Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-1 || January 2023 || PP. 139-149 https://doi.org/10.55544/ijrah.3.1.25

Detecting android malware and Prevention Using Supervised Learning

Dr. K. Khan
Associate Professor, Jabalpur University, INDIA

www.ijrah.com || Vol. 3 No. 1 (2023): January Issue

Date of Submission: 05-01-2023	**Date of Acceptance:** 21-01-2023	**Date of Publication:** 31-01-2023

ABSTRACT

The Android smartphone's growth may be attributed to the phone's open-source design and high performance. Malware has been created partially because of Android's widespread use. When it comes to smartphones, Android is the most popular OS. That's why there's so much malicious software aimed at this system. Malicious software may be identified as such by analyzing its permission attributes. But this is a complex issue to solve. In this research, we use a golden jackal optimized support vector machine (GJOSVM) to classify software and evaluate whether or not it presents a threat. To achieve this goal, a dataset including 2850 sections of malicious software and 2866 sections of benign software was generated. Each piece of software in the dataset has 112 permission characteristics, and there is also a class feature that indicates whether or not the program is harmful. Each phase of the training and testing procedures used 10-fold cross-validation. The effectiveness of the models was measured using accuracy, F-1 Score, precision, and recall.

Keywords- android mobiles, detecting malware, golden jackal optimized support vector machine (GJOSVM), Android Package files (APK).

I. INTRODUCTION

Malware is a significant danger to the cyber security of ournation's critical infrastructure, our service industries, and our entire civilization. Smartphones and tablets have exploded in popularity in recent years, and now they're powerful enough to replace many desktop computers' functions. Applications for usage on such gadgets have been developed by a wide range of entities, such as government and banking institutions [1]. Most of our most private and essential documents are now saved on the cloud, and we can view them from anywhere with a mobiledevice. Malware developers have taken note of this trend. Droid Dream, an aspect of Android malware found in over 50 apps on the official Android market, is only one example of many established incidents of Android malware. The built-in security measures of Android are essentially inadequate, and data may be leaked by even benign apps. Smartphones often serve as a repository for sensitive information, including photographs, text messages, and login passwords [2]. This makes them an easy target for bad actors. Smartphones using Google's Android OS are the market leaders. Android devices, however, account for roughly 97% of malware. The fact that practically every transaction that can be completed ona computer can now be completed on a mobile device isthe driving force behind these advancements, and it is also the fundamental reason why they have occurred. At the very beginning of choice for mobile devices are the dimensions, as well as the benefits that come with the measurements at the point where transportation is concerned [3].

As processing capabilities have increased and as interest in gadgets has grown, it has gained a lot of traction among attackers. Attackers will almost always target sites that are of very high interest to a large number of people. In the digital age, if a specific person or organization is not targeted, the objective is to spread the malware to the most significant number of users possible. When looking at the mobile OSs that are used all over the globe, the two that stand out as the most popular are Android and iOS [4]. Other OSs have a consumption rate that is just 1.7% of the total, in contrast to these two OSs, which account for 98.3% of the entire usage in the globe. The number one spot goes to the Android OS, which has a use rate of 70 percent, while the number two spot goes to the iOS OS, which has a rate of 28.3 percent. Machine learning algorithms have become particularly significant inareas

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-1 || January 2023 || PP. 139-149 https://doi.org/10.55544/ijrah.3.1.25

where antivirus software is inadequate to guarantee that mobile platforms, which can run software that is becoming more complicated, may become better protected against harmful software [5]. This is because mobile platforms can run software that is becoming increasingly complex. Based on authorizations and API requests, and even though these methods gather conversations between applications on smartphones and Android systems, any interaction that occurs within the applicable limitations isn't considered in the assessment. As a result, it is not enough to detect malicious software that is not asking for suspicious resources. Malware assaults have so spread to mobile devices, making it imperative that we take measures to secure our mobile infrastructure [6]. In this work, a golden jackal-optimized support vector machine is employed to find malicious Android phone attacks. The results of our experiments prove that our technique successfully identifies Android malware.

The rest of the sections of the paper are structured asfollows. In Section 2, we give a literature review on similarefforts in Android malware detection. Our detection system, including the feature extraction method, is described fully in Section 3. In Section 4, we detail the experiment and its findings. Finally, we conclude the task in Section 5.

II. RELATED WORK

They build the link between the permission and API usinga machine learning technique to detect malware by mining the patterns of approval and API function calls obtained and utilized by Android applications. Despite this, the harmful samples they have gathered are not sufficient [7]. A framework for feature-based learning that focuses on thebehaviors of requested permissions and API requests and that applies the SVM, Decision Tree, and Bagging algorithms. However, they only extract authorization and API as features, which leads to a poor level of accuracy since they only remove a few different kinds of characteristics [8]. Despite this, research on mobile malware is still in its infant stage. The methods that are now available to identify mobile malware and other flaws in security have varied degrees of both strengths and drawbacks [9]. The random forest algorithm uses threedistinct feature selection methods. The effects of implementing three alternative feature selection methods effective, high weight and effective group feature selectionare evaluated. Applying feature selection approaches improves accuracy regarding metrics and needed time, according to experiments on the Drebin dataset [10]. They employed an evolutionary algorithm to find Android smartphone malware. They contrasted our system with several cutting-edge algorithms to assess it. Finally, their suggested strategy can detect zero-day malware [11]. Numerous ML-based methods for detecting malware on Android have been presented. Multiple difficulties arise from ignorance of the technologies available for detecting malware on Android devices [12]. Additionally, to ensure device compatibility, authorization, and hardware characteristics are simultaneously stated in the manifest file of an application (app). To characterize applications, we extract permissions, API requests, and hardwarecharacteristics [13]. The TANMAD algorithm, a two-step Android malware detection method, first narrows the potential malware families to be detected before using sub- graph isomorphism matching. The modeling of object reference information by creating directed graphs, or ORGB, is the main innovation of their study [14].

III. METHODOLOGY

The main goal is to create a classifier that, for the most part, classifies training data as positive and only labels training or testing data as negative when it sufficiently deviates from training data. Given that innocuous Android apps are far simpler to find than malicious ones, it will be the perfect choice for our purposes. The antivirus software business known as Zeman gave us the files that are included in the dataset so that we may do this research. To extract functionality from pre-packaged Android apps (APKs), we use an open-source project known as Androguard. Our study's suggested flow is shown in figure 1.

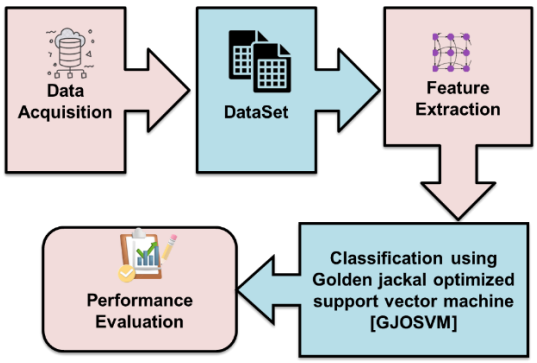

Fig. 1. Flow of GJOSVM

Data Acquisition and Dataset

There are 2870 legitimate apps and 2854 malicious ones in the newly produced dataset. Virus Total and Virus Share have verified the presence of harmful and non-malicious Android apps in this dataset [15]. This information cannot be downloaded by any user, which defeats the purpose of the infection. Due to the sensitive nature of the work that will be performed via the use of the corporate e-mail account, specific authorization for harmful software has been secured by corresponding with the proprietors of this website through e-mail. The whole collection consists entirely of binary information. A value of 0 for any of the 117 characteristics implies that the program does not seek authorization for the feature in question, whereas a value of 1 indicates that it does. A

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-1 || January 2023 || PP. 139-149 https://doi.org/10.55544/ijrah.3.1.25

value of 0 for this classattribute implies that the program is safe, whereas a value of one indicates that it is malicious. The apps' access controls are shown in Table 1.

Table 1. Features of Android APK authorization

internet	use_credentials	keep_screen_on	write_external_storage
mount_format_filesystems	broadcast_sms	read_owner_data	read_phone_state
mount_unmount_filesystems	read_sync_settings	write_sync_settings	get_tasks
access_fine_location	access_all_downloads	write_internal_storage	camera
flashlight	baidu_location_service	write_contacts	vibrate
wake_lock	battery_status	broadcast_wap_pushf	disable_keyguard
get_accounts	expand_status_bar	write_apn_settings	change_network_state
battery_stats	ua_data	modify_phone_state	bluetooth
restart_packages	access_coarse_updates	read_messaging_extension_data	nfc
bind_accessibility_service	send_messages	bind_remoteviews	get_package_size
kill_background_processes	interact_across_users_full	install_packages	bluetooth_admin
raised_thread_priority	authenticate_accounts	set_debug_app	access_superuser
bind_input_method	network_state	clear_app_cache	broadcast_wap_push
reorder_tasks	get_contacts	send_respond_via_message	receive_wap_push
persistent_activity	wake_lockc	read_logs	cd_messagel
access_location_extra_com.	manage_accounts	write_secure_settings	vibrategcmgs
read_contacts	flashlightghardware_c.	write_call_log	receive_boot_completed
receive_sms	change_wifi_state	read_datagpersonal_infol	access_wifi_state
read_sms	write_media_storage	delete_packages	send_sms
call_phone	bind_wallpaperturb	cd_message	system_alert_window
write_sms	connectivity_internal	hardware_test	set_wallpaper
set_wallpaper_hints	read_call_log	location	modify_audio_settings
record_audio	access_mock_location	change_wifi_multicast_state	read_calendar
broadcast_sticky	signal_persistent_processes	ua_datal	bind_vpn_service
maps_receivel	internetgcmg	bind_print_service	bind_notification_listener_service
process_outgoing_calls	change_configuration	receive_user_present	bind_device_admin
bind_wallpaper	read_profile	write_profile	access_network_state
read_external_storage	receive_mms	network	read_settings
write_settings	set_activity_watcher	access_download_manager	access_coarse_location

Feature Extraction

To successfully implement any kernel, we must first isolatethe most crucial aspects of the application. APK files, the standard format for Android application packaging, are quite similar to ordinary Java jar files. To process these files and extract features, we use the open-source software Androguard. Androguard has a user interface that is not too complicated and may be used to do analysis and reverse engineering on Android apps.

Every APK requires a manifest file that, among other things, requests authorization to access specific protected components of the Android OS. Accessibility for various hardware devices, sensitive aspects of the OS, and specific sensitive features of other programs are all included inthese pieces. For instance,the "android.permission.INTERNET" permission demands the ability to access the Internet, but the "android.permission.READ CONTACTS" permission desires the ability to read the mobile contacts database of the user.

After we have obtained the list of rights that are being sought, we split it into two categories: built-in permissions that are considered standard and permissions that are not regarded as standard. We build a binary vector for legal permissions, and each item corresponds to a built-in permission. The entry is given a value of 1 if the program wants that permission and a value of 0 if it does not seek that permission. In the case of non-standard permissions, we break the strings up into three sections: the prefix (which is often "com" or "org"), the portion containing the organization and product, and the permission name itself. We don't pay attention to any instances of the phrases"android" or "permission" since they are so common.

k-Fold Cross-validation

The technique for segmenting the data set that is utilizedfor training the model through executing the calculation procedures of the models in classification processes is called k-fold cross-validation. In addition to these assessments, cross-validation is an additional method that may be used to evaluate learning algorithms. This method involves segmenting the data and comparing the segments to one another. In the process of cross-validation, the training set and the validation set are repeatedly combined so that each data point gets the opportunity to be verified. The k-fold cross-validation method is the fundamental kindof cross-validation. K-fold cross-validation is the popular technique for model selection and error estimates of classifiers. This is mainly attributable to the fact that it is both versatile and useful when used in data mining applications. The k-fold cross-validation approach utilized in this work is shown essentially in figure 2. Figure 2shows the results of a k value is 10 cross-validation. The dataset is partitioned into k pieces in this approach. Iteratively, models are trained on k-1 parts and tested on a single sample. When k iterations are performed, k outputs are generated. Simply averaging the gathered findings will give you the average metrics of the models' performance.

Classification using GJOSVM

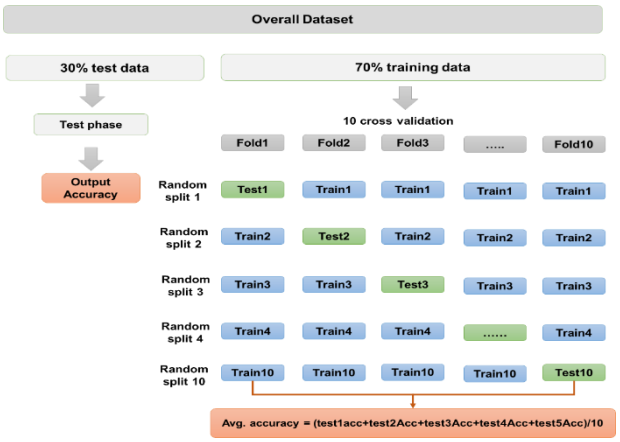

Fig. 2. k-fold cross validation different feature sets, tweaking algorithm settings, orchanging which genetic markers are used. The fitness Inspired by the strategies used by golden jackals, a type of canid found in many regions of the globe, Golden Jackal Optimization (GJO) is a natural-based optimization method. Metaheuristic algorithms, like GJO, are problem- solving techniques that take natural cues. The GJO algorithm is based on many behaviors seen in the golden jackal. Jackals, for instance, have earned a reputation for versatility because of their capacity to thrive in habitats as varied as deserts and woodlands. In addition to being formidable foes, they use shrewd methods of hunting. Define the viral detection challenge by considering theviruses' properties, the data at hand, and the processes already in use. It's up to you to figure out what goes into it and how you'll judge success. Produce an initial set ofsolutions representing possible detection procedures. Several factors, including genetic markers, machine learning algorithms, and feature extraction methods, may affect the accuracy of a detection

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-1 || January 2023 || PP. 139-149 https://doi.org/10.55544/ijrah.3.1.25

system. Therefore there are many possible solutions. Evaluate the viability and performance of each option in the population. Here, we put the parameters and characteristics we've chosen for viral detection through their paces and assess how well they function by calculating metrics like detection accuracy, sensitivity, specificity, and false positive rate. Explore possible solutions by simulating the hunting behavior of golden jackals. Solutions, which stand in for detection strategies, may be improved by adjusting their parameters or characteristics in light of the collective knowledge measurements and convergence criteria used to evaluatethe performance of GJO and other algorithms are just as important as the quality and variety of the original population.

For detecting purposes, we use the SVM algorithm, whose defining characteristic is its foundation in structural risk reduction. Optimize learning's generalizability or the extentto which a small training set can ensure a sizeable independent test set that maintains a small error. Littlesequences determined by regular access to the unusually short series in the sample might include normal intermittent, causing the SVM classifier to produce classification error; thus, the implementation of a detection module, which provided follows the level of risk using malware to make decisions. Taking into mind the fact that the impact of malicious software on a smartphone's operating system and its user is distinct from the damages brought about by the introduction of a risk factor (also known as RF or Risk Factor), RF is applied to every one ofthe system's brief sequences. Act of malice committed withthe intention of providing a weight, the correct basis. If the behavior of the system and user poses a more significant security danger, which results in an RF that is more than 1, the value is set to 1. The introduction of risk (also knownas Risk Rank or RR) is a program that serves as a measure of the quantitative detection of malware. The RR is definedas follows:

$$RR = \sum_{i=0}^{n} ncs_i \times RF_{ncsi} \quad \text{…….. (1)}$$

Establish a malware detection threshold known as D, whose value will be based on the experiment's findings. Based on our findings, a D value of 17 will serve as the most effective detection threshold. When the RR is found to be more than the D that was computed, the program is finally identified as malicious software.

IV. RESULT AND DISCUSSION

Classifications have been carried out using the Android Malware Dataset's 112 characteristics to determine if apps are malicious or not. Experiments used a computer that hadan Intel® i5® 10200H CPU operating at 2.40 GHz, an NVIDIA GTX1650Ti GPU, and 24 GB of RAM. In the approach of cross-validation used for training, the classification models were decided to have a value of k equal to 10. While training the models, each of the 116 inputs and the single class feature was used, together with all of the characteristics included in the dataset. Performance metrics are used to analyze and compare the performance of various suggested models. Metrics like “accuracy, precision, recall, and the F-1 Score” were used in this investigation. While training the proposed model,the kernel function was analyzed and found to be an RBF (Radial Basis Function) with a numerical tolerance of 0.0010 and an iteration of 100.

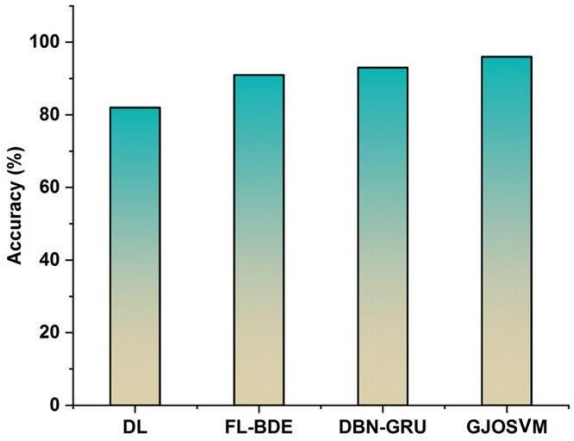

Fig.3. Accuracy

Figure 3 shows the accuracy of the proposed system. The accuracy of malware detection systems can vary depending on various factors, including the techniques and algorithmsused, the quality and diversity of the dataset, and the sophistication of the malware samples. Achieving high accuracy is an ongoing challenge due to the constantly evolving nature of malware. DL has attained 82 %, FL- BDE has acquired 91 %, DBN-GRU has reached 93 %,and the proposed system achieves 96 % accuracy. It shows that the proposed approach has more effective than the existing one. The Equation (2) for determining accuracy is as follows:

$$Accuracy = (True\ Positives\ True\ Negatives) / (True\ Positives\ True\ Negatives + False\ Positives + False\ Negatives) \quad \text{…….(2)}$$

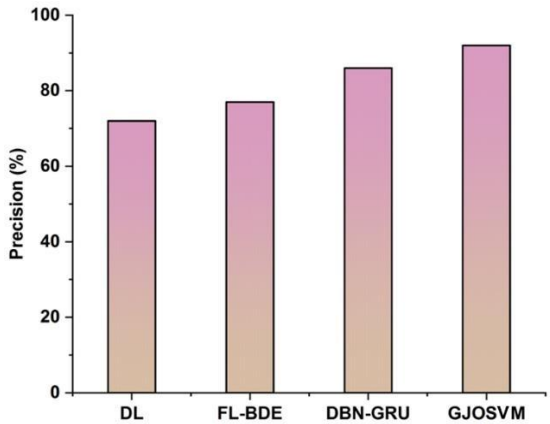

Fig. 4. Precision

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-1 || January 2023 || PP. 139-149 https://doi.org/10.55544/ijrah.3.1.25

Figure 4 shows the precision of the proposed system. The accuracy of a malware detection system is measured by how many malicious samples out of a whole set are really malicious. It is a test of how well positive malware predictions can be made. The equation (3) for determining precision is as follows:

$$Precision = True\ Positives / (True\ Positives + False\ Positives) \quad \text{.....(3)}$$

Accurately recognizing malware while not incorrectly labeling safe files as harmful is only possible with a systemthat has a low false positive rate, which is shown by high precision. In security-sensitive contexts, where false positives may have dire repercussions, accuracy in malware detection systems is a crucial parameter. DL has attained 72 %, FL-BDE has acquired 77 %, and DBN-GRU has reached 86 %, whereas the proposed methodachieves 92 % of precision. It shows that the proposed approach has more effective than the existing one.

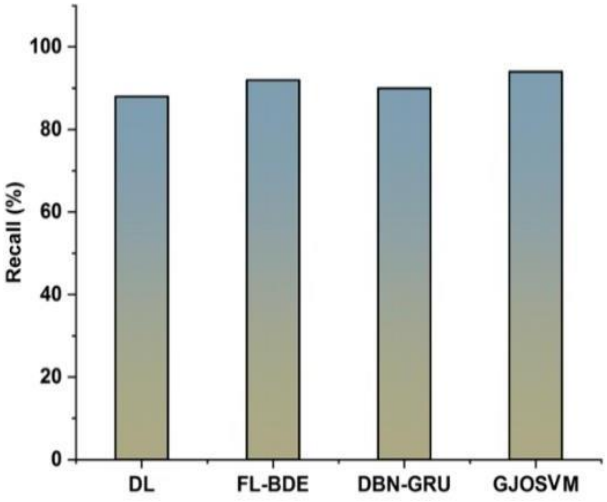

Fig. 5. Recall

Figure 5 shows the recall of the proposed system. The recall metric calculates the percentage of malware samples properly recognized relative to the overall malware samples in the dataset. This metric is also known as sensitivity or actual positive rate. It measures how well a malware detection system can detect malware samples. The Equation (4) for the recall is as follows:

$$Recall = True\ Positives /(True\ Positives + False\ Negatives) \quad \text{.....(4)}$$

It measures how well a system can detect malware in a dataset. DL has attained 88 %, FL-BDE has acquired 92 %,DBN-GRU has reached 90 %, whereas the proposed method achieves 94 % of recall. It demonstrates that the suggested technique is more successful than the existing one.

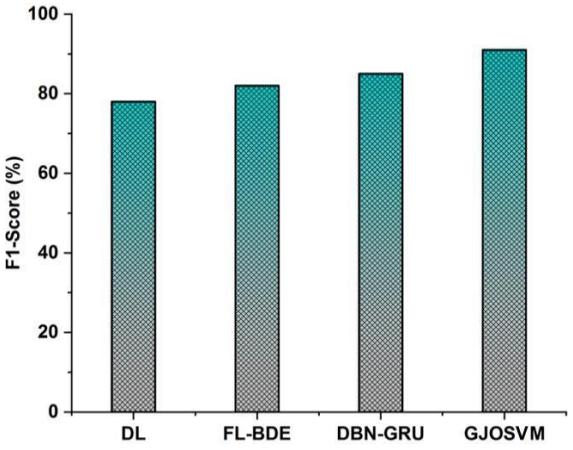

Fig. 6. F1-Score

A balanced evaluation of a malware detection system's performance is presented by the F1-score, a statistic that combines accuracy and recalls into a single number. It takes into account both the accuracy with which malware samples may be detected as well as the capacity to detect all instances of malware. The F1-score calculation equation (5) is as follows:

$$F1 - score = 2 * (Precision * Recall) /(Precision + Recall) \quad \text{.....(5)}$$

The F1-score ranges from 0 to 1, with 0 denoting subpar performance and 1 signifying flawless accuracy and recall. DL has attained 78 %, FL-BDE has acquired 82 %, and DBN-GRU has reached 85 %, whereas the proposed system attains 91 % of the f1-score. It shows that the proposed approach has more effective than the existing one.

V. CONCLUSION

In this work, classification procedures were carried out utilizing GJOSVM techniques utilizing the data of 2850 harmful apps and 2866 non-malicious applications used in the Android OS. To conduct in-depth performance assessments, 10-fold cross-validation was used. The suggested model has values of 96% for accuracy, 92% for precision, 94% for recall, and 91% for F-1 Score. These values are all much higher than the average. It is feasible to create antivirus software that is more effective by using the models that are advised for the identification of malware. In subsequent investigations, the dataset will be enlarged, and various machine-learning approaches will be used to identify malware.

REFERENCES

[1] Mbunge, E., Muchemwa, B., Batani, J. and Mbuyisa, N., 2023. A review of deep learning models to detect malware in Android applications. Cyber Security

and Applications, p.100014.
[2] Mijwil, M.M., 2020. Malware Detection in Android OS Using Machine Learning Techniques. Data Science and Applications, 3(2), pp.5-9.
[3] Kavuri, S., & Narne, S. (2020). Implementing effective SLO monitoring in high-volume data processing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(2), 558. http://ijsrcseit.com
[4] Kavuri, S., & Narne, S. (2021). Improving performance of data extracts using window-based refresh strategies. International Journal of Scientific Research in Science, Engineering and Technology, 8(5), 359-377. https://doi.org/10.32628/IJSRSET
[5] Narne, S. (2023). Predictive analytics in early disease detection: Applying deep learning to electronic health records. African Journal of Biological Sciences, 5(1), 70–101. https://doi.org/10.48047/AFJBS.5.1.2023.
[6] Narne, S. (2022). AI-driven drug discovery: Accelerating the development of novel therapeutics. International Journal on Recent and Innovation Trends in Computing and Communication, 10(9), 196. http://www.ijritcc.org
[7] Rinkesh Gajera , "Leveraging Procore for Improved Collaboration and Communication in Multi-Stakeholder Construction Projects", International Journal of Scientific Research in Civil Engineering (IJSRCE), ISSN : 2456-6667, Volume 3, Issue 3, pp.47-51, May-June.2019
[8] Rinkesh Gajera , "Integrating Power Bi with Project Control Systems: Enhancing Real-Time Cost Tracking and Visualization in Construction", International Journal of Scientific Research in Civil Engineering (IJSRCE), ISSN : 2456-6667, Volume 7, Issue 5, pp.154-160, September-October.2023URL : https://ijsrce.com/IJSRCE123761
[9] Rinkesh Gajera, 2023. Developing a Hybrid Approach: Combining Traditional and Agile Project Management Methodologies in Construction Using Modern Software Tools, ESP Journal of Engineering & Technology Advancements 3(3): 78-83.
[10] Paulraj, B. (2023). Enhancing Data Engineering Frameworks for Scalable Real-Time Marketing Solutions. Integrated Journal for Research in Arts and Humanities, 3(5), 309–315. https://doi.org/10.55544/ijrah.3.5.34
[11] Balachandar, P. (2020). Title of the article. International Journal of Scientific Research in Science, Engineering and Technology, 7(5), 401-410. https://doi.org/10.32628/IJSRSET23103132
[12] Paulraj, B. (2022). Building Resilient Data Ingestion Pipelines for Third-Party Vendor Data Integration. Journal for Research in Applied Sciences and Biotechnology, 1(1), 97–104. https://doi.org/10.55544/jrasb.1.1.14
[13] Paulraj, B. (2022). The Role of Data Engineering in Facilitating Ps5 Launch Success: A Case Study. International Journal on Recent and Innovation Trends in Computing and Communication, 10(11), 219–225. https://doi.org/10.17762/ijritcc.v10i11.11145

[14] Paulraj, B. (2019). Automating resource management in big data environments to reduce operational costs. Tuijin Jishu/Journal of Propulsion Technology, 40(1).https://doi.org/10.52783/tjjpt.v40.i1.7905
[15] Balachandar Paulraj. (2021). Implementing Feature and Metric Stores for Machine Learning Models in the Gaming Industry. European Economic Letters (EEL), 11(1). Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1924

[16] Bhatt, S. (2020). Leveraging AWS tools for high availability and disaster recovery in SAP applications. International Journal of Scientific Research in Science, Engineering and Technology, 7(2), 482. https://doi.org/10.32628/IJSRSET2072122

[17] Bhatt, S. (2023). A comprehensive guide to SAP data center migrations: Techniques and case studies. International Journal of Scientific Research in Science, Engineering and Technology, 10(6), 346. https://doi.org/10.32628/IJSRSET2310630

[18] Kavuri, S., & Narne, S. (2020). Implementing effective SLO monitoring in high-volume data processing systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(6), 558. https://doi.org/10.32628/CSEIT206479

[19] Kavuri, S., & Narne, S. (2023). Improving performance of data extracts using window-based refresh strategies. International Journal of Scientific Research in Science, Engineering and Technology, 10(6), 359. https://doi.org/10.32628/IJSRSET2310631

[20] Swethasri Kavuri, " Advanced Debugging Techniques for Multi-Processor Communication in 5G Systems, IInternational Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.360-384, September-October-2023. Available at doi : https://doi.org/10.32628/CSEIT239071
[21] Mehra, A. (2023). Strategies for scaling EdTech startups in emerging markets. International Journal of Communication Networks and Information Security, 15(1), 259–274. https://ijcnis.org
[22] Mehra, A. (2021). The impact of public-private partnerships on global educational platforms. Journal of Informatics Education and Research, 1(3), 9–28. http://jier.org

[23] Ankur Mehra. (2019). Driving Growth in the

Creator Economy through Strategic Content Partnerships. International Journal for Research Publication and Seminar, 10(2), 118–135. https://doi.org/10.36676/jrps.v10.i2.1519
[24] Mehra, A. (2023). Leveraging Data-Driven Insights to Enhance Market Share in the Media Industry. Journal for Research in Applied Sciences and Biotechnology, 2(3), 291–304. https://doi.org/10.55544/jrasb.2.3.37

[25] Ankur Mehra. (2022). Effective Team Management Strategies in Global Organizations. Universal Research Reports, 9(4), 409–425. https://doi.org/10.36676/urr.v9.i4.1363
[26] Mehra, A. (2023). Innovation in brand collaborations for digital media platforms. IJFANS International Journal of Food and Nutritional Sciences, 12(6), 231. https://doi.org/10.XXXX/xxxxx
[27] Ankur Mehra. (2022). Effective Team Management Strategies in Global Organizations. Universal Research Reports, 9(4), 409–425. https://doi.org/10.36676/urr.v9.i4.1363
[28] Mehra, A. (2023). Leveraging Data-Driven Insights to Enhance Market Share in the Media Industry. Journal for Research in Applied Sciences and Biotechnology, 2(3), 291–304. https://doi.org/10.55544/jrasb.2.3.37

[29] Ankur Mehra. (2022). Effective Team Management Strategies in Global Organizations. Universal Research Reports, 9(4), 409–425. https://doi.org/10.36676/urr.v9.i4.1363
[30] Ankur Mehra. (2022). The Role of Strategic Alliances in the Growth of the Creator Economy. European Economic Letters (EEL), 12(1). Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1925

[31] Santhosh Palavesh. (2019). The Role of Open Innovation and Crowdsourcing in Generating New Business Ideas and Concepts. International Journal for Research Publication and Seminar, 10(4), 137–147. https://doi.org/10.36676/jrps.v10.i4.1456
[32] Santosh Palavesh. (2021). Developing Business Concepts for Underserved Markets: Identifying and Addressing Unmet Needs in Niche or Emerging Markets. Innovative Research Thoughts, 7(3), 76–89. https://doi.org/10.36676/irt.v7.i3.1437
[33] Palavesh, S. (2021). Co-Creating Business Concepts with Customers: Approaches to the Use of Customers in New Product/Service Development. Integrated Journal for Research in Arts and Humanities, 1(1), 54–66. https://doi.org/10.55544/ijrah.1.1.9
[34] Santhosh Palavesh. (2022). Entrepreneurial Opportunities in the Circular Economy: Defining Business Concepts for Closed-Loop Systems and Resource Efficiency. European Economic Letters (EEL), 12(2), 189–204. https://doi.org/10.52783/eel.v12i2.1785
[35] Santhosh Palavesh. (2022). The Impact of Emerging Technologies (e.g., AI, Blockchain, IoT) On Conceptualizing and Delivering new Business Offerings. International Journal on Recent and Innovation Trends in Computing and Communication, 10(9), 160–173. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10955
[36] Santhosh Palavesh. (2021). Business Model Innovation: Strategies for Creating and Capturing Value Through Novel Business Concepts. European Economic Letters (EEL), 11(1). https://doi.org/10.52783/eel.v11i1.1784
[37] Santhosh Palavesh. (2023). Leveraging Lean Startup Principles: Developing And Testing Minimum Viable Products (Mvps) In New Business Ventures. Educational Administration: Theory and Practice, 29(4), 2418–2424. https://doi.org/10.53555/kuey.v29i4.7141
[38] Palavesh, S. (2023). The role of design thinking in conceptualizing and validating new business ideas. Journal of Informatics Education and Research, 3(2), 3057.
[39] Vijaya Venkata Sri Rama Bhaskar, Akhil Mittal, Santosh Palavesh, Krishnateja Shiva, Pradeep Etikani. (2020). Regulating AI in Fintech: Balancing Innovation with Consumer Protection. European Economic Letters (EEL), 10(1). https://doi.org/10.52783/eel.v10i1.1810
[40] Sri Sai Subramanyam Challa. (2023). Regulatory Intelligence: Leveraging Data Analytics for Regulatory Decision-Making. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 1426–1434. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10893
[41] Challa, S. S. S. (2020). Assessing the regulatory implications of personalized medicine and the use of biomarkers in drug development and approval. European Chemical Bulletin, 9(4), 134-146.
[42] D.O.I10.53555/ecb.v9:i4.17671
[43] EVALUATING THE EFFECTIVENESS OF RISK-BASED APPROACHES IN STREAMLINING THE REGULATORY APPROVAL PROCESS FOR NOVEL THERAPIES. (2021). Journal of Population Therapeutics and Clinical Pharmacology, 28(2), 436-448. https://doi.org/10.53555/jptcp.v28i2.7421
[44] Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2019). Investigating the use of natural language processing (NLP) techniques in automating the extraction of regulatory requirements from unstructured data sources. Annals of Pharma Research, 7(5), 380-387.
[45] Ashok Choppadandi. (2022). Exploring the Potential of Blockchain Technology in Enhancing Supply Chain Transparency and Compliance with Good Distribution Practices (GDP). International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 336–343. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/109

81
[46] Challa, S. S. S., Chawda, A. D., Benke, A. P., & Tilala, M. (2020). Evaluating the use of machine learning algorithms in predicting drug-drug interactions and adverse events during the drug development process. NeuroQuantology, 18(12), 176-186. https://doi.org/10.48047/nq.2020.18.12.NQ20252
[47] Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2023). Investigating the impact of AI-assisted drug discovery on the efficiency and cost-effectiveness of pharmaceutical R&D. Journal of Cardiovascular Disease Research, 14(10), 2244.
[48] Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2022). Quality Management Systems in Regulatory Affairs: Implementation Challenges and Solutions. Journal for Research in Applied Sciences and Biotechnology, 1(3), 278–284. https://doi.org/10.55544/jrasb.1.3.36
[49] Ranjit Kumar Gupta, Sagar Shukla, Anaswara Thekkan Rajan, & Sneha Aravind. (2022). Strategies for Effective Product Roadmap Development and Execution in Data Analytics Platforms. International Journal for Research Publication and Seminar, 13(1), 328–342. Retrieved from https://jrps.shodhsagar.com/index.php/j/article/view/1515
[50] Ranjit Kumar Gupta, Sagar Shukla, Anaswara Thekkan Rajan, & Sneha Aravind. (2022). Leveraging Data Analytics to Improve User Satisfaction for Key Personas: The Impact of Feedback Loops. International Journal for Research Publication and Seminar, 11(4), 242–252. https://doi.org/10.36676/jrps.v11.i4.1489
[51] Ranjit Kumar Gupta, Sagar Shukla, Anaswara Thekkan Rajan, Sneha Aravind, 2021. "Utilizing Splunk for Proactive Issue Resolution in Full Stack Development Projects" ESP Journal of Engineering & Technology Advancements 1(1): 57-64.
[52] Sagar Shukla, Anaswara Thekkan Rajan, Sneha Aravind, Ranjit Kumar Gupta, Santosh Palavesh. (2023). Monetizing API Suites: Best Practices for Establishing Data Partnerships and Iterating on Customer Feedback. European Economic Letters (EEL), 13(5), 2040–2053. https://doi.org/10.52783/eel.v13i5.1798
[53] Sagar Shukla. (2021). Integrating Data Analytics Platforms with Machine Learning Workflows: Enhancing Predictive Capability and Revenue Growth. International Journal on Recent and Innovation Trends in Computing and Communication, 9(12), 63–74. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11119
[54] Shukla, S., Thekkan Rajan, A., Aravind, S., & Gupta, R. K. (2023). Implementing scalable big-data tech stacks in pre-seed start-ups: Challenges and strategies for realizing strategic vision. International Journal of Communication Networks and Information Security, 15(1).
[55] Sneha Aravind. (2021). Integrating REST APIs in Single Page Applications using Angular and TypeScript. International Journal of Intelligent Systems and Applications in Engineering, 9(2), 81 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6829
[56] Aravind, S., Cherukuri, H., Gupta, R. K., Shukla, S., & Rajan, A. T. (2022). The role of HTML5 and CSS3 in creating optimized graphic prototype websites and application interfaces. NeuroQuantology, 20(12), 4522-4536. https://doi.org/10.48047/NQ.2022.20.12.NQ77775
[57] Nikhil Singla. (2023). Assessing the Performance and Cost-Efficiency of Serverless Computing for Deploying and Scaling AI and ML Workloads in the Cloud. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 618–630. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6730
[58] Rishabh Rajesh Shanbhag, Rajkumar Balasubramanian, Ugandhar Dasi, Nikhil Singla, & Siddhant Benadikar. (2022). Case Studies and Best Practices in Cloud-Based Big Data Analytics for Process Control. International Journal for Research Publication and Seminar, 13(5), 292–311. https://doi.org/10.36676/jrps.v13.i5.1462
[59] Siddhant Benadikar. (2021). Developing a Scalable and Efficient Cloud-Based Framework for Distributed Machine Learning. International Journal of Intelligent Systems and Applications in Engineering, 9(4), 288 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6761
[60] Siddhant Benadikar. (2021). Evaluating the Effectiveness of Cloud-Based AI and ML Techniques for Personalized Healthcare and Remote Patient Monitoring. International Journal on Recent and Innovation Trends in Computing and Communication, 9(10), 03–16. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/11036
[61] Rishabh Rajesh Shanbhag. (2023). Exploring the Use of Cloud-Based AI and ML for Real-Time Anomaly Detection and Predictive Maintenance in Industrial IoT Systems. International Journal of Intelligent Systems and Applications in Engineering, 11(4), 925 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6762
[62] Nikhil Singla. (2023). Assessing the Performance and Cost-Efficiency of Serverless Computing for Deploying and Scaling AI and ML Workloads in the Cloud. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 618–630. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/673
[63] Nikhil Singla. (2023). Assessing the Performance and Cost-Efficiency of Serverless Computing for Deploying and Scaling AI and ML Workloads in the Cloud. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 618–630. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6730
[64] Challa, S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2019). Investigating the use of natural language processing (NLP) techniques in automating the extraction of regulatory requirements from unstructured data

sources. Annals of PharmaResearch, 7(5), 380-387.
[65] Ritesh Chaturvedi. (2023). Robotic Process Automation (RPA) in Healthcare: Transforming Revenue Cycle Operations. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 652–658. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/11045
[66] Chaturvedi, R., & Sharma, S. (2022). Assessing the Long-Term Benefits of Automated Remittance in Large Healthcare Networks. Journal for Research in Applied Sciences and Biotechnology, 1(5), 219–224. https://doi.org/10.55544/jrasb.1.5.25
[67] Chaturvedi, R., & Sharma, S. (2022). Enhancing healthcare staffing efficiency with AI-powered demand management tools. Eurasian Chemical Bulletin, 11(Regular Issue 1), 675-681. https://doi.org/10.5281/zenodo.13268360
[68] Dr. Saloni Sharma, & Ritesh Chaturvedi. (2017). Blockchain Technology in Healthcare Billing: Enhancing Transparency and Security. International Journal for Research Publication and Seminar, 10(2), 106–117. Retrieved from https://jrps.shodhsagar.com/index.php/j/article/view/1475
[69] Dr. Saloni Sharma, & Ritesh Chaturvedi. (2017). Blockchain Technology in Healthcare Billing: Enhancing Transparency and Security. International Journal for Research Publication and Seminar, 10(2), 106–117. Retrieved from https://jrps.shodhsagar.com/index.php/j/article/view/1475
[70] Saloni Sharma. (2020). AI-Driven Predictive Modelling for Early Disease Detection and Prevention. International Journal on Recent and Innovation Trends in Computing and Communication, 8(12), 27–36. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/11046
[71] Chaturvedi, R., & Sharma, S. (2022). Assessing the Long-Term Benefits of Automated Remittance in Large Healthcare Networks. Journal for Research in Applied Sciences and Biotechnology, 1(5), 219–224. https://doi.org/10.55544/jrasb.1.5.25
[72] Pavan Ogeti, Narendra Sharad Fadnavis, Gireesh Bhaulal Patil, Uday Krishna Padyana, Hitesh Premshankar Rai. (2022). Blockchain Technology for Secure and Transparent Financial Transactions. European Economic Letters (EEL), 12(2), 180–188. Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1283
[73] Ogeti, P., Fadnavis, N. S., Patil, G. B., Padyana, U. K., & Rai, H. P. (2023). Edge computing vs. cloud computing: A comparative analysis of their roles and benefits. Volume 20, No. 3, 214-226.
[74] Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2020). Machine learning applications in climate modeling and weather forecasting. NeuroQuantology, 18(6), 135-145. https://doi.org/10.48047/nq.2020.18.6.NQ20194
[75] Narendra Sharad Fadnavis. (2021). Optimizing Scalability and Performance in Cloud Services: Strategies and Solutions. International Journal on Recent and Innovation Trends in Computing and Communication, 9(2), 14–21. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10889
[76] Gireesh Bhaulal Patil. (2022). AI-Driven Cloud Services: Enhancing Efficiency and Scalability in Modern Enterprises. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 153–162. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6728
[77] Padyana, U. K., Rai, H. P., Ogeti, P., Fadnavis, N. S., & Patil, G. B. (2023). AI and Machine Learning in Cloud-Based Internet of Things (IoT) Solutions: A Comprehensive Review and Analysis. Integrated Journal for Research in Arts and Humanities, 3(3), 121–132. https://doi.org/10.55544/ijrah.3.3.20
[78] Patil, G. B., Padyana, U. K., Rai, H. P., Ogeti, P., & Fadnavis, N. S. (2021). Personalized marketing strategies through machine learning: Enhancing customer engagement. Journal of Informatics Education and Research, 1(1), 9. http://jier.org
[79] Padyana, U. K., Rai, H. P., Ogeti, P., Fadnavis, N. S., & Patil, G. B. (2023). AI and Machine Learning in Cloud-Based Internet of Things (IoT) Solutions: A Comprehensive Review and Analysis. Integrated Journal for Research in Arts and Humanities, 3(3), 121–132. https://doi.org/10.55544/ijrah.3.3.20
[80] Krishnateja Shiva. (2022). Leveraging Cloud Resource for Hyperparameter Tuning in Deep Learning Models. International Journal on Recent and Innovation Trends in Computing and Communication, 10(2), 30–35. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10980
[81] Shiva, K., Etikani, P., Bhaskar, V. V. S. R., Palavesh, S., & Dave, A. (2022). The rise of robo-advisors: AI-powered investment management for everyone. Journal of Namibian Studies, 31, 201-214.
[82] Etikani, P., Bhaskar, V. V. S. R., Nuguri, S., Saoji, R., & Shiva, K. (2023). Automating machine learning workflows with cloud-based pipelines. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 375–382. https://doi.org/10.48047/ijisae.2023.11.1.375
[83] Etikani, P., Bhaskar, V. V. S. R., Palavesh, S., Saoji, R., & Shiva, K. (2023). AI-powered algorithmic trading strategies in the stock market. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 264–277. https://doi.org/10.1234/ijsdip.org_2023-Volume-11-Issue-1_Page_264-277
[84] Bhaskar, V. V. S. R., Etikani, P., Shiva, K., Choppadandi, A., & Dave, A. (2019). Building explainable AI systems with federated learning on the

cloud. Journal of Cloud Computing and Artificial Intelligence, 16(1), 1–14.
[85] Ogeti, P., Fadnavis, N. S., Patil, G. B., Padyana, U. K., & Rai, H. P. (2022). Blockchain technology for secure and transparent financial transactions. European Economic Letters, 12(2), 180-192. http://eelet.org.uk
[86] Vijaya Venkata Sri Rama Bhaskar, Akhil Mittal, Santosh Palavesh, Krishnateja Shiva, Pradeep Etikani. (2020). Regulating AI in Fintech: Balancing Innovation with Consumer Protection. European Economic Letters (EEL), 10(1). https://doi.org/10.52783/eel.v10i1.1810
[87] Dave, A., Shiva, K., Etikani, P., Bhaskar, V. V. S. R., & Choppadandi, A. (2022). Serverless AI: Democratizing machine learning with cloud functions. Journal of Informatics Education and Research, 2(1), 22-35. http://jier.org
[88] Dave, A., Etikani, P., Bhaskar, V. V. S. R., & Shiva, K. (2020). Biometric authentication for secure mobile payments. Journal of Mobile Technology and Security, 41(3), 245-259.
[89] Saoji, R., Nuguri, S., Shiva, K., Etikani, P., & Bhaskar, V. V. S. R. (2021). Adaptive AI-based deep learning models for dynamic control in software-defined networks. International Journal of Electrical and Electronics Engineering (IJEEE), 10(1), 89–100. ISSN (P): 2278–9944; ISSN (E): 2278–9952
[90] Narendra Sharad Fadnavis. (2021). Optimizing Scalability and Performance in Cloud Services: Strategies and Solutions. International Journal on Recent and Innovation Trends in Computing and Communication, 9(2), 14–21. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10889
[91] Joel lopes, Arth Dave, Hemanth Swamy, Varun Nakra, & Akshay Agarwal. (2023). Machine Learning Techniques And Predictive Modeling For Retail Inventory Management Systems. Educational Administration: Theory and Practice, 29(4), 698–706. https://doi.org/10.53555/kuey.v29i4.5645
[92] Nitin Prasad. (2022). Security Challenges and Solutions in Cloud-Based Artificial Intelligence and Machine Learning Systems. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 286–292. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10750
[93] Prasad, N., Narukulla, N., Hajari, V. R., Paripati, L., & Shah, J. (2020). AI-driven data governance framework for cloud-based data analytics. Volume 17, (2), 1551-1561.
[94] Jigar Shah , Joel lopes , Nitin Prasad , Narendra Narukulla , Venudhar Rao Hajari , Lohith Paripati. (2023). Optimizing Resource Allocation And Scalability In Cloud-Based Machine Learning Models. Migration Letters, 20(S12), 1823–1832. Retrieved from https://migrationletters.com/index.php/ml/article/view/10652
[95] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
[96] Shah, J., Narukulla, N., Hajari, V. R., Paripati, L., & Prasad, N. (2021). Scalable machine learning infrastructure on cloud for large-scale data processing. Tuijin Jishu/Journal of Propulsion Technology, 42(2), 45-53.
[97] Narukulla, N., Lopes, J., Hajari, V. R., Prasad, N., & Swamy, H. (2021). Real-time data processing and predictive analytics using cloud-based machine learning. Tuijin Jishu/Journal of Propulsion Technology, 42(4), 91-102
[98] Secure Federated Learning Framework for Distributed Ai Model Training in Cloud Environments. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(1), 31-39. https://ijope.com/index.php/home/article/view/145
[99] Paripati, L., Prasad, N., Shah, J., Narukulla, N., & Hajari, V. R. (2021). Blockchain-enabled data analytics for ensuring data integrity and trust in AI systems. International Journal of Computer Science and Engineering (IJCSE), 10(2), 27–38. ISSN (P): 2278–9960; ISSN (E): 2278–9979.
[100] Hajari, V. R., Prasad, N., Narukulla, N., Chaturvedi, R., & Sharma, S. (2023). Validation techniques for AI/ML components in medical diagnostic devices. NeuroQuantology, 21(4), 306-312. https://doi.org/10.48047/NQ.2023.21.4.NQ23029
[101] Hajari, V. R., Chaturvedi, R., Sharma, S., Tilala, M., Chawda, A. D., & Benke, A. P. (2023). Interoperability testing strategies for medical IoT devices. Tuijin Jishu/Journal of Propulsion Technology, 44(1), 258.
[102] DOI: 10.36227/techrxiv.171340711.17793838/v1
[103] P. V., V. R., & Chidambaranathan, S. (2023). Polyp segmentation using UNet and ENet. In Proceedings of the 6th International Conference on Recent Trends in Advance Computing (ICRTAC) (pp. 516-522). Chennai, India. https://doi.org/10.1109/ICRTAC59277.2023.10480851
[104] Athisayaraj, A. A., Sathiyanarayanan, M., Khan, S., Selvi, A. S., Briskilla, M. I., Jemima, P. P., Chidambaranathan, S., Sithik, A. S., Sivasankari, K., & Duraipandian, K. (2023). Smart thermal-cooler umbrella (UK Design No. 6329357).
[105] Challa, S. S. S., Chawda, A. D., Benke, A. P., & Tilala, M. (2023). Regulatory intelligence: Leveraging data analytics for regulatory decision-making. International Journal on Recent and Innovation Trends in Computing and Communication, 11, 10.
[106] Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2019). Investigating the use of natural language processing (NLP) techniques in automating the extraction of regulatory requirements from unstructured data sources. Annals of Pharma Research, 7(5),
[107] Challa, S. S. S., Tilala, M., Chawda, A. D., &

Benke, A. P. (2021). Navigating regulatory requirements for complex dosage forms: Insights from topical, parenteral, and ophthalmic products. NeuroQuantology, 19(12), 15.

[108] Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2022). Quality management systems in regulatory affairs: Implementation challenges and solutions. Journal for Research in Applied Sciences