National College of Ireland

Integrating Edge and Cloud Computing for Actionable Insights in Military Decision-Making

MSc Research Project
Cloud Computing

Anuhya Kodam
Student ID: 22104402

School of Computing
National College of Ireland

Supervisor: Sean Heeney

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Anuhya Kodam
Student ID:	22104402
Programme:	Cloud Computing
Year:	2023-24
Module:	MSc Research Project
Supervisor:	Sean Heeney
Submission Due Date:	14/12/2023
Project Title:	Integrating Edge and Cloud Computing for Actionable Insights in Military Decision-Making
Word Count:	4529
Page Count:	12

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	14th December 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Integrating Edge and Cloud Computing for Actionable Insights in Military Decision-Making

Anuhya Kodam
22104402

Abstract

In military operations, critical decisions made with time-sensitive data can often determine success or failure, yet delayed decision-making has led to substantial losses in military lives. This project addresses this issue by focusing on the integration of edge and cloud computing paradigms. Leveraging an existing public dataset centered on terrorist prediction, the project meticulously cleans and preprocesses data using Pandas, NumPy, and Matplotlib within a Jupyter Notebook environment. By employing Scikit-learn's Random Forest and Decision Tree algorithms, the project generates predictive insights through machine learning models. Serialized as pickle files, these trained models enable future utilization. Furthermore, a Flask-based web application, equipped with HTML templates, facilitates user interaction for decision-making support. Through Boto3 SDK integration, the application seamlessly connects to Amazon S3, efficiently storing decision outcomes. This project aims to showcase the integration's synergy between edge devices and cloud services. By processing data at the edge and subsequently storing it in the cloud for further analysis, it presents a user-friendly interface empowering military decision-makers with actionable insights derived from predictive analytics. The core findings underscore the successful integration of technologies, providing a scalable and efficient framework for real-time decision support in military operations, ultimately aiming to reduce losses attributable to delayed decisions.

1 Introduction

In today's fast-paced military landscape, the imperative for quick and well-informed decision-making stands as an unparalleled priority. Despite the pivotal role of cutting-edge cloud computing technologies, challenges persist, prominently seen in the latency concerning data processing and decision-making timelines. Edge computing functions as a valuable supplement to cloud computing, facilitating the delegation of computation and storage responsibilities to the network periphery. This strategy enhances resource management efficiency and bolsters the overall performance of the system Abbas and Khan (2023). This study aims to delve into the integration of edge computing with the established framework of cloud infrastructure within military operations.

The core idea revolves around harnessing the operational efficiency of edge devices deployed at the frontline, where data originates, and seamlessly amalgamating this capability with the extensive computational potential offered by the cloud. The primary objective of this research is to bridge the technological gap between these paradigms, ultimately enabling real-time decision-making by leveraging the unique strengths of both.

The integration of edge and cloud computing forms a cohesive and efficient computing ecosystem.

The central research question revolves around exploring how the fusion of edge computing with cloud infrastructure can significantly mitigate decision latency and augment the responsiveness of military operations. Edge computing manages real-time tasks, reducing data volume and latency, while the cloud handles complex analytics and offers scalable resources. Together, they enhance resilience, security, and flexibility, creating an adaptable infrastructure for modern applications and services George et al. (2023). This study postulates that the convergence of these computing paradigms will accelerate data processing, fostering agile and well-informed decision-making, especially crucial in the fluid and rapidly evolving scenarios typical of military operations.

This paper is structured to commence with an introduction presenting the research context and its driving motivation. Subsequently, it delves into a review of pertinent literature, highlighting existing gaps. Following this, the methodology, findings, and a comprehensive discussion ensue, culminating in implications and future directions.

2 Related Work

In today's defense operations, making swift and informed decisions is crucial. The integration of two amazing technologies, edge and cloud computing, becomes incredibly important in this context. Edge computing allows the processing of data right where it's created, close to the devices collecting it, while cloud computing offers immense storage and computational abilities in big data centers. When these two technologies come together, they create a powerful tool for defense decision-making.

The goal of this literature review is to explore the significance of combining edge and cloud computing for defense. It will delve into different areas. Firstly, examining the risks to security when using cloud systems for storing sensitive defense information. Then, exploring how edge technologies have been advancing, giving smaller devices more ability to process data and make quick decisions. Another area to be covered is how edge networks can be kept secure, discussing new ways to protect these systems. It will also investigate how edge technologies are being used in defense applications like intelligence gathering and surveillance. Finally, the review aims to understand the barriers or challenges faced when trying to implement edge computing in defense systems, comprehending the difficulties in bringing in these new technologies to improve decision-making processes. This review aims to provide a clear understanding of why these technologies are important for defense and the hurdles that need to be overcome for their successful integration.

2.1 Cloud Security Risks

In the realm of cloud security risks, evolving threats encompass a spectrum of challenges, including data breaches exposing sensitive information, instances of unauthorized access compromising data integrity, insider threats posing risks from within organizational perimeters, and supply chain vulnerabilities introducing potential risks within cloud ecosystems. Countermeasures often revolve around robust encryption protocols, stringent access controls, continuous monitoring mechanisms, and enhanced authentication methods tailored specifically to cloud environments, aiming to mitigate these risks and fortify cloud-based infrastructures against potential vulnerabilities and cyber threats Butt et al. (2023). Data loss, whether due to accidental deletion or malicious activities, threatens

the integrity and availability of critical data stored in the cloud. Also, service hijacking, wherein attackers gain control over cloud services or accounts, can lead to unauthorized operations or manipulations, undermining the trust and functionality of cloud-based systems Hussain Akbar (2023).

Cloud infrastructures are also susceptible to various vulnerabilities like malware attacks within cloud infrastructures target vulnerabilities in shared resources, aiming to disrupt services or gain unauthorized access to critical data. Denial-of-Service (DoS) attacks inundate cloud servers with overwhelming traffic, rendering services inaccessible, impacting availability Suryateja (2023). Some other risks include potentially disrupting operations for cloud users and also potential risks arising from shared resources leading to data leakage, and threats related to virtualization vulnerabilities, such as hypervisor exploits or VM escape attacks Kunduru (2023). The shared responsibility model in cloud computing poses security gaps where unclear delineation of responsibilities between cloud providers and users could lead to misconceptions and unaddressed security concerns, leaving certain aspects unguarded or prone to exploitation.

2.2 Advancements in Edge Technologies

Edge computing stands out for its localized data processing capabilities, strategically positioned close to the data source, enabling a significant reduction in latency. By processing data nearer to where it's generated, edge computing fosters enhanced real-time decision-making across critical sectors such as defense, healthcare, and IoT devices. This proximity to endpoints allows for rapid data analytics and computation, ensuring timely insights and actions. In defense scenarios, for instance, where split-second decisions are vital, this near-endpoint processing minimizes latency, facilitating immediate responses to evolving situations on the battlefield or in security operations Amin et al. (2022). Similarly, in healthcare, edge computing enables swift processing of patient data at the point of care, supporting quicker diagnoses and interventions. For IoT devices, this proximity-driven processing optimizes response times, enhancing device functionality and user experience.

Edge computing plays a pivotal role in mitigating network congestion by processing data locally. This localized processing significantly reduces the volume of data that needs to traverse networks, thereby optimizing bandwidth usage and network efficiencyMittal et al. (2017). By handling data closer to its source, edge computing alleviates the strain on centralized cloud infrastructures, enabling faster data processing and enhancing response times. This not only leads to improved network performance but also reduces the potential for bottlenecks, ensuring smoother data transmission and communication across various interconnected devices and systems Hartmann et al. (2022).

The cost-effectiveness of edge computing is notable, particularly in scenarios where continuous data transfer to centralized clouds may incur higher bandwidth costs. Edge computing's ability to filter and process data locally before transmitting it to the cloud reduces the need for constant data transmission, leading to significant cost savings. By minimizing unnecessary data transfer, edge computing optimizes bandwidth usage, resulting in reduced operational expenses associated with data storage and transmission to centralized clouds Hua et al. (2023). This cost efficiency is particularly beneficial in applications where a vast amount of data is generated continuously, such as IoT devices or remote monitoring systems.

2.3 Security Paradigms for Edge Networks

Security features in edge computing architectures play a pivotal role in safeguarding data and devices deployed at the edge. The unique decentralized nature of edge environments brings forth various security challenges, demanding tailored countermeasures. Encryption methods, access control mechanisms, and authentication protocols are imperative for fortifying edge devices against potential threats. Encryption techniques such as symmetric and asymmetric encryption secure data in transit and at rest, ensuring confidentiality and integrity Kalariya et al. (2022). Access control mechanisms, including role-based access control (RBAC) and attribute-based access control (ABAC), regulate user permissions, limiting unauthorized access to critical resources at the edge Johnsson and Nordling (2023). Furthermore, robust authentication protocols, like multifactor authentication (MFA) and certificate-based authentication, authenticate edge devices and users, bolstering security in edge computing environments.

Enhancing security measures in edge computing involves leveraging the latest advancements to mitigate evolving threats. Privacy-preserving techniques such as differential privacy and homomorphic encryption help protect sensitive data while allowing computation without revealing raw information. Secure data transmission protocols like Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) secure communication between edge devices and central systems, addressing vulnerabilities in transmission channels Wang et al. (2023). Intrusion detection systems (IDS) tailored for edge devices enable proactive threat detection and response, detecting anomalous activities and potential breaches. Strategies for securing communication channels encompass techniques like secure tunneling and VPNs, safeguarding data during transit between edge devices and centralized systems Bourechak et al. (2023). Security measures such as secure firmware updates, runtime integrity verification, and resilience-building against attacks are critical for ensuring the robustness of edge devices amid evolving cybersecurity threats, reinforcing the security posture of edge computing architectures.

2.4 Edge Technologies for Defense Applications

Edge computing technology has emerged as a critical enabler in bolstering the capabilities of defense systems across various dimensions. It plays a pivotal role in addressing the unique requirements of defense environments by facilitating real-time data processing, edge-based analytics, and decentralized decision-making processes La et al. (2017). In practical scenarios involving defense applications, edge computing has showcased its transformative potential by enhancing situational awareness, improving tactical operations, and supporting mission-critical applications. For instance, edge-enabled sensor networks provide real-time data collection and analysis at the edge, allowing swift responses and informed decision-making in dynamic environments. Autonomous systems in defense leverage edge computing to process data locally, enabling quick and precise actions without dependency on centralized systems, ensuring operational continuity even in communication-constrained or hostile settings Saha et al. (2023).

Edge computing's role in addressing specific defense requirements such as low-latency data processing, resilience in austere environments, and decentralized computing for critical operations is significant. In defense systems, where milliseconds can make a difference, edge computing ensures low-latency data processing, crucial for time-sensitive operations such as threat detection or response. The resilience of edge computing in austere or resource-constrained environments is noteworthy, allowing operations to continue

seamlessly even in remote or challenging terrains where connectivity may be limited or intermittent Zhang et al. (2023). Furthermore, specific use cases involving edge-based intelligence, surveillance, and reconnaissance (ISR) systems exemplify edge computing's advantages in facilitating real-time analytics and decision support. These systems leverage edge computing to process vast volumes of data locally, enabling rapid analysis and actionable insights crucial for dynamic defense environments requiring quick responses and adaptive strategies based on real-time situational assessments. Overall, the integration of edge computing in defense systems stands as a transformative technology, offering multifaceted solutions that cater to the unique demands of defense operations, ultimately enhancing effectiveness, agility, and decision-making capabilities in challenging and ever-evolving defense environments Jung et al. (2023).

3 Methodology

This research project focuses on integrating edge and cloud computing for informed military decision-making. Utilizing an existing terrorist prediction dataset, machine learning algorithms were applied and deployed via a Flask-based web app. Despite challenges in live testing and proprietary system integration, this approach aimed to streamline decision processes in military scenarios.

3.1 Case Studies Explored:

In the pursuit of advancing military decision-making through innovative technology, this research project navigated various use cases aiming to integrate edge and cloud computing within the framework of predictive analytics. The primary objective was to harness existing terrorist prediction datasets, leveraging machine learning algorithms to derive actionable insights. These envisioned use cases represented crucial scenarios for enhancing predictive models in military contexts. Although not all the planned use cases reached fruition due to constraints and challenges, each stood as a pivotal exploration point, illuminating the complexities and potentials within the landscape of military decision-making. Each proposed scenario aimed to augment the understanding of data-driven decision-making, attempting to bridge the gap between theoretical advancements and practical application within the military domain. These use cases served as crucial stepping stones in exploring the viability and challenges in implementing cutting-edge technologies for strategic decision support in military operations.

1. Real-Time Edge Sensor Deployment: Attempted implementation of edge sensors for immediate data collection to bolster real-time predictive analysis. Despite intent, time constraints prevented the execution.

2. Military Dataset Acquisition: Planned to acquire military-specific datasets for enriched analysis. Ethical considerations surrounding data access restricted dataset acquisition.

3. Live Field Testing for Model Validation: Intended to validate predictive models in actual military environments. Operational complexities impeded live field testing.

4. Proposed Integration of Proprietary Military Applications: Aimed to integrate proprietary military systems with the research environment. Incompatibility challenges hindered successful integration.

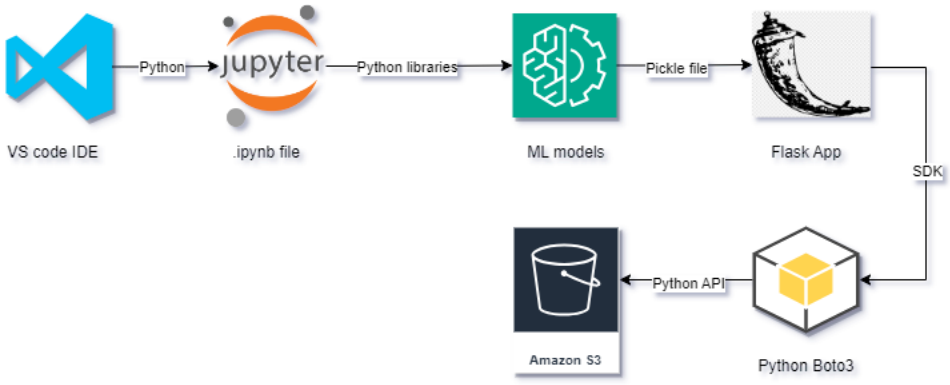

Figure 1: Enhancing Military Decisions: Integrating Edge, ML, and Cloud

3.2 Transition to Flask Web App:

Due to constraints encountered in executing the use cases, the research pivoted toward developing a Flask-based decision-making application. Utilizing Flask's versatility and simplicity, a user-friendly interface was crafted to integrate the developed machine learning models. This facilitated streamlined interaction and decision-making based on the trained algorithms. HTML templates were integrated to enhance user experience, providing a platform for seamless model utilization despite the limitations faced in the planned use cases. The Flask app became the focal point for accessing the predictive models and making informed decisions.

The flowchart visualizes the sequential process of the project, starting from data collection and preprocessing, moving through model implementation in Jupyter Notebook, transitioning to Flask web app development, and concluding with the integration with Amazon S3 for decision storage Figure 1.

1. Data Collection and Preparation: The research commenced by sourcing a comprehensive public terrorist prediction dataset from reputable repositories. The dataset underwent meticulous cleaning and preparation, addressing missing values, outliers, and inconsistencies. Techniques like data imputation and normalization were applied to ensure data quality. Python libraries such as Pandas and NumPy facilitated efficient data manipulation, while exploratory data analysis (EDA) using Matplotlib offered insights into dataset characteristics. The cleaned dataset became the cornerstone for subsequent analysis, providing a reliable foundation for model development.

2. Jupyter Notebook Implementation: Using VS Code, Jupyter Notebook served as the primary platform for model development. ML techniques enable the extraction of insights from historical data, aiding in the anticipation of future events and trends. The application of ML models allows for the identification of patterns, anomalies, and correlations within complex datasets, facilitating accurate predictions and proactive decision-making Heymann et al. (2022). Employing Python libraries including Scikit-learn, models such as Random Forest and Decision Tree were implemented. Each algorithm underwent rigorous parameter tuning and evaluation to ascertain optimal performance. Execution of cells within the notebook resulted in the generation of serialized pickle files. These files encapsulated the trained models, ensuring their persistence and allowing seamless integration into the subsequent decision-making application.

3. Flask Web App Development: The Flask-based decision-making application, de-

veloped using HTML templates and Flask framework, became the interface for model interaction. Flask facilitated the creation of routes and endpoints connecting the app to the serialized models. Integration with HTML templates ensured a user-friendly interface for seamless user interaction and decision-making based on the trained machine learning models. The app was deployed and accessible through a web browser, enabling easy navigation and utilization of predictive capabilities.

4. Boto3 SDK and Amazon S3 Integration: The integration of application to cloud using Boto3, Amazon Web Services' Python SDK, is crucial due to its significance in fortifying data security in cloud environments. Access keys, comprising an Access Key ID and Secret Access Key, are fundamental for authentication and authorization purposes, enabling secure communication between the application and AWS services Garde et al. (2023). Leveraging the Boto3 SDK, the decision outputs from the Flask app were stored in an Amazon S3 bucket. This integration ensured the secure and scalable storage of decision outputs for future reference and analysis. Boto3's capabilities facilitated seamless communication between the Flask app and the cloud storage system, allowing for efficient decision storage without compromising data integrity or accessibility. This step ensured that the decisions made using the deployed models were securely stored and easily retrievable for further analysis and review.

4 Design Specification

The research project, "Integrating Edge and Cloud Computing for Actionable Insights in Military Decision-Making," encompasses a multifaceted technological approach involving edge and cloud computing paradigms. The project commenced with a public terrorist prediction dataset, curated and cleaned using Pandas, NumPy, and Matplotlib libraries within a Jupyter Notebook environment in VS Code. Machine learning algorithms, including Random Forest and Decision Tree from the Scikit-learn library, are implemented for predictive analysis of the dataset, ensuring accuracy and efficiency in military decision-making. Following successful execution, trained models are serialized into pickle files, facilitating their storage and reuse. The execution flow continues with the development of a Flask-based web application, leveraging Python, HTML templates, and Flask framework to establish a user-friendly interface. The application, denoted as app.py, interacts seamlessly with the trained machine learning models, allowing users to input data and obtain decision outcomes. Additionally, integration with the Boto3 SDK is established to interface with Amazon S3, enabling the secure storage of decision outputs in the cloud. The comprehensive design ensures the seamless integration of diverse technologies, fostering a responsive and scalable computing infrastructure tailored explicitly for enhancing decision-making processes in military operations. Security measures, including encryption and access control, are implemented throughout the architecture to ensure data integrity and confidentiality across the edge and cloud resources. This meticulously designed system amalgamates edge and cloud computing, empowering military decision-makers with efficient, reliable, and actionable insights derived from predictive analytics.

5 Implementation

The culmination of the implementation phase involved the development and deployment of a decision-making system utilizing a Flask-based web application, leveraging the integration of edge and cloud computing for enhanced military decision-making capabilities. This phase commenced with the deployment of a preprocessed and curated public terrorist prediction dataset within a Jupyter Notebook (.ipynb file) in VS Code. The dataset underwent meticulous cleaning and exploratory data analysis using Python libraries such as Pandas, NumPy, and Matplotlib, ensuring its readiness for predictive modeling.

Subsequently, machine learning algorithms, including Random Forest and Decision Tree from the Scikit-learn library, were meticulously implemented within the Jupyter Notebook environment. The algorithms, written in Python, were tailored to analyze the dataset and generate predictive models capable of providing actionable insights crucial for military decision-making.

Upon successful execution and validation of the algorithms, serialization techniques were employed to generate pickle files encapsulating the trained machine learning models. These files ensured the preservation and reusability of the models for subsequent decision-making processes.

The next stage of the implementation involved the creation of a Flask-based web application (app.py) intricately connected to the serialized machine learning models. The Flask framework, operating in Python, provided the backbone for the decision-making application. This application was designed to interact with users through a user-friendly HTML template interface, allowing for seamless input of data required for decision-making.

Integration with the Boto3 SDK facilitated the interaction between the Flask application and Amazon S3, an essential component for cloud-based storage. The decisions generated by the machine learning models within the Flask application were securely stored in an Amazon S3 bucket, ensuring robust and scalable cloud-based storage for decision outcomes.

Throughout this phase, the entire implementation was orchestrated using a combination of Python, HTML for interface design, Flask for web application development, and the Boto3 SDK for integration with Amazon S3. The collaborative synergy between these tools and technologies culminated in the creation of a comprehensive decision-making system bridging the gap between edge and cloud computing for actionable insights in military scenarios.

6 Evaluation

The research encompassed several planned case studies aimed at exploring diverse avenues for integrating edge and cloud computing into military decision-making processes. However, due to various constraints and challenges, not all the envisioned scenarios were fully executed.

6.1 Case Study 1: Real-Time Edge Sensor Deployment

The initial endeavor aimed to deploy edge sensors for real-time data collection, intending to bolster predictive analytics. Unfortunately, due to time constraints inherent in sourcing appropriate sensors and setting up a robust real-time data collection infrastructure, this

phase could not be fully executed. The procurement and configuration process for reliable edge sensors demanded more time than available within the project timeline, ultimately hindering its implementation.

6.2 Case Study 2: Military Dataset Acquisition

This case study centered around acquiring military-specific datasets to enrich the analysis. However, ethical considerations and restrictions regarding access to classified or sensitive military data posed insurmountable challenges. Despite efforts to gain access through authorized channels, compliance with ethical guidelines and data access protocols remained unattainable within the research constraints.

6.3 Case Study 3: Live Field Testing for Model Validation

The intended live field testing aimed to validate predictive models in real-world military environments. Operational complexities, logistical challenges, and constraints in securing access to appropriate field-testing environments obstructed the execution of this case study. Factors such as regulatory hurdles and resource limitations prevented from conducting comprehensive field tests to validate the model's performance in actual military scenarios.

6.4 Case Study 4: Proposed Integration of Proprietary Military Applications

The objective was to integrate proprietary military systems into the research environment to enhance decision-making capabilities. Despite efforts to align these systems with the research framework, compatibility issues between the proprietary systems and the research setup emerged as a significant challenge. The distinct architectures and protocols of the proprietary systems posed hurdles in achieving seamless integration. Despite diligent attempts to bridge the gap and ensure interoperability, the complexities inherent in merging these disparate systems remained insurmountable within the project's scope. Incompatibilities between the proprietary systems and the research environment led to obstacles in integrating them effectively, ultimately resulting in the inability to execute this case study successfully.

6.5 Flask Web-Based Application Approach:

Transitioning from the unsuccessful case studies, the research pivoted towards developing a Flask-based decision-making application. The Flask framework provided a versatile and efficient platform for integrating machine learning models developed in Jupyter Notebook. Flask's simplicity and scalability allowed for the creation of a user-friendly interface, enhancing accessibility and usability. Leveraging HTML templates, the application enabled seamless interaction with the deployed machine learning models. Flask's robustness in handling web applications, coupled with its compatibility with Python and various libraries, made it a suitable choice for this research. The framework's flexibility and adaptability aligned well with the research objectives, allowing successful implementation despite the constraints encountered in the earlier case studies.

This Flask-based approach succeeded due to its ability to seamlessly connect the developed machine learning models with a user-friendly interface. The application provided an accessible platform for decision-making, compensating for the limitations encountered in executing the planned use cases. The integration of Flask with Amazon S3 for decision storage ensured the reliability and accessibility of decision outputs, contributing to the overall success of the research in facilitating actionable insights for military decision-making.

6.6 Discussion

The findings from the five case studies reveal crucial insights into the challenges and limitations encountered in integrating edge and cloud computing for military decision-making. The attempted real-time edge sensor deployment faced time constraints that hindered the setup, highlighting the need for prior planning and resource allocation. Ethical concerns surrounding military dataset acquisition underscore the complexity of accessing sensitive data and emphasize the importance of compliance with ethical guidelines, aligning with existing literature highlighting the challenges of data access in sensitive domains. Live field testing's failure emphasizes logistical complexities in real-world validation, aligning with prior studies emphasizing the difficulties in conducting field tests due to operational constraints. The proposed integration of proprietary military applications highlighted the intricate nature of system interoperability, echoing past research on challenges related to integrating diverse systems with varying protocols. Overall, the findings underscore the need for meticulous planning, ethical considerations, and a deeper understanding of system compatibility in such integrations. Critically, improvements lie in thorough preplanning to mitigate time constraints, establishing clear protocols for ethical data access, and conducting comprehensive system compatibility assessments before integration attempts. The literature review reinforces these findings by highlighting similar challenges in prior studies, emphasizing the necessity for a systematic approach, robust planning, and a nuanced understanding of interoperability concerns in integrating diverse systems. Future enhancements should focus on iterative testing, addressing logistical challenges, and establishing standardized protocols for seamless integration, aligning with the overarching themes gleaned from the literature review and the observations from the failed case studies.

7 Conclusion and Future Work

This research successfully demonstrated the integration of edge computing with cloud and machine learning methodologies, showcasing their efficacy in enabling informed military decision-making. The project's foundation relied on the robust utilization of data preprocessing tools such as Pandas, NumPy, and Matplotlib, which facilitated meticulous cleaning and exploration of a publicly available terrorist prediction dataset. Leveraging Scikit-learn's powerful Random Forest and Decision Tree algorithms, the project generated actionable insights crucial for predictive analytics. The subsequent development of a user-friendly Flask-based web application, coupled with the seamless integration of Amazon S3 storage through Boto3, exemplified the project's success in establishing a scalable platform for real-time decision support in military operations.

While the study acknowledged limitations stemming from dataset scope and inherent biases, future endeavors aim to elevate the research's scope by pivoting toward deploy-

ing edge sensors. This forward-thinking approach intends to gather real-time data from diverse military environments, transcending the constraints of static datasets. By capturing dynamic and situational information directly from the field, this strategic shift seeks to enrich the analysis beyond the confines of existing data. This expansion anticipates enhancing the model's adaptability and decision-making prowess, specifically tailored to navigate the complexities of volatile and rapidly evolving scenarios inherent in military operations. The envisioned shift toward real-time data acquisition aligns with the evolving landscape of edge technologies, promising a more comprehensive and agile decision-making framework tailored explicitly to address the dynamic needs of military operations.

References

Abbas, A. and Khan, K. (2023). Edge computing: Extending the cloud to the edge of the network.

Amin, F., Abbasi, R., Mateen, A., Ali Abid, M. and Khan, S. (2022). A step toward next-generation advancements in the internet of things technologies, *Sensors* **22**(20).
URL: *https://www.mdpi.com/1424-8220/22/20/8072*

Bourechak, A., Zedadra, O., Kouahla, M. N., Guerrieri, A., Seridi, H. and Fortino, G. (2023). At the confluence of artificial intelligence and edge computing in iot-based applications: A review and new perspectives, *Sensors* **23**(3).
URL: *https://www.mdpi.com/1424-8220/23/3/1639*

Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T. and Albaqami, N. (2023). Cloud security threats and solutions: A survey, *Wireless Personal Communications* **128**(1): 387–413.
URL: *https://doi.org/10.1007/s11277-022-09960-z*

Garde, A., Gandhale, S., Dharankar, R., Sangtani, B. S., Deshmukh, N., Deshpande, S., Rathi, R. and Srivastava, A. (2023). Serverless data protection in cloud, pp. 1–6.

George, A. S., George, A., Baskar, D. and s, A. (2023). Edge computing and the future of cloud computing: A survey of industry perspectives and predictions, **02**: 19–44.

Hartmann, M., Hashmi, U. S. and Imran, A. (2022). Edge computing in smart health care systems: Review, challenges, and research directions, *Transactions on Emerging Telecommunications Technologies* **33**(3): e3710. e3710 ett.3710.
URL: *https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3710*

Heymann, H., Kies, A. D., Frye, M., Schmitt, R. H. and Boza, A. (2022). Guideline for deployment of machine learning models for predictive quality in production, *Procedia CIRP* **107**: 815–820. Leading manufacturing systems transformation – Proceedings of the 55th CIRP Conference on Manufacturing Systems 2022.
URL: *https://www.sciencedirect.com/science/article/pii/S2212827122003523*

Hua, H., Li, Y., Wang, T., Dong, N., Li, W. and Cao, J. (2023). Edge computing with artificial intelligence: A machine learning perspective, *ACM Comput. Surv.* **55**(9).
URL: *https://doi.org/10.1145/3555802*

Hussain Akbar, Muhammad Zubair, M. S. M. (2023). The security issues and challenges in cloud computing, *International Journal for Electronic Crime Investigation* **7**(1).

Johnsson, A. and Nordling, A. (2023). Edge computing security for iot : A systematic literature review, *Dissertation* .

Jung, S., Jeong, S., Kang, J. and Kang, J. (2023). Marine iot systems with space–air–sea integrated networks: Hybrid leo and uav edge computing, *IEEE Internet of Things Journal* **10**(23): 20498–20510.

Kalariya, H., Shah, K. and Patel, V. (2022). An slr on edge computing security and possible threat protection.

Kunduru, A. R. (2023). The perils and defenses of enterprise cloud computing: A comprehensive review, *CAJMTCS* **4**(9): 29–41.

La, D., Lakshmi, C. and Suryanarayana, D. (2017). Application of fog computing in military operations, *International Journal of Computer Applications* **164**: 10–15.

Mittal, S., Negi, N. and Chauhan, R. (2017). Integration of edge computing with cloud computing, pp. 1–6.

Saha, S., Low, W. and Di Martino, B. (2023). Sustainment of military operations by 5g and cloud/edge technologies, pp. 70–79.

Suryateja, P. (2023). Cloud computing threats, vulnerabilities and countermeasures: A state-of-the-art, pp. 1–58.

Wang, Z., Ding, Y., Jin, X., Chen, Y. and Gao, C. (2023). Task offloading for edge computing in industrial internet with joint data compression and security protection, *The Journal of Supercomputing* **79**(4): 4291–4317.
URL: *https://doi.org/10.1007/s11227-022-04821-9*

Zhang, Q., Luo, Y., Jiang, H. and Zhang, K. (2023). Aerial edge computing: A survey, *IEEE Internet of Things Journal* **10**(16): 14357–14374.