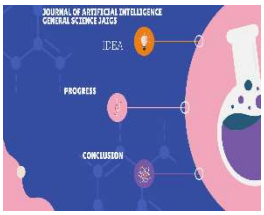
Vol.3,Issue 01, March 2024
Journal of Artificial Intelligence General Science JAIGS

Home page http://jaigs.org



Harmonizing Compliance: Coordinating Automated Verification Processes within Cloud-based AI/ML Workflows

Sohana Akter

Department of Computer Science, University of Rajshahi-Bangladesh

*Corresponding Author: Sohana Akter

ARTICLEINFO
Article History:
Received: 05.03.2024
Accepted: 10.03.2024
Online: 10.04.2024
Keyword: Cloud computing, workflow orchestration, security enforcement, deep learning, anomaly detection, healthcare, COVID-19.

ABSTRACT

The significance of ensuring security and upholding data privacy within cloud-based workflows is widely recognized in research domains. This importance is particularly evident in contexts such as safeguarding patients' private data managed within cloud-deployed workflows, where maintaining confidentiality is paramount, alongside ensuring secure communication among involved stakeholders. In response to these imperatives, our paper presents an architecture and formal model designed to enforce security measures within cloud workflow orchestration. Central to our proposed architecture is the emphasis on continuous monitoring of cloud resources, workflow tasks, and data streams to detect and preempt anomalies in workflow orchestration processes. To accomplish this, we advocate for a multi-modal approach that integrates deep learning, one-class classification, and clustering techniques. In essence, our proposed architecture offers a comprehensive solution for enforcing security within cloud workflow orchestration, harnessing advanced methodologies like deep learning for anomaly detection and prediction. This approach is particularly pertinent in critical sectors such as healthcare, especially during unprecedented events like the COVID-19 pandemic.

Introduction

Cloud computing has emerged as a dominant paradigm for managing and delivering computations, applications, and services over the Internet [1]. The computational capabilities offered by the cloud span a wide range of services, including storage, processing, and application services, enabling researchers to conduct computationally intensive workflows with ease. This shift to cloud-based workflows has significantly reduced costs associated with software systems [1], establishing itself as a promising design paradigm for workflow deployment, processing, and orchestration. While typical large-scale scientific workflows involve interconnected tasks characterized by complexity, fault tolerance, and dynamic execution aimed at producing scientific results, cloud workflows specifically refer to workflows deployed and executed on the cloud. These workflows offer features such as transparency, scalability, multi-tenancy, and real-time monitoring [2].

Despite the benefits of cloud computing, several research challenges must be addressed to fully realize its potential. These challenges include security threats in the cloud domain, encompassing integrity, authorization, availability, reliability, and trust. Ensuring secure access, deployment, execution, and management of workflows across cloud platforms is crucial for both providers and consumers. Numerous security threats in cloud computing have been identified [3] and scrutinized [4–8], including data breaches, leaks, denial of service (DoS) attacks, and malicious insiders, arising from issues such as multi-tenancy and loss of data control. A holistic security solution involving security enforcement, trust chains in clouds, and adherence to policies and regulations is essential to ensure security and privacy across multiple participants and heterogeneous environments.

The emergence of security challenges within cloud workflows has prompted researchers to explore various domains related to security enforcement in dynamically executed and orchestrated cloud workflows. However, existing research on workflow management has primarily focused on anomaly detection, task scheduling, and workflow resource provisioning and management, often overlooking the critical aspect of security enforcement. Few studies have exclusively addressed security aspects of cloud workflow orchestration, management, and enforcement [13], typically focusing on anomaly detection and prediction using techniques like HTM, statistical clustering, regression, and unsupervised machine learning (ML). However, these studies often lack clear definitions of security attributes and fail to specify the characteristics of cloud workflows, which are resource-aware, time-series, and highly dynamic. Additionally, they tend to focus solely on specific security dimensions, neglecting other dimensions that could enhance security enforcement when integrated. Furthermore, previous attempts have concentrated on security/anomaly detection and prediction, neglecting the need for resource and workflow adaptation strategies to mitigate security threats and potential attacks.

To address some of these limitations, we propose a security anomaly/attack detection and prediction framework for cloud workflow orchestration. Our framework includes a multi-dimensional security enforcement framework, a scheme integrating static and dynamic features for predicting anomalies/attacks, an unsupervised learning technique, and an adaptation model for flexible representation and planning of resource requirements over time. This paper presents a comprehensive discussion of related work, a case study utilizing a COVID-19 dataset, an architecture for enforcing end-to-end security in cloud workflow orchestration, a detailed formulation of the cloud workflow security enforcement model and associated learning pipeline algorithms, implementation details, experimental scenarios, results discussion, and conclusions with suggestions for future work.

Previous Research:

With the rapid expansion of cloud services, the realm of security within the cloud computing ecosystem has received substantial attention, as threats and vulnerabilities evolve alongside the growth of cloud services. Understanding related risks inherent in emerging cloud services is pivotal to advancing state-of-the-art security solutions. These risks typically arise from three primary attack vectors: external users, internal users, and cloud providers [20, 21]. Over time, security threats within cloud service environments have evolved, encompassing common issues such as data breaches, data loss, denial-of-service (DoS) attacks, malicious insiders, service traffic hijacking, vulnerabilities in shared technologies, malware, cyber-attacks, network intrusions, threats at the virtual machine (VM) level, and challenges related to data transparency.

Recent advancements in deep learning have spurred researchers to explore its potential in addressing cloud security threats. However, existing approaches often lack a comprehensive solution covering all security threats. Many of these approaches focus on detecting patterns associated with specific threats within single deployment scenarios. For instance, researchers utilized a multi-layer neural network to detect and recognize malicious behaviors exhibited by users, transforming user behavior data into a comprehensible format for classification purposes.

In their work, the authors introduced PredictDeep, a security analytical framework for both known and unknown anomaly detection and prediction within Big Data systems. PredictDeep consists of three core modules: a graph model designer, a feature extractor, and an anomaly predictor. While renowned for its scalability and real-time anomaly monitoring capabilities,

PredictDeep assumes the accuracy of all log files without injected fake data and relies on the integrity of the deployment infrastructure.

Intrusion detection systems (IDS) are pivotal in monitoring networks, services, and workflows for violations or malicious activities within cloud services orchestration. Detecting novel attacks in such scenarios presents a formidable challenge. Deep learning-based intrusion detection techniques have shown promise in predicting unknown attacks and detecting malicious activities. Authors introduced an IDS utilizing a deep reinforcement learning-based architecture to address and classify new and complex attacks. They implemented a reward vector to enhance classification accuracy. Additionally, another study tackled multi-cloud cooperative intrusion detection and improved decision-making using a deep neural network (DNN) model based on historical feedback data. Similarly, a deep learning-based IDS aimed to detect suspicious attacks within a cloud computing environment by monitoring network traffic, demonstrating high detection rates and accuracy.

Other research efforts have focused on enhancing cloud workflow security enforcement. For instance, developers involved in the ASCLEPIOS project utilized cryptographic and access control techniques to safeguard user data privacy within a cloud-based eHealth framework. Similarly, the PICASO project introduced a framework for cross-organization sharing of electronic health records through a cloud-based solution, implementing security and privacy measures alongside service orchestration. Additionally, authors conducted a literature review on security in Function as a Service (FaaS) orchestration systems, observing a focus on data confidentiality but a lack of consideration for data integrity. Another study classified existing works employing machine learning and deep learning techniques for online malware detection in the cloud, revealing high accuracy in detecting malware but not addressing end-to-end security enforcement for workflows within a cloud environment.

Case Study: Cloud Workflow Management in the Context of the COVID-19 Pandemic

The global healthcare landscape has encountered unprecedented challenges since the emergence of the Novel Coronavirus (COVID-19) outbreak, officially declared a pandemic by the World Health Organization in March 2020. The rapid spread of novel virus strains has placed significant strain on healthcare systems worldwide, necessitating collaborative efforts among healthcare providers, governmental agencies, and research institutions to develop effective treatments or vaccines. Amidst these endeavors, safeguarding facilities, confidential data, and workflows from potential malicious attacks has become imperative to ensure the integrity of the entire process.

Throughout the COVID-19 pandemic, there has been a dramatic surge in reliance on online resources and cloud-based infrastructure systems. Lockdown measures, contact-tracing applications, and the widespread adoption of remote working and distance-learning platforms have contributed to this increased reliance. However, this surge has also led to a notable increase in cyber-attacks and breaches of data confidentiality and integrity.

To demonstrate the applicability and effectiveness of a security enforcement architecture and to identify primary security threats in cloud workflow orchestration, we present a case study focused on a cloud workflow tailored to manage a COVID-19 dataset.

Cloud Workflow and COVID-19 Dataset

Figure 1 illustrates a health monitoring cloud workflow developed using epidemiological data from a COVID-19 outbreak dataset. This workflow utilizes a deep learning model to predict the length of hospital stay for COVID-19 patients. The dataset was meticulously collected and curated from national, provincial, and municipal health reports, as well as other online sources. Geocoded data includes symptoms, key dates (onset, admission, confirmation), and travel histories of individual patients. Comprising 2,500,000 records, each representing a unique patient case, the dataset contains 33 columns such as patient ID, age, gender, onset symptoms date, hospital admission date, confirmation date, additional information, chronic disease indicators, specific symptoms, and patient outcomes. Detailed explanations for each field are provided. We utilized this cloud workflow example to identify and assess various security breaches that may be encountered.

Security Threats:

The body of literature concerning cloud-based infrastructures extensively discusses various security concerns, including insider attacks, data loss, and Denial of Service (DoS) attacks. This section examines anomaly detection within a cloud workflow orchestration environment, where attacks may target different entities and components, including workflow data, tasks, resources, monitoring, and adaptation elements. Below, we outline several examples of security breaches in a cloud workflow environment.

Cloud Workflow Data Breach:

Data attacks encompass a range of malicious activities, such as data injection intended to corrupt datasets or compromise them through suspicious sharing or downloads. Unauthorized data access and anomalous admin user activities are also common anomalies. For example, within our cloud workflow, an attacker might inject redundant or fabricated data to disrupt the training and prediction processes, compromising the quality of the prediction model. Such tampering could lead to critical issues, such as patient harm, or overload the Machine Learning (ML) training process, erroneously triggering Quality of Service (QoS) degradation and unnecessary workflow adaptation.

Cloud Workflow Task Breach:

A cloud workflow comprises multiple tasks that may run in parallel or sequentially with varying dependency levels. Task attacks encompass a broad spectrum of anomalies, including malware infections, query injections, and DoS attacks. Moreover, attackers may strategically target sensitive processes or tasks that serve as dependencies for numerous other tasks, amplifying the potential damage.

Resource Breach:

Various resources within the cloud environment, such as Virtual Machines (VMs), CPUs, memory, and networks, are susceptible to different types of attacks. These attacks may involve unauthorized resource access or overwhelming service requests. False reporting of resource overload or overutilization in monitoring logs could trigger compromised nodes to initiate unnecessary and costly workflow adaptation processes.

Monitoring and Adaptation Component Breach:

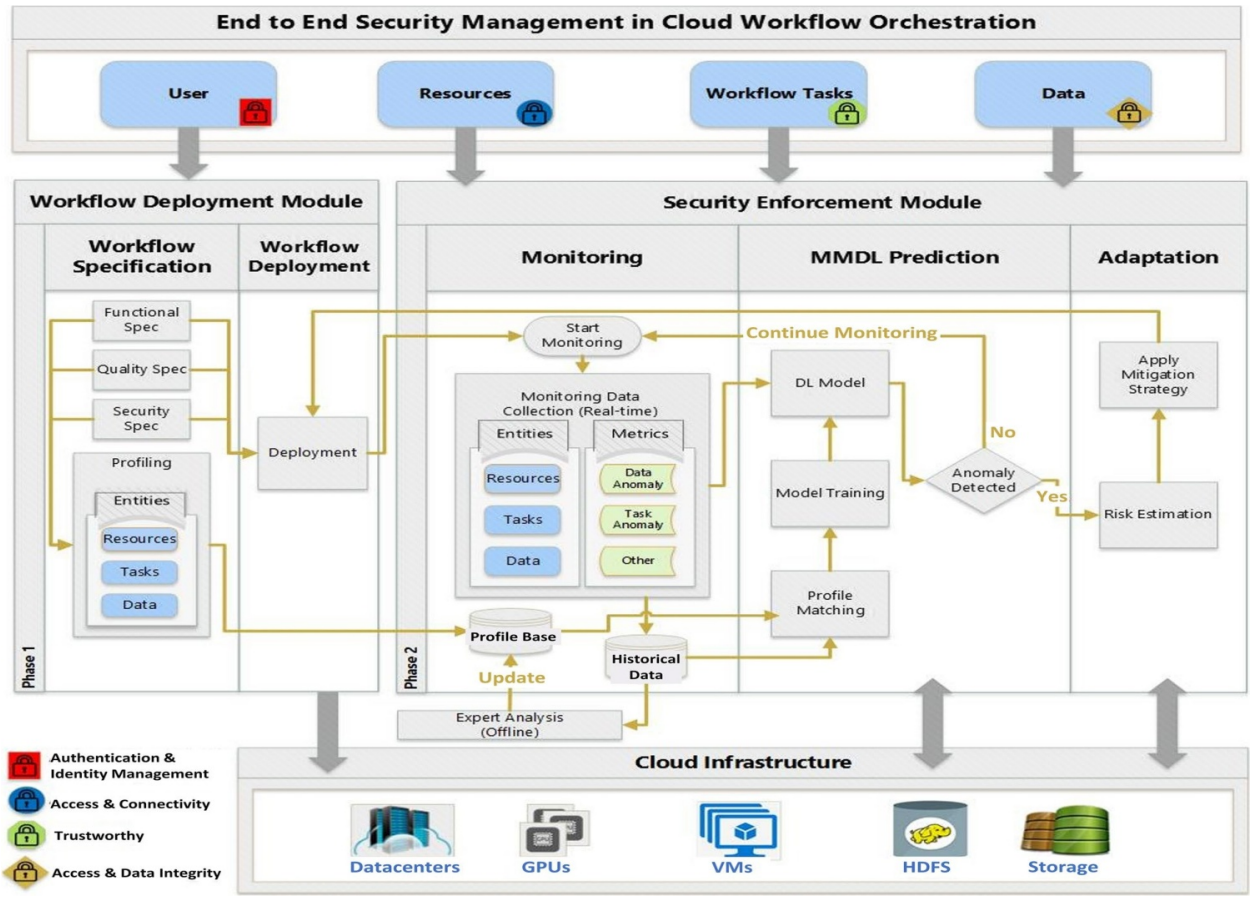
Monitoring and adaptation components play a crucial role in any cloud workflow orchestration environment, as they are vital for resource management and performance optimization. Within this workflow example, an attack against a monitoring system could coerce the compromised monitoring task into generating false resource underutilization logs, thereby evading necessary adaptation and resulting in performance degradation leading to a DoS attack. Another instance of such an attack involves automatic system reconfiguration, where a compromised node falsely identifies a problem and triggers unnecessary adaptation actions.

These types of attacks have a detrimental impact on the performance and integrity of a cloud workflow orchestration system. In this work, we focus on anomaly detection in cloud workflow data, resources, tasks, and monitoring components. Therefore, we propose monitoring resources such as CPU utilization, memory usage, I/O operations, and network activity, as well as task profiles and performance metrics. In the following section, we present our proposed security enforcement mechanism for cloud workflow orchestration.

End-to-End Security Enforcement in Cloud Workflow Orchestration:

This section outlines and describes our end-to-end security enforcement architecture, as illustrated in Figure 2. It comprises two main modules: a workflow deployment module and a security enforcement module. Both modules utilize the underlying processing and storage resources (e.g., VMs, GPUs, Storage) from the cloud infrastructure to execute various storage and processing tasks. Security enforcement measures implemented within our architecture are applied to four main entities: users, resources, workflow tasks, and data.

Subsequently, we provide a detailed description of each component of the architecture, highlighting the security features that enhance security, data integrity, and authentication.



Workflow Deployment Module:

This module consists of two sub-components: the workflow specification and the workflow deployment components. The workflow specification component delineates the functional and non-functional requirements, encompassing quality and security parameters, for the workflow. It also generates profiles for entities such as tasks, data, and resources. Conversely, the workflow deployment component manages the deployment and execution lifecycle of the workflow across the cloud infrastructure. The outcome of this module is a functioning workflow monitored by the security enhancement module, which is tasked with detecting and/or predicting encountered security threats and initiating necessary adaptation actions to mitigate them.

Security Enforcement Module:

The security enforcement module comprises three sub-components: monitoring, Multi-Modal Deep Learning Autoencoder (MMDLA)-based prediction, and adaptation sub-modules. These sub-modules collaborate to achieve comprehensive cloud workflow monitoring, anomaly

detection, and prediction. Finally, they implement an adaptation strategy to mitigate risks identified through various anomaly evaluations.

Monitoring Sub-Module:

This sub-module continuously collects and monitors runtime data and logs from monitored entities, including tasks, data, and resources. The collected data serve purposes of training and prediction and are stored in a historical database for further analysis.

MMDLA Sub-Module:

Utilizing the data gathered by the monitoring sub-module, this module trains a multi-modal deep learning autoencoder model for dimensionality reduction. Additionally, it trains a profile matching classification model using the dimensionally reduced data to predict anomalies. The training process of the MMDLA model combines input data generated from the entities profiling module (static) with real-time logs data from monitoring (dynamic). The resulting MMDLA model reduces data dimensionality to enhance efficiency and effectiveness, providing reduced dimensional data as input to an anomaly detection machine learning algorithm for anomaly detection.

Upon detection of an anomaly, the anomaly evaluation process identifies the type and threat level of the anomaly. Subsequently, the anomaly evaluation information is forwarded to the risk estimation process and eventually stored in a database for expert validation, such as identifying suspicious user behavior. A detailed description and implementation of the key features of this module's components are provided in subsequent sections.

Cloud Infrastructure:

This component fulfills the architecture's resource requirements concerning the various resources necessary for processing and storing data. Processing tasks encompass activities such as MMDLA model training for dimension reduction, training and classification of anomaly detection models, and monitoring of data storage.

Cloud Workflow Security Enforcement Module:

In this section, we explore the operational framework of the MMDLA prediction-based security enforcement module. Initially, we define key terminologies crucial for understanding the prediction model. Subsequently, we address the problem formulation. Lastly, we elucidate the learning pipeline algorithms employed for the proposed solution approach.

Feature Reduction Using Deep Autoencoder:

As discussed earlier, each task's feature vector comprises four static features and six time-series features. To train a model utilizing two-dimensional feature vectors, we must flatten the time-series feature matrix into a one-dimensional feature vector and merge it with the static features. However, this process can result in the creation of a high-dimensional feature vector. Specifically, the total number of features in the vector would be $4 + 6k_i$, where k_i is the number of observations of the dynamic features. For instance, if $k_i = 100$, the total number of flattened features would be 604. Hence, a feature reduction technique becomes necessary.

We opt for the AutoEncoder technique for two main reasons:

AutoEncoder enables unsupervised feature reduction, aligning with a crucial aspect of our proposed model.

We propose a multi-modal deep learning (MMDLA) based AutoEncoder model by integrating Long Short-Term Memory (LSTM) – a specific type of recurrent neural network (RNN) – with a Deep FeedForward network (DFN). This MMDLA model streamlines the feature reduction process by learning from the temporal relationships among time-series features.

conclusion

In conclusion, our research underscores the critical significance of optimizing compliance through automated checks orchestrated within cloud-based AI/ML workflows. As organizations increasingly rely on cloud infrastructure for deploying AI and ML solutions, ensuring adherence to regulatory standards and internal policies emerges as a top priority.

Our proposed methodology demonstrates the efficacy of integrating automated compliance checks into cloud-based AI/ML workflows. By leveraging orchestration tools and embedding compliance checks across various workflow stages, organizations can proactively detect and address compliance issues, thereby mitigating the risk of regulatory breaches and safeguarding their reputation.

Furthermore, our study highlights the advantages of automation in boosting efficiency and scalability while upholding compliance. By automating compliance checks, organizations streamline workflow processes, minimize manual interventions, and ensure consistency in meeting regulatory obligations.

Looking ahead, there is a need for further exploration and development in this realm to explore additional avenues for enhancing compliance in cloud-based AI/ML workflows. This involves delving into advanced techniques for automated compliance monitoring, integrating real-time anomaly detection, and leveraging machine learning algorithms for predictive compliance analysis.

In summary, our research contributes to ongoing endeavors aimed at fortifying compliance practices in cloud-based AI/ML workflows. This enhancement empowers organizations to fully leverage the potential of these technologies while effectively managing associated risks.

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