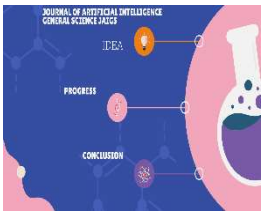
Vol.3,Issue 01, March 2024
Journal of Artificial Intelligence General Science JAIGS

Home page http://jaigs.org



Ensuring Compliance Integrity in AI ML Cloud Environments: The Role of Data Guardianship

Samadrita Ghosh

UK Export Finance, Data Insight Analyst in London

*Corresponding Author: Samadrita Ghosh

ARTICLEINFO
Article History:
Received:
05.03.2024
Accepted:
10.03.2024
Online: 10.04.2024
Keyword: data integrity; AI systems; cloud computing; blockchain

ABSTRACT

Artificial intelligence (AI) has become ubiquitous across various industries, including security, healthcare, finance, and national defense. However, alongside its transformative potential, there has been a concerning rise in malicious exploitation of AI capabilities. Simultaneously, the rapid advancement of cloud computing technology has led to the emergence of cloud-based AI systems. Unfortunately, vulnerabilities inherent in cloud infrastructure also pose security risks to AI services. We recognize the critical role of maintaining the integrity of training data, as any compromise therein directly impacts the effectiveness of AI systems. In response to this challenge, we emphasize the paramount importance of preserving data integrity within AI systems. To address this need, we propose a data integrity architecture guided by the National Institute of Standards and Technology (NIST) cybersecurity framework. Leveraging blockchain technology and smart contracts presents a suitable solution for addressing integrity challenges, given their features of shared and decentralized ledgers. Smart contracts enable automated policy enforcement, facilitate continuous monitoring of data integrity, and help mitigate the risk of data tampering.

Introduction

Artificial Intelligence (AI) stands out as one of the most disruptive technological advancements in recent history. Originating in 1956, AI has witnessed exponential growth, evidenced by significant milestones such as AlphaGo's triumph over the world Go champion in 2016 and Google's launch of Waymo's self-driving taxi service in 2018. Its applications span across diverse sectors, including national security, finance, healthcare, criminal justice, transportation, and smart cities. However, alongside its transformative potential, AI has also been exploited for malicious purposes, as seen in attacks such as adversarial examples in self-driving cars and coordinated assaults on AI-controlled robotic systems.

The dynamic progression of AI development intersects with the rapid evolution of cloud computing technology, offering new opportunities for AI researchers and developers. Cloud-based AI systems leverage the infrastructure provided by Cloud Service Providers (CSPs), enabling efficient resource utilization and accessibility from any location with internet connectivity. While cloud computing offers numerous advantages, it also presents challenges, particularly regarding data integrity and privacy. Users must entrust their data to potentially untrusted environments, raising concerns about breaches in data integrity and security.

The significance of data integrity within AI systems cannot be overstated. Compromised training data can lead to erroneous outcomes, posing significant risks, especially in critical domains. Consequently, safeguarding data integrity emerges as a critical imperative. Addressing these challenges necessitates a proactive approach, integrating security considerations into the design and implementation of AI systems.

In this context, we propose an architecture aimed at tackling data integrity issues within cloud-based AI systems. Drawing inspiration from the National Institute of Standards and Technology (NIST) cybersecurity framework, our architecture provides a structured approach to ensure continuous data integrity provisioning. By leveraging blockchain technology and smart contracts, we enhance the integrity of the machine learning pipeline, bolstering trust and security in cloud-based AI environments.

Our contributions include the proposal of a system architecture aligned with NIST cybersecurity principles, comprising modules that address key aspects of security and integrity. Additionally, we integrate blockchain and smart contracts into our architecture to automate policy enforcement and enhance trust between users and CSPs.

The remainder of this paper is structured as follows: Section 2 explores existing vulnerabilities and threats in AI and cloud environments, while Section 3 reviews related research. In Section 4, we detail our proposed architecture, followed by an evaluation and discussion in Section 5. Finally, we conclude our findings in Section 6.

AI Landscape

In the AI ecosystem, three primary avenues exist for potential adversarial interference [4]:

1. Attacks targeting the data utilized for training and decision-making.
2. Attacks aimed at the classifier within the training environment.
3. Attacks against models within the deployment environment.

These adversarial scenarios are inherent to the machine learning pipeline and require a comprehensive examination of vulnerabilities and challenges present in both AI and cloud environments.

To elucidate these challenges, this section delves into the typical AI data pipeline and highlights integrity issues across its phases, as depicted in Figure 1. Additionally, Table 1 provides an overview of potential attack methods associated with each phase.

AI Environment and Vulnerabilities

A1. Data Acquisition and Curation

Prior to effectively learning a task-specific model, an AI system necessitates access to extensive datasets. In the data acquisition phase, users compile training datasets aligning with their objectives. For instance, in tasks like image classification, datasets comprise image collections. Data may be sourced from various outlets, including proprietary datasets or established repositories such as CIFAR10 or MNIST. During data curation, users engage in activities like formatting, noise removal, and labeling. This phase is crucial as it directly influences model accuracy.

Vulnerabilities and Attacks—Data Poisoning: This threat arises when attackers introduce erroneous or mislabeled data to train AI models. For instance, stop sign images may be mislabeled to evade detection by algorithms, posing risks on roads. Meticulous control over training datasets is vital to safeguard AI decision-making processes. Additionally, data poisoning has been observed in recommender systems, where adversaries inject manipulated data to influence suggestions.

A2. Model Design

In this phase, users select AI algorithms and set hyperparameters such as the number of nodes, layers, and learning rates.

A3. Implementation

The implementation phase involves training and testing. Training establishes the system's baseline behavior by iteratively running algorithms with input datasets to minimize error. Testing validates the model's performance using datasets not utilized in training.

Vulnerabilities and Attacks—Backdoor Attack: These attacks, primarily targeting the training phase, rely on data poisoning to introduce examples with triggers into the dataset. This manipulation associates the trigger with a target class, causing misclassification during inference.

A4. Inferences

Once prepared, the model is applied to systems or applications. Inputs, such as digital images, are classified based on the trained model, providing results.

Vulnerabilities and Attacks—Adversarial Examples: Among prevalent threats are adversarial examples, where attackers manipulate inputs to induce errors. Imperceptible perturbations in digital images can lead algorithms to misclassify them. Various types of adversarial examples exist, including FGSM, DeepFool, JSMA, BIM, and Universal Perturbations.

A5. Check and Updates

Administrators routinely assess system accuracy and performance. If necessary, systems undergo retraining for model updates.

How to Defend AI Systems

The challenges underscore AI systems' susceptibility to data alteration. Inaccurately labeled data can lead to diminished accuracy and erroneous behavior. Various strategies have been devised to protect AI systems, categorized into AI-algorithm-based and architecture-based defenses. The former fortifies AI systems against ML attacks, while the latter designs architectures to prevent system infiltration, reducing the risk of data manipulation.

AI-Algorithm-Based Defenses

Researchers continuously seek defense mechanisms against AI system attacks, though adversaries persistently seek methods to circumvent them. Below, we present several examples of AI-algorithm-based defense mechanisms along with the attacks they effectively counter. These mechanisms are classified into two categories: complete defense and detection-only.

1. Adversarial Training: This widely adopted defense mechanism targets adversarial examples encountered during the inference phase. By retraining the model with adversarial examples while retaining correct labels, the model learns to disregard adversarial inputs, thereby enhancing accuracy. However, a drawback is that the model becomes 'immune' only to attacks it has been trained against previously.

2. Data Compression: JPEG compression has been shown to effectively counter adversarial attacks like FGSM and DeepFool by removing high-frequency components in images. However, excessive compression may lead to loss of accuracy.

3. Randomization: Adding random resizing and padding operations during inference can mitigate adversarial effects by introducing variability into input images.

4. Gradient Regularizations and Adversarial Training: Combining gradient regularization with adversarial training can enhance robustness against attacks like FGSM and JSMA. However, this approach significantly increases the training complexity.

5. SafetyNet: This method utilizes a Radial Basis Function SVM classifier to detect adversarial examples based on differences in ReLU activation patterns, effectively identifying examples generated by various attacks.

6. Convolution Filter Statistics: By analyzing statistics on convolutional layer outputs, a cascade classifier can detect adversarial examples with high accuracy.

7. Perturbation Rectifying Network (PRN): PRN aims to defend against universal perturbations by adding additional 'pre-input' layers to the model. A separate detector trained on Discrete Cosine Transform features identifies perturbations, enabling accurate classification.

8. GAN-Based Defenses: Generative Adversarial Networks (GANs) have been utilized to improve robustness against adversarial perturbations. For instance, generator networks generate adversarial perturbations while the classifier learns to correctly classify both original and adversarial examples.

9. Denoising/Feature Squeezing: Feature input spaces are often excessively large, offering adversaries numerous options. Feature squeezing reduces input features, making it harder for adversaries to generate adversarial examples. Spatial smoothing and color bit depth reduction are effective squeezing methods.

These AI-algorithm-based defense mechanisms offer various strategies to mitigate the impact of adversarial attacks on AI systems, contributing to enhanced robustness and security.

Table 2. Examples of AI-Algorithm-based defense mechanisms.

Defense Mechanisms	Effective to	Category
Adversarial training	Adversarial examples	Complete-defense
Data compression	FGSM, DeepFool	Complete-defense
Randomization	Adversarial examples	Complete-defense
Gradient regularizations + adversarial training	FGSM, JSMA	Complete-defense
SafetyNet	FGSM, BIM, DeepFool	Detection-only
Convolution filter statistics	Adversarial examples	Detection-only
Perturbation Rectifying Network (PRN)	Universal perturbations	Complete-defense
GAN-based	Adversarial perturbations	Complete-defense
Denoising/Feature squeezing	Adversarial perturbation to an image	Detection-only

Each of these defense mechanisms possesses its own strengths, weaknesses, and trade-offs. However, it is imperative to highlight that researchers and developers continue to explore and refine these algorithm-based defense mechanisms to achieve superior results.

Architecture-Based Defense

Architecture-based defense operates by constructing an architecture aimed at preventing adversaries from infiltrating the system, thereby reducing the likelihood of malicious modification of ML datasets. Certain features can be integrated into the architecture to bolster its resilience against data integrity violations, including:

- Strengthening the authentication mechanism to prevent fake users from impersonating legitimate ones.

- Enhancing the authorization mechanism by restricting user permissions based on their designated roles, thereby preventing unauthorized users from engaging in arbitrary behavior and ensuring that only authorized users can interact with the services.

- Monitoring datasets' integrity throughout the ML lifecycle phases using hash algorithms. This enables comparison of dataset hashes to detect any alterations by attackers.

- Implementing logging and monitoring of data flow and user activities to promptly identify suspicious actions.

As depicted in Table 3, we summarize the merits and weaknesses of these two defense mechanisms by assigning a plus (+) sign to indicate the phases covered by each mechanism and a minus (-) sign to indicate the phases not covered. Given that AI-algorithm-based defense operates at the algorithm level, it covers the ML lifecycle phases from implementation (A3) to check and updates (A5). However, it may fall short in ensuring data integrity during the collection and curation of training datasets (A1) and algorithm configuration (A2). Conversely, architecture-based defense, with the implementation of the aforementioned examples, can span phases A1 to A5.

Nevertheless, in our view, optimal defense for cloud-based AI systems entails incorporating both mechanisms, as they each possess strengths and weaknesses that can complement one another. We will delve further into our proposed architecture-based method in Section 4.

Table 3. AI-Algorithm-based vs. Architecture-based in ML pipeline.

Phase	AI-Algorithm-Based	Architecture-Based
Data acquisition and curation	–	+
Model design	–	+
Implementation	+	+
Inferences	+	+
Check and updates	+	+

Cloud Environment

Cloud computing technology offers numerous advantages for its users, including simplicity and rapid deployment. Instead of investing in building infrastructure with their own resources, users can conveniently leverage the services provided by Cloud Service Providers (CSPs). However, entrusting a third party to manage their systems and data necessitates a high level of trust in the chosen entity [52]. Additionally, users must remain vigilant about vulnerabilities and threats inherent in cloud computing. When utilizing cloud services, users transfer their resources from their secure perimeter to a CSP whose security measures may not be fully known. Furthermore, there are risks associated with data transmission. In the context of cloud-based AI systems, users are required to migrate sensitive data such as training data, models, parameters, and configurations to the CSP. Compromise of these data could result in unintended system behaviors.

Drawing from the list of risks outlined by the Open Web Application Security Project (OWASP), we identify potential vulnerabilities and threats within the cloud environment. OWASP enumerates ten potential risks in cloud computing [53], and we focus on those related to data integrity within the scope of our paper. We categorize the challenges in the cloud environment into two main areas: system access and cloud infrastructure.

In the first category, risks pertain to accountability, data ownership, service credibility, and data integration. Users face concerns regarding the credibility and security of their data when storing and transmitting it to the CSP. Entrusting data to a third party introduces an additional layer of risk [54].

In the second category, risks center around multi-tenancy and infrastructure security. A distinguishing feature of cloud computing is its shared infrastructure, where multiple tenants share cloud resources and services. Failures in the multi-tenancy system pose potential risks, such as inadvertent access by one user to another user's data on the same host. Further details are provided in Table 4.

Category	Risks [53]	Vulnerabilities	Issues
System Access	R1. Accountability and Data Ownership, R6. Service and Data Integration	C1. Account and service hijacking	Adversary could gain access to the cloud resources and services
		C2. Malicious insiders	Leaked important data to adversary
		C3. Lack of authentication and authorization mechanisms	Impersonate real user to compromise the data, resources, and services
Cloud Infrastructure	R7. Multi-tenancy, R9. Infrastructure Security	C4. Insecure API gateway	Exposed to unauthorized data access that could lead to a black-box attack
		C5. Security misconfiguration	Breach in API, account and service hijacking
		C6. Multi-tenancy failure	One tenant can access neighbor's data or resources. Adversary could use it to harm data integrity

System Access

C1. Account and Service Hijacking: This threat arises from various tactics such as phishing, fraud, exploiting software vulnerabilities, and credential reuse. Attackers can illicitly acquire user credentials, thus gaining unauthorized access to services [55–57].

C2. Malicious Insiders: This threat, familiar to most organizations, involves individuals with insider access exploiting their privileges. The severity of the repercussions depends on the level of access, as individuals with higher privileges can access sensitive data and services. Malicious insiders pose significant risks, including theft of confidential data, reputational damage, financial losses, and productivity disruptions [55–57].

C3. Lack of Authentication and Authorization Mechanisms: Authentication and authorization serve as the primary defenses against unauthorized access to the cloud environment. Authentication verifies the identity of users, distinguishing between legitimate users and adversaries, while authorization controls data access by defining the access levels for each authenticated user. Absence of these mechanisms can lead to various compromises, such as unauthorized access to personal information and cloud services, loss of data privacy, and data leakage [55–57].

Cloud Infrastructure

C4. Insecure API Gateway: API gateways facilitate client interactions with cloud services. Inadequate security measures in API gateways can expose organizations to numerous threats, including anonymous access, credential reuse, and non-encrypted data transmission. Additionally, insecure API gateways can lead to account and service hijacking, data loss, and leakage. Vulnerabilities in API gateways can be exploited in black-box attacks in cloud-based AI systems, enabling adversaries to misuse insecure APIs to query ML models [55–57].

C5. Security Misconfiguration: Misconfigurations may occur at various levels, including frameworks, web servers, application stacks, or browsers. For instance, using a browser with weak security settings can lead to security misconfiguration. Such misconfigurations may result in interface breaches, API vulnerabilities, or account and service hijacking. It is imperative to regularly audit security configurations and utilize browsers or frameworks that enforce robust security policies [55].

C6. Multi-Tenancy Failure: Multi-tenancy is fundamental in cloud computing, allowing cloud vendors to share resources among multiple users. However, failures in multi-tenancy can compromise system integrity and expose users' data. For example, one user may inadvertently access another user's data, posing risks of data tampering by adversaries. Ensuring robust multi-tenancy mechanisms is crucial to maintaining data integrity in cloud environments [55].

Proposed Architecture

Architecture Requirements

After analyzing the vulnerabilities and challenges outlined in Section 2, we have identified several requirements necessary for constructing a robust data integrity architecture for cloud-based AI systems, as summarized in Table 6. Below, we present our proposed solutions that address these requirements:

Identity and Access Control Management: Proper identification and authorization of users before accessing cloud services are crucial for preventing data integrity compromises. Lack of authentication and authorization mechanisms can leave the system vulnerable to adversaries. Our solution involves using digital signatures to verify users' identities each time they access the system and its services.

Consistency and Completeness: Maintaining consistency and completeness of ML datasets is vital to ensure accurate results. Any tampering or imbalance in the training data can lead to biased decisions by the AI system. We address this requirement by employing hash functions to monitor and verify data integrity. Additionally, we record this information in a blockchain, leveraging its decentralized nature to detect and signal any data alterations.

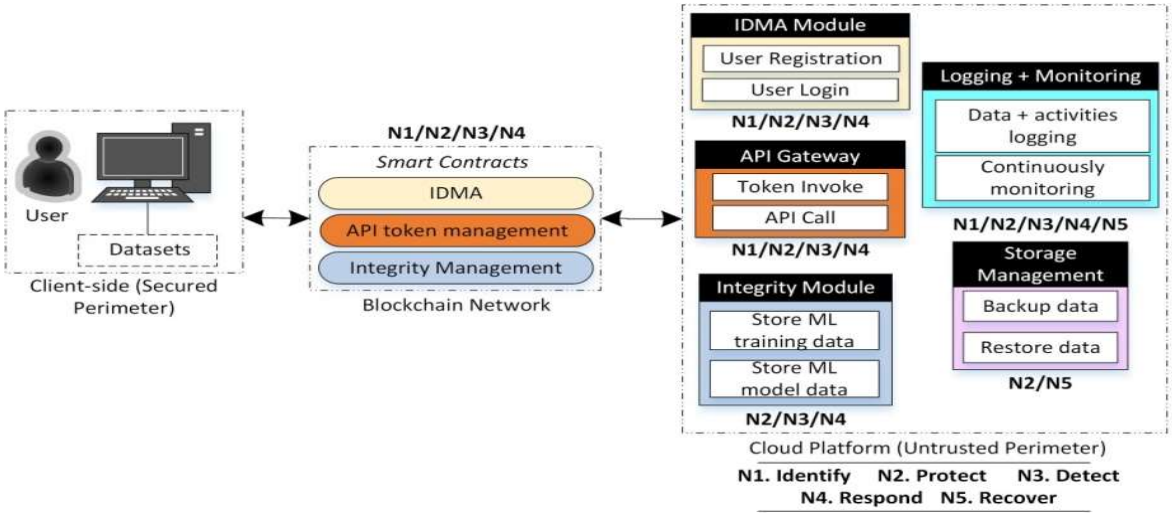
Non-Repudiation: Malicious insiders pose a significant threat to system integrity, as they can exploit their access privileges to leak or modify data undetected. To address this, users are required to sign data changes to verify their identity. Furthermore, we implement logging and monitoring mechanisms to track and flag any unusual user activities within the system.

Trusted Service Level Agreement (SLA): SLAs serve as contractual agreements between customers and CSPs, establishing trust between both parties. However, the possibility of breaches or trust issues remains. Our solution involves using smart contracts to automate and enforce SLAs, minimizing vulnerabilities exposed to unauthorized parties. This approach enhances policy enforcement across AI pipeline phases and mitigates cloud vulnerabilities.

Each of these proposed solutions aims to strengthen the overall security posture of cloud-based AI systems, addressing specific vulnerabilities and ensuring robust data integrity protection.

Table 6. Requirements for data integrity architecture for Cloud-based AI Systems.

Requirement	Covered AI Pipeline	Covered Cloud Vulnerabilities	Description	Our Proposed Solutions
Identity and Access Control Management	A2	C1, C3, C4, C5	Prevent adversary to impersonate the real user to login to cloud environment and gain control over the data.	We use a digital signature to verify the user's identity every time they enter the system and use services.
Consistency and Completeness	A1, A5		Prevent adversary to alter the training data, mislabelled the training data to another value, and disrupt the consistency in datasets.	We use a hash function to keep track to ensure no violation of data integrity and record it in the blockchain.
Non-repudiation	A2	C2	Prevent malicious insiders that has direct access to services and data to leak the information to the adversary or even modify it undetected.	Whenever users changes the data, they need to sign it to verify their identity.
Trusted SLA	A1, A2, A5	C1–C6	Trust issues between user and CSP.	We use smart contracts to bind the trust between users and CSP that can automate the SLA process.



Architecture Details

We present our proposed architecture that fulfills the four requirements outlined above in Figure 2.

In this architecture, there are three main components: the user on the client-side, smart contracts in the blockchain network, and the cloud platform/CSP (assumed to be untrustworthy). Users interact with the cloud platform by performing actions such as uploading ML datasets, training ML models, and using AI services via API calls. To

ensure data integrity throughout the ML lifecycle in the cloud environment, we propose an architecture based on the NIST cybersecurity framework. The mapping of our modules to the NIST framework guidance is depicted in Figure 2, and the analysis of the mapping is discussed in Section 5. The architecture consists of five modules: Identity Management and Access Control (IDMA), API Gateway, Integrity Module (IM), Logging Monitoring, and Storage Management. Additionally, we design six protocols for the first three modules: IDMA, API gateway, and IM.

Identity Management and Access Control Module (IDMA): This module handles user authentication and access control by assigning roles to users and ensuring proper authentication before accessing cloud services. Users must prove their authenticity before accessing the cloud system to prevent impersonation by adversaries. New users are assigned roles and permissions upon registration. Role-Based Access Control (RBAC) is utilized as a policy enforcement mechanism, with three roles defined: General User, Log Admin, and System Admin.

1. General User: Authorized to access personal data and cloud services through API calls with an additional token.
2. Log Admin: Authorized to access logging data for system analysis.
3. System Admin: Authorized to manage user roles and access user information.

Conclusion:

In the ever-evolving realm of AI and machine learning (ML) technologies, the fusion with cloud computing has unlocked unprecedented avenues for innovation and efficiency. However, alongside these advancements, significant challenges pertaining to data integrity, security, and compliance have emerged within cloud-based AI/ML ecosystems. As organizations increasingly rely on these technologies to inform critical decision-making processes, safeguarding data integrity and ensuring compliance with regulatory frameworks have become paramount priorities.

Throughout this paper, we have explored the intricate relationship between AI/ML technologies and cloud computing environments, identifying vulnerabilities, threats, and potential solutions to mitigate risks and bolster data guardianship. From the initial data acquisition and curation phase to the deployment of AI models and ongoing monitoring, each stage of the AI/ML lifecycle presents unique challenges that demand attention to maintain data integrity and regulatory compliance.

We have delineated a comprehensive architecture that integrates both algorithm-based defenses and architecture-based mechanisms to fend off threats such as data poisoning, adversarial attacks, and unauthorized access. Through the utilization of cryptographic techniques, blockchain technology, and role-based access control, organizations can establish resilient defenses to uphold data integrity, authenticate users, and enforce access controls within cloud-based AI/ML ecosystems.

Moreover, we have emphasized the significance of adhering to regulatory frameworks such as GDPR, HIPAA, and CCPA, which impose rigorous requirements for safeguarding sensitive data and upholding individual rights. By embedding compliance measures into the design and implementation of AI/ML systems, organizations can ensure transparency, accountability, and trustworthiness in their data practices.

In summary, the endeavor to safeguard compliance and data guardianship in AI/ML cloud ecosystems necessitates a multifaceted approach encompassing technological innovations, regulatory adherence, and organizational best practices. By adopting a proactive stance towards data security, privacy, and regulatory compliance, organizations can harness the full potential of AI/ML technologies while mitigating risks and fostering trust among stakeholders. As we navigate the evolving landscape of AI/ML and cloud computing, the pursuit of data guardianship will remain a foundational imperative for organizations striving to thrive in the digital era.

References:

[1]. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 189-208. DOI: https://doi.org/10.60087/jaigs.v2i1.p208

[2]. Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 47-66. DOI: https://doi.org/10.60087/jaigs.v1i1.p66

[3]. Islam, M. M. (2024). Exploring Ethical Dimensions in AI: Navigating Bias and Fairness in the Field. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 13-17.**DOI:** https://doi.org/10.60087/jaigs.v1i1.p18

[4]. Khan, M. R. (2024). Advances in Architectures for Deep Learning: A Thorough Examination of Present Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 24-30. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p30

[5]. Shuford, J., & Islam, M. M. (2024). Exploring the Latest Trends in Artificial Intelligence Technology: A Comprehensive Review. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1). **DOI:** https://doi.org/10.60087/jaigs.v2i1.p13

[6]. Islam, M. M. (2024). Exploring the Applications of Artificial Intelligence across Various Industries. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 20-25.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p25

[7]. Akter, S. (2024). Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 25-30.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p30

[8]. Rana, S. (2024). Exploring the Advancements and Ramifications of Artificial Intelligence. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 30-35.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p35

[9]. Sarker, M. (2024). Revolutionizing Healthcare: The Role of Machine Learning in the Health Sector. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 35-48.

DOI: https://doi.org/10.60087/jaigs.v2i1.p47

[10]. Akter, S. (2024). Harnessing Technology for Environmental Sustainability: Utilizing AI to Tackle Global Ecological Challenges. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 49-57.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p57

[11]. Padmanaban, H. (2024). Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 57-69.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p69

[12]. Padmanaban, H. (2024). Navigating the Role of Reference Data in Financial Data Analysis: Addressing Challenges and Seizing Opportunities. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 69-78.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p78

[13]. Camacho, N. G. (2024). Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 79-89.**DOI:** https://doi.org/10.60087/jaigs.v2i1.p89

[14]. PC, H. P., & Sharma, Y. K. (2024). Developing a Cognitive Learning and Intelligent Data Analysis-Based Framework for Early Disease Detection and Prevention in Younger Adults with Fatigue. *Optimized Predictive Models in Health Care Using Machine Learning*, 273.

[15]. Padmanaban, H. (2024). Quantum Computing and AI in the Cloud. *Journal of Computational Intelligence and Robotics*, *4*(1), 14–32. Retrieved from https://thesciencebrigade.com/jcir/article/view/116

[16]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572317_Critical_study_of_software_models_used_cloud_application_development/links/65ad55d7ee1e1951fbd79df6/Critical-study-of-software-models-used-cloud-application-development.pdf

[17]. Padmanaban, P. H., & Sharma, Y. K. (2019). Implication of Artificial Intelligence in Software Development Life Cycle: A state of the art review. *vol*, *6*, 93-98.https://www.researchgate.net/profile/Harish-Padmanaban-2/publication/377572222_Implication_of_Artificial_Intelligence_in_Software_Development_Life_Cycle_A_state_of_the_art_review/links/65ad54e5bf5b00662e333553/Implication-of-Artificial-Intelligence-in-Software-Development-Life-Cycle-A-state-of-the-art-review.pdf

[18]. Harish Padmanaban, P. C., & Sharma, Y. K. (2024). Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning. *Advances in Aerial Sensing and Imaging*, 267-294. **https://doi.org/10.1002/9781394175512.ch12**

[19]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.https://patents.google.com/patent/US20230385176A1/en

[20]. Padmanaban, H. (2023). Navigating the intricacies of regulations: Leveraging AI/ML for Accurate Reporting. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 401-412.DOI: https://doi.org/10.60087/jklst.vol2.n3.p412

[21]. PC, H. P. Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence.https://shodhganga.inflibnet.ac.in/handle/10603/487443

[22]. Latif, M. A., Afshan, N., Mushtaq, Z., Khan, N. A., Irfan, M., Nowakowski, G., ... &Telenyk, S. (2023). Enhanced classification of coffee leaf biotic stress by synergizing feature concatenation and dimensionality reduction. *IEEE Access*.
DOI: https://doi.org/10.1109/ACCESS.2023.3314590

[23]. Irfan, M., Mushtaq, Z., Khan, N. A., Mursal, S. N. F., Rahman, S., Magzoub, M. A., ... & Abbas, G. (2023). A Scalo gram-based CNN ensemble method with density-aware smote oversampling for improving bearing fault diagnosis. *IEEE Access*, *11*, 127783-127799.
DOI: https://doi.org/10.1109/ACCESS.2023.3332243

[24]. Irfan, M., Mushtaq, Z., Khan, N. A., Althobiani, F., Mursal, S. N. F., Rahman, S., ... & Khan, I. (2023). Improving Bearing Fault Identification by Using Novel Hybrid Involution-Convolution Feature Extraction with Adversarial Noise Injection in Conditional GANs. *IEEE Access*.

DOI: https://doi.org/10.1109/ACCESS.2023.3326367

[25]. Rahman, S., Mursal, S. N. F., Latif, M. A., Mushtaq, Z., Irfan, M., & Waqar, A. (2023, November). Enhancing Network Intrusion Detection Using Effective Stacking of Ensemble Classifiers With Multi-Pronged Feature Selection Technique. In *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-6). IEEE.

DOI: https://doi.org/10.1109/ETECTE59617.2023.10396717

[26]. Latif, M. A., Mushtaq, Z., Arif, S., Rehman, S., Qureshi, M. F., Samee, N. A., ... & Al-masni, M. A. Improving Thyroid Disorder Diagnosis via Ensemble Stacking and Bidirectional Feature Selection.
https://doi.org/10.32604/cmc.2024.047621

[27]. Ara, A., &Mifa, A. F. (2024). INTEGRATING ARTIFICIAL INTELLIGENCE AND BIG DATA IN MOBILE HEALTH: A SYSTEMATIC REVIEW OF INNOVATIONS AND CHALLENGES IN HEALTHCARE SYSTEMS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *3*(01), 01-16.

DOI: https://doi.org/10.62304/jbedpm.v3i01.70

[28]. Bappy, M. A., & Ahmed, M. (2023). ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH

MACHINE LEARNING MODELS. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *2*(04), 15-26.
DOI: https://doi.org/10.62304/jbedpm.v2i04.67

[29]. Bappy, M. A. (2024). Exploring the Integration of Informed Machine Learning in Engineering Applications: A Comprehensive Review. *American Journal of Science and Learning for Development*, *3*(2), 11-21.
DOI: https://doi.org/10.51699/ajsld.v3i2.3459

[30]. Uddin, M. N., Bappy, M. A., Rab, M. F., Znidi, F., &Morsy, M. (2024). Recent Progress on Synthesis of 3D Graphene, Properties, and Emerging Applications.
DOI: https://doi.org/10.5772/intechopen.114168

[31]. Hossain, M. I., Bappy, M. A., &Sathi, M. A. (2023). WATER QUALITY MODELLING AND ASSESSMENT OF THE BURIGANGA RIVER USING QUAL2K. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(03), 01-11.
DOI: https://doi.org/10.62304/jieet.v2i03.64

[32]. Zhu, M., Zhang, Y., Gong, Y., Xing, K., Yan, X., & Song, J. (2024). Ensemble Methodology: Innovations in Credit Default Prediction Using LightGBM, XGBoost, and LocalEnsemble. *arXiv preprint arXiv:2402.17979*.

https://doi.org/10.48550/arXiv.2402.17979

[33]. Yafei, X., Wu, Y., Song, J., Gong, Y., &Lianga, P. (2024). Generative AI in Industrial Revolution: A Comprehensive Research on Transformations, Challenges, and Future Directions. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(2), 11-20.

DOI: https://doi.org/10.60087/jklst.vol.3n2.p20

[34]. Xu, J., Wang, H., Zhong, Y., Qin, L., & Cheng, Q. (2024). Predict and Optimize Financial Services Risk Using AI-driven Technology. *Academic Journal of Science and Technology*, *10*(1), 299-304.

https://drpress.org/ojs/index.php/ajst/article/view/19205

[35]. Ness, S., Sarker, M., Volkivskyi, M., & Singh, N. (2024). The Legal and Political Implications of AI Bias: An International Comparative Study. *American Journal of Computing and Engineering*, *7*(1), 37-45.
DOI: https://doi.org/10.47672/ajce.1879

[36]. Sarker, M. (2022). Towards Precision Medicine for Cancer Patient Stratification by Classifying Cancer By Using Machine Learning. *Journal of Science & Technology*, *3*(3), 1-30.

DOI: https://doi.org/10.55662/JST.2022.3301

[37]. Manoharan, A., &Sarker, M. REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT-GENERATION THREAT DETECTION.

DOI :https://www.doi.org/10.56726/IRJMETS32644

[38]. Lee, S., Weerakoon, M., Choi, J., Zhang, M., Wang, D., & Jeon, M. (2022, July). CarM: Hierarchical episodic memory for continual learning. In *Proceedings of the 59th ACM/IEEE Design Automation Conference* (pp. 1147-1152).

https://doi.org/10.1145/3489517.3530587

[39]. Lee, S., Weerakoon, M., Choi, J., Zhang, M., Wang, D., & Jeon, M. (2021). Carousel Memory: Rethinking the Design of Episodic Memory for Continual Learning. *arXiv preprint arXiv:2110.07276*.

https://doi.org/10.48550/arXiv.2110.07276

[40]. Weerakoon, M., Heaton, H., Lee, S., & Mitchell, E. (2024). TopoQual polishes circular consensus sequencing data and accurately predicts quality scores. *bioRxiv*, 2024-02.

doi: https://doi.org/10.1101/2024.02.08.579541

[41]. Pillai, A. S. (2023). Advancements in Natural Language Processing for Automotive Virtual Assistants Enhancing User Experience and Safety. *Journal of Computational Intelligence and Robotics*, *3*(1), 27-36.

https://thesciencebrigade.com/jcir/article/view/161

[42]. Sharma, Y. K., & Harish, P. (2018). Critical study of software models used cloud application development. *International Journal of Engineering & Technology, E-ISSN*, 514-518.

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=Fxv3elcAAAAJ&citation_for_view=Fxv3elcAAAAJ:d1gkVwhDpl0C

[43]. PC, H. P., Mohammed, A., & RAHIM, N. A. (2023). *U.S. Patent No. 11,762,755*. Washington, DC: U.S. Patent and Trademark Office.

https://patents.google.com/patent/US11762755B2/en

[44]. Miah, S., Rahaman, M. H., Saha, S., Khan, M. A. T., Islam, M. A., Islam, M. N., ... & Ahsan, M. H. (2013). Study of the internal structure of electronic components RAM DDR-2 and motherboard of nokia-

3120 by using neutron radiography technique. *International Journal of Modern Engineering Research (IJMER)*, *3*(60), 3429-3432

https://shorturl.at/nCJOQ

[45]. Rahaman, M. H., Faruque, S. B., Khan, M. A. T., Miah, S., & Islam, M. A. (2013). Comparison of General Relativity and Brans-Dicke Theory using Gravitomagnetic clock effect. *International Journal of Modern Engineering Research*, *3*, 3517-3520.

https://shorturl.at/hjm37

[46]. Miah, M. H., & Miah, S. (2015). The Investigation of the Effects of Blackberry Dye as a Sensitizer in TiO2 Nano Particle Based Dye Sensitized Solar Cell. *Asian Journal of Applied Sciences*, *3*(4).

https://shorturl.at/iyJQV

[48]. Miah, S., Miah, M. H., Hossain, M. S., & Ahsan, M. H. (2018). Study of the Homogeneity of Glass Fiber Reinforced Polymer Composite by using Neutron Radiography. *Am. J. Constr. Build. Mater*, *2*, 22-28.

https://shorturl.at/joDKZ

[49]. Miah, S., Islam, G. J., Das, S. K., Islam, S., Islam, M., & Islam, K. K. (2019). Internet of Things (IoT) based automatic electrical energy meter billing system. *IOSR Journal of Electronics and Communication Engineering*, *14*(4 (I)), 39-50.

[50]. Nadia, A., Hossain, M. S., Hasan, M. M., Islam, K. Z., & Miah, S. (2021). Quantifying TRM by modified DCQ load flow method. *European Journal of Electrical Engineering*, *23*(2), 157-163.

https://shorturl.at/csuO3

[51]. Miah, S., Raihan, S. R., Sagor, M. M. H., Hasan, M. M., Talukdar, D., Sajib, S., ... & Suaiba, U. (2022). Rooftop Garden and Lighting Automation by the Internet of Things (IoT). *European Journal of Engineering and Technology Research*, *7*(1), 37-43.

DOI: https://doi.org/10.24018/ejeng.2022.7.1.2700

[52]. Prasad, A. B., Singh, S., Miah, S., Singh, A., & Gonzales-Yanac, T. A Comparative Study on Effects of Work Culture on employee satisfaction in Public & Private Sector Bank with special reference to SBI and ICICI Bank.

[53]. Ravichandra, T. (2022). A Study On Women Empowerment Of Self-Help Group With Reference To Indian Context.

https://www.webology.org/data-cms/articles/20220203075142pmwebology%2019%20(1)%20-%2053.pdf

[54]. Kumar, H., Aoudni, Y., Ortiz, G. G. R., Jindal, L., Miah, S., & Tripathi, R. (2022). Light weighted CNN model to detect DDoS attack over distributed scenario. *Security and Communication Networks*, *2022*.

https://doi.org/10.1155/2022/7585457

[55]. Ma, R., Kareem, S. W., Kalra, A., Doewes, R. I., Kumar, P., & Miah, S. (2022). Optimization of electric automation control model based on artificial intelligence algorithm. *Wireless Communications and Mobile Computing*, *2022*.

https://doi.org/10.1155/2022/7762493

[56]. Devi, O. R., Webber, J., Mehbodniya, A., Chaitanya, M., Jawarkar, P. S., Soni, M., & Miah, S. (2022). The Future Development Direction of Cloud-Associated Edge-Computing Security in the Era of 5G as Edge Intelligence. *Scientific Programming*, *2022*.

https://doi.org/10.1155/2022/1473901

[57]. Al Noman, M. A., Zhai, L., Almukhtar, F. H., Rahaman, M. F., Omarov, B., Ray, S., ... & Wang, C. (2023). A computer vision-based lane detection technique using gradient threshold and hue-lightness-saturation value for an autonomous vehicle. *International Journal of Electrical and Computer Engineering*, *13*(1), 347.

https://shorturl.at/ceoyJ

[58]. Patidar, M., Shrivastava, A., Miah, S., Kumar, Y., & Sivaraman, A. K. (2022). An energy efficient high-speed quantum-dot based full adder design and parity gate for nano application. *Materials Today: Proceedings*, *62*, 4880-4890.

https://doi.org/10.1016/j.matpr.2022.03.532

[59]. Gitte, M., Bawaskar, H., Sethi, S., & Shinde, A. (2014). Content based video retrieval system. *International Journal of Research in Engineering and Technology*, *3*(06), 123-129. https://scholar.google.co.in/citations?view_op=view_citation&hl=en&user=XlLBRR4AAAAJ&citation_for_view=XlLBRR4AAAAJ:u5HHmVD_uO8C

[60]. Shivakumar, S. K., & Sethii, S. (2019). *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*. Apress.

https://shorturl.at/bdFQ9

[61]. Sethi, S., & Panda, S. (2024). Transforming Digital Experiences: The Evolution of Digital Experience Platforms (DXPs) from Monoliths to Microservices: A Practical Guide. *Journal of Computer and Communications*, *12*(2), 142-155.

DOI: https://doi.org/10.4236/jcc.2024.122009

[62]. Sethi, S. (2018). Healthcare blockchain leads to transform healthcare industry. *International Journal of Advance Research, Ideas and Innovations in Technology*, *4*(1), 607-608.

[62]. Sethi, S., & Shivakumar, S. K. (2023). DXPs Digital Experience Platforms Transforming Fintech Applications: Revolutionizing Customer Engagement and Financial Services. *International Journal of Advance Research, Ideas and Innovations in Technology*, *9*, 419-423.

[63]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). DXP Security. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 183-200.

DOI https://doi.org/10.1007/978-1-4842-4303-9_6

[64]. Sethi, S., & Panda, S. (2023). The Evolution of Monolithic DXPs to Microservice based DXPs. *Authorea Preprints*.

DOI https://doi.org/10.36227/techrxiv.24328504.v1

[65]. Sethi, S., Panda, S., & Kamuru, R. (2023). Comparative study of middle tier caching solution. *International Journal of Development Research*, *13*(11), 64225-64229.

[66]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Designing the Integration Layer. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 149-179.

DOI https://doi.org/10.1007/978-1-4842-4303-9_5

[67]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). DXP Performance Optimization. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 235-259.

DOI https://doi.org/10.1007/978-1-4842-4303-9_9

[68]. Shivakumar, S. K., & Sethii, S. (2019). Building Digital Experience Platforms.

https://link.springer.com/book/10.1007/978-1-4842-4303-9

[69]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Quality Attributes and Sizing of the DXP. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 215-234.

DOI https://doi.org/10.1007/978-1-4842-4303-9_8

[70]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). End to End DXP Case Study. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 299-320.

DOI https://doi.org/10.1007/978-1-4842-4303-9_11

[71]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Transforming legacy banking applications to banking experience platforms. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 261-295.

DOI https://doi.org/10.1007/978-1-4842-4303-9_10

[72]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). DXP Information Security. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 201-212.

DOI https://doi.org/10.1007/978-1-4842-4303-9_7

[73]. Shivakumar, S. K., Sethii, S., Shivakumar, S. K., & Sethii, S. (2019). Introduction to Digital Experience Platforms. *Building Digital Experience Platforms: A Guide to Developing Next-Generation Enterprise Applications*, 3-26.

DOI https://doi.org/10.1007/978-1-4842-4303-9_1

[74]. Sethi, S. (2023). Platforms Based Approach and Strategy for Fintech applications. *Authorea Preprints*.

DOI https://doi.org/10.36227/techrxiv.24329533.v1