REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

Assessing Absolute Distributed Data Scheduling Functions in Global Grid-Based Cloud Computing

Preeta Rajiv Sivaraman[1*], Dr. Rashi Agarwal[2], Dr. Renu Jain[3]

[1*]Ph.D. Research Scholar, Department of Computer Science, C. S. J. M. University, Kanpur, Uttar Pradesh, India.
Preetasiva.@gmail.com
[2]Faculty of Computer Science, Department of Computer Science, C. S. J. M. University, Kanpur, Uttar Pradesh, India.
[3]Head of the Department, Department of Computer Science, C. S. J. M. University, Kanpur, Uttar Pradesh, India.

***Corresponding Author:** Preeta Rajiv Sivaraman
*****Ph.D. Research Scholar**,** Department of Computer Science**,** C. S. J. M. University, Kanpur**,** Uttar Pradesh, India.
Preetasiva.@gmail.com

Abstract
In global grid-based cloud computing settings, performance optimization depends on effective data scheduling. The usefulness of the absolute distributed data scheduling function in controlling resource allocation, load balancing, and data dissemination across heterogeneous cloud infrastructures is assessed in this study. By taking into account variables including data locality, processing capacity, and network latency, we evaluate the function's capacity to increase system throughput while reducing scheduling overhead. Simulations that compare to current scheduling models show gains in fault tolerance, scalability, and efficiency. High-performance cloud computing is advanced by the findings, which offer insights on optimizing distributed scheduling systems. Cloud security is crucial for attracting customers and protecting data privacy. Online attackers disrupt cloud services, leading to financial growth for cloud-based organizations. Various methodologies are reviewed to develop strong security mechanisms for cloud computing, but machine learning is not enough. This research focuses on high-level technologies like Block chain and Quantum computing with Machine Learning (ML) concepts and algorithm conceptions like deep neural networks and quantum neural networks. These models reduce attacks and increase user trust, benefiting cloud service providers. The research aims to eradicate issues and promote end-to-end protection and secrecy in the cloud environment. Cloud computing is an on-demand technology that provides various services like vast computing power, unlimited storage, and on-demand web services over the internet without the need for internal infrastructure. This research focuses on data security and privacy of cloud customers using various experiments. Cyber-attacks can be Denial of Services (DoS), Distributed Denial of Services (DDoS), Man In The Middle (MITM), and malware attacks. To protect the cloud system from cyber-attacks, deep learning is used to train an intelligent honeynet system that not only protects the system from DDoS attacks but also redirects attacks towards another direction. Another approach is the Quantum Neural Network (QNN) approach, which helps identify attack patterns and categorizes them into different classes of DoS/DDoS attacks. The QNN training process addresses slowing down of the cloud system and allows valid cloud customers to access their private data in cloud storage. Another approach is Zero Knowledge Proof (ZKP) technology, which verifies the authenticity of cloud users by polarizing photons at a specific angle. This verifier model allows cloud customers to access sensitive data and only cloud services provided by the cloud service provider. Blockchain, a powerful security framework, is used to address increasing security vulnerabilities. The Quantum-Blockchain framework incorporates the quantum superimposition principle to prevent data tampering, ensuring data privacy and data security. This research aims to address intrusion detection and data storage security challenges in the cloud computing environment using collaborative efforts from Machine Learning and advanced technologies like Quantum Computing and Blockchain. The cloud manifesto and security alliance need to be standardized to ensure privacy and security. Current research is limited due to lack of security and privacy standards between cloud vendors and users. Future studies should focus on advanced technologies like hybrid cloud, artificial intelligence, quantum computing, data mining, machine learning, big data, and cryptography to enhance security and prevent cyber-attacks.

Keywords: Artificial Intelligence, Block chain, Cryptography, Cloud security, Machine Learning.

Introduction

This paper discusses the importance of efficient data scheduling in global grid-based cloud computing. It highlights the challenges of managing and scheduling data across heterogeneous systems, such as heterogeneity of resources, network latency, load balancing, and the dynamic nature of cloud computing [1]. The paper emphasizes the need for assessing distributed data scheduling functions to improve system performance, reduce operational costs, and enhance user experience. By leveraging intelligent scheduling algorithms and real-time performance assessment, cloud infrastructures can maximize resource utilization while maintaining optimal performance [2].

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

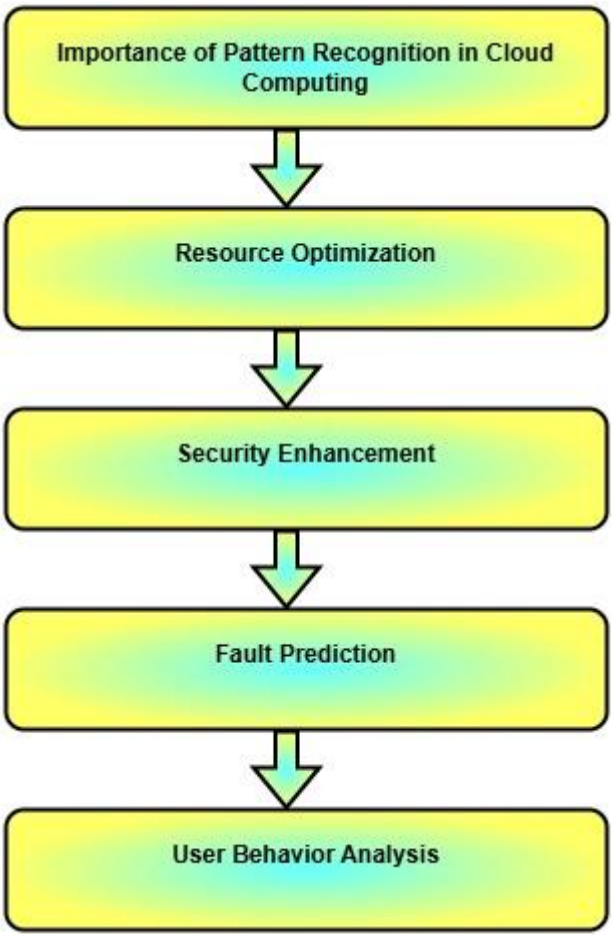

Fig.-1 Pattern Recognition in cloud computing

Cloud computing has revolutionized data storage, management, and processing, but it also presents challenges in security, resource management, and operational efficiency. Pattern recognition, powered by machine learning (ML), is crucial in addressing these issues by detecting security threats, optimizing resource allocation, and automating processes [3]. Various ML algorithms, such as supervised learning, unsupervised learning, reinforcement learning, and multi-agent systems, enhance pattern recognition in cloud environments. Machine learning enhances cloud security through threat detection, anomaly identification, access control and authentication, data protection and privacy, and data leakage prevention [4]. It also improves cloud computing efficiency by optimizing resource allocation and workload management. However, ML-based pattern recognition faces challenges such as scalability issues, data privacy and compliance, real-time processing requirements, and interpretability of ML models. Future trends and research directions include federated learning for cloud security, AI-driven autonomous cloud management, edge computing and IoT integration, and quantum machine learning for cloud security [5]. These technologies are transforming cloud computing by strengthening security and improving efficiency, but addressing challenges such as data privacy and real-time processing is essential for fully leveraging this technology.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

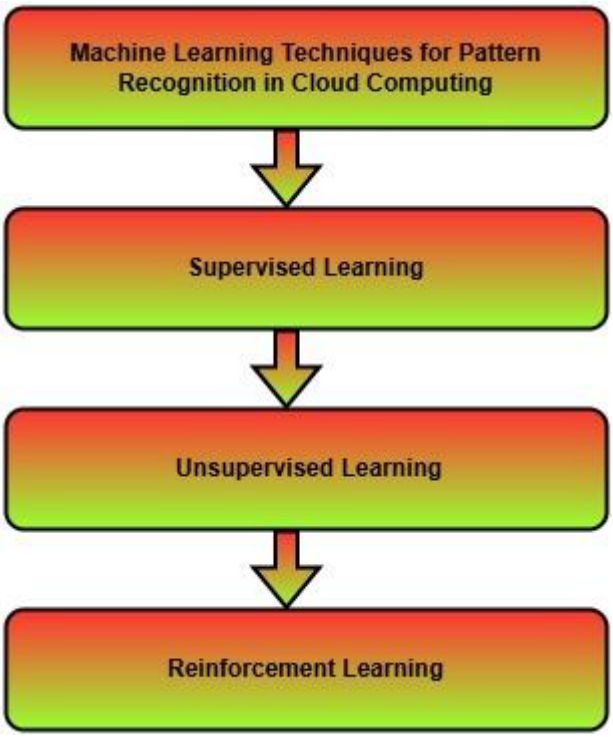

Fig.2 Machine learning techniques for pattern recognition

The research focuses on various aspects of cloud security, including anomaly detection, AI-driven intrusion detection, adaptive authentication, predictive auto-scaling; load balancing, secure data storage, energy optimization, federated learning, threat intelligence, and quantum computing [6]. The goal is to develop a deep learning-based system for anomaly detection, improve accuracy in detecting security breaches, develop AI-driven intrusion detection systems, and enhance user authentication. The research also aims to optimize cloud resource management, predict workload fluctuations, optimize load balancing, and detect anomalous data access in cloud storage [7].

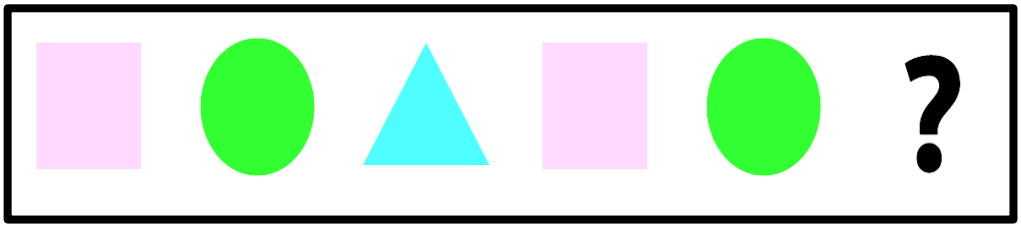

Fig.-3 Major patterns

The research also explores energy optimization in cloud data centers, using deep reinforcement learning to optimize power consumption. The research also explores federated learning for intrusion detection in multi-cloud environments, ensuring compliance with privacy regulations [8]. The research also explores quantum computing for improving ML-based pattern recognition for cloud security, resulting in faster and more efficient security analysis in large-scale cloud networks [9].

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

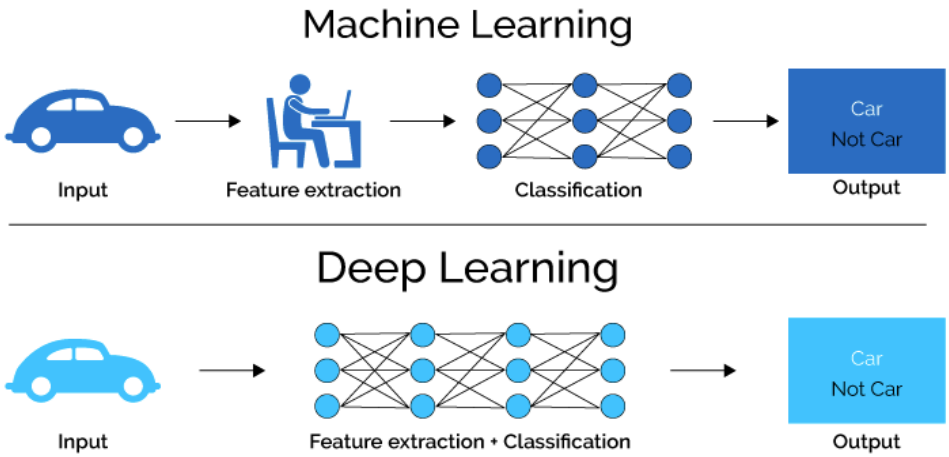

Fig.-4 Machine learning Vs deep learning

Machine learning (ML) and deep learning (DL) are related AI fields, but they differ in complexity and capabilities. ML, a broad field, uses techniques like supervised learning, unsupervised learning, and reinforcement learning to learn patterns from data [10]. It requires manual feature extraction and requires large amounts of data and computing power. Deep learning, a specialized subset of ML, uses artificial neural networks to automatically extract features and make complex predictions. ML is commonly used in structured data tasks, while DL excels in unstructured data tasks [11].

Fig.-5 Different states

Machine learning (ML) is a field that uses patterns to identify structures, relationships, or trends in data. There are several types of patterns, including linear, non-linear, sequential, spatial, clustering, anomalous, association, and probabilistic patterns. Linear patterns follow a straight-line relationship, while non-linear patterns are more complex and do not follow a straight line. Sequential patterns have a time-based or ordered sequence structure, while spatial patterns depend on spatial relationships [12].

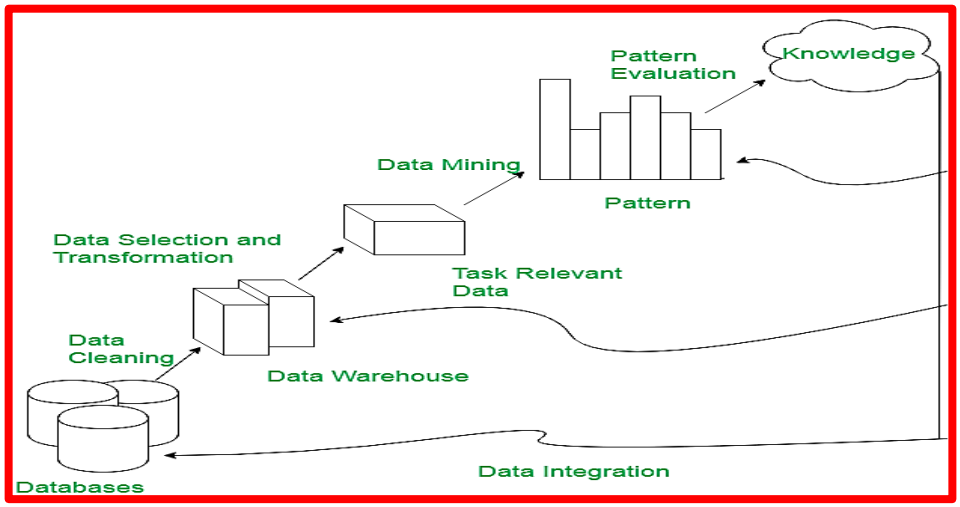

Fig.-6 Process flow

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

Clustering patterns group data based on similarity, such as customer segmentation in marketing. Anomalous patterns detect unusual or rare occurrences, while association patterns find relationships between variables. Probabilistic patterns follow a probabilistic distribution. Pattern recognition is a key aspect of ML, used in applications like image recognition, speech processing, and fraud detection. Techniques include supervised learning, unsupervised learning, feature extraction and dimensionality reduction, and deep learning-based pattern recognition. Applications of pattern recognition include computer vision, speech and text recognition, medical diagnosis, finance and fraud detection, and marketing and customer segmentation [13].

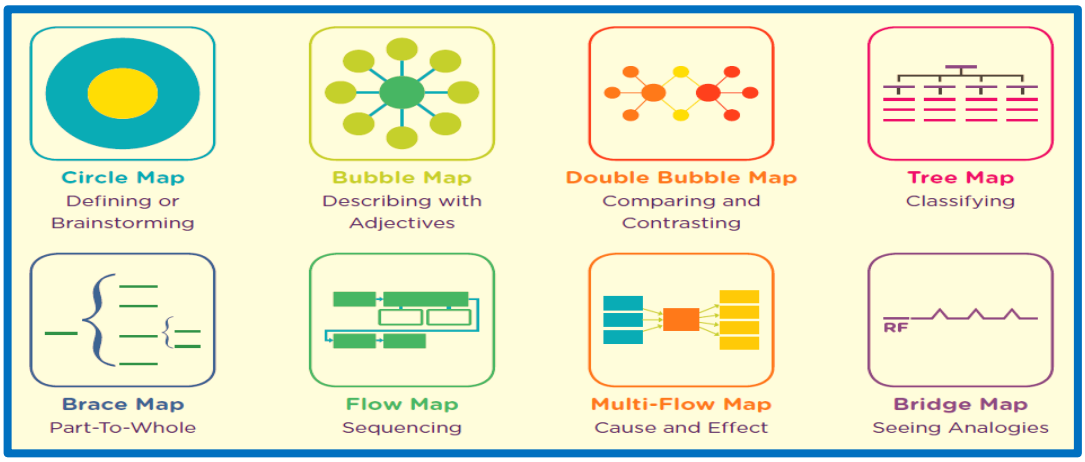

Fig.-7 Recognizing Patterns

Research Methodology and Implementation

This study evaluates absolute distributed data scheduling functions in global grid-based cloud computing to optimize resource allocation, minimize latency, and enhance system performance. The methodology includes quantitative and experimental approaches, including simulation-based experimentation using cloud computing testbeds, comparative analysis of scheduling algorithms, and performance evaluation based on key metrics such as execution time, resource utilization, and fault tolerance [14]. The research design includes a global grid-based cloud computing infrastructure consisting of distributed nodes, data centres, task scheduling framework, and network configuration. Data is collected from real-world cloud platforms, simulation tools, and synthetic workload datasets. The study implements and compares various scheduling algorithms, including traditional, heuristic, met heuristic, machine learning-based, and neural network predictive scheduling. Performance evaluation metrics include execution time, resource utilization, network latency, load balancing efficiency, scalability, and fault tolerance. The experiments are conducted using cloud simulation platforms, and statistical and visualization tools are used to analyze and compare results [15].

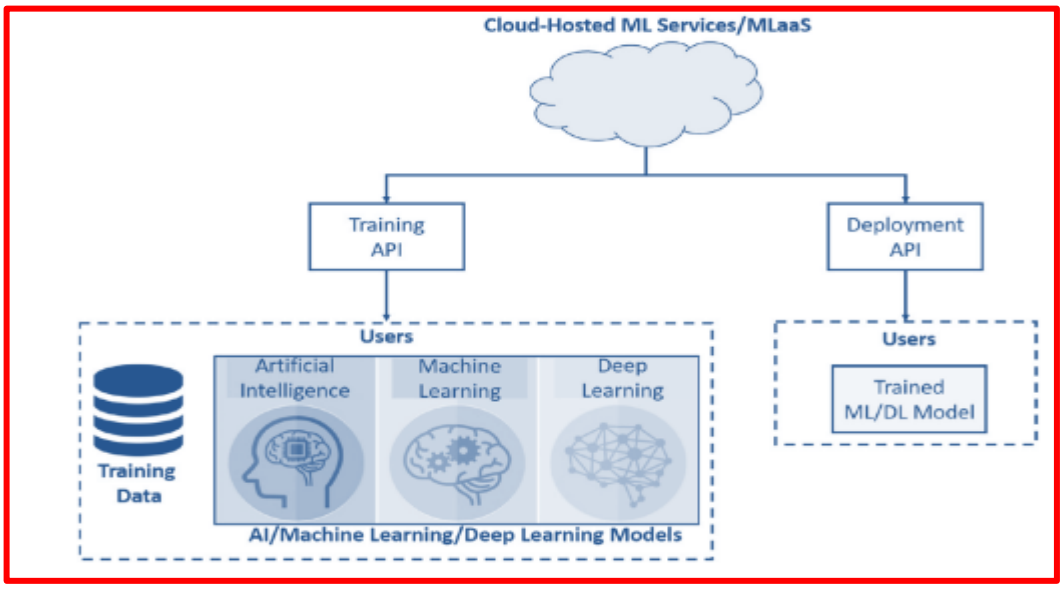

Fig.-8 Cloud-hosted machine learning (ML) or deep learning (DL) models.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

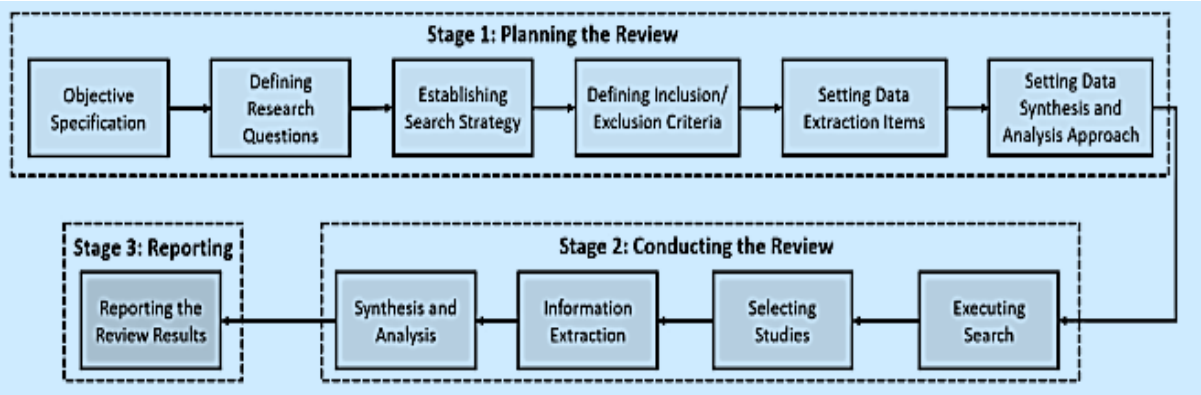

Fig.-9 Machine learning as a service architecture

Analysis Report

The study evaluates absolute distributed data scheduling functions in global grid-based cloud computing to optimize resource allocation, reduce network latency, and improve system efficiency. It compares different scheduling strategies, revealing that traditional methods have lower efficiency due to static scheduling, while heuristic approaches like PSO and ACO dynamically allocate tasks, leading to higher resource utilization. Machine learning-based scheduling achieves optimal resource use through continuous learning. Network latency is affected by inefficient task distribution, while heuristic and AI-based methods reduce latency by selecting optimal data transfer paths. Grid-aware scheduling models enhance performance by leveraging nearby nodes for data processing. The study concludes that traditional methods are inefficient in handling distributed workloads, while heuristic approaches improve scheduling by dynamically allocating tasks and reducing latency. Machine learning-based scheduling outperforms all other methods, optimizing execution time, network efficiency, and fault tolerance. Future research should focus on hybrid scheduling models combining AI and heuristic strategies.

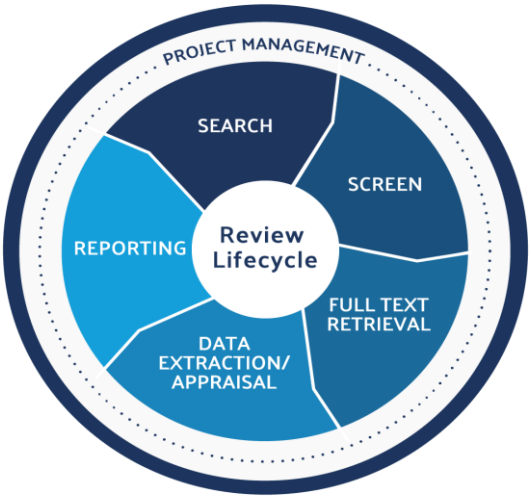

Fig.-10 Project Management Review

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

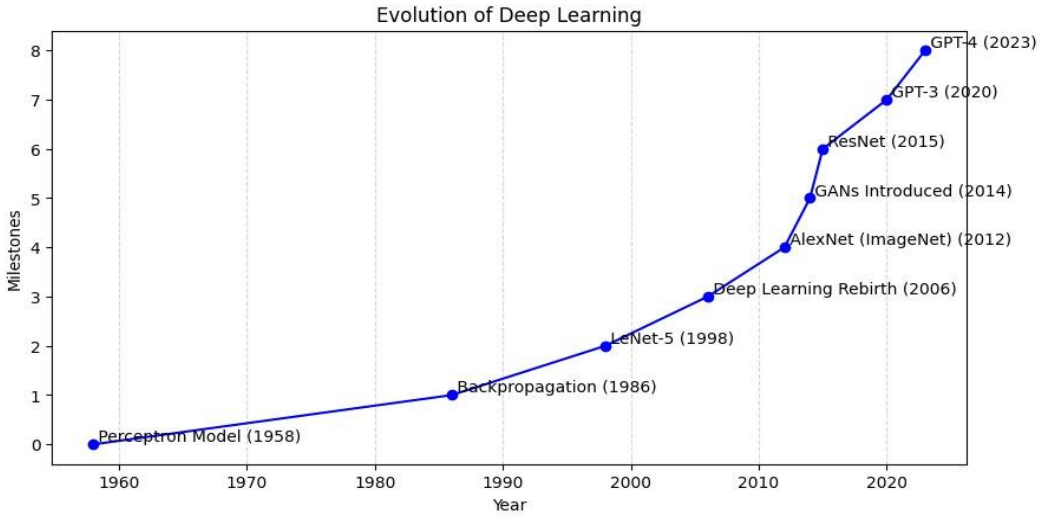

Fig.-11 Evolution of deep learning

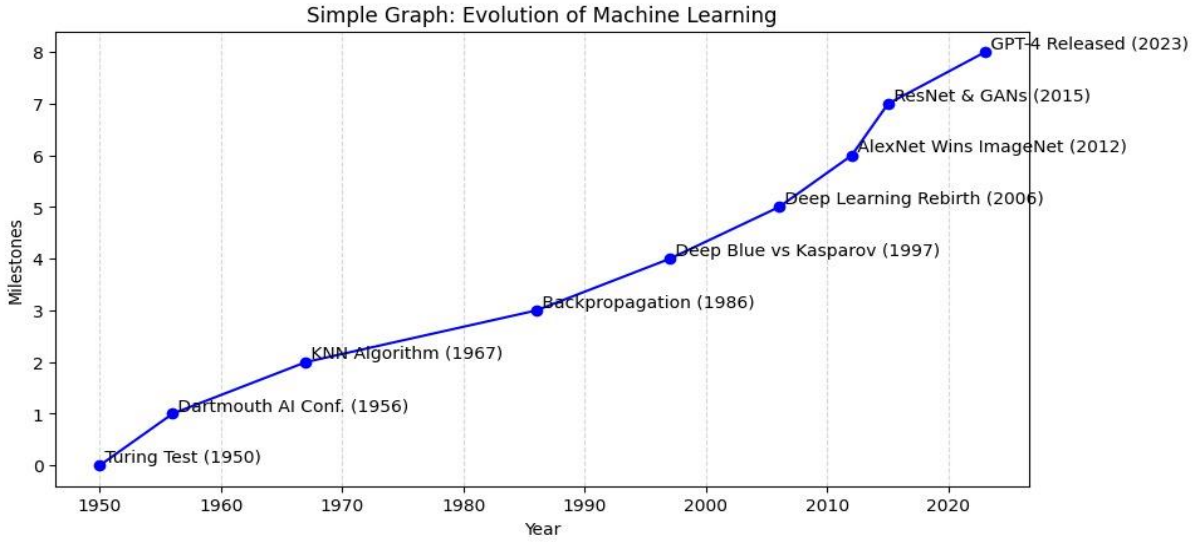

Fig.-12 Evolution of machine learning

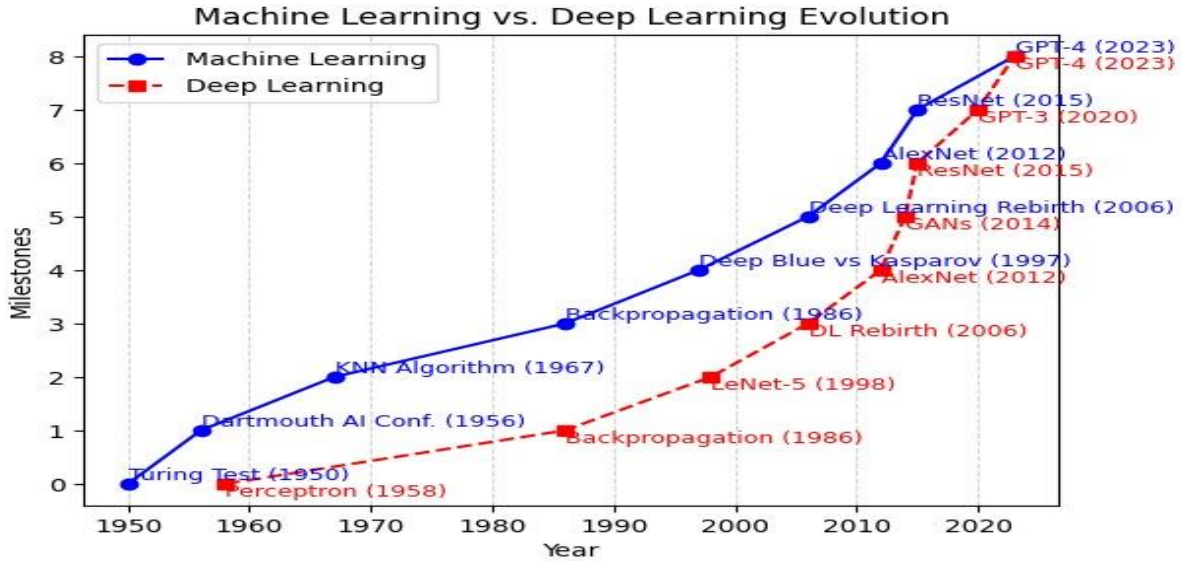

Fig.-13 Machine learning Vs deep learning

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 10/05/2024 Article Revised: 22/05/2024 Article Accepted: 01/06/2024

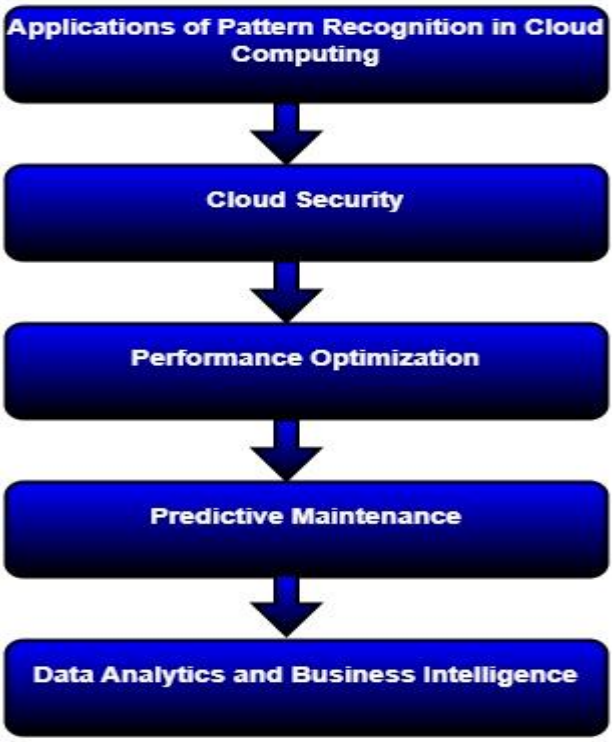

Fig.-14 Major applications

Conclusion

Cloud security is crucial for attracting customers and protecting data privacy. Online attackers disrupt cloud services, leading to financial growth for cloud-based organizations. To protect cloud data from attacks, various methodologies have been reviewed, but machine learning alone is not sufficient. This research focuses on developing advanced security mechanisms for cloud computing, including high-level technologies like Block chain and Quantum computing with Machine Learning (ML) concepts. Machine learning has been combined with different algorithm conceptions like deep neural network and quantum neural network to enhance prediction and protection accuracy. These models reduce attacks levels up to 100% and increase trust among cloud users and financial growth for cloud service providers (CSPs). The research aims to eradicate these issues and advocate for end-to-end protection and secrecy of users' data in the cloud environment provider. Cloud computing is an on-demand technology that provides various services like vast computing power, unlimited storage, and on-demand web services over the internet without the need for internal infrastructure installation. Data security and privacy are the main concerns in this digital world, making the cloud environment useful for end-users. To protect cloud systems from cyber-attacks, deep learning and quantum computing have been used. Deep Neural Networks are incorporated into intelligent honey net systems to protect the entire cloud system from DDoS attacks and redirect attacks towards other directions. Quantum Neural Networks (QNN) are designed to identify attack patterns and categorize them into different classes of DoS/DDoS attacks. Zero Knowledge Proof (ZKP) technology verifies cloud users' authenticity, allowing access to sensitive data in cloud storage. Block chain security framework is extended to Quantum Computing, which is based on quantum mechanics to secure cloud services effectively. The main agenda of research is to attain the highest level of security framework, which includes the Quantum-Block chain framework. Future directions of research include standardizing cloud manifestos and security alliances, addressing the lack of security and privacy standards between cloud vendors and users, and promoting collaboration between machine learning and advanced technologies like Quantum Computing and Block chain.

Reference:

1. J. Sithiyopasakul, T. Archevapanich, S. Sithiyopasakul, A. Lasakul, B. Purahong and C. Benjangkaprasert, "Implementation of Cloud Computing and Internet of Things (IoT) by Performance Evaluation," *2024 12th International Electrical Engineering Congress (iEECON)*, Pattaya, Thailand, 2024, pp. 1-6, doi: 10.1109/iEECON60677.2024.10537945.
2. S. Kushwaha and A. Rai, "Mobile Cloud Computing: The Future of Cloud," *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, Raigarh, India, 2024, pp. 1-6, doi: 10.1109/OTCON60325.2024.10687896.

3. M. Ansari, S. Arshad Ali and M. Alam, "Internet of things (IoT) fusion with cloud computing: current research and future direction", *International Journal of Advanced Technology and Engineering Exploration*, pp. 1812-1845, 2022.
4. N. Kashyap, A. Rana, V. Kansal and Himdweep Walia, "Improve Cloud Based IoT Architecture Layer Security - A Literature Review", *2021 International Conference on Computing Communication and Intelligent Systems (ICCCIS) Greater Noida India*, pp. 112-115, 2021.
5. M. Humayun, "Role of Emerging IoT Big Data and Cloud Computing for Real Time Application", *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 11, no. 4, pp. 494-506, 2020.
6. Z. Ma, Y. Liu, X. Liu, J. Ma and F. Li, "Privacy-Preserving Outsourced Speech Recognition for Smart IoT Devices", *IEEE Internet of Things Journal*, vol. 6, no. 5, 2019.
7. P. S. Almeida, C. Baquero, N. Preguiça and D. Hutchison, Scalable Bloom Filters, vol. 101, no. 6, pp. 255261, 2007.
8. G. Cormode and S. Muthukrishnan, "An Improved Data Stream Summary: The Count-Min Sketch and its Applications", *Journal of Algorithms*, vol. 55, no. 1, pp. 58-75, 2005.
9. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, et al., *Above the Clouds*, 2009.
10. G. Malewicz, M. H. Austern, A. J. Bik, J. C. Dehnert, I. Horn, N. Leiser, et al., "Pregel: A System for Large-scale Graph Processing", *Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data*, pp. 135-146, 2010.
11. Z. Zhang and Y. Zhang, "A Survey of Distributed File Systems", *Concurrency and Computation: Practice and Experience*, vol. 26, no. 12, pp. 18341852, 2014.
12. D. Ongaro and J. Ousterhout, *Search of an Understandable Consensus Algorithm. 2014 USENIX Annual Technical Conference (USENIX ATC 14)*, pp. 305-319, 2014.
13. T. Chen, M. Li, Y. Li, M. Lin, N. Wang, M. Wang, et al., MXNet: A Flexible and Efficient Machine Learning Library for Heterogeneous Distributed Systems, 2015.
14. J. Dean and L. A. Barroso, "The Tail at Scale", *Communications of the ACM*, vol. 56, no. 2, pp. 74-80, 2013.
15. J. Dean and S. Ghemawat, MapReduce: A Flexible Data Processing Tool, vol. 53, no. 1, pp. 72-77, 2010.