10-28-2024

The Role of Cybersecurity in Bioinformatics for Aviation and Aerospace Safety

Sharon L. Burton
Embry-Riddle Aeronautical University, burtons6@erau.edu

Crimson Publishers
Wings to the Research

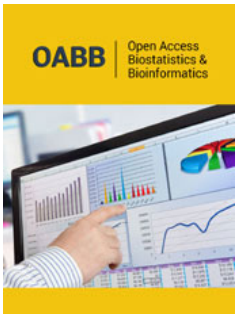
Opinion

The Role of Cybersecurity in Bioinformatics for Aviation and Aerospace Safety

Sharon L Burton*

Embry-Riddle Aeronautical University, Daytona Brach, FL, USA

ISSN: 2578-0247



***Corresponding author:** Sharon L Burton, Embry-Riddle Aeronautical University, Daytona Brach, FL, USA

Submitted: October 17, 2024
Published: October 28, 2024

Volume 4 - Issue 1

How to cite this article: Sharon L Burton*. The Role of Cybersecurity in Bioinformatics for Aviation and Aerospace Safety. Open Acc Biostat Bioinform. 4(1). OABB.000576. 2024.
DOI: 10.31031/OABB.2024.04.000576

Introduction: Present the Topic and State Your Thesis

The intersection of bioinformatics and cybersecurity is critical to ensuring the privacy, integrity, and safety of biological data [1]. Bioinformatics is an interdisciplinary field that embodies the cyber age through its reliance on sophisticated algorithms, cloud computing, and secure data management practices, reflecting the profound digital transformation across various scientific disciplines [2].

Bioinformatics connects to aerospace and aviation through the use of computational tools and data analysis to enhance safety and performance (Federal Aviation Administration [FAA], n.d.) [3]. The FAA applies bioinformatics in biomarker research and informatics to analyze aero-medically relevant data, such as aviation accident investigations and human subjects research studies (FAA, n.d.). This data helps assess the impact of various factors on aviator performance and improve aviation safety (FAA, n.d.).

Bioinformatics has revolutionized modern biology, mainly with the advent of genomic sequencing-the process of determining the complete DNA sequence of an organism's genome, including all of its genes and non-coding regions [4]; proteomics the large-scale study of proteins, including their structures, functions, and interactions that aims to comprehend the role of proteins in biological processes and how they contribute to the overall functioning of an organism, and other molecular biology techniques [5]. In the context of aerospace and aviation, bioinformatics also plays a crucial role. The Federal Aviation Administration (FAA) employs bioinformatics and computational tools to analyze aero-medically relevant data, such as aviation accident investigations and human subjects research studies. Also, the FAA's use of bioinformatics helps assess the impact of various factors on aviator performance, ultimately enhancing aviation safety and performance.

However, the increasing reliance on computational tools in bioinformatics brings new cybersecurity challenges. Because of its sensitive nature, specifically genomic data, biological information demands enhanced security measures to safeguard against misuse [6]. In this opinion piece, I argue that the growing role of bioinformatics in healthcare, research, and synthetic biology highlights the urgent need for more robust cybersecurity protocols to protect sensitive biological information from potential threats.

Developing the Argument

Data privacy and security in bioinformatics

One of the most pressing concerns in bioinformatics is the protection of genomic data, which can reveal highly personal and sensitive information about individuals, such as their susceptibility to diseases, genetic traits, and even behavioral tendencies such as impulsivity, risk-taking, or social behavior [7]. If genomic data falls into the wrong hands, it can be exploited for discrimination in areas like employment, insurance, or healthcare [8]. The Sheldon et

al. [8] report offers current practices, challenges, and proposes solutions for securing genomic data, accentuating the significance of cybersecurity measures to avert misuse and discrimination. The challenge is compounded by the fact that genomic data cannot be "reset" or changed like a password or credit card number. Therefore, protecting this data is paramount.

Cybersecurity protocols such as encryption, secure transmission, and access controls are crucial in bioinformatics workflows. For instance, data encryption can ensure that genomic information is secure during transmission and storage [8]. Moreover, regulatory frameworks like the EU General Data Protection Regulation (GDPR) stress the need for rigorous data protection to include personal information like genetic data [9]. Without the measures, breaches could lead to substantial personal and societal harm.

In the context of aerospace and avionics, bioinformatics data protection is equally critical. The Federal Aviation Administration (FAA) employs bioinformatics and computational tools to analyze aero-medically relevant data, such as aviation accident investigations and human subjects research studies. The FAA's use of bioinformatics helps assess the impact of various factors on aviator performance, ultimately enhancing aviation safety and performance. Cybersecurity in this sector ensures that sensitive biomedical data, which could impact both human health and aviation operations, remains secure and uncompromised (FAA, n.d.). By drawing parallels between the protection of genomic data in bioinformatics and the sensitive data used in aerospace and avionics, this opinion draws attention to the universal need for robust cybersecurity measures across diverse fields. Protecting sensitive information, whether it pertains to human health or aviation safety, is paramount to maintaining trust and security in critical systems.

Cybersecurity vulnerabilities in bioinformatics tools

Numerous bioinformatics tools are open source, such as BioPython, BioPerl, and BioJava; these open-source tools support persistent data sharing and inspire innovation and partnership within the scientific community [10,11]. On the other hand, the open-source nature of these tools also makes them vulnerable to exploitation by cybercriminals. Software vulnerabilities in bioinformatics tools or genomic databases could be exploited to manipulate, alter, or corrupt research data, leading to compromised scientific findings [12].

For example, an attacker using open-source bioinformatics tools could introduce subtle changes to genomic datasets stored in a public database; this change could go undetected by researchers and possibly lead to incorrect conclusions in studies or clinical diagnostics [12]. Greenbaum [1] has noted that these attacks can sabotage the integrity of scientific research, destabilizing the trustworthiness of essential and crucial data used in public health decisions, as well as in aviation and aerospace operations. Also, ensuring effective cybersecurity measures and decisions is paramount to protecting data, thereby ensuring the reliability of research outcomes, and maintaining public confidence in health, aviation, and aerospace recommendations. Addressing these vulnerabilities requires regular security audits, vulnerability assessments, and the implementation of secure coding practices to protect bioinformatics systems from such attacks [1].

Integration with cloud computing and its security challenges

With the vast amounts of data generated in bioinformatics, cloud computing has become essential for storage and computational purposes [13]. Cloud platforms like Amazon Web Services (AWS) and Google Cloud offer scalable infrastructure to handle the enormous datasets typical of bioinformatics research. However, the move to cloud computing introduces new security challenges, such as securing data during transmission [14], managing encryption keys [15], and ensuring that cloud providers adhere to stringent security standards [16].

In particular, cloud-based bioinformatics services need to implement robust encryption protocols for data storage and transmission [16]. This action ensures that sensitive information, such as genomic sequences, is protected even if the cloud provider's infrastructure is compromised [16]. Regular security audits and robust access controls are necessary to mitigate the risks associated with cloud-based data management in bioinformatics.

Biosecurity concerns in synthetic biology

Bioinformatics, at the intersection of cybersecurity and biology, plays a crucial role in synthetic biology, where computational models are used to design and engineer new biological organisms [17]. While synthetic biology offers vast potential for medical and industrial applications, it also raises significant biosecurity and cybersecurity concerns. Cybercriminals could theoretically use synthetic biology tools to engineer harmful pathogens, making biosecurity a vital issue [17].

Risk mitigation is significant [18,19]. Cybersecurity frameworks must incorporate biosecurity protocols, ensuring that bioinformatics tools are not used for nefarious purposes, such as creating biological weapons. Governments and international organizations need to collaborate with cybersecurity experts [19] and bioinformaticians to monitor potential threats and implement controls that prevent misuse of bioinformatics in synthetic biology [20].

Counterarguments: Addressing Opposing Viewpoints

In this rapidly evolving cyber age and landscape of bioinformatics, the integration of biology, computer science, and data analytics has revolutionized fields like genomics, proteomics, and personalized medicine. However, alongside these scientific advancements comes a growing concern about the security and privacy of sensitive biological data. Genomic information, in particular, contains highly personal details, making it a prime target for cyberattacks, data breaches, and misuse. As bioinformatics increasingly relies on digital tools and large-scale data storage, it intersects with the critical need for robust cybersecurity measures.

In this opinion, the expanding role of bioinformatics in aerospace and aviation, research, synthetic biology, and even healthcare demands comprehensive cybersecurity protocols to protect sensitive biological information from potential threats and ensure the integrity of scientific progress. In the aerospace and aviation sectors, bioinformatics data protection is equally critical. The Federal Aviation Administration (FAA) employs bioinformatics and computational tools to analyze aero-medically relevant data, such as aviation accident investigations and human subjects research studies. The FAA's use of bioinformatics helps assess the impact of various factors on aviator performance, ultimately enhancing aviation safety and performance. Cybersecurity in this sector ensures that sensitive biomedical data, which could impact both human health and aviation operations, remains secure and uncompromised (FAA, n.d.).

A counterargument is that the collaborative and open-source nature of bioinformatics software promotes transparency and accelerates scientific discovery. Critics might argue that imposing too many cybersecurity restrictions could stifle innovation and limit access to significant bioinformatics tools. However, this perspective overlooks the growing cybersecurity threats in an increasingly digital world. While openness and collaboration are critical, they must be balanced with robust security measures to prevent exploitation. Moreover, many open-source projects already incorporate security best practices, such as community-driven vulnerability reporting, which can help maintain both transparency and security.

Another counterargument is that bioinformatics data, while sensitive, may not pose the same immediate security risks as other types of data, such as financial or military information NIST [21]. However, this argument underestimates the long-term risks associated with genomic data breaches. As genetic information becomes more integrated into healthcare and aerospace systems, the misuse of such data could have devastating personal and societal consequences. For instance, unauthorized access to genetic data could lead to genetic discrimination, the creation of personalized bioweapons, or even operational disruptions in aviation, all of which represent significant threats.

Conclusion: Summarizing the Main Points and Emphasizing the Significance

In conclusion, bioinformatics has transformed biological research and personalized medicine, offering new insights into the complexities of biological systems. However, as bioinformatics continues to grow, so too do the security challenges associated with managing and protecting sensitive biological data. The intersection of bioinformatics and cybersecurity is of increasing importance, given the potential for privacy breaches, data manipulation, and even biosecurity threats [6]. Stronger cybersecurity protocols, including data encryption, secure cloud computing practices, and vulnerability assessments, are necessary to safeguard the integrity of bioinformatics research and the privacy of genomic data [8].

Furthermore, the role of bioinformatics extends into aerospace and aviation, where it significantly enhances aviation safety through the analysis of biomarker data and accident investigations. The Federal Aviation Administration (FAA) utilizes bioinformatics tools to assess aviator performance and implement safety measures, highlighting the critical intersection of biology and aviation technology (FAA, n.d.). Addressing specific cybersecurity risks in the aerospace industry, such as potential manipulation or breaches of bioinformatics data, is vital to ensure flight safety, human factors research, and aero-medical studies are protected [8].

The need for cybersecurity in healthcare and synthetic biology is mirrored in aviation and aerospace and draws a parallel across various fields. Compromised bioinformatics data could impact not only personal privacy and healthcare decisions but also operational safety in aviation [7]. Public awareness and stringent security measures are crucial to ensuring the benefits of bioinformatics are realized while minimizing potential risks, reinforcing the importance of comprehensive cybersecurity protocols across all sectors [9]. This holistic approach underscores the necessity of protecting sensitive biological information, ensuring the reliability of research outcomes, and maintaining trust in both healthcare and aviation operations.

References

1. Greenbaum D (2023) The convergence of biotechnology and cybersecurity: A primer on the emerging field of cyberbiosecurity. In: Greenbaum D (Ed.), Cyberbiosecurity, Springer, Cham, Switzerland, pp. 1-6.
2. Kushwah S, Kumar A, Mani A (2024) Introduction to bioinformatics: Past, present and future. In: Chaudhary A, Sethi SK, Verma A (Eds.), Unraveling new frontiers and advances in bioinformatics. Springer, Switzerland, pp. 1-17.
3. Federal Aviation Administration [FAA]. (n.d.). Biomedical sciences section.
4. Eisenstein M (2024) Super-speedy sequencing puts genomic diagnosis in the fast lane. Nature 626(8000): 915-917.
5. Mangalaparthi KK, Pandey A (2024) Technology spotlight advances in proteomic technologies and their applications in hematology. The Hematologist 21(1):
6. Ni E, Gürsoy G, Gerstein M (2023) Security vulnerabilities and countermeasures for the biomedical data life cycle. In: Greenbaum D (Eds.), Cyberbiosecurity. Springer, Cham, Switzerland, pp. 79-93.
7. Brauneck A, Schmalhorst L, Weiss S, Baumbach L, Völker U, et al. (2024) Legal aspects of privacy-enhancing technologies in genome-wide association studies and their impact on performance and feasibility. Genome Biol 25(154): 1-18.
8. Sheldon J, Ross S, Morris T, Brown I, Zhu F, et al. (2024) Genomics cybersecurity concerns, challenges, and a modular test lab. Proceedings of the 2024 ACM Southeast Conference, ACM Digital Library Home, pp. 86-94.
9. Manzano A, Weging S, Bezdan D, Borg J, Cahill T, et al. (2023) Enhancing European capabilities for application of multi-omics studies in biology and biomedicine space research. Iscience 26(9): 107289.
10. Xu M, Xu C, Chen M, Xiao Z, Wang Y, et al. (2023) Comparative analysis of commonly used bioinformatics software based on omics. Gene Reports 32: 101800.
11. Ziemann M, Poulain P, Bora A (2023) The five pillars of computational reproducibility: Bioinformatics and beyond. Briefings in Bioinformatics 24(6): bbad375.

12. Li Y, Ma L, Shen L, Lv J, Zhang P (2019) Open source software security vulnerability detection based on dynamic behavior features. Plos One 14(8): e0221530.

13. Koppad S, Gkoutos GV, Acharjee A, Annappa B (2021) Cloud computing enabled big multi-omics data analytics. Bioinformatics and Biology Insights 15: 1-6.

14. Zulifqar I, Anayat S, Khara I (2021) A review of data security challenges and their solutions in cloud computing. International Journal of Information Engineering and Electronic Business 13(3): 30-38.

15. Abdulsalam YS, Hedabou M (2022) Security and privacy in cloud computing: Technical review. Future Internet 14(1): 11.

16. Tabrizchi H, Rafsanjani MK (2020) A survey on security challenges in cloud computing: Issues, threats, and solutions. The Journal of Supercomputing 76(3): 9493-9532.

17. Shankar DD, Azhakath AS, Khalil N, Sajeev J, Mahalakshmi T, et al. (2024) Data mining for cyber biosecurity risk management-A comprehensive review. Computers & Security 137: 103627.

18. Dodla TR, Jones LA (2023) Mitigating knowledge management internal and external risk factors: A literature review of best practices. Scientific Bulletin 28(1): 44-54.

19. Jones LA (2021) A content analysis review of literature to create a useable framework for reputation risk management. In: Johnson R (Ed.), Handbook of research on multidisciplinary perspectives on managerial and leadership psychology, IGI Global, p. 43.

20. Patrick S, Barton J (2024) Mitigating risks from gene editing and synthetic biology: Global governance priorities. Carnegie Endowment for International Peace.

21. NIST (2023) Cybersecurity of genomic data: NIST IR 8432, Computer Security Resource Center, Information Technology Laboratory.