19] https://www.datarevenue.com/en-blog/machine-learning-project-architecture

[20] Qiumei Cheng, Chunming Wu, Haifeng Zhou, Dezhang Kong, Dong Zhang, Junchi Xing, Wei Ruan ; "Machine learning based malicious payload identification in software-defined networking"; Journal of Network and Computer Applications; Volume 192, 2021, 103186, ISSN 1084-8045; https://doi.org/10.1016/j.jnca.2021.103186.

[21] P. S and V. S, "Challenges In Cloud Anomaly Detection Using Machine Learning Approaches," 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 2022, pp. 1-6, doi: 10.1109/ICERECT56837.2022.10060686.

[22] S. Goodarzy, M. Nazari, R. Han, E. Keller and E. Rozner, "Resource Management in Cloud Computing Using Machine Learning: A Survey," 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 2020, pp. 811-816, doi: 10.1109/ICMLA51294.2020.00132.

[23] Stefan von Buddenbrock; School of Physics, University of the Witwatersrand, Johannesburg 2050, South Africa "Performance of various event generators in describing multijet final states at the LHC", arXiv:1901.08328v1 [hep-ex] 24 Jan 2019.

[24] Alejandro Olvera Anton, Universitat Polit`ecnica de Catalunya Facultat d'Inform`atica de Barcelona; "Implementation and Evaluation of Profile-based Prediction for Energy Consumption in a Cloud Platform", October 2017, https://upcommons.upc.edu/bitstream/handle/2117/114454/129056.pdf?sequence=1&isAllowed=y.

[25] A. Kaur, B. Kaur, P. Singh, M. S. Devgan and H. K. Toor, "Load Balancing Optimization Based on Deep Learning Approach in Cloud Environment," I.J. Information Technology and Computer Science, vol. 3, no. I, pp. 8-18, 2020.