Research Paper | Education | E-ISSN No : 2454-9916 | Volume : 10 | Issue : 10 | October 2024

ENHANCING AVIATION CYBERSECURITY THROUGH AI INTEGRATION

Aarish Kotadiya
Research Scholars Program, Harvard Student Agencies, In collaboration with Learn with Leaders

ABSTRACT

This study examines whether the integration of AI (artificial intelligence) enhances cybersecurity in aviation. Cybersecurity's goal is to provide a safe data transfer while maintaining integrity and confidentiality. In aviation, companies strive for efficiency in their operations. The use of computers and AI-driven components is to build trust among passengers and companies. Scientific reports were carried out with different perspectives to look at the various implications of technology. AI has helped respond to cyber threats quickly and more efficiently than humans. However, it has introduced new complexities that require human intervention. Experts must respond to the level of threats to prevent false alarms. Qualitative data is used throughout the research to see how different components respond to threats effectively. Overall, it was found that there should be a balance between technology and humans to safeguard passengers' data instead of companies being completely reliant on such technology to a greater extent.

KEYWORDS: Aviation Cybersecurity, Artificial Intelligence, Threat Detection, Darktrace

INTRODUCTION

The world continues to grow faster than ever due to the rise of AI and technology. 2023 global air traffic grew by 36.9% compared to the previous year. More than 2.3 billion passengers in Europe passed through the region (IATA, 2024). The huge influx of passengers is caused by "space and time compression," a phenomenon allowing passengers worldwide to travel to various parts of the globe. Due to globalization, people can meet others, allowing innovations across multiple sectors of the economy. However, innovations have introduced a series of new complexities and problems, such as AI and cybersecurity. The integration of such technologies has enabled mass production and interconnectedness among people. If, by chance, these technologies were to be intercepted by cyberattacks, it could cost companies millions of dollars and affect numerous stakeholders. Thus, while it has proven efficient in dealing with cyber threats, airline industries should not completely rely on it as it can introduce new vulnerabilities across different systems and domains.

LITERATURE REVIEW

The literature review explores how AI has been integrated into aviation cybersecurity, focusing on its benefits and potential limitations. By analyzing industry reports, case studies, and expert opinions, the review delves into the evolving role of AI in detecting and responding to cyber threats, as well as the challenges of balancing human intervention with technological advancements.

Boeing. (n.d.). *Cybersecurity & Intelligence Messaging*. https://www.boeing.com/defense/cybersecurity-and-intelligence-messaging#solutions

Boeing's official website discusses the recent technologies it has made to combat cyberattacks. One such component is the "Hardware Wall," which can transfer large pieces of data safely and has obtained government certification from the United States. Furthermore, the help of AI in Boeing's mass production has enabled efficiency in the company, which is vital in the aviation sector today. However, Boeing cannot be completely reliant on AI alone. In its reports, Boeing encouraged a diverse range of components to be selected in its fleet production.

Jarvis, T. (2022, October 9). Piloting airline cyber security with artificial intelligence (AI). *Darktrace*. https://darktrace.com/blog/piloting-airline-cyber-security-with-ai

Tony Jarvis highlights the use of "Dark Trace" in aircraft. While AI continues to innovate and learn, he argues that it is simply too fast for humans to respond to cyber threats. The analysis of the components revealed three key features: "Detect, Respond, and Prevent." However, knowledge gaps were found, like technologies that can create problems such as "false positives," thereby creating confusion on board.

Terekhov, V. (2024, August 13). *Exploring the Importance of Aviation Cybersecurity in the USA*. Attract Group. Retrieved August 21, 2024, from https://attractgroup.com/blog/the-importance-of-aviation-cybersecurity/

Vladimir Terekhov underlines the importance of cybersecurity in the aviation industry. He used three different case studies to illustrate his points. One of his case studies was of British Airways when they underwent a data breach, causing theft of financial and personal records of 380,000 passengers. In one of his quotes, he summarizes that for successful aviation security, there must be a mix between AI and people to create a balance. He also discusses the need for better proactive aviation security

as the world becomes more interconnected than ever.

International scientific report on the safety of advanced AI: interim report. (2024, May 16). GOV.UK. https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai/international-scientific-report-on-the-safety-of-advanced-ai-interim-report

A detailed scientific report was carried out, assessing the risk of AI in multiple sectors, such as aviation and the medical field. It came with a series of recommendations that included aligning the purpose of AI with the people's intentions. The report acknowledges the potential of AI, but safety regulations and legal documents will need to be in place to ensure it is used safely and responsibly. Overall, the scientific report was made so people can benefit from using AI together while safeguarding the risk it poses. The experts at the source are from 30 different countries (EU and United Nations), which allows for a diverse range of perspectives on the uses of AI.

METHODOLOGY

This study adopts a qualitative secondary research approach to investigate the role of AI in enhancing aviation cybersecurity. The research relies on published literature, reports, and case studies, focusing on AI-driven components used in aviation, such as Boeing's "Hardware Wall" and Darktrace's cybersecurity solutions. The secondary approach was chosen due to the availability of credible and diverse sources providing extensive insights into the field, allowing for a comprehensive understanding of current AI applications. However, limitations include reliance on pre-existing data, which may not capture the latest advancements or case-specific factors in real-time aviation cybersecurity challenges.

Efficiency of AI

The rapid innovation of AI has made transferring data safe and more efficient in dealing with cybersecurity. Such integration of technology has made AI go beyond human capabilities. Chatbots can now respond and give answers to humans faster than a normal person. As a result, people can now use AI to analyze such problems to respond to threats more efficiently. For example, the introduction of AI—a driven component such as Darktrace can be able to "Detect, Respond, and Prevent" threats. These three features are vital to feeding data in the cockpit when an airplane is dealing with a single cyberattack. Darktrace features allow for a quick and immediate response. (Jarvis, 2022). With AI able to analyze different situations in a shorter time, "analysts could gain approximately 20% of their time back to focus on proactive cyber security measures." A poll conducted by Darktrace reported that 89% of the IT security team believes that AI-driven cyber threats could impact their organization (Heinemeyer, 2024). This shows that AI has immense potential in various companies to enhance their security.

AI-Driven Components

Current AI-driven components are found in airline manufacturers such as Boeing. According to their official website, they have reported using "Hardware Wall" software, which is part of their defense mechanism, particularly in the military field. It is installed with cross-section domains, which can transfer data safely and securely. This can prevent data breaches and protect a nation's airspace from being attacked. Such technology has already received certification from the United States federal government, proving its trustworthiness (Boeing, n.d.). The United States and Boeing have received international customers, such as Canada, trying to find similar "information sharing capabilities." This has allowed Boeing a diverse range of options to keep innovating in dealing with cyber threats (Roby, 2010).

Vulnerabilities and Complexities

While AI efficiently deals with cyberattacks, aviation companies should not rely solely on them. Instead, a mixture of humans and technologies should be involved to bolster cyber threats. For example, in 2019, British Airways was fined GBP 20 million after 380,000 customers were affected by a data breach. The ICO later stated that cybercriminals could penetrate British Airways' security weaknesses, which led them to have access to customers' financials and personal information (Terekhov, 2024). Cybercriminals could use "Modernizr," a JavaScript used in Browers; by capturing the scripts with detailed codes, they could control the domain. ICO later claimed that British Airways had not taken the issue seriously until a third party notified it (Hunton, 2020). As a result, greater human involvement is needed to keep customers' security accountable.

AI-driven components can help respond to cyber threats, but human intervention is still required when dealing with such technology. Several interviews were held with Darktrace customers, and one common complaint is a "high number of false positives" and high operating costs (Blog, 2023). False positives occur when web applications incorrectly scan a false threat. A growing number of complaints could threaten the airline industry as it can cause problems on board. For example, false indications of failures on board can increase pilots' workload and confuse them. According to Gov.UK, AI tends to memorize stuff when trained, but when introduced to a foreign object, it will detect it as an "error." Furthermore, the report requires "technical expertise to evaluate the safety cases" so they can assess the threat and level of response needed (UK government, 2024). OCM later reported that Darktrace had similar issues after the learning period. As a result, airline industries should not be completely reliant on them. A security team of experts must always be in place when cybersecurity in aviation is concerned, as privacy violations can be similar to what happened with British Airways in 2019.

CONCLUSION

AI has paved the way for people to combat cyber threats in the 21st century. As innovations keep progressing, so do cyberattacks, as they become more complex. Hence, using chatbots and other features, AI can respond to attacks faster. In a world with constant data and privacy transfer, human involvement is needed to uphold personal information. However, there are some limitations to this study. For example, different companies have different structures and requirements that could influence the implementation of AI in their security

systems. Hence, human-based training may need to be evaluated to justify the need for more human intervention.

REFERENCES

1. Boeing. (n.d.). Cybersecurity & Intelligence Messaging. https://www.boeing.com/defense/cybersecurity-and-intelligence-messaging#solutions
2. CyGlass. (2023, February 8). The Dark Side of DarkTrace - Five takeaways for customers and partners. https://cyglass.com/news-and-events/dark-side-darktrace/
3. International scientific report on the safety of advanced AI: interim report. (2024, May 16). GOV.UK. https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai/international-scientific-report-on-the-safety-of-advanced-ai-interim-report
4. Heinemeyer, M. (2024, March 7). Defending against the new normal in cybercrime: AI. Darktrace. https://darktrace.com/blog/ai-automation-and-cybercrime-as-a-service-the-new-normal-facing-defenders
5. Hunton Andrews Kurth LLP. (2020, October 16). ICO fines British Airways 20 million pounds for security breach. https://www.huntonak.com/privacy-and-information-security-law/ico-fines-british-airways-20-million-for-security-breach
6. Jarvis, T. (2022, October 9). Piloting airline cyber security with artificial intelligence (AI). Darktrace. https://darktrace.com/blog/piloting-airline-cyber-security-with-ai
7. Roby, M. (2010, August 6). Boeing to showcase Secure Information-Sharing Technology. https://www.darkreading.com/cyber-risk/boeing-to-showcase-secure-information-sharing-technology
8. Terekhov, V. (2024, August 13). Exploring the importance of aviation cybersecurity in the USA. Attract Group. https://attractgroup.com/blog/the-importance-of-aviation-cybersecurity/