AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 1(2026)

A Scalable AI-Driven Framework for Cybersecurity Training Simulator with Live Network Traffic Visualization

B. J. Praveen Kumar[1], Panja Varshitha[2], Rachapally Bhargavi[2], Porika Soumya Mishra[2], Thotte Ravi Teja[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering (Data Science)

[1,2]Vaagdevi College of Engineering (UGC-Autonomous), Bollikunta, Warangal, 506005, Telangana

Abstract

As cyber threats evolve, Denial of Service (DoS) attacks remain a primary concern due to their ability to paralyze critical infrastructure by overwhelming server resources. Traditional defense mechanisms, such as static firewalls and signature-based antivirus solutions, often lack the scalability required to mitigate high-volume traffic flooding. This study proposes a proactive DoS mitigation framework leveraging real-time network traffic monitoring and distributed Big Data analytics. The system integrates a high-throughput packet inspection mechanism with a Hadoop MapReduce framework to perform parallelized traffic analysis. By evaluating request payloads against dynamic server capacity thresholds, the framework distinguishes legitimate traffic from malicious flooding attempts at the network edge. The architecture comprises a robust server listening module, a MapReduce-driven network monitor for large-scale packet processing, and a traffic simulation environment to validate system resilience. Experimental evaluations indicate that the proposed framework effectively filters volumetric attacks while maintaining seamless service availability for authorized users. This approach demonstrates that integrating distributed computing paradigms into network security significantly enhances institutional capacity to withstand large-scale cyber disruptions.

Keywords: Denial of Service (DoS), Hadoop MapReduce, Big Data Security, Network Traffic Monitoring, Packet Filtering, Distributed Systems.

1. Introduction

Cybersecurity has become a critical domain in today's digitally interconnected world, driven by the rapid expansion of networked systems and the increasing sophistication of cyber threats. Protecting information assets is now a top priority for governments, organizations, and individuals, as traditional static security mechanisms are no longer sufficient to handle dynamic and evolving attack patterns. In response, Artificial Intelligence (AI) has emerged as a powerful tool for enhancing cybersecurity through real-time threat detection, anomaly identification, and predictive analysis. However, a significant challenge remains in bridging the gap between theoretical knowledge and practical application, particularly in cybersecurity training environments where hands-on experience is limited. To address this issue, this work proposes an integrated approach that combines AI techniques with cloud infrastructure, specifically Amazon Web Services (AWS), to develop an interactive and scalable training platform. The proposed system simulates real-world network environments, enabling users to generate controlled attack scenarios and analyze network behavior using a MapReduce-based data processing framework for anomaly detection. By incorporating real-time monitoring and visualization through dynamic dashboards, the system provides an intuitive and practical learning experience, allowing trainees to understand the impact of malicious activities and develop essential analytical skills required for modern Security Operations Centers (SOCs).

The key research contributions of this work are summarized as follows: (i) the design and

implementation of an interactive network simulation environment tailored for cybersecurity training; (ii) the integration of AI-driven anomaly detection with a MapReduce-based framework for scalable analysis of network traffic; (iii) the development of a real-time monitoring and visualization dashboard to enhance situational awareness; (iv) the use of cloud-based infrastructure (AWS) to ensure scalability, flexibility, and accessibility; and (v) the provision of a hands-on, experiential learning platform that effectively bridges the gap between theoretical cybersecurity concepts and practical implementation.

2. Literature Survey

Chowdhury and Gkioulos [1] identified simulation systems positioned between CRs and TTXs. We grouped these systems into two categories based on their applicability to management training. The first includes tools oriented toward strategic planning or investment decisions. while Holik et al. [2] emulated communication in digital substations for operator training. These methods focus on technical realism. In contrast, our approach is designed for management-level participants and focuses on decision-making rather than technical replication, enabling efficient and scalable training without requiring infrastructure models or deep technical knowledge. Ukwandu et al. [3] developed a taxonomy identifying seven participant team types, highlighting the diversity of roles in cyber exercises. These classifications underscore the complexity of CR exercises.

Ostby et al. [4] addressed the importance of support roles, while Granåsen and Andersson [5] proposed performance metrics to assess exercise effectiveness. Turning to wargaming, Johnson [6] identifies four levels: tactical, command–tactical, operational, and strategic. At the tactical and command–tactical levels, wargames involve fine-grained detail and simulate concrete actions. In cyber exercises, this corresponds to tasks typically conducted in CRs or testbeds. Perla [7] distinguished wargames from TTXs by noting their outcome-driven progression. Our method applies this principle by updating the scenario based on participant decisions. Military wargames often explore cyber operations within a broader context but rarely address organization-level incident management. Švábenský [8] proposed combining CRs with serious games, which use game-based mechanics to enhance engagement and learning outcomes in non-entertainment contexts.

According to [9], the civilian organizational hierarchy is generally structured as follows, from lowest to highest: front-line problem-solving workers, front-line management, middle management, and top management. From a national and military perspective, the hierarchy consists of national strategic, military strategic, operational, and tactical levels. The national strategic level defines long-term national goals and provides the overarching context for civilian and military operations. The authors in [10] used the naive Bayes classifier from the Weka package and KDD’99 data for training and testing. Data were grouped into the four attack types (probe and scan, DoS, U2R and R2L) and their classifier achieved 96%, 99%, 90% and 90% testing accuracy, respectively. The cumulative false positive rate was 3%. The authors in [11] developed a framework using a simple form of Bayesian network using the KDD’99 data and used categories to depict different attack scenarios. Solving an anomaly detection problem, the reported results were 97%, 96%, 9%, 12% and 88% accuracy for normal, DoS, R2L, U2R and probe or scan categories, respectively.

In [12], the authors used an SVM classifier to detect DDoS attacks in a software-defined network. Experiments were conducted on the DARPA dataset, comparing the SVM classifier with other standard classification techniques. Although the classifier had higher accuracy, the SVM took more time, which is

an obvious flaw. In [13], the authors used a least-squares SVM to decrease the training time on large datasets. Using three different feature extraction algorithms, they reduced the number of features from 41 to 19. The data were resampled to have around 7000 instances for each of the five classes of the KDD'99 dataset. Research in [14] utilized a robust SVM, which is a variation of SVM where the discriminating hyperplane is averaged to be smoother and the regularization parameter is automatically determined. Preprocessing training and testing of data was done on the Basic Security Module from the DARPA 1998 dataset. It showed 75% accuracy with no false positives and 100% accuracy with 3% false positives. In [15], the authors utilized decision trees to generate detection rules against denial-of-service and command injection attacks on robotic vehicles. Results showed that different attacks had different impacts on robotic behaviour.

3. Proposed System

The proposed system operates through a sequence of interconnected steps involving simulation, distributed processing, anomaly detection, and visualization. The proposed system integrates a network simulation layer with a MapReduce-based anomaly detection engine to provide a real-time monitoring dashboard as shown in figure. 1. Users simulate file transfers on a network (Port 3333), generating traffic data that is independently analysed by the Network Monitor (Port 4444). The core logic, simulated via MapReduce, classifies packets as normal or attack based on a size-based heuristic (e.g., MB), instantly updating internal counters. The results are immediately visualized on a JFreeChart Dashboard, offering trainees a direct, real-time understanding of how distributed processing and simple AI rules can detect and respond to network anomalies.

Network Simulation and Data Generation: The process begins with the Main and Network classes providing a graphical user interface where a user configures a network with simulated users. The user then initiates a file transfer (upload or download) via the Network class, selecting a file size and a simulated user ID. This action triggers two key concurrent processes: the file transfer itself handled by the Server (Port 3333) and the generation of network traffic data representing the file size, which is sent to the monitoring component.

Network Monitoring and Data Collection: A dedicated component, the Network Monitor (Port 4444), runs as a separate server listening for traffic flow information generated by the simulation. Upon receiving this data (the simulated file size), the monitor component initiates the core analysis by calling the simulated MapReduce job. This separates the function of secure data storage/transfer from the function of security monitoring and analysis, mimicking a decoupled enterprise environment.

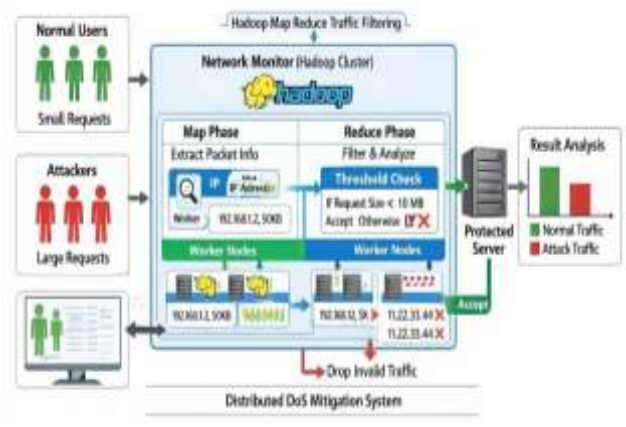


Figure. 1: Proposed system architecture.

Anomaly Detection via MapReduce Simulation: The received traffic data (file size) is passed to the Hadoop runner class, which simulates the execution of a distributed job. The core security logic resides in the MapReduce class, specifically its map function. Here, the raw size data is converted to megabytes, and the AI-driven logic (currently a simple rule: size > 50 MB) is applied to determine the packet status. If the size exceeds the threshold, the traffic is flagged as "abnormal" (attack), otherwise, it is flagged as "normal." This step updates static

counters (Network Monitor.normal and Network Monitor.attack) in real-time.

Real-Time Dashboard Visualization: As the MapReduce process classifies packets and updates the counters, the monitoring results are immediately ready for display. The user can click a button on the NetworkMonitor GUI to launch the Chart class. This class uses the JFreeChart library to dynamically pull the updated normal and attack packet counts from the NetworkMonitor and render them into a Comparison Bar Graph. This dashboard provides an instantaneous visual feedback loop, allowing the trainee to observe the direct impact of their simulated actions (e.g., uploading a large "attack" file) on the network's security status.

Secure File Handling and Response: Separately, the Server and Process Thread handle the actual file upload/download requests. Importantly, the system can demonstrate a security response: if a simulated attack is detected (or explicitly commanded by the user), the Process Thread logs a message indicating that the file is being ignored due to "Malicious Content detected," completing the training cycle of detection and response within the simulated environment.

4. Result Description

The results section presents the operational performance of the developed cybersecurity simulation system designed for monitoring network activity and secure file transmission. The system integrates user nodes, a network monitor, and a server module to simulate real-time communication within a controlled environment. Various stages such as file upload, validation, storage, request handling, and download processes are demonstrated through graphical and console-based outputs. The obtained results verify the effectiveness of the system in monitoring network behaviour and managing secure data transfer operations.

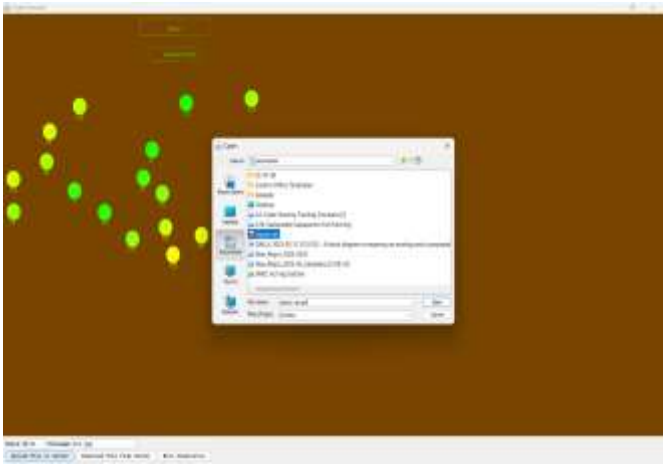


Figure. 2: File Upload Interface

Figure 2 depicts a cybersecurity simulation interface designed for monitoring network activity. Multiple nodes, representing users, are displayed as green and yellow circles labelled with IDs (e.g., U1, U2, U12), indicating active participants in the network. At the top, buttons for “Server” and “Network Monitor” suggest interactive controls for viewing server status and monitoring traffic. A file upload dialog is open, allowing a user to select a file for upload, highlighting the simulator’s functionality for file transfer and network monitoring. At the bottom, controls for selecting user ID, file name, and buttons for uploading, downloading, and exiting the simulation are visible, providing real-time interaction and operational testing of the cyber security environment. The visual layout demonstrates a dynamic, interactive system for testing network security scenarios.

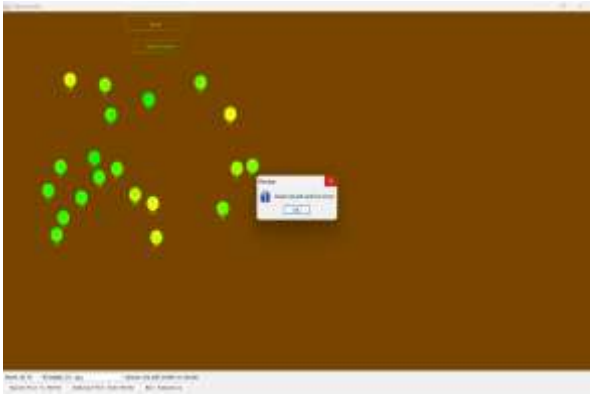


Figure. 3: File accepted by the network monitor

Figure 3 shows a continuation of the same cybersecurity simulation interface. A message box is displayed in the centre with an information icon, stating that the file is in range of size limit and has been accepted by server. The background retains the network visuals with user ID nodes in green and yellow. At the bottom of the interface, the system logs indicate the file and the user interface includes buttons to upload and download files to the server or exit the simulation. The desktop taskbar and open programs remain the same as in the previous figure.





Figure. 4: accepted as it is under the limit.

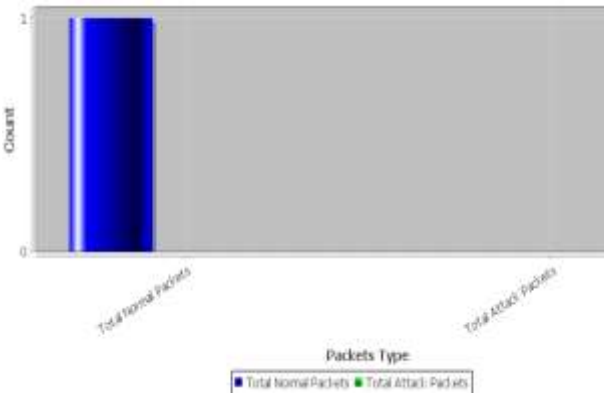


Figure. 5: Comparison graph of normal and attack packets detected by the MapReduce server.

Figure 4 shows a console window indicating that the Network Packet Monitoring MapReduce Server has successfully started. It confirms a connection from a client computer with IP address 127.0.0.1 and logs that an Excel file was within the allowed size limit and has been transmitted to the server for storage. Figure 5 presents a comparative bar chart illustrating the distribution of Total Normal Packets and Total Attack Packets within the monitored network traffic. The visualization clearly shows a dominant concentration of normal packets, represented by the tall blue bar, while the attack packet category is either extremely small or nearly absent in comparison. This indicates that the captured dataset is highly imbalanced, with legitimate network communication forming most of the traffic and only negligible malicious activity detected during monitoring. Such a distribution suggests that the network environment was largely stable and secure during data collection, but it also highlights a potential challenge for machine learning models, as severe class imbalance may affect training performance and require balancing techniques such as resampling or weighting to ensure accurate intrusion detection.



Figure. 6: Console Log of Cyber Crime & Security Server Activity and File Transactions

Figure 6 presents the console output specifically functioning as the "Cyber Security Storage Server." This window serves as a transaction log, documenting the server's operational status and recent activity. The log confirms that the "Cyber Security Server Started" and records multiple successful "Connected Computers :127.0.0.1" events. Crucially, it tracks file management operations, repeatedly noting that "charan.res saved at server" and confirming the successful delivery of a file with the entry " File sent to user 1," which aligns with the observed

download actions from the network simulation. In summary, the console validates the server's connectivity, data storage, and the successful delivery of the requested file to user U1.

5. Conclusion

The AI-driven Cyber Security Simulator successfully integrates network monitoring, MapReduce-based traffic analysis, and AI-based anomaly detection into a single platform. The project provides a realistic simulation of multiple network users performing file uploads and downloads while continuously monitoring packet-level traffic for malicious activity. Real-time feedback, secure file handling, and visual representation of network behavior enhance the understanding of cyber security dynamics. The system effectively detects abnormal traffic, prevents malicious file storage, and demonstrates the practical utility of combining AI and MapReduce for network security.

References

[1]. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. Comput. Sci. Rev. 2021, 40, 100361.

[2]. Holik, F.; Yayilgan, S.Y.; Olsborg, G.B. Emulation of Digital Substations Communication for Cyber Security Awareness. Electronics 2024, 13, 2318.

[3]. Ukwandu, E.; Farah, M.A.B.; Hindy, H.; Brosset, D.; Kavallieros, D.; Atkinson, R.; Tachtatzis, C.; Bures, M.; Andonovic, I.; Bellekens, X. A review of cyber-ranges and test-beds: Current and future trends. Sensors 2020, 20, 7148.

[4]. Ostby, G.; Lovell, K.N.; Katt, B. EXCON Teams in Cyber Security Training. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019; IEEE: New York, NY, USA, 2019; pp. 14–19.

[5]. Granåsen, M.; Andersson, D. Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study. Cogn. Technol. Work 2016, 18, 121–143.

[6]. Johnson, J. The “Four Levels” of Wargaming: A New Scope on the Hobby. 2014. Available online: https://www.beastsofwar.com/featured/levels-wargames-exploring-scopes-hobby/

[7]. Perla, P. The Art of Wargaming: A Guide for Professionals and Hobbyists; Naval Institute Press: Annapolis, MD, USA, 2012.

[8]. Švábenský, V.; Cermak, M.; Vykopal, J.; Laštovička, M. Enhancing cybersecurity skills by creating serious games. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, ITiCSE, Larnaca, Cyprus, 2–4 July 2018; pp. 194–199.

[9]. Mihm, J.; Loch, C.H.; Wilkinson, D.; Huberman, B.A. Hierarchical Structure and Search in Complex Organizations. Manag. Sci. 2010, 56, 831–848.

[10]. Panda, M.; Patra, M.R. Network intrusion detection using naive bayes. Int. J. Comput. Sci. Netw. Secur. 2007, 7, 258–263.

[11]. Amor, N.B.; Benferhat, S.; Elouedi, Z. Naive bayes vs decision trees in intrusion detection systems. In Proceedings of the 2024 ACM Symposium on Applied Computing, Nicosia, Cyprus, 14–17 March 2024; pp. 420–424.

[12]. Kokila, R.; Selvi, S.T.; Govindarajan, K. DDoS detection and analysis in SDN-based environment using support vector machine classifier. In Proceedings of the 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, India, 17–19 December 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 205–210.

[13]. Amiri, F.; Yousefi, M.R.; Lucas, C.; Shakery, A.; Yazdani, N. Mutual information-based feature selection for intrusion detection systems. J. Netw. Comput. Appl. 2011, 34, 1184–1199.

[14]. Hu, W.; Liao, Y.; Vemuri, V.R. Robust Support Vector Machines for Anomaly Detection in Computer Security. In Proceedings of the ICMLA, Los Angeles, CA, USA, 23–24 June 2003; pp. 168–174.

[15]. Vuong, T.P.; Loukas, G.; Gan, D.; Bezemskij, A. Decision tree-based detection of denial of service and command injection attacks on robotic vehicles. In Proceedings of the 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 16–19 November 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–6.

[16]. Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36

[17]. Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. Journal of Science & Technology, 10(6), 28–36. https://doi.org/10.46243/jst.2025.v10.i06.pp28-36

[18]. Todupunuri, A. (2025). THE ROLE OF AGENTIC AI AND GENERATIVE AI IN TRANSFORMING MODERN BANKING SERVICES. American Journal of AI Cyber Computing Management, 5(3), 85–93. https://doi.org/10.64751/ajaccm.2025.v5.n3.pp85-93

[19]. Todupunuri, A. . (2024). Artificial Intelligence Ethics: Investigating Ethical Frameworks, Bias Mitigation, and Transparency in AI Systems to Ensure Responsible Deployment and Use of AI Technologies. International Journal of Innovative Research in Science,Engineering and Technology, 13(09), 1–14. https://doi.org/10.15680/ijirset.2024.1309002

[20]. Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. American Journal of AI Cyber Computing Management, 5(4), 463–474. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474

[21]. Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI Cyber Computing Management, 5(4), 451–462. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462

[22]. Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[23]. Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH, 1(4).

https://doi.org/10.56975/jaafr.v1i4.501636

[24]. Srinivasa Kalyan Immadi. (2025). Harnessing Artificial Intelligence In Oracle Hcm: Revolutionising Workforce Management With Automation And Predictive Analytics. International Journal of Data Science and IoT Management System, 4(4), 7–13. https://doi.org/10.64751/ijdim.2025.v4.n4.pp7-13

[25]. S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology, 16(1). https://doi.org/10.71097/ijsat.v16.i1.1403

[26]. Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.

[27]. Cyril, H. P. (2025). Event-Driven Provisioning Architectures For Modern Telecom Networks: Overcoming Legacy Limitations And Enabling Autonomous 6g Operations. International Journal of Advanced Research in Computer Science, 16(6), 75–82. https://doi.org/10.26483/ijarcs.v16i6.7389

[28]. Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s), 1270–1285. https://doi.org/10.12732/ijam.v38i4s.685

[29]. Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.

[30]. Reddy, S. K. R. (2021). Strengthening the Security of Loyalty Reward Systems: An In-Depth Analysis of Emerging Cyber Threats and Protection Mechanisms. Journal of Computational Analysis and Applications, 29(6).

[31]. Poojari, R. (2026). Privacy-Preserving Generative AI in Healthcare Systems Using Federated Learning Approaches. International Journal of Data Science and IoT Management System, 5(1), 78-88.

[32]. Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50

[33]. Saikumar, B. (2024). Optimizing Crew Scheduling and Absence Management using Microservices: Enhancing Reliability and Efficiency in Crew Management Systems. International Journal of Enhanced Research in Management & Computer Applications, 13(11), 50–55. https://doi.org/10.55948/ijermca.2024.0116

[34]. Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. International Journal of Enhanced Research in Science, Technology & Engineering, 12(11), 111–117. https://doi.org/10.55948/ijerste.2023.111