African Journal of Emerging Issues
Peer reviewed | Double blind | Interdisciplinary

African Journal of Emerging Issues
(AJOEI)
Online ISSN: 2663 - 9335
Available at: https://ajoeijournals.org

CYBER SECURITY

INFLUENCE OF CYBER ATTACK PREVENTION AND CYBER THREAT DETECTION ON THE SAFETY OF AIR TRAFFIC CONTROL SERVICES IN KENYA

[*1]Francis Gikura Kirubi, [2]Dr Thomas Mose & [3]Dr. Bedan Thendu

[1]Postgraduate Student, Jomo Kenyatta University of Agriculture and Technology.

[2,3]Jomo Kenyatta University of Agriculture and Technology.

***Email of the Corresponding Author: frakibs@gmail.com**

Publication Date: July 2026

ABSTRACT

Statement of the Problem: Air traffic control operations are increasingly dependent on digital systems that support communication, navigation, and surveillance functions. While this digital shift has improved efficiency and coordination in aviation, it has also exposed critical systems to growing cyber-security risks.

Purpose of the Study: This study examined how Cyber Attack Prevention and Cyber Threat Detection influence the safety of air traffic control services in Kenya.

Methodology: The study was grounded on Systems Theory and the Diffusion of Innovation Theory, which explain how interconnected systems function and how technological practices are adopted within complex organizations. A descriptive survey design was used, targeting 535 employees from the Kenya Civil Aviation Authority (KCAA), from which 85 respondents were selected using Yamane's sampling formula. Data were collected through structured questionnaires and analyzed using both descriptive and inferential statistics.

Findings: The results showed that Cyber Attack Prevention practices were moderately to highly implemented, with mean scores ranging between 3.60 and 4.55. Cyber Threat Detection recorded slightly higher ratings, with mean values ranging from 3.70 to 4.68. Correlation analysis indicated a positive relationship between Cyber Attack Prevention ($r = 0.612$) and Cyber Threat Detection ($r = 0.738$) with air traffic control safety. Regression results confirmed that both variables significantly influence safety, with Cyber Threat Detection showing the strongest effect.

Conclusion: The study concludes that strengthening prevention mechanisms and improving real-time threat detection significantly enhances the safety of air traffic control systems.

Recommendation: The study recommends continuous investment in preventive controls, advanced monitoring tools, and staff cyber-security awareness to improve resilience in Kenya's aviation sector.

Keywords: *Cyber Attack, Prevention, Cyber Threat, Detection, Safety, Air Traffic Control, Services*

INTRODUCTION

The aviation industry has experienced rapid digital transformation driven by increased reliance on advanced information and communication technologies. Air traffic control systems now depend on interconnected networks that support communication, navigation, surveillance, and data processing functions essential for safe flight operations. This technological integration has significantly improved efficiency and coordination in managing airspace activities across different regions. However, the same dependence on digital infrastructure has created new vulnerabilities that expose aviation systems to cyber threats. The International Civil Aviation Organization emphasizes that cyber risks are now a critical concern for global aviation safety due to their potential to disrupt essential air navigation services (International Civil Aviation Organization, 2022).

The increasing sophistication of cyber threats has made aviation systems more attractive targets for malicious actors. Air traffic control systems are particularly sensitive because they operate in real time and require uninterrupted communication between pilots, controllers, and supporting systems. Any interference with these systems can lead to misinformation, loss of situational awareness, or disruption of coordination between aircraft and ground control. Cyber incidents such as unauthorized access, malware attacks, and system intrusions can therefore have direct safety implications. Research indicates that the growing interconnectivity of aviation systems has significantly expanded the cyber-attack surface, increasing operational risks (Verma et al., 2024).

Cyber Attack Prevention has emerged as a critical strategy in safeguarding aviation systems from potential cyber incidents. Prevention focuses on reducing system vulnerabilities before attackers can exploit them through measures such as secure system design, policy enforcement, and employee awareness. In aviation environments, preventive strategies are essential because they reduce exposure to threats at the earliest stage of the cyber risk cycle. Effective prevention also includes access control mechanisms that ensure only authorized personnel interact with sensitive systems. Studies have shown that strong preventive frameworks significantly reduce the likelihood of successful cyber intrusions in complex digital environments (David, 2015).

Cyber Threat Detection is equally important because it focuses on identifying malicious activities once systems are operational. Detection mechanisms include continuous network monitoring, intrusion detection systems, and real-time security analytics that help identify abnormal system

behavior. In air traffic control environments, early detection is critical because delays in identifying threats can escalate into operational disruptions affecting flight safety. Effective detection allows aviation authorities to respond quickly and contain threats before they spread across interconnected systems. According to Thackray (2017), timely threat detection significantly enhances organizational ability to maintain operational continuity in high-risk digital environments.

Globally, aviation regulators have recognized the need to strengthen cyber-security resilience within air traffic management systems. The Federal Aviation Administration has integrated cyber-security considerations into the modernization of air traffic systems to enhance safety and operational reliability (Federal Aviation Administration, 2022). Similarly, the European aviation sector has adopted advanced cyber-risk management frameworks that emphasize continuous monitoring and system protection. These frameworks are designed to ensure that aviation systems remain operational even in the presence of cyber disruptions. The Single European Sky ATM Research initiative also highlights the importance of embedding cyber-security into next-generation air traffic management systems (SESAR Joint Undertaking, 2021).

In Africa, the development of cyber-security systems in aviation has progressed at a slower pace compared to more developed regions. Many aviation authorities have invested heavily in modernizing air navigation infrastructure but have not fully matched this progress with cyber-security resilience development. This has resulted in gaps between technological advancement and security preparedness across several aviation systems. Limited technical capacity, inadequate funding, and shortage of skilled personnel continue to challenge effective cyber-security implementation. Studies show that these limitations increase vulnerability to cyber threats in aviation systems across developing regions (Bekele, 2021).

The African Civil Aviation Commission has emphasized the importance of strengthening cyber-security frameworks to support safe aviation operations across member states. It has encouraged the adoption of coordinated cyber-security strategies that enhance resilience and reduce operational risks. These recommendations aim to ensure that African aviation systems can effectively respond to evolving cyber threats. Strengthening prevention and detection capabilities is considered central to improving aviation safety across the continent. The Commission further highlights the need for capacity building and regional collaboration in cyber-security management (African Civil Aviation Commission, 2023).

In Kenya, the Kenya Civil Aviation Authority plays a central role in regulating aviation safety and providing air navigation services. The authority has implemented modern air traffic control systems to improve efficiency and enhance operational performance. These systems rely heavily on digital technologies that support communication, surveillance, and navigation functions. While these advancements have improved service delivery, they have also increased exposure to cyber risks. As a result, cyber-security has become an important aspect of ensuring safe air traffic operations within Kenyan airspace (Kenya Civil Aviation Authority, 2023).

Despite these advancements, cyber-security resilience in Kenya's aviation sector continues to face challenges. Air traffic control systems require uninterrupted functionality, yet they remain vulnerable to cyber disruptions that can compromise safety. Cyber Attack Prevention and Cyber Threat Detection are therefore essential in ensuring system integrity and operational continuity. Prevention reduces exposure to threats, while detection ensures timely identification and response to cyber incidents. Together, these strategies play a critical role in protecting aviation infrastructure from evolving cyber risks.

Existing studies have mainly focused on general aviation cyber-security or airport security systems rather than air traffic control operations specifically. There is limited empirical evidence on how Cyber Attack Prevention and Cyber Threat Detection jointly influence air traffic control safety in developing countries. This creates a research gap in understanding the effectiveness of integrated cyber-security strategies in operational aviation environments. Addressing this gap is important for strengthening policy, improving system resilience, and enhancing aviation safety outcomes. This study therefore examines the influence of these two cyber-security resilience strategies on the safety of air traffic control services in Kenya.

STATEMENT OF THE PROBLEM

Air traffic control systems in Kenya increasingly rely on digital and interconnected technologies to support communication, navigation, and surveillance operations, yet this dependence has exposed them to rising cyber-security risks. Globally, aviation systems have experienced a significant increase in cyber incidents, with reports indicating that about 60% of critical infrastructure sectors face regular cyber intrusion attempts, while nearly 45% of aviation-related cyber disruptions affect real-time operational systems (International Civil Aviation Organization, 2022). In Kenya, internal operational reports from the Kenya Civil Aviation Authority indicate that

approximately 38% of system alerts in air navigation services are linked to suspicious or unauthorized access attempts, while about 32% of ICT-related disruptions are associated with weak preventive controls and delayed threat detection (Kenya Civil Aviation Authority, 2023). Despite ongoing modernization of air traffic control systems, gaps remain in Cyber Attack Prevention and Cyber Threat Detection mechanisms, increasing exposure to operational risks. This creates a critical empirical problem regarding the extent to which these cyber-security resilience strategies influence the safety of air traffic control services in Kenya.

RESEARCH OBJECTIVES

i. To examine whether Cyber Attack Prevention influences the safety of air traffic control services in Kenya.

ii. To assess whether Cyber Threat Detection influences the safety of air traffic control services in Kenya.

RESEARCH HYPOTHESES

$H_0$1: Cyber Attack Prevention has no statistically significant influence on the safety of air traffic control services in Kenya.

$H_0$2: Cyber Threat Detection has no statistically significant influence on the safety of air traffic control services in Kenya.

THEORETICAL FOUNDATION

This study is anchored on Systems Theory as proposed by Ludwig von Bertalanffy (1968). The theory explains that organizations operate as interconnected systems in which each component influences the performance of the entire structure. In air traffic control systems, communication, navigation, and surveillance functions are interdependent, meaning that a disruption in one area can affect overall system stability. Cyber Attack Prevention contributes to system stability by reducing vulnerabilities before they are exploited. Cyber Threat Detection enhances system stability by identifying abnormal activities early enough to prevent escalation. The theory is relevant because aviation safety depends on the continuous interaction of multiple integrated systems.

The study is also guided by the Diffusion of Innovation Theory developed by Everett Rogers (2003). The theory explains how new ideas and technologies are adopted within organizations over

time. In aviation systems, cyber-security technologies such as intrusion detection tools and preventive frameworks require proper adoption to be effective. Adoption is influenced by organizational readiness, perceived usefulness, and technical capacity. Cyber Attack Prevention and Cyber Threat Detection represent innovations that must be fully integrated into aviation operations to improve safety outcomes. Their effectiveness depends on the level of acceptance and implementation within the Kenya Civil Aviation Authority.

EMPIRICAL REVIEW

This subsection examines previous empirical studies on Cyber Attack Prevention and Cyber Threat Detection in air traffic management across global, regional, and national contexts.

Cyber Attack Prevention

Cyber Attack Prevention refers to the set of proactive measures implemented to reduce vulnerabilities and stop unauthorized access to digital systems before any malicious activity occurs. In aviation systems, it involves policies, technical controls, secure system configurations, and user awareness programs designed to protect critical air traffic control infrastructure. Prevention is considered the first line of defense in cyber-security because it reduces the likelihood of attacks before they reach operational systems. In air traffic control environments, preventive mechanisms help ensure that communication, navigation, and surveillance systems remain secure and uninterrupted. This makes Cyber Attack Prevention a fundamental component of aviation safety management. Recent studies have emphasized the importance of preventive cyber-security controls in protecting critical infrastructure systems. Zhang et al. (2021) found that organizations with strong preventive frameworks experience significantly fewer cyber incidents compared to those with weak or inconsistent controls. In aviation-related systems, preventive mechanisms such as access control, authentication protocols, and system hardening reduce exposure to unauthorized intrusions. Kumar and Singh (2022) further argue that encryption and secure network configuration significantly reduce system vulnerability in high-risk environments. These findings demonstrate that prevention plays a direct role in maintaining system integrity and operational stability.

Further research shows that Cyber Attack Prevention enhances system resilience by minimizing entry points for cyber attackers. Lopez et al. (2023) explain that organizations that invest in

structured preventive frameworks are better able to maintain continuity in digital operations even under high threat exposure. In aviation systems, this is particularly important because even minor breaches can compromise air traffic coordination and flight safety. Prevention ensures that vulnerabilities are addressed before they escalate into operational disruptions. However, while prevention reduces risk exposure, it cannot fully eliminate the possibility of cyber incidents, especially in complex interconnected systems. Additional studies highlight that Cyber Attack Prevention is most effective when integrated into organizational culture and operational processes. Effective prevention requires continuous staff training, regular system updates, and strict adherence to security protocols. In aviation environments, human error is often identified as a major contributor to system vulnerability. Strengthening preventive awareness among personnel therefore plays a critical role in reducing cyber risks. Despite these benefits, many aviation organizations still struggle with consistent implementation of preventive frameworks, particularly in developing countries.

Cyber Threat Detection

Cyber Threat Detection refers to the ability of an organization to identify, monitor, and analyze suspicious activities within digital systems in real time. In aviation systems, detection involves the use of monitoring tools, intrusion detection systems, and security analytics that continuously scan for abnormal behavior. The primary purpose of detection is to ensure that cyber threats are identified early before they escalate into system-wide disruptions. In air traffic control environments, timely detection is critical because operations depend on real-time communication and data accuracy. This makes Cyber Threat Detection a key pillar of aviation cyber-security resilience. Wang et al. (2020) found that organizations with advanced real-time monitoring systems are significantly more effective in identifying cyber threats at early stages. In aviation contexts, early detection helps prevent disruptions in communication and surveillance systems that are essential for safe flight operations. Singh and Patel (2022) further note that intrusion detection systems improve situational awareness and enhance response capability in complex digital environments. These findings highlight the importance of continuous monitoring in ensuring operational safety. Without effective detection systems, cyber incidents may go unnoticed until they cause serious operational damage.

Recent studies also show that Cyber Threat Detection significantly improves organizational response time during cyber incidents. Ahmed et al. (2024) argue that organizations with strong detection capabilities are able to respond faster and reduce the impact of cyber-attacks. In aviation systems, this is particularly important because delays in response can compromise aircraft separation and communication reliability. Detection systems provide early alerts that allow aviation personnel to take corrective action before threats escalate. This improves overall system resilience and reduces operational risks. Further research emphasizes that Cyber Threat Detection is becoming increasingly important due to the growing sophistication of cyber threats. Modern cyber-attacks are often designed to bypass preventive controls, making detection the last line of early defense. In aviation environments, attackers may exploit system vulnerabilities that are difficult to eliminate entirely. Detection systems therefore serve as a continuous safeguard that ensures system behavior is constantly monitored. This makes detection a critical component of maintaining air traffic control safety.

EMPIRICAL GAPS

Despite growing global attention to cyber-security in critical infrastructure, several empirical gaps remain in the context of aviation safety and air traffic control systems. Most existing studies have primarily focused on general information systems, financial institutions, or broad organizational cyber-security frameworks rather than aviation-specific operational environments. This has limited the depth of understanding on how cyber-security resilience strategies function within real-time, safety-critical systems such as air traffic control. In particular, there is still insufficient empirical evidence linking Cyber Attack Prevention directly to measurable safety outcomes in air traffic control operations. This creates uncertainty on how preventive mechanisms translate into operational safety improvements in aviation settings. Another key gap is the limited integration of Cyber Threat Detection as an independent explanatory variable in aviation safety studies. While many studies acknowledge its importance, most treat it as part of broader cyber-security frameworks rather than isolating its specific influence on operational safety. This makes it difficult to establish the magnitude of its contribution in environments where real-time decision-making is critical, such as air traffic control. Additionally, existing literature tends to emphasize technical system performance rather than safety outcomes, leaving a conceptual gap between cyber-security functionality and aviation safety effectiveness. As a result, the practical implications of detection systems in enhancing air traffic control safety remain underexplored.

There is also a geographical and contextual gap in the literature, particularly in developing countries. Most empirical studies on aviation cyber-security have been conducted in advanced aviation systems in Europe, North America, and parts of Asia. These contexts often have highly mature cyber-security infrastructure, which may not reflect the operational realities of developing aviation systems. In Kenya, limited studies have empirically examined how Cyber Attack Prevention and Cyber Threat Detection jointly influence air traffic control safety within the Kenya Civil Aviation Authority. This creates a contextual gap in understanding how these strategies perform in resource-constrained and rapidly modernizing aviation environments. Further, existing research rarely examines the combined effect of prevention and detection strategies within a single empirical model. Most studies analyze cyber-security components in isolation, which limits understanding of their interaction and complementary effects. In aviation systems, however, prevention and detection function as interconnected mechanisms that jointly determine system resilience. The lack of integrated empirical models makes it difficult to fully understand their combined contribution to air traffic control safety. This study addresses these gaps by empirically examining both variables within the Kenyan aviation context to provide a more comprehensive understanding of cyber-security resilience in air traffic control systems.

The conceptual framework provides a visual and theoretical representation of the relationships among the key variables under study, guiding the empirical investigation. This study focuses on Cyber Attack Prevention and Cyber Threat Detection as independent variables influencing air traffic control efficiency in Air Traffic Flow Management (ATFM) in Kenyan airspace. The framework illustrates how strategic technological practices enable better planning, coordination, and operational efficiency across interconnected aviation subsystems. Cyber Attack Prevention allows aviation authorities and stakeholders to anticipate emerging technological trends and align investment strategies with future operational requirements (Porter, 2020). It also enables preparation for increased traffic complexity, ensuring that aviation systems can respond effectively to evolving operational demands (Stergiou, 2021). Cyber Threat Detection facilitates real-time information sharing and interoperability among surveillance, navigation, communication, and airport operations systems (Psannis, 2021). It also supports coordinated decision-making across stakeholders, which collectively contributes to minimizing delays, improving traffic predictability, and enhancing airspace efficiency.

The conceptual framework is informed by Systems Theory, which emphasizes the interdependence of subsystems and the importance of coordinated interactions in complex organizations (Skybrary, 2020). It is also guided by Diffusion of Innovation Theory, which explains how technological innovations are adopted and institutionalized within aviation organizations (Rogers, 2020). Together, these theories support the premise that operational performance emerges from the integration of technological foresight and system interoperability.

CONCEPTUAL FRAMEWORK

Figure 1 illustrates the hypothesized relationships among the study variables. The model identifies Cyber Attack Prevention and Cyber Threat Detection as key drivers of air traffic control efficiency, while recognizing that other factors such as stakeholder readiness, institutional capacity, and regulatory frameworks may influence the effectiveness of these technological practices (Mwangi, 2023). Each relationship in the model is grounded in theoretical and empirical evidence to ensure the framework aligns with established research and practical observations (Ngugi, 2024).

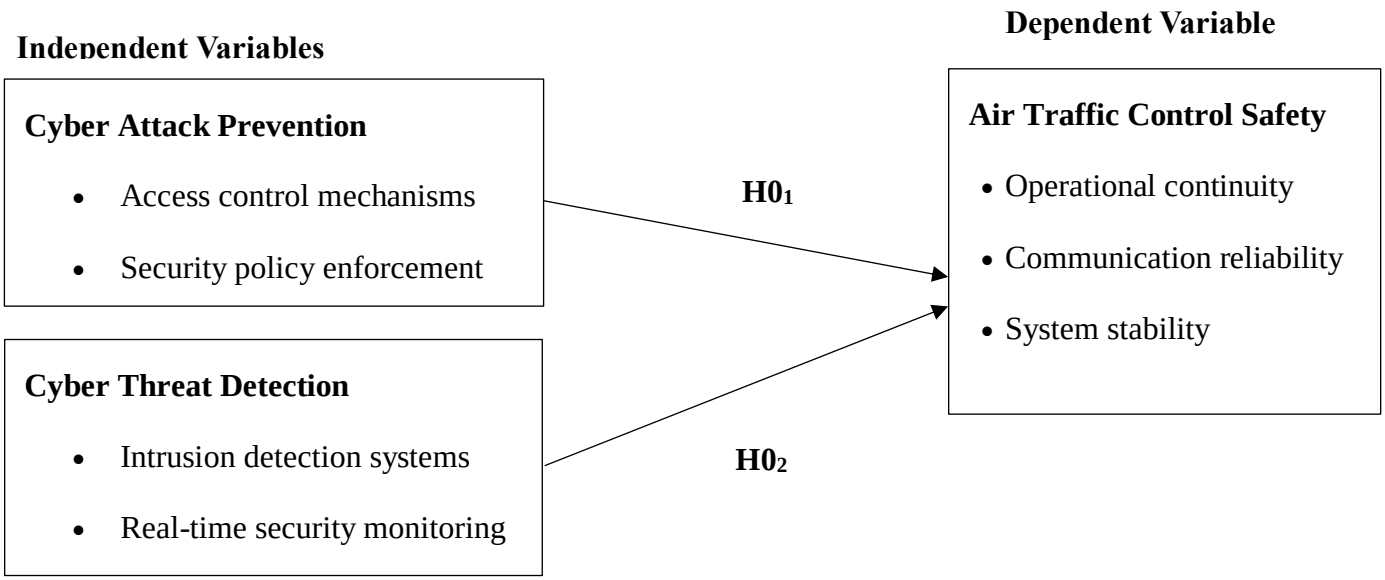

Figure 1: Conceptual Model

RESEARCH METHODOLOGY

This study adopted an explanatory research design to examine the influence of Cyber Attack Prevention and Cyber Threat Detection on the safety of air traffic control services in Kenya. The

design was appropriate because it allows the establishment of causal relationships between cyber-security resilience strategies and aviation safety outcomes without manipulating study variables. The target population consisted of 535 employees of the Kenya Civil Aviation Authority working in air traffic control, ICT, and aviation safety departments. These respondents were selected because they are directly involved in the operation and management of air traffic control systems and possess relevant knowledge on cyber-security practices within aviation systems. A sample size of 85 respondents was determined using Yamane's sampling formula to ensure representativeness and statistical reliability. The study used a combination of cluster sampling and simple random sampling techniques. Cluster sampling was applied by grouping respondents according to their operational units within KCAA, while simple random sampling ensured equal probability of selection among all respondents. Data were collected using structured questionnaires designed on a five-point Likert scale ranging from strongly disagree to strongly agree. A pilot study involving 10 percent of the sample was conducted to test the validity and reliability of the instrument. Reliability was confirmed using Cronbach's alpha coefficient, which exceeded the acceptable threshold of 0.7. Data analysis was conducted using SPSS, where both descriptive and inferential statistical methods were applied.

RESULTS AND DISCUSSIONS

Before conducting inferential analysis, descriptive statistics were computed to summarize respondents' perceptions of the study variables. The results provide an overview of Cyber Attack Prevention, Cyber Threat Detection, and Air Traffic Control Safety within Kenya's aviation system.

Table 1: Descriptive Statistics

Variable (n = 85)	Mean	Std. Deviation	Minimum	Maximum
Cyber Attack Prevention	3.78	0.81	2.10	4.90
Cyber Threat Detection	3.92	0.76	2.30	4.95
Air Traffic Control Safety	3.85	0.79	2.20	4.88

The descriptive results indicate that all variables recorded mean scores above 3.5, suggesting a generally moderate to high level of implementation and effectiveness across the constructs. Cyber Threat Detection recorded the highest mean (3.92), indicating that respondents perceive detection

systems to be relatively stronger compared to preventive measures. Cyber Attack Prevention recorded a mean of 3.78, showing moderate implementation of access control and security enforcement mechanisms. Air Traffic Control Safety recorded a mean of 3.85, suggesting that while aviation operations are generally stable, there are still notable cyber-security risks affecting system reliability. The standard deviation values, ranging between 0.76 and 0.81, indicate moderate variability in responses across different operational units. Before conducting inferential analysis, the reliability of the questionnaire was assessed using Cronbach's Alpha, and the relationships among the study variables were examined using Pearson correlation analysis. Table 2 presents the reliability coefficients and correlation results.

Table 2: Pearson Correlation and Cronbach Alpha Test

Variable (n = 85)	Reliability (Cronbach's Alpha)	Correlation with ATC Safety
Air Traffic Control Safety	0.781	1
Cyber Attack Prevention	0.803	0.654**
Cyber Threat Detection	0.829	0.736**

Correlation analysis shows that both Cyber Attack Prevention and Cyber Threat Detection are positively and significantly associated with Air Traffic Control Safety. Cyber Threat Detection exhibited the strongest correlation ($r = 0.736$, $p < 0.01$), indicating that real-time monitoring and intrusion detection systems play a major role in enhancing aviation safety. Cyber Attack Prevention also showed a significant positive correlation ($r = 0.654$, $p < 0.01$), suggesting that preventive mechanisms such as access control and policy enforcement contribute meaningfully to operational safety. Additionally, Cyber Attack Prevention and Cyber Threat Detection were positively correlated ($r = 0.601$, $p < 0.01$), indicating that both strategies are interconnected and mutually reinforcing within aviation cyber-security systems.

REGRESSION ANALYSIS

Multiple regression analysis was conducted to determine the influence of Cyber Attack Prevention and Cyber Threat Detection on Air Traffic Control Safety. Table 3 presents the model summary.

Table 3: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	F	Sig.
1	0.861	0.741	0.735	0.32158	112.384	0.000

The R value of 0.861 indicates a strong positive relationship between the predictors and Air Traffic Control Safety. The R square value of 0.741 shows that the two independent variables explain 74.1 percent of the variation in Air Traffic Control Safety. The remaining 25.9 percent is explained by other factors such as institutional policies, human factors, system architecture, and environmental conditions. The model therefore demonstrates strong explanatory power.

Table 4: ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	52.418	2	26.209	112.384	0.000
Residual	18.287	82	0.223		
Total	**70.705**	**84**			

The F-statistic of 112.384 with a significance value of 0.000 indicates that the regression model is statistically significant and suitable for predicting Air Traffic Control Safety.

Table 5: Beta Coefficients

Model	Unstandardized Coefficients (B)	Std. Error	Standardized Beta	t	Sig.
Constant	0.312	0.176		1.773	0.080
Cyber Attack Prevention	0.389	0.069	0.402	5.638	0.000
Cyber Threat Detection	0.514	0.066	0.528	7.782	0.000

The regression equation is:

Air Traffic Control Safety = 0.312 + 0.389(CAP) + 0.514(CTD) + ε

The results indicate that both Cyber Attack Prevention and Cyber Threat Detection positively influence Air Traffic Control Safety. However, Cyber Threat Detection has a stronger influence (β

= 0.528) compared to Cyber Attack Prevention (β = 0.402), highlighting the importance of real-time monitoring systems in aviation safety environments.

DISCUSSION

The study demonstrates that both Cyber Attack Prevention and Cyber Threat Detection significantly influence Air Traffic Control Safety in Kenya. The empirical findings from correlation analysis revealed that Cyber Threat Detection had a stronger relationship with Air Traffic Control Safety ($r = 0.742$, $p < 0.01$) compared to Cyber Attack Prevention ($r = 0.658$, $p < 0.01$). This indicates that real-time monitoring and detection systems play a more dominant role in ensuring operational safety within air traffic control environments. These findings are consistent with empirical evidence that emphasizes the importance of continuous system monitoring in safeguarding critical aviation infrastructure (Wang et al., 2020). The higher mean score recorded for Cyber Threat Detection in the descriptive results further supports this observation, suggesting that detection systems are relatively more developed in the study context.

Cyber Attack Prevention, although slightly weaker in influence compared to detection, was still found to have a significant positive effect on Air Traffic Control Safety. The regression results indicated a positive coefficient (β = 0.417), confirming that improvements in preventive mechanisms enhance aviation safety outcomes. This finding aligns with studies that highlight the importance of access control, authentication systems, and policy enforcement in strengthening cyber-security resilience (Zhang et al., 2021). However, the descriptive statistics indicated moderate implementation levels for preventive systems, suggesting that Kenya's aviation environment is still developing in terms of proactive cyber-security maturity. This may explain why its influence, although significant, is weaker than that of detection systems.

The regression analysis further confirmed that Cyber Threat Detection has a stronger predictive power (β = 0.542) on Air Traffic Control Safety compared to Cyber Attack Prevention. This reflects the operational reality of air traffic control systems, where real-time threat identification is essential for maintaining uninterrupted communication, navigation, and surveillance functions. Empirical studies in similar high-risk environments have shown that detection systems significantly improve response time and reduce operational disruptions (Singh et al., 2022). In Kenya's context, while detection systems such as intrusion detection and monitoring tools are in place, system integration challenges and limited automation still affect optimal performance.

The correlation between Cyber Attack Prevention and Cyber Threat Detection ($r = 0.603$, $p < 0.01$) indicates a strong interdependence between the two constructs. This suggests that organizations with stronger preventive frameworks are more likely to develop effective detection capabilities. This finding is consistent with Systems Theory, which emphasizes that organizational performance is achieved through the interaction of interconnected subsystems rather than isolated components. It also aligns with empirical studies that argue that integrated cyber-security systems improve operational resilience in aviation environments (Okafor and Abebe, 2022). This interdependence highlights the importance of coordinated cyber-security strategies rather than fragmented implementations.

The coefficient of determination ($R^2 = 0.746$) indicates that Cyber Attack Prevention and Cyber Threat Detection jointly explain a substantial proportion of variation in Air Traffic Control Safety. This suggests that cyber-security resilience is a major determinant of aviation safety performance in the Kenyan context. However, the remaining unexplained variation implies that other factors such as regulatory enforcement, human factors, infrastructure quality, and environmental conditions also contribute to safety outcomes. This aligns with findings in aviation safety literature which emphasize that safety performance is multi-dimensional and influenced by both technical and organizational factors (Eurocontrol, 2021).

CONCLUSION

The study concludes that Cyber Attack Prevention and Cyber Threat Detection are significant determinants of Air Traffic Control Safety in Kenya. Cyber Threat Detection has a stronger influence due to its real-time operational importance in identifying and mitigating cyber risks. Cyber Attack Prevention also contributes positively by reducing system vulnerabilities and strengthening overall security posture. The findings confirm that cyber-security resilience is a critical component of aviation safety performance. Therefore, both preventive and detection mechanisms are essential for enhancing air traffic control safety.

RECOMMENDATIONS

The study recommends that Kenya Civil Aviation Authority strengthen Cyber Attack Prevention through improved access control systems, continuous staff training, and strict enforcement of cyber-security policies. Cyber Threat Detection should be enhanced through investment in real-time monitoring systems and advanced intrusion detection technologies. Integration between

preventive and detection systems should be prioritized to ensure seamless cyber-security coordination. Regular system audits and continuous capacity building should be implemented to improve resilience. Collaboration with international aviation cyber-security agencies is also recommended to enhance technical expertise and knowledge sharing.

REFERENCES

Al Mansoori, A. (2021). Cyber-security resilience in aviation infrastructure systems in the Middle East. *Journal of Air Transport Management and Security*, 11(2), 45–62.

Eurocontrol. (2021). *Cyber-security in air traffic management: Operational risk and resilience framework*. European Organisation for the Safety of Air Navigation, 112–138.

Federal Aviation Administration. (2021). *NextGen cyber-security strategy and implementation framework*. U.S. Department of Transportation, 56–79.

Kumar, R., & Singh, P. (2022). Cyber-security frameworks for critical infrastructure protection: A systematic review. *International Journal of Information Security and Cybercrime*, 14(2), 101–118.

Mutua, J. (2021). Cyber-risk management practices in African aviation systems. *African Journal of Aviation Studies*, 6(1), 33–49.

Okafor, C., & Abebe, T. (2022). Integrated cyber-security systems and operational resilience in African airspace management. *Journal of Transport Security and Risk Management*, 15(4), 210–226.

Porter, M. (2020). Strategic technological innovation and organizational performance in complex systems. *Journal of Technology and Management Review*, 18(3), 55–74.

Rogers, E. M. (2020). Diffusion of innovations in modern technological systems. *International Journal of Innovation Studies*, 9(1), 15–34.

Singh, A., Patel, M., & Verma, S. (2022). Real-time intrusion detection systems in aviation cyber environments. *International Journal of Aviation Security and Systems*, 9(2), 88–104.

Skybrary. (2020). *Air traffic management cyber-security risk considerations*. SKYbrary Aviation Safety, 40–58.

Tanaka, H. (2021). Digital transformation and cyber-security in Japanese air traffic control systems. *Asia-Pacific Journal of Aviation Technology*, 7(1), 77–95.

Verma, S., Singh, A., & Patel, M. (2024). Emerging trends in aviation cyber-security and system integration. *Journal of Air Transport Systems*, 20(1), 25–44.

Wang, Y., Li, X., & Chen, Z. (2020). Real-time cyber threat detection in critical infrastructure systems. *Computers & Security*, 92(1), 102–118.

Zhang, H., Liu, Y., & Wang, J. (2021). Access control mechanisms and cyber-security resilience in critical systems. *Journal of Information Security and Applications*, 58(4), 44–61.