ISSN: 3006-4023 (Online), Vol. 1, Issue 1
Journal of Artificial Intelligence General Science (JAIGS)

journal homepage: **https://jaigs.org/index.php/JAIGS**

Cybersecurity Threat Detection using Machine Learning and Network Analysis

Amaresh Kumar
Engineering Manager, John Deere, USA.

Abstract

Cybercriminals continually develop innovative strategies to confound and frustrate their victims, necessitating constant vigilance to protect the availability, confidentiality, and integrity of digital systems. Machine learning (ML) has emerged as a powerful technique for intelligent cyber analysis, enabling proactive defenses by studying recurring patterns of successful attacks. However, two significant drawbacks hinder the widespread adoption of ML in security analysis: high computing overheads and the need for specialized frameworks. This study aims to quantify the extent to which a hub can enhance ecosystem safety. Typical cyberattacks were executed on an Internet of Things (IoT) network within a smart house to validate the hub's efficacy. Furthermore, the resistance of the intrusion detection system (IDS) to adversarial machine learning (AML) attacks was investigated, where models are targeted with adversarial samples exploiting weaknesses in the pre-trained detector.

Keywords— Intrusion Detection Systems, Adversarial Machine Learning, Internet of Things, Cyber-Physical Systems.

Article Information:
Article history: Received: 01/01/2024 Accepted: 05/01/2024 Online: 22/01/2024 Published: 22/01/2024
Corresponding author: Amaresh Kumar

Introduction

Various terms such as "Internet of Things," "Cyber-Physical System," "Ubiquitous Computing," and "Pervasive Computing" are commonly used to refer to the ongoing automation trend. Despite their differences, these terms allude to different aspects of system automation. In the realm of automation, the adoption of Cyber-Physical Systems (CPS) is rapidly becoming standard practice [1]. CPS involves converting an existing physical system into a computerized one by incorporating diverse hardware and software components, along with predefined operational procedures. Through CPS, even rudimentary instruments can emulate sophisticated technology. However, traditional electronic devices often have limitations such as restricted data processing capabilities, high power consumption, and limited storage capacity. A new generation of electronic systems is currently under development, aiming to integrate computational processes with physical systems. This integration forms the core concept of CPS.

Computational algorithms are computer programs designed to perform various functions when executed on a computer. They enable computers connected to a network to control and monitor a wide range of distinct physical processes simultaneously, facilitating the creation of automated technologies that require fewer operators [2]. This reduces the likelihood of system failures caused by individual users. Examples of smart technology include "smart" devices, buildings, and automobiles. In the context of Cyber-Physical Systems (CPS), the Internet of Things (IoT) serves as the driving force behind the advancement of the global economy. It finds application in the development of "smart" homes and urban environments.

CPSs have garnered attention as versatile means of performing tasks across various domains, including power grids, industrial automation, transportation systems, military, and healthcare equipment [3-7]. Given their integration with these systems, disruptions or damages to CPSs could potentially have far-reaching effects on a nation's economy, public health, or data security. These effects could lead to significant societal impacts.

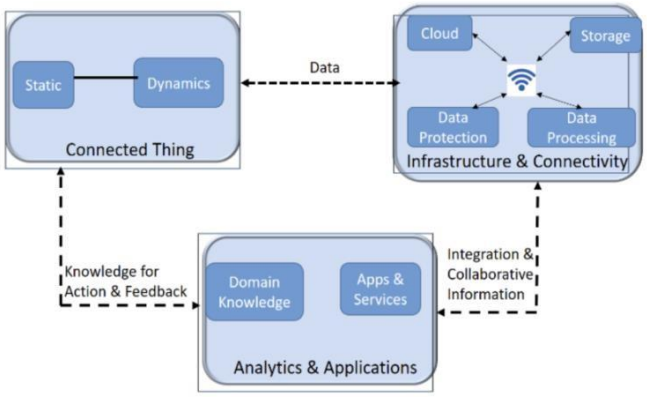
As the deployment of Cyber-Physical Systems (CPSs) becomes more prevalent, spanning international borders, the risk of cyber attacks targeting these systems increases. Therefore, it is crucial to develop robust countermeasures against a wide array of potential security vulnerabilities to safeguard CPSs. Security measures must be implemented across all levels of the organizational structure of CPSs, from the most basic components to the most advanced ones, to protect critical infrastructure from cyber threats.

CPSs offer valuable features such as remote control and management, self-organization, environmental sensing, location data sharing, and sensor data monitoring, making them indispensable in various contexts. With major nations investing in IoT-based projects to enhance citizen welfare and elevate living standards, the global market for CPSs is thriving. CPS applications span diverse domains, including renewable energy, electric vehicles, healthcare, government, infrastructure, smart homes, and more. Initiatives like India's smart cities project, launched in 2015, underscore the growing momentum of smart city initiatives worldwide. However, security concerns, including privacy, authenticity, and access control, along with interoperability challenges among existing technologies, pose significant technical hurdles to the widespread adoption of CPS initiatives in future smart cities.

Machine learning (ML) offers a solution to complex problems where conventional programming approaches fall short. ML enhances computer-human interaction by enabling problem-solving in areas where custom-built algorithms are impractical. ML algorithms learn from examples of correct behavior, serving as meta-algorithms for generating algorithms based on desired outputs. This approach streamlines computer interaction, requiring users to provide data for computation rather than explicit procedures.

The study of ML not only expands the range of problems that computers can solve but also deepens our understanding of learning processes. ML research delves into the computational foundations of learning, informing our comprehension of the brain's workings and inspiring novel ML model designs. It bridges the gap between computation and learning, offering insights into practical challenges and making a meaningful impact on society. ML methods hold promise for addressing numerous practical and commercial challenges, driving advancements in various domains.

Through systematic research, we can uncover the strengths and weaknesses of existing frameworks and identify key problem features, paving the way for innovative solutions to pressing issues.



Literature Review

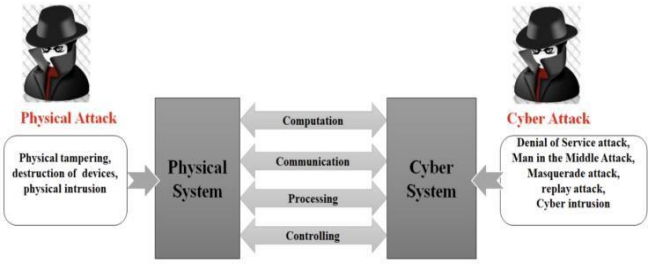
The cyber-physical system (CPS) integrates both digital and physical domains, facilitating communication, computation, and control between the cyber and physical systems. As depicted in Figure 2, this interconnectedness renders CPS vulnerable to both cyber and physical attacks.

Physical attacks target the physical infrastructure and control systems of CPS, ranging from sabotage of equipment to unauthorized access within facilities. Attackers exploit vulnerabilities to manipulate the underlying architecture, such as providing uncontrolled voltage flow to disrupt hardware functionality. For instance, attackers may tamper with environment-based sensor devices, like temperature sensors, leading to malfunctions in the CPS processing units.

In the cyber domain, various types of attacks pose threats to CPS, including denial of service (DoS), man-in-the-middle, masquerade, replay attacks, and cyber intrusions. Cyber attacks involve unauthorized nodes infiltrating networks and assuming trusted identities, compromising CPS hardware, software, networks, and data.

Physical security is paramount for CPS, necessitating stringent measures to safeguard data, devices, and networks. Access control, monitoring, and testing serve as cornerstones of physical security. Access control restricts resource access to authorized individuals, thereby bolstering cyber defenses by preventing unauthorized access. Surveillance plays a crucial role in incident prevention and response, enabling the detection of malicious activities within networks. Additionally, physical security facilitates damage control in the event of an attack, serving as both a preventive measure and an emergency response system.

To enhance CPS security, comprehensive network security assessments are essential to identify and mitigate vulnerabilities effectively, thereby fortifying the system against potential intrusions. Identifying system weaknesses is critical for preemptive security measures and proactive defense strategies.



Methodology

This section introduces the future-oriented IoT attack detection method, termed Random Forest-Synthetic Minority Over Sampling (RF-SMOTE). The RF algorithm constructs each tree using a bootstrap sample of the initial training data, as outlined by its developers. When presented with an information vector, RF traverses each tree in the forest to fulfill the order, with the connection strength diminishing as the number of trees (m) decreases. Demonstrating superior efficiency and accuracy over simple decision tree calculations, RF can handle large datasets without overfitting, even when dealing with seemingly irrelevant data.

In scenarios where classification orders lack consistency across a dataset, resulting in data imbalance, RF, like other classifiers, may encounter challenges. To mitigate errors in classification, the RF algorithm was refined to address data imbalances. Notably, RF prioritizes accuracy in predictions for the majority class, potentially leaving the minority class with less accurate predictions.

The oversampling mechanism in RF-SMOTE adjusts the number of random selections from the k nearest neighbors, generating synthetic instances by calculating the difference between the viable case vector and its nearest neighbor vector and then scaling this difference by a random value between 0 and 1 before incorporating it into the existing feature vector.

The proposed RF-SMOTE model comprises four phases: data collection, data analysis, segmentation, and threat or attack recognition. Figure 3 visually summarizes the RF-SMOTE model, illustrating its workflow and key components.

In general, the N-BaIoT and NSL-KDD datasets, extensively employed in the Internet of Things domain, serve as the foundational data sources for our study. The N-BaIoT dataset, a multivariate and sequential dataset, comprises 7,062,606 data points and encompasses 115 real-number attributes, including instances of attacks like Mirai, which pose challenges in classification and categorization.

After partitioning the data, we apply RF-SMOTE to classify the diverse types of traffic present in both datasets. RF, known for its efficacy in handling massive datasets, is favored for its utilization of high-quality data standards, generation of numerous decision trees (DTs), and assembly of these DTs into an ensemble for robust classification. The decision tree method prioritizes branches based on information gain and entropy values.

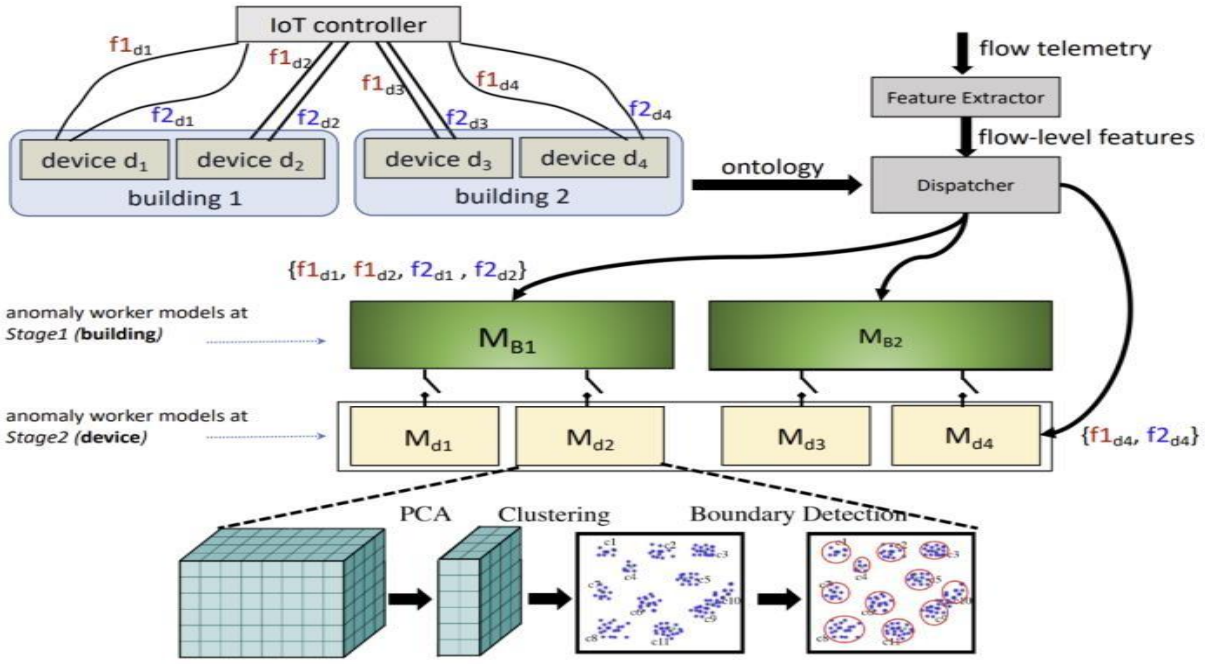
To address the task of detecting and identifying attacks on our Internet of Things (IoT) infrastructure, we develop a machine learning technique. This technique involves training our model with a benign traffic profile (a one-class classifier) for each IoT controller, subsequently flagging any deviations from the expected traffic patterns as

suspicious, as inferred from the system ontology. Figure 4 provides a high-level overview of our anomaly detection system's architecture, where models are trained at both the building level (Stage 1: Mbi) and the device level (Stage 2: Mdk) for each IoT controller.

Results and Analysis.

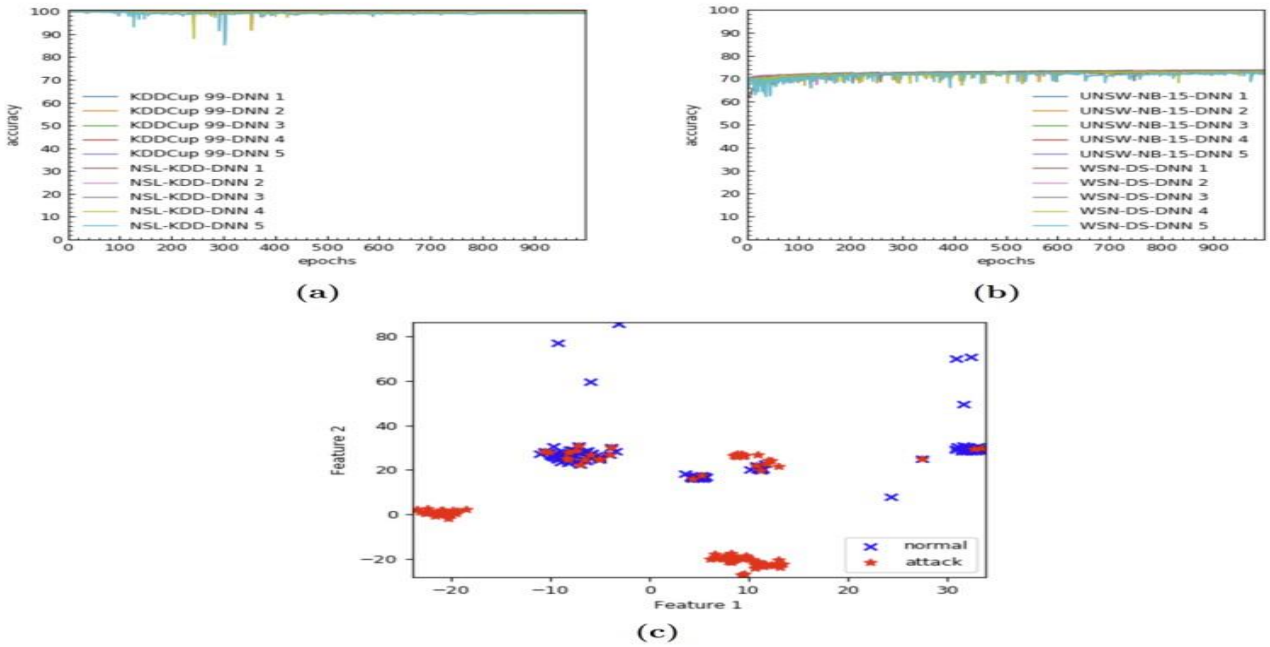
In this study, we introduce a novel approach to attack detection employing a new model architecture for Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS). This architecture comprises an input layer, five hidden layers, and an output layer. By leveraging the RF-SMOTE model in hierarchical layers, we enhance pattern detection in IDS data and effectively extract complex characteristics.

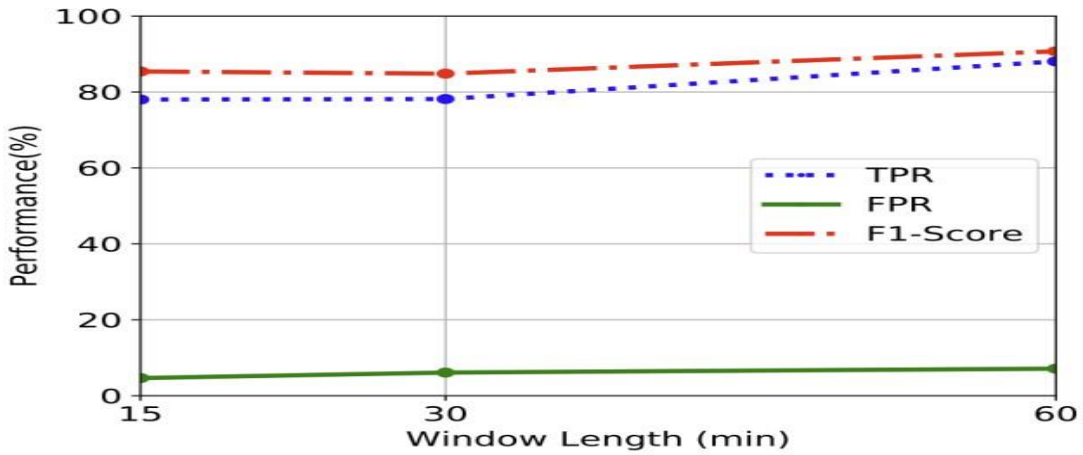
The RF-SMOTE model facilitates the progression of data from one layer to the next, with the final layer responsible for classification. Specifically, in the KDDCup 99 dataset, the input layer consists of 41 neurons, while in the NSL-KDD and UNSW-NB15 datasets, a similar configuration is utilized.



For the WSN-DS dataset, there are 17 neurons in the input layer, and for the CICIDS 2017 dataset, there are 77 neurons. In all datasets, the output layer consists of one neuron for binary classification and varying numbers for multiclass classification: five for KDDCup 99, five for NSL-KDD, ten for UNSW-NB15, five for WSN-DS, and eight for CICIDS 2017. The RF-SMOTE model is trained using backpropagation to enhance its learning capabilities. Typically, the units in the input layer are fully connected to the hidden layer, and similarly, the hidden layer is fully connected to the output layer.

Interestingly, despite achieving a similar overall accuracy of around 92%, feature-set-2 fails to detect attack instances entirely, highlighting the limitations of coarse-grained flow telemetry in accurately modeling network behaviors. Furthermore, feature-set-3 exhibits a lower True Positive Rate (TPR) compared to feature-set-1 (88.0%) and feature-set-2 (59.5%). Through our experimentation, we observed that feature-set-1 yields superior results for both attack detection and False Positive Rate (FPR). This superiority is attributed to feature-set-1's ability to capture more information from the timeseries waveform, enabling it to detect subtle variations in traffic volumes. In contrast, feature-set-2 lacks the capability to capture fine-grained behaviors, resulting in inferior performance. Additionally, when analyzing specific attacks, we found that feature-set-1 could detect all attack streams, albeit with a slight delay, particularly for early attack instances.





Conclusion:

The impetus behind this study stems from the recognition that IoT devices, despite their widespread integration into homes and Critical National Infrastructures (CNIs), pose significant security vulnerabilities, rendering them susceptible to various forms of cyber attacks. Often referred to as the "weakest link" in secure infrastructures, the ubiquitous nature of IoT devices within networks underscores the critical need for advanced methodologies to bolster the security of IoT systems. Furthermore, there is an urgent requirement for techniques to detect and mitigate cyber attacks targeting IoT networks, thereby mitigating their adverse impacts.

Traditionally, energy efficiency has not been a primary consideration in the design of Continuous Processing Systems (CPSs), which are frequently operated continuously. However, the proliferation of modern battery-operated devices within CPSs necessitates a shift towards long-term, low-energy consumption CPS solutions. Balancing the imperatives of security and energy efficiency in CPSs presents a significant challenge. Striking a harmonious balance between security and energy efficiency is complex, as enhancing security often comes at the expense of energy efficiency and increased operational costs.

In this paper, we propose a novel approach aimed at achieving a delicate equilibrium between energy savings and system security in CPSs. By addressing the intricate interplay between these priorities, our proposed approach endeavors to pave the way for the development of CPSs that are both resilient against cyber threats and energy-efficient, thereby contributing to the advancement of secure and sustainable technological ecosystems.

References

[1]. Ramírez, J. G. C. (2023). Incorporating Information Architecture (ia), Enterprise Engineering (ee) and Artificial Intelligence (ai) to Improve Business Plans for Small Businesses in the United States. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(1), 115-127.
DOI: https://doi.org/10.60087/jklst.vol2.n1.p127

[2]. Ramírez, J. G. C. (2024). AI in Healthcare: Revolutionizing Patient Care with Predictive Analytics and Decision Support Systems. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 31-37.
DOI: https://doi.org/10.60087/jaigs.v1i1.p37

[3]. Ramírez, J. G. C. (2024). Natural Language Processing Advancements: Breaking Barriers in Human-Computer Interaction. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 31-39.
DOI: https://doi.org/10.60087/jaigs.v3i1.63

[4]. Ramírez, J. G. C., & mafiqul Islam, M. (2024). Application of Artificial Intelligence in Practical Scenarios. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19.
DOI: https://doi.org/10.60087/jaigs.v2i1.41

[5]. Ramírez, J. G. C., & Islam, M. M. (2024). Utilizing Artificial Intelligence in Real-World Applications. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 14-19.

DOI: https://doi.org/10.60087/jaigs.v2i1.p19

[6]. Ramírez, J. G. C., Islam, M. M., & Even, A. I. H. (2024). Machine Learning Applications in Healthcare: Current Trends and Future Prospects. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1).
DOI: https://doi.org/10.60087/jaigs.v1i1.33

[7]. RAMIREZ, J. G. C. (2023). How Mobile Applications can improve Small Business Development. *Eigenpub Review of Science and Technology*, *7*(1), 291-305. **https://studies.eigenpub.com/index.php/erst/article/view/55**

[8]. RAMIREZ, J. G. C. (2023). From Autonomy to Accountability: Envisioning AI's Legal Personhood. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(9), 1-16.
https://researchberg.com/index.php/araic/article/view/183

[9]. Ramírez, J. G. C., Hassan, M., & Kamal, M. (2022). Applications of Artificial Intelligence Models for Computational Flow Dynamics and Droplet Microfluidics. *Journal of Sustainable Technologies and Infrastructure Planning*, *6*(12). https://publications.dlpress.org/index.php/JSTIP/article/view/70

[10]. Ramírez, J. G. C. (2022). Struggling Small Business in the US. The next challenge to economic

recovery. *International Journal of Business Intelligence and Big Data Analytics*, *5*(1), 81-91. https://research.tensorgate.org/index.php/IJBIBDA/article/view/99

[11]. Ramírez, J. G. C. (2021). Vibration Analysis with AI: Physics-Informed Neural Network Approach for Vortex-Induced Vibration. *International Journal of Responsible Artificial Intelligence*, *11*(3). https://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/77

[12]. Shuford, J. (2024). Interdisciplinary Perspectives: Fusing Artificial Intelligence with Environmental Science for Sustainable Solutions. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 1-12. **DOI:** https://doi.org/10.60087/jaigs.v1i1.p12

[13]. 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

[14]. 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

[15]. 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

[16]. 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

[17]. 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

[18]. 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

[19]. 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

[20]. 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

[21]. 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

[22]. 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

[23]. 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

[24]. 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. https://books.google.com.bd/books?hl=en&lr=&id=gtXzEAAAQBAJ&oi=fnd&pg=PA273&dq=Developing+a+Cognitive+Learning+and+Intelligent+Data+Analysis-Based+Framework+for+Early+Disease+Detection+and+Prevention+in+Younger+Adults+with+Fatigue&ots=wKUZk_Q0IG&sig=WDlXjvDmc77Q7lvXW9MxIh9Iz-Q&redir_esc=y#v=onepage&q=Developing%20a%20Cognitive%20Learning%20and%20Intelligent%20Data%20Analysis-Based%20Framework%20for%20Early%20Disease%20Detection%20and%20Prevention%20in%20Younger%20Adults%20with%20Fatigue&f=false

[25]. 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

[26]. 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

[27]. 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

[28]. 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**

[29]. 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

[30]. 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

[31]. 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

[32]. Islam, M. S., Ahsan, M. S., Rahman, M. K., & AminTanvir, F. (2023). Advancements in Battery Technology for Electric Vehicles: A Comprehensive Analysis of Recent Developments. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *2*(02), 01-28. https://globalmainstreamjournal.com/index.php/IEET/article/view/63

[33]. Ahsan, M. S., Tanvir, F. A., Rahman, M. K., Ahmed, M., & Islam, M. S. (2023). Integration of Electric Vehicles (EVs) with Electrical Grid and Impact on Smart Charging. *International Journal of Multidisciplinary Sciences and Arts*, *2*(2), 225-234. https://jurnal.itscience.org/index.php/ijmdsa/article/view/3322

[34]. Rahman, M. K., Tanvir, F. A., Islam, M. S., Ahsan, M. S., & Ahmed, M. (2024). Design and Implementation of Low-Cost Electric Vehicles (Evs) Supercharger: A Comprehensive Review. *arXiv preprint arXiv:2402.15728*.

https://doi.org/10.48550/arXiv.2402.15728