IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Machine Learning and Deep Learning Based Approach to Secure Cloud Computing Paradigm

Sangeeta Devi[1], Munish Saran[2], Pranjal Maurya[3],Rajan Kumar Yadav[4] , Upendra Nath Tripathi[5], Manish Mishra[6]

[1,2,3,4,5] Department of Computer Science, [6]Department of Electronics
DDUGU, Gorakhpur, Uttar Pradesh, India

ABSTRACT :

In this paper we explains the relationship between machine learning (ML) and cloud computing (CC), emphasizing the problems, opportunities, and solutions. It displays the ways that cloud computing (CC) has changed the Internet service industry as well as the financial effects with data collection and analysis. In particular, security concerns in distributed models are discussed, and edge computing—a cloud computing (CC) variant meant for data that must be processed quickly—is introduced.

The distribution of rights, data encryption, and the transfer of data accountability from providers of services to end users are all covered in this essay. The paper addresses security concerns with integrity, availability, and threat identity by dissecting cloud computing across service and delivery architectures. It proposes machine learning (ML) methods as a remedy for data quality control and security.

The difficulties in integrating Cloud Computing (CC) and machine learning (ML), such as data interchange latency, scalability optimization, model deployment, management of resources, data security and monitoring, are highlighted in this study. A strategy for educating businesses about cloud computing (CC) and machine learning (ML) is offered. The final section of the summary emphasizes how cloud computing (CC) and deep learning as well as machine learning (ML) are evolving to influence computing and analytics in the future and increase an organization's competitiveness in the digital era.

Keywords: Cloud computing, machine learning, deep learning, data encryption etc.

I. INTRODUCTION:

Overview Techniques for deep learning (DL) have shown promise as useful instruments for improving security across a range of industries. More reliable and effective security solutions are made possible by these methods, which take advantage of artificial neural networks' capacity to learn from and recognize patterns in massive volumes of data [1][2]. Deep learning algorithms provide a number of advantages when it comes to cloud computing security, which directly affects how affordable the goods are. Automated threat detection is one of the main advantages of using DL in cloud security. Large amounts of data, including system logs, network traffic logs, and user activity, can be automatically analyzed by DL algorithms to find anomalies and possible security risks [2], [3].

This, along with other DL-related uses, lessens the requirement for human monitoring and analysis, which facilitates quicker detection of security incidents, prompt reaction, mitigation, and lower time and resource expenditures. In light of this, DL reduces the possibility of human error, and this can result in security breaches and related expenses, by automating a variety of security processes.

Deep learning-powered automated systems may carry out duties reliably and precisely, increasing overall security performance [4], [5]. More precise threat detection and categorization are made possible by DL models, which discover relationships and trends in data. By identifying trends and irregularities that conventional rule-based systems could miss, the application of deep learning enables enterprises to maximize resource distribution and cut down on superfluous expenses.

Recently, a new paradigm for facilitating and delivering Internet services has emerged: cloud computing (CC) [1]. For today's cloud models, a budgetary limitation and expanded budget to store, analyze, and communicate data have changed substantially [2, 3]. The need to access end users, particularly for data storage and operations, despite requiring direct user organization is known as cloud computing. Distributed computing gives users on an Internet platform access to both general and specific information[4]. But CC has a lot of security problems, like clients and other problems that cause delays while utilizing rapid computing models[5, 6]. Edge computing is a variation of CC that offers distributed computing capability at the system's edge to application developers and providers of services in order to handle time-sensitive data [7]. A modification to the distribution system's security mechanism is incorporated into the approach to distribution for this strategy .

Furthermore, data that is to be encrypted and transmitted between distribution networks and the cloud itself must be encrypted using a specific encryption procedure. Additionally, the property will be in charge of the end hub, which will restrict the choice of security specifications.

By performing data processing at the edge, data accountability can be transferred beyond the supplier of service to the end user.CC covers delivery modes including public, community, and hybrid clouds in addition to service models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Threats to integrity, accessibility, and privacy are the key security problems in CC.

Cloud services include management software services and limitless resource data storage. Large-scale hardware and infrastructure (used to offer support services) are supported by the cloud model [9]. Not every cloud implementation is appropriate for every service, every provider, or every user [10]. This paper explains CC security problems and concerns along with algorithm of machine learning (ML) solutions.

ML algorithms are utilized to handle data more effectively and to address security issues[11]. This article's goal is to use machine learning techniques to find security risks and legal issues in distributed computing. The primary factor influencing the transformation of distribution items into company services to lower labor and real estate expenses is their growing acceptance.

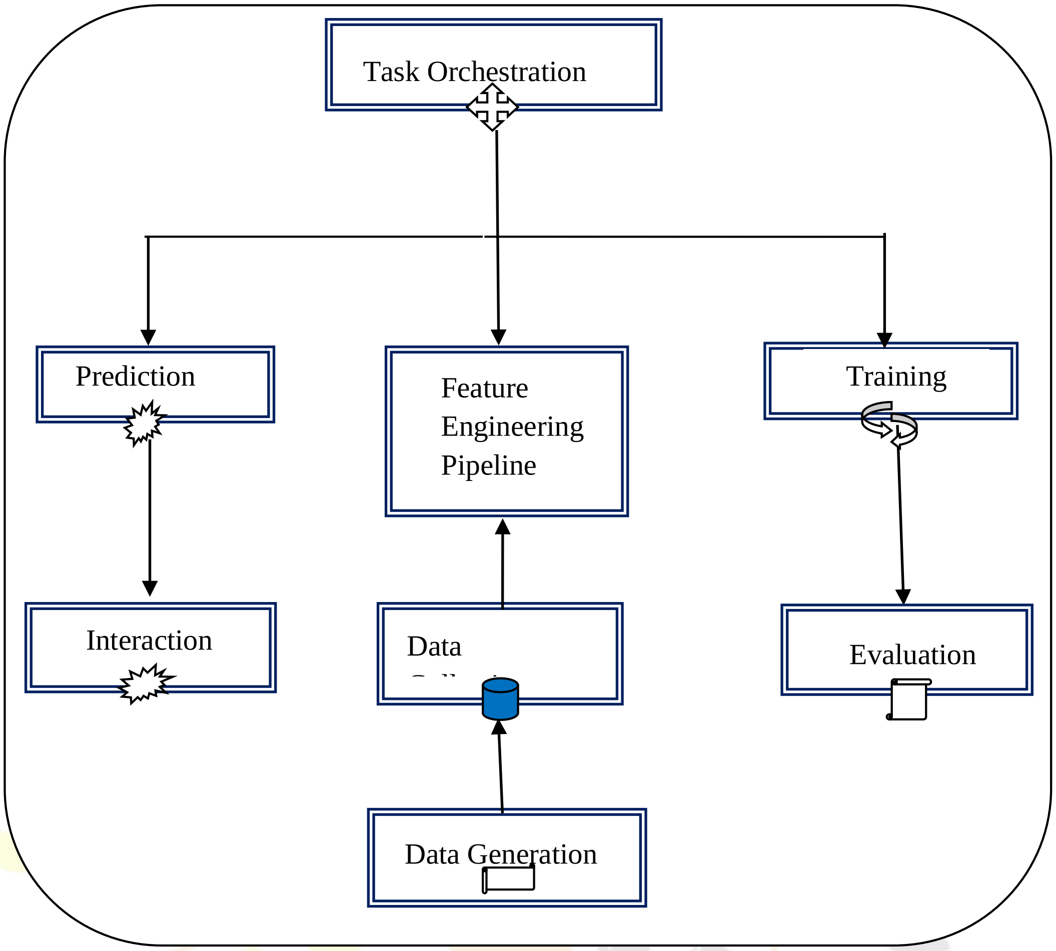


Figure 1: Component of Machine Learning

Because suitable solutions can address the issues they raise, managing security and privacy threats in a distributed context is crucial[14]. Practical initiatives were done to solve security challenges and distributed computing utilizing machine learning methods. These issues were reviewed and discussed. The need for secure, reliable, and efficient delivery services motivates a lot of people. We also know that consumers who select cloud service providers won't be able to afford any discounts on privacy and security issues, which frequently put a significant financial strain on providers of cloud services. It is crucial to assess the security risks encountered and associated with criminal activity using various algorithms with the assistance of cloud service providers [10].

We are primarily looking at the distributed computing security concern. We discuss algorithms that are used to enhance performance and fix issues. The most concerning topic of the present is cloud environment security. Some cloud hacks often make mention of even big cloud service providers like Amazon and Google that have sufficient security mechanisms in place. Cloud computing uses the Machine Learning as a Service (MLaaS) as a service paradigm to create defenses against various cloud assaults. Many malware detection systems that improve intrusion detection accuracy and enable business operations have been developed with the aid of machine learning algorithms.

Applying a deep learning strategy for cloud security Algorithms and models for deep learning are essential for improving cloud computing security. These models are used in many cloud security applications, such as log analysis, access control, anomaly detection, malware detection, and intrusion detection [2], [3], [9]. As previously said, the primary significance of deep learning models is their capacity to identify irregularities, comprehend intricate patterns, and adjust to changing risks. But when it comes to deciding which particular cloud security models to use, it all relies on the nature of the issue, the accessibility of data, computational resources, and sensitivity, as well as the architecture of the current system and other criteria that are unique to the company. In the area of cloud security, some of the often utilized deep learning techniques and algorithms are CNN, RNN, LSTM, GAN, DRL, etc. There are various ways in which organizations might use deep learning algorithms with their cloud security plans. As was already said, integrating deep learning into cloud computing security can benefit enterprises in a number of ways [10]. Adequate strategies and resources are necessary for the successful implementation of deep learning techniques, regardless of the tasks they are applied to, such as data analysis, anomaly detection, malware detection and classification, detection of intrusions and prevention, user authentication, and access control [2], [11], [12].

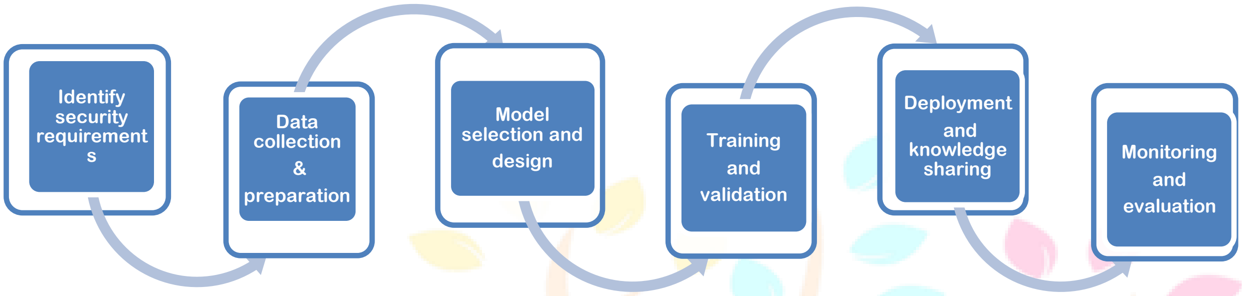

Identify security requirement s
Data collection & preparation
Model selection and design
Training and validation
Deployment and knowledge sharing
Monitoring and evaluation

Figure. 2. Key steps of Integrate deep learning into cloud security.

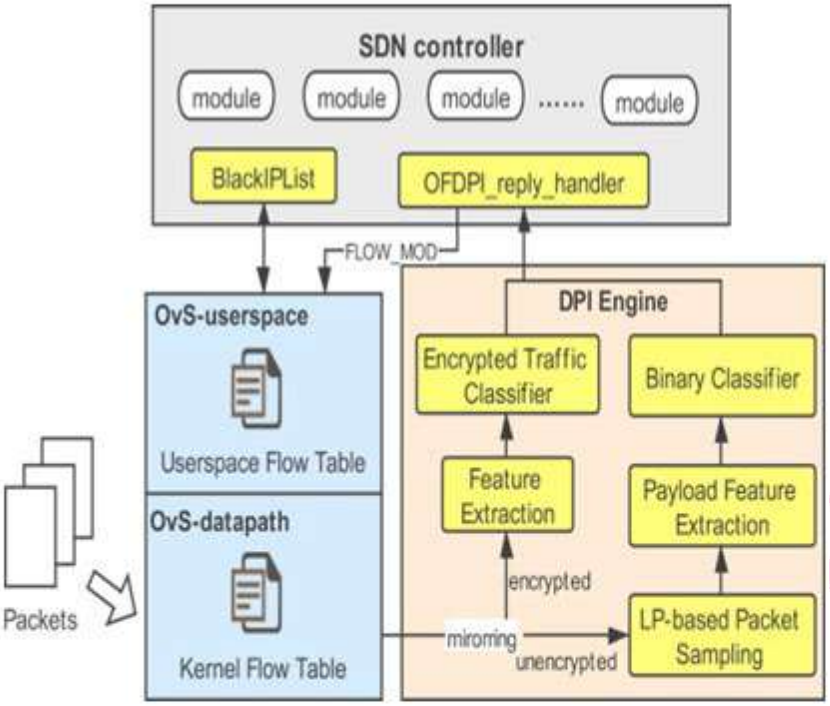
The main steps for integrating deep learning with cloud security are displayed in Figure 1. These are the measures that businesses may take to properly incorporate deep learning with their privacy and security plans for cloud computing. Nonetheless, a more comprehensive assessment would be necessary for the enterprises who wish to incorporate deep learning into their current security structures and solutions. Assessing the system's strengths and flaws is a necessary first step towards implementation. This would make it simpler to identify tasks and places that might allow or need the incorporation of DL.

II Architecture of Machine Learning:

As part of the aforementioned displaying system, we take into consideration a generic handling, preparation, and distribution stage with specific capabilities useful for the machine learning domain. This stage is built upon the fundamental semantic middleware foundation and utilizes its abilities to intervene in the association between its conclusion nodes. It serves as a platform that is provided as a collection of cloud-based web services that leverages various PaaS and SaaS features, such as massive information management, ML preparation models, workflows, etc. It promotes global transparency, tall accessibility, versatility, executions, and tall security standards by using the flexibility of cloud resources [16].

Layers of communication and data are adaptable to different degrees of reflection that align with the breadth of the subject at hand. With the least amount of effort and risk, this tool can help to actualize realistic machine learning scenarios. It also gives us the ability to argue for policies, procedures, operations and strategies, rules, and refinements, but most importantly, it gives us control over how ML-enabled systems are affected throughout their existence. The system display will be built using a based on the cloud micro-service transport design, which also serves as a model for the fundamental arrangement of controlling elements and subtleties According to their intended use and nature, this frequently satisfies the requirements for the fundamental communication designs, modifications, and interfaces of delivered applications, involving various parties within a wide range of complexities and distinguishing characteristics [17].

A protocol-agnostic approach conduct is required for the higher levels of management in such a system of widely dispersed gatherings of people, starting from the fundamental framework and extending to the basic administration of minimal conventions and middleware conversation for information transfer or procurement. In addition to being trustworthy for obtaining, modeling, preparing, and utilizing the results either offline or online, it also provides automation tools to link many frameworks that will extend beyond the confines of the company [18].7].



Ref.Figure 3: 03[20]

Supported use cases are evolving from a single information source (such as an expert who evaluates a photo) requesting an ML evaluation via an online benefit to a third-party application server using an association with a comprehensive benefit with a global impact. Based on the popularity of commercially available PaaS and SaaS services and leveraging the latest technological developments in a stable and supervised setting, agreements with trade handle requirements across a variety of distributed and disparate systems with different assets.

Endeavour administration is able to gather, aggregate, and subsequently evaluate actual time and authentic data of any variety, volume, and speed thanks to ingenious inventions, counting occasion managing, and information leaking methods from the IoT sector. This enables us to create connections with these low-friction advancements devices, arrange layered APIs, and actualize integration streams. The flexibility of APIs is what is causing this change; it frees up data and eliminates the need for tedious integration in order to achieve extraordinary speed and agility. It enables the creation of additional channels for underutilized services and customer interactions and accelerates development through modified and undiscovered utility in support of other framework interoperability and widely disparate local asset attributes.

III. DIFFICULTIES WITH USING ML TECHNIQUES IN CLOUD COMPUTING:

A wide range of machine learning techniques are important for improving and optimizing cloud computing features. When employing Machine Learning (ML) strategies in cloud computing, controlling and optimizing the intricate interactions across different domains presents the biggest challenge.

- Information Exchange and Idleness: Obtaining excessively large datasets with preparation and induction is a common requirement for machine learning models [21]. The storage of these datasets on the cloud and their subsequent interchange to the machine learning environment can result in significant bottlenecks in exchange of data times and organizational idleness. This can result in longer preparation periods and later demonstration forecasts.

- Scalability: One benefit of cloud computing is its flexible flexibility, which allows you to allocate resources as needed. However, it might be difficult to modify ML computations and models to effectively leverage this versatility. Careful design is needed to ensure that both the ML calculation and framework can fully utilize the available cloud resources without sacrificing functionality or incurring unnecessary expenses.

* Resource Management and Fetched: Cloud computing offers flexibility, but if resources are not managed well, it can also result in increased expenses. [21] ML workloads can require a lot of resources, therefore it's critical to ensure that the right resources—such as virtual machines and GPUs—are assigned to set up and deduct assignments in order to keep costs under control. It's also critical to identify and get rid of asset waste.

* Security and Protection of Data: Cloud-based machine learning entails sending and storing sensitive data in scenarios involving third parties. Ensuring the security and safety of this data may be of utmost importance [20]. Basic measures to protect sensitive data include information encryption, secure key management, and adherence to major directives (such as GDPR).

* Model Organization and Integration: It can be challenging to send machine learning models in a cloud-based setting and integrate them with already-in-use programs or systems. Challenges that need to be addressed are form control, compatibility difficulties, and ensuring dependable execution between the preparatory and initiation stages.

* Vendor Lock-In: A variety of cloud providers provide intriguing ML administrations and APIs. Although these distinctions may yield financial benefits, they may also result in merchant lock-in, which complicates the transfer of machine learning workloads between different cloud platforms [21].

* Hybrid and Multi-Cloud Situations: Many businesses operate in crossover scenarios, in which part of the machine learning pipeline is hosted on-site while other parts are hosted on the cloud. It can be difficult to effectively plan and manage these half-breed configurations, as well as to ensure consistent performance and information intelligence across various contexts.

* Monitoring and Research: Robust checking tools and refinements are needed to monitor the performance and health of machine learning models and foundations in a cloud context. In a cloud environment, it may be more difficult to look into problems with distributed computing, asset disputes, or inconsistencies in information.

IV. RESOURCE SCHEDULING: The objective is to resolve the issues and difficulties arising from the combination of machine learning and cloud computing. The approximate appointment procedure is as follows:

* Cloud selection: Choose the right cloud service structure (IaaS, PaaS, or SaaS) based on how the machine learning algorithm calculates and stores data. Based on concerns about data security and privacy, select a cloud deployment approach (public, community, or hybrid).

* Data Preparation and Export: To the selected cloud platform, import and pre-generate the necessary data from domestic or external sources. minimizes latency and network constraints by optimizing data transfer techniques.

* Implementing and optimizing algorithms: Make use of pre-selected machine learning algorithms in conjunction with suitable frameworks, programming languages, and cloud computing choices. uses cloud computing resources to optimize algorithms for distributed computing, parallelism, and scalability.

* Scaling and Allocating Resources: VMs, GPUs, and storage should be dynamically allocated in the cloud according to machine learning requirements. The optimizes performance by managing various workloads with the help of an auto scaling engine.

* Compliance and Data Security: To safeguard sensitive data while it is being transferred and kept in the cloud, use encryption techniques. Make sure that the best air security and data privacy laws—like the GDPR—are followed.

* Model Integration and Deployment: Use cloud infrastructure for deploying a model of machine learning that has been trained for real-time analysis or prediction. When necessary, integrate templates with currently available programs or services.

* Performance Assessment and Tracking: Install monitoring software to keep an eye on resource utilization, performance, and system health. the examination of data on performance to find disparities and enhance the distribution of funding for effectiveness.

We may apply and optimize machine learning while solving problems by using cloud resources in an efficient manner by adhering to the planning process.

V. CONCLUSION:

This research investigates the nexus between cloud computing (CC) and machine learning (ML), comprehending the obstacles and remedies related to their amalgamation. Because cloud computing offers powerful resources and supports data storage, analysis, and administration, it has revolutionized the way that we deliver and utilize services throughout the internet. Although there are significant issues with remote computing, data transmission, and data security.

Algorithms for machine learning are becoming increasingly effective methods for addressing these issues through improved resource management, enhanced security, and enhanced cloud computing efficiency. Data interchange latency, scalability optimization, management of resources, data security, dispersion models, and cloud administration were among the important concerns that we highlighted and talked about.

The successful integration of CC and ML can be achieved with careful consideration and strategic planning. A method to deal with these problems is provided by the suggested resource allocation map. By selecting the best cloud services model, preparing and enhancing data, implementing and assessing procedures, guaranteeing data privacy and compliance, upholding standards, and efficiently monitoring performance, organizations can fully utilize CC and ML to drive creativity and efficiency.

This paper emphasizes the significance of tackling the difficulties and seizing the opportunities presented by its integration as cloud computing and machine learning keep developing. The future of computation and data analysis is ultimately being shaped by the convergence of CC and ML, which promises to enhance performance, security, and resource efficiency.

Through adept navigation of the intricate realm of cloud-based machine learning, enterprises can assert their technological leadership and recuperate a competitive edge in the contemporary era.

VI REFERENCES:

[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.

[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”,October2017, 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.