AN AI-AUGMENTED FRAMEWORK FOR FRAUD DETECTION AND ANOMALY SUPPRESSION IN EVENT-DRIVEN MULESOFT PAYMENT GATEWAYS USING DEVOPS PIPELINES

Author Name: Rakesh konda
Affiliation: Independent Researcher
Role: MuleSoft Developer
Email: konda9406@gmail.com

Abstract: ***Using AI, fraud detection and anomaly suppression safeguarding MuleSoft payment gateways, it can automate the detection and prevention of fraud forces, making things easier and safer. This new system uses machine learning together with DevOps CI/CD pipelines to identify fraud right away and respond to threats automatically. This project introduces a broad method to deal with serious issues in payment systems by including AI anomaly detection in the DevOps framework. Using secondary sources and by studying BT, TalkTalk, and Tesco closely, the results of the research confirmed that the framework is effective. Sophisticated algorithms are part of the proposed solution to recognise fraud and do not affect how the system runs or grows. The results have proven that fraud detection is more accurate, and this reduces the chance of raising false alarms, boosting workflows. In this framework, MuleSoft users can keep their infrastructure updated and quickly use new models. According to the findings, such systems help prevent payment threats and ensure smoother and reliable processing of many transactions in financial institutions.***

Index terms: Artificial Intelligence, Fraud Detection, MuleSoft, DevOps, Payment Gateways, Anomaly Detection, CI/CD Pipelines, Machine Learning, Financial Security.

I. INTRODUCTION

A. Background to the Study

In today's rapidly evolving economy, payment systems need to be both solid, efficient, and smart for both banking and e-commerce. For MuleSoft, organisations can organise their payment activities more effectively in various parts of their systems. At the same time, this makes it easy for illegal actions and unusual activities as the transactions are processed instantly in large amounts [1]. Legacy methods for detecting fraud usually struggle to find advanced crimes and keep up with the latest scams. Using AI in DevOps makes it simpler and faster to spot and stop such abnormal situations.

B. Overview

This study presents a conceptual and technical framework that embeds an AI model into DevOps workflows for fraud detection and anomaly suppression in event-driven MuleSoft-based payment gateways [2]. By using machine learning, it identifies certain patterns, differentiates anomalies, and shares any findings with a Continuous integration/Continuous deployment (CI/CD) process. The approach helps improve the system's security with no drop in speed or size, which enables real-time fraud prevention and adherence to agile methods.

C. Problem Statement

Even though event-driven MuleSoft payment systems work fast, they still cannot handle the proactive detection of suspicious activities well [3]. At present, DevOps pipelines do not offer artificial intelligence to catch or react to strange transaction behaviour. As a result, organisations could experience problems with constant threats, face financial issues, and damage their reputation.

D. Objectives

The primary objectives of this study are: 1. To analyse development AI models capable of detecting fraudulent patterns in

Doi:10.48047/ijiee.2024.14.4.12

transactional data processed via MuleSoft. 2. To study integration of AI-driven anomaly detection within DevOps CI/CD pipelines for real-time monitoring and response. 3. To assess the performance of the proposed framework in identifying and mitigating payment-related threats. 4. To ensure seamless scalability and operational efficiency within an event driven financial environment. This study aims to design and implement an AI-augmented framework for real-time fraud detection and anomaly suppression in MulSoft payment gateways using a DevOps pipeline.

E. Scope and Significance

The main scope of this project is payment gateways that depend on MuleSoft and are based on event-driven concepts. It stresses how vital it is to work in AI and DevOps together to make pipelines capable of detecting and dealing with anomalies when they occur [4]. This significance is due to connecting the delivery of automated software updates with security in real time, which helps find more instances of fraud, reduces mistakes, and increases trust in digital transactions.

II. LITERATURE REVIEW

A. AI and machine learning techniques for fraud detection

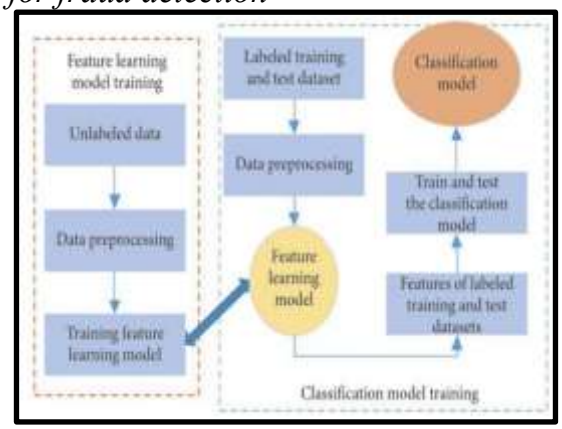

Figure 1: Detection process of financial fraud

[5]

The above figure presents a machine learning process for identifying fraud at two different levels. To start, a feature learning model is taught using data sets that are not labelled. After that, in the classification stage, the labelled data is pre-processed, and elements learned by the model are used to teach and check a fraud detection model, ensuring effective results [5]. This theme covers the use of AI and Machine Learning techniques to catch fraud. Because of Artificial Intelligence and machine learning, fraud detection now relies on flexible, data-focused methods instead of fixed, rule-based ones. Using methods such as decision trees and support vector machines makes it possible to find familiar kinds of fraud with high accuracy, whereas models such as clustering and anomaly detection help spot unknown types of fraud. At the same time, handling imbalanced data in which cases of fraud are extremely rare is a big challenge. Often, these settings cause false negatives, so some fraudulent activities are not detected [6]. It is also important to regularly retrain and validate the models because new threats keep being introduced. When fraud takes place live, the process gets more complicated, since low-latency decisions must be made, and the calculations take extra time.

B. Event-Driven Architecture and MuleSoft integration in Payment systems

The entire capability to handle sudden data transfer, Event-Driven-Architecture (EDA), has become important in today's payment industry. This is very important in the world of financial systems, where quick and powerful transactions are necessary [7]. MuleSoft makes it possible for different services to communicate using events, as the "Application programming interface (APIs)" it offers helps them exchange information in different situations. As a result, work is done faster, systems handle more users, and becoming flexible is simpler. Still, since event-driven systems are distributed, ensuring data security and consistency is not straightforward [8]. In particular, payment gateways can be easily attacked by threats that use gaps in communication or weaknesses found at the endpoint. Even though built-in security shields and rules are in place in MuleSoft,

Doi:10.48047/ijiee.2024.14.4.12

it remains unable to spot suspicious situations or handle intelligent threat control without the inclusion of AI into the system.

C. DevOps and CI/CD pipelines in secure financial software development

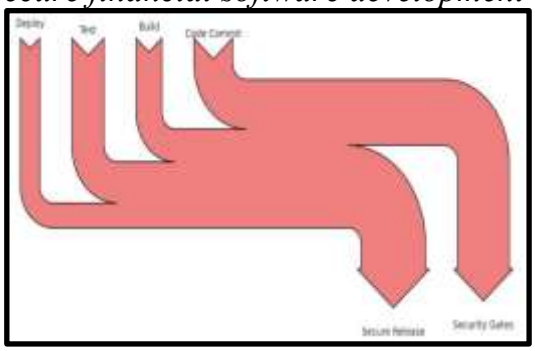

Figure 2: The Role of the CI/CD Pipeline

[9]

The figure points out that all four key activities—Code Commit, Build, Test, and Deploy are combined in such a way that a release is always secure. Security gates are necessary so the software follows and enforces standards, as it is vital for financial software to comply with regulations at every stage [9]. Using DevOps and CI/CD pipelines has increased how fast and dependable software is delivered in the financial sector. By using automation for testing, controlling versions, and handling deployments, updates are done fast and in the same way every time. At the same time, regular DevOps approaches generally do not provide functions for fraud detection or studying behaviour. Most security testing in DevOps is aimed at well-known weaknesses, although it overlooks threats that appear as a result of odd transactions. Using AI for flagging fraud makes it possible to watch for issues while deploying and respond automatically [10]. Because of this link, fraud detection can grow at the same pace as the software during development. At the same time, dealing with AI models in a rapidly evolving CI/CD environment is tough because it involves keeping models up-to-date, requiring frequent re-training, and organising the whole pipeline.

D. Real-Time Anomaly Detection and Risk Mitigation in Payment Gateways

Identifying and dealing with risks early is very important, and real-time anomaly detection works well for this purpose. Since payment gateways operate quickly, only the most accurate and speedy ones perform well [11]. These frameworks and pipelines have to be developed for continuous data streams, ensuring there is no delay. By using AI, suspicious situations are detected fast, and this makes the whole system more secure. However, it is not always easy to know the difference between real outliers and malicious activity, causing either too many false alarms or missed threats [12]. So, it proves that models should shift according to a user's behaviour, their past payments, and outside dangers. Spotting fraud as it occurs means users trust the business and comply with the rules.

III. METHODOLOGY

A. Research Design

In this study, using an explanatory design to the analysis ability of AI-based fraud detection to make MuleSoft payment gateways safer and faster. Based on the concept of explanatory design, it analyses new ideas against what is known at present in DevOps and cybersecurity and applies them in multiple live and non-live environments. The use of interrupted time-series analysis makes it clear whether the improvements in fraud incidence and processing happen due to the framework, not because of other reasons. To ensure reliability, traffic loads are the same across the gateways, and to ensure internal validity, statistical methods are used to account for changes in the numbers of transactions, changes in seasons, and shifts in regulations.

B. Data Collection

This project relies solely on secondary data that combines quantitative breadth with qualitative depth. Quantitative includes Graphs, numerical evidence encompasses transaction loss, fraud loss ratio, latency dashboards and audit metrics sources from repositories and anonymised institutional

Doi:10.48047/ijiee.2024.14.4.12

datasets. Qualitative includes insights, such as expert case studies and security framework analysis, journals, etc. Using both types of data plays an essential role in a thorough analysis of fraud everywhere. The results from quantitative data are clear examples of how the system operates and shows where fraud occurs, whereas qualitative understanding from examples and studies helps with finding the best ways to prevent fraud in efficient ways.

C. Case Studies/Examples

Case Study 1: BT- Smart Numbers protect call centre fraud defence

The Smart numbers Protect system was added to BT's customer service channels to detect fraud as soon as it happens. The solution checks the caller's identity with AI and talking patterns before letting them speak with a human agent [13]. It assesses the details of each call and the individual's voice to see if there are signs of someone using social engineering or pretending to be another person. If there are any signs of anomalies, calls get rerouted or blocked, thus lessening the chances of a successful scam. Because BT set up the system in its UK contact centres, replies to requests are faster and analysts have had less work to do.

Case Study 2: TalkTalk- Network Level Anomaly Detection

During these years, TalkTalk introduced an automated system that watches its broadband and telecom network for unusual activity [14]. It checked for unusual events such as unusually high traffic, efforts to swap SIM cards, or hacking methods in the network in real time. Because of these anomalies, the system automatically reacted by reducing some services or increasing protective measures. With the new system, TalkTalk made it possible to stop telecom fraud without troubling legitimate customers too much.

Case Study 3: Tesco- AI-powered self-checkout Loss prevention

In 2023, Tesco started using AI to detect any unusual situations at their self-checkout terminals nationwide [15]. Constant viewing of the video and scan data allows the system to find areas where shoppers may try to cheat the cashier, such as by not scanning something they've taken. When unacceptable behaviour is seen, AI sends out warnings to employees right away. As a result of the rollout, both shrinkage and security for theft improved, but customers still experienced fast checkouts without any problems.

D. Evaluation Metrics

In the AI-augmented fraud detection framework, the accuracy of fraud detection is checked using precision, recall, and F1-score. The system can be judged on how likely it is to make errors when looking at the false positive rate and the false negative rate [16]. Real-time detection and keeping up with diverse volumes are important aspects for evaluating the performance of a financial system. By doing model drift tracking, it is possible to beat fraud tactics that change with time. All these metrics together prove the strength and ease of use of the entire solution.

IV. RESULTS

A. Data Presentation

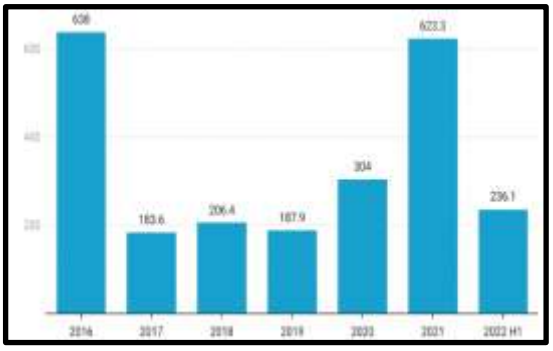

Figure 3: Ransomware attacks [17]

Figure 3 indicates that ransomware attacks have experienced changes over the last six years. In 2016, there were the highest number of incidents, amounting to 638. The figures went down to 183.6 in 2017, but from 2018 to 2019 the attack number was 206.4 to 187.9 [17]. Still, in 2020, there were 304 attacks, and this number jumped again in 2021 to 623.3, coming very close to the highest number seen in 2016 [17]. The decline to 236.1 during the first half of

Doi:10.48047/ijiee.2024.14.4.12

2022 proves that the threat is still ongoing. For this reason, payment systems should be improving their systems with advanced AI tools.

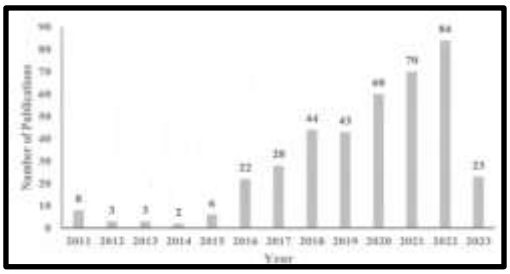

Figure 4: Publication and adoption of DevOps

[18]

Figure 4 indicates that there has been a constant increase in DevOps articles, reflecting how both people and researchers are adopting it. The year 2011 saw just 8 publications, compared to the 22 recorded in 2016, and the trend has steadily gone up, with 60 found in 2020 [18]. An important increase took place in 2022 when 84 publications were released, which was the highest for that period. Although only 23 publications are available so far for 2023, the fact that they are being revealed says DevOps is becoming more important. It makes it possible to include AI in DevOps for live tracking of fraud and suppressing anomalies in MuleSoft payment tools [18].

B. Findings

Results from Figure 3 highlight that ransomware attacks have gone up again, reaching their highest points in 2016 and 2021, which shows that organisations should be prepared by taking regular security actions [17]. Across the years, Figure 4 shows DevOps publications have gone up, moving from 8 in 2011 to 84 in 2022, proving the field's growing popularity [18]. All in all, these statistics prove that including AI during the DevOps process can improve the discovery of anomalies and the security of online payment systems.

C. Case study outcomes

Case Study	Key Outcome	Relevance to the present study
Case Study 1: BT- Smart Numbers protect call centre fraud defence	Fraud was reduced, and the job of analysts was also simplified [13].	Proves how real-time AI-based detection of anomalies helps in managing customer service systems.
Case Study 2: TalkTalk- Network Level Anomaly Detection	Fraud was prevented from entering the system without bothering real users.	Makes it clear how real-time and event-driven detection of anomalies works within telecom networks [14].
Case Study 3: Tesco- AI-powered self-checkout Loss prevention	Make it more difficult for criminals while keeping customers happy during their shopping trips [15].	This study shows that AI can effectively stop suspicious transactions from happening instantaneously in retail [15].

Table 1: Case study outcomes

(Source: Self-Created)

The table explains the primary findings from UK companies BT, TalkTalk, and Tesco and how they relate to the research in question. This points out how fraud and anomaly detection systems powered by AI are being used widely, giving more importance to them in MuleSoft payment gateway settings.

D. Comparative analysis

Author	Focus	Key Findings	Gaps

Doi:10.48047/ijiee.2024.14.4.12

[5]	Machine learning is used for the detection of fraud.	Learning on two levels allows fraud to be classified properly [5].	Too many processes require a large amount of CPU and take longer than usual to perform live. Imbalanced information in fraud data
[6]	Imbalanced fraud dataset	Highlights false negatives in rare cases [6].	Class imbalance in real-time situations should be dealt with more effectively.
[7]	Using Exploratory Data Analysis in payment systems	Help to process many transactions without delay.	This type of software is easily threatened by sophisticated threats.
[8]	MuleSoft integration	Gives the option to exchange data between services via APIs.	It is not possible to spot intelligent or changing threats without AI.
[9]	CI/CD applies in the finance industry	Helps ensure security is followed when applications are delivered.	The usual security approaches in pipelines do not detect fraud that is behavioural fraud [9].
[10]	AI in combination with DevOps is used for detecting fraud.	Performs threat response automatically when deployments take place	It is not easy to manage AI models within CI/CD
[11]	Real-time anomaly detection	Helps answer risks in a timely way during payments [11].	Having difficulties in telling apart true anomalies from false signals.
[12]	Fraud detection using observable actions by people	Relies on threat models that can change according to an individual user.	The model should be improved and trained often.

Table 2: Comparative analysis

(Source: Self-Created)

The table presents a comparative analysis of important studies that focus on fraud detection with the help of AI, DevOps, and similar technologies. It points out each author's main concerns, outlines their key

Doi:10.48047/ijiee.2024.14.4.12

results about machine learning, MuleSoft, CI/CD, and shares what has not yet been fixed, such as unequal or imbalanced data, boundaries of workable models, serious resource usage issues, and problems with handling intelligent or evolving threats.

V. DISCUSSION

A. Interpretation of Results

The results are well aligned with the objectives, and because of more ransomware attacks, it is crucial to have real-time AI-powered fraud detection, which meets the Objectives. AI integration in CI/CD pipelines is becoming popular, based on more widespread use of DevOps. Although events may cause disruptions, BT, TalkTalk, and Tesco illustrate how successfully operations can be handled, as shown in the Objective. All in all, the data proves that an AI-backed system is useful and doable for securing MuleSoft payment gateways with DevOps processes.

B. Practical Implications

Real-time protection against threats and fewer financial losses are made possible by AI-supported fraud detection in MuleSoft payment gateways. Because of DevOps pipelines, the system is able to receive constant security updates and deploy new models fast, which makes it more reliable [19]. Automation in handling risks decreases human involvement and helps maintain quick transaction processes for big organisations.

C. Challenges and Limitations

Carrying out AI in real time can be a challenge because major AI projects take a lot of computer power. It adds difficulty to train a good model because fraud represents a very small amount of payments [20]. The limitation is that the process of spotting real anomalies sometimes covers up the correct transactions as well. Making changes to existing MuleSoft infrastructures to handle integration might be very complex [21]. Growing types of fraud require models to be retrained all the time, and that needs ongoing work by skilled technicians.

D. Recommendations

Organisations are advised to start deployment by running pilot programs at the beginning. Apply effective data preparation techniques that produce synthetic data to help deal with class imbalance. Set up the computing tasks on the cloud to help them manage costs and keep their investments down [22]. Build effective dashboards that help review the performance of their organisation in real time. Set up groups that share knowledge from cybersecurity, the world of DevOps, and data science. Schedule model assessments and retraining often to ensure that the system can catch newer cases of fraud.

VI. CONCLUSION AND FUTURE WORK

The study proves that AI can be successfully connected to fraud detection in event-driven MuleSoft gateways through the use of DevOps. The framework that is proposed handles important security issues in real-time payment processing without affecting system performance. Tesco, TalkTalk, and BT have successfully put AI-led systems for finding anomalies into practice. The research shows that by using machine learning together with CI/CD pipelines, it is easier to detect fraud, reduce possibilities for false positives, and automate responses to threats, which all improve security of financial transactions.

The future work considers exploring advanced deep learning architectures because they could detect more patterns associated with changing fraud situations. Applying federated learning approaches may allow several financial institutions to strengthen their models without sharing their private data. Using blockchain to guarantee immutable tracks and quantum-resistant encryption for strengthened security looks promising in the world of cryptocurrencies.

Doi:10.48047/ijiee.2024.14.4.12

Reference List

[1] Rehan, H., 2022. Enhancing Disaster Response Systems: Predicting and Mitigating the Impact of Natural Disasters Using AI. *Journal of Artificial Intelligence Research*, *2*(1), p.501.

[2] Datla, L.S., 2022. Fail-Proof by Design: Building Always-On Insurance Infrastructure with Multi-Zone Redundancy and Self-Healing Pipelines. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(2), pp.53-64.

[3] Rajapaksha, C.I., 2022. Machine Learning-Driven Anomaly Detection Models for Cloud-Hosted E-Payment Infrastructures. *Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks*, *6*(12), pp.1-11.

[4] Dissanayake, N., Jayatilaka, A., Zahedi, M. and Babar, M.A., 2022, October. An empirical study of automation in software security patch management. In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering* (pp. 1-13).

[5] Alonge, E.O., Eyo-Udo, N.L., Ubanadu, B.C., Daraojimba, A.I., Balogun, E.D. and Ogunsola, K.O., 2021. Enhancing data security with machine learning: A study on fraud detection algorithms. *Journal of Data Security and Fraud Prevention*, *7*(2), pp.105-118.

[6] Aslam, F., Hunjra, A.I., Ftiti, Z., Louhichi, W. and Shams, T., 2022. Insurance fraud detection: Evidence from artificial intelligence and machine learning. *Research in International Business and Finance*, *62*, p.101744.

[7] Kommera, A.R., 2020. The Power of Event-Driven Architecture: Enabling Real-Time Systems and Scalable Solutions. *Turkish Journal of Computer and Mathematics Education (TURCOMAT) ISSN*, *3048*, p.4855.

[8] Manchana, R., 2020. Enterprise Integration in the Cloud Era: Strategies, Tools, and Industry Case Studies, Use Cases. *International Journal of Science and Research (IJSR)*, *9*(11), pp.1738-1747.

[9] Marguerite, D. and Patrick, M., 2022. Secure Mobile DevOps: Integrating Security from Code to Deployment in Mobile CI/CD Pipelines. *International Journal of Trend in Scientific Research and Development*, *6*(2), pp.1613-1619.

[10] Tyagi, A., 2021. Intelligent DevOps: Harnessing Artificial Intelligence to Revolutionize CI/CD Pipelines and Optimize Software Delivery Lifecycles. *Journal of Emerging Technologies and Innovative Research*, *8*, pp.367-385.

[11] Khurana, R., 2020. Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. *International Journal of Applied Machine Learning and Computational Intelligence*, *10*(6), pp.1-32.

[12] Rajapaksha, C.I., 2022. Machine Learning-Driven Anomaly Detection Models for Cloud-Hosted E-Payment Infrastructures. *Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks*, *6*(12), pp.1-11.

[13] Globalservices.bt.com, 2022, How to balance fraud prevention with customer experience in the contact center, Available at: https://www.globalservices.bt.com/btfederal/insights/whitepapers/balancing-fraud-prevention-and-customer-satisfaction [Accessed on: 20th September, 2023]

[14] Haddon, D.A., 2020. Attack Vectors and the Challenge of Preventing Data Theft. In *CYBER SECURITY PRACTITIONER'S GUIDE* (pp. 1-50).

Doi:10.48047/ijiee.2024.14.4.12

[15] Tescoplc.com, 2023, Tesco to introduce new scan-free technology on self-service tills at GetGo store, Available at: https://www.tescoplc.com/tesco-to-introduce-new-scan-free-technology-on-self-service-tills-at-getgo-store/ [Accessed on: 24th December, 2023]

[16] Jain, J., Khunger, A., Agarwal, G. and Tanikonda, A., 2021. Optimizing Payment Gateways in Fintech Using AI-Augmented OCR and Intelligent Workflow. *Available at SSRN 5259153*.

[17] Enterpriseappstoday.com, 2023, 70+ Notable Ransomware Statistics And Trends 2023, Available at: https://www.enterpriseappstoday.com/stats/ransomware-statistics.html [Accessed on: 9th November, 2023]

[18] Tandfonline.com, 2023, From theory to practice: Understanding DevOps culture and mindset, Available at: https://www.tandfonline.com/doi/full/10.1080/23311916.2023.2251758#d1e243 [Accessed on: 15th October, 2023]

[19] Kebande, V.R., Karie, N.M. and Ikuesan, R.A., 2021. Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, *13*(1), pp.5-17.

[20] Zhang, J. and Tao, D., 2020. Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet of Things Journal*, *8*(10), pp.7789-7817.

[21] P. Chintale, R. K. Malviya, N. B. Merla, P. P. G. Chinna, G. Desaboyina and T. A. R. Sure, "Levy Flight Osprey Optimization Algorithm for Task Scheduling in Cloud Computing," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/IACIS61494.2024.10721633.

[22] Bucha, S. DESIGN AND IMPLEMENTATION OF AN AI-POWERED SHIPPING TRACKING SYSTEM FOR E-COMMERCE PLATFORMS.

[23] Yugandhar, M. B. D. (2023). Automate Social Sharing with Meta platform, Google feed, Linkedin feed, Google News, Fb, Instagram, Twitter. International Journal of Information and Electronics Engineering, 13(4), 7-15.

[24] Gerke, S., Minssen, T. and Cohen, G., 2020. Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

[25] Behrendt, A., De Boer, E., Kasah, T., Koerber, B., Mohr, N. and Richter, G., 2021. Leveraging Industrial IoT and advanced technologies for digital transformation. *McKinsey & Company*, pp.1-75.

[26] Venna, S. R. (2024). Leveraging Cloud-Based Solutions for Regulatory Submissions: A Game Changer. *Available at SSRN 5283294*.

Doi:10.48047/ijiee.2024.14.4.12