AI and Automation in Sports

Ryan Grimes
Computer Science Department
Hampton University
Hampton, VA

Abstract - Artificial Intelligence (AI) and automation has been one of the most popular topics of the century. It has been integrated into education, medicine, and transportation to make tasks easier and increase productivity. AI and automation is constantly being discussed for being a double edged sword. On one side, it makes tasks capable of being completed faster and oftentimes more accurate, but the other side argues that it lacks accountability. Before AI and automation is introduced to a system , it is integral to analyze the pros and cons of said implementation. This research focuses on the integration of AI and automation in sports and how its risks can affect athlete data, match outcomes, and device reliability. Past research has examined accuracy and health benefits; however, device security, data flow, and contingency planning in the event of an attack or breach has not been acknowledged. This study investigates these gaps by examining how AI-driven wearables and automated officiating systems function; how data flow is mapped; and what vulnerabilities affect confidentiality, integrity, and availability. Literature reviews and input from sports management and computer science professionals, athletes, and trainers will illustrate what protections are currently available and what they think of the trade-offs. The results will highlight key risks, identify potential solutions, and offer guidance for sports organizations and tech developers so that AI and automation in sports can be both innovative *and* secure.

I. Introduction

From the Olympics to the World Cup, sports have united the world for centuries. As time has progressed, all sports have evolved in some way. Within the past few decades, technology has been integrated into sports more than ever. For example, tennis uses Electronic Line Calling (ELC) and the Hawk-eye system to highlight if a ball hits the designated court lines before going out of bounds, and baseball uses Statcast and the Hawk-eye system to mark the location of a pitch and the velocity and location of a hit ball. These systems have been implemented in sports broadcasting since 2001 [14]. More recently, Rugby has implemented concussion-sensing mouthpieces and NFL has implemented Riddell technology to detect hard collisions in helmets [9].

With that being said, AI and automation in sports has gone from being for broadcasting to being for player protection. These innovations provide greater fairness, accuracy, and safety while also improving performance and training. However, as developers rely on automation more, the oversight of systems should be increased. If a pitched baseball was called a ball but the umpire called it a strike, whose call is more valid? Currently, the umpire's opinion is more valuable, but when it comes to challenges and replays, the hawk-eye system is appreciated more. Another potential fault is the cybersecurity risks associated with the use of digital data collection. What systems and procedures are put in place to prevent football teams from manipulating helmet data so they can hide a player's concussion in the event they do not want said player to miss a game? In general, devices that collect biometric readings, location tracking, and injury reports are potential targets for cyberattacks. In the event of compromisation, player privacy and data integrity will be jeopardized.

This research will explore both the benefits and risks of sports technology by focusing on the intersection of AI, automation, and cybersecurity. In addition, the importance of safeguarding athlete data, maintaining system integrity, and ensuring ethical use of AI on and off the field will be emphasized.

II. Methodology

The purpose of this research being conducted is to understand the intersection of AI, automation, and cybersecurity in the athletic industry. The primary audience for this report is professionals directly involved in the development, deployment, management, and usage of AI and automation in data collection. Key groups within the target audience are sports management professionals, physical therapists, athletic trainers, sports medicine staff, and athletes. By using this audience, readers will be able to attain crucial insight about security practices, perceived risks, and the trade-offs involved in adopting new sports technologies.

In order to properly display these findings, qualitative and quantitative data is analyzed to support claims. Quantitative data is retrieved from surveys and qualitative data is obtained through a literature review. There are two surveys posted on various media platforms in order to collect data from a diverse audience. One survey is for athletes and professionals in sports, and the other is for computer science students and professionals. By using these participants, a perspective from both customers and developers is found.

The literature review will cover the scope of AI in sports, current applications of AI in sports, flow and architecture of data, and mitigation techniques for known vulnerabilities. The scope of AI in sports and its current applications will be identified by reviewing existing implementations of AI and automation. Those findings will be used to understand how the scope and applications influence the sports industry. The flow and architecture of data will be found by analyzing existing research and technical documents. These findings are necessary in order to identify where sensitive data is collected, stored, and transmitted. The identification of known vulnerabilities and mitigation techniques are some of the most important tasks. Whenever a problem is identified, a solution should be produced.

III. Literature Review

Research papers and articles will be analyzed to identify what is already known about AI and its integration in sports. The findings will be synthesized to identify current vulnerabilities, past mitigation techniques, and future trends. The following articles are critical in understanding the integration of AI in sports:

> *Artificial intelligence security: Threats and countermeasures* by Wenxin Kuang provides a comprehensive overview of AI system threats. This will serve

as a framework for identifying security vulnerabilities within sports AI and automated officiating systems [1].

Privacy, ethics, transparency, and accountability in AI systems for wearable devices by Petar Radanliev analyzes the cybersecurity risks specific to wearables and addresses the concerns of player privacy, the use of ethical data, and the transparency of the system. This source is critical for assessing risks [3].

A comprehensive review of computer vision in sports: Open issues, future trends and research directions by Banoth Thulasya Naik provides crucial technical detail on how wireless devices can be eavesdropped on. This source illustrates how data is mapped and vulnerabilities present during transmission [4].

NFL implementing Hawk-Eye system to measure first downs by Reuters provides a high-profile example of automated officiating systems. Digital first-down markers provide a solid example of an automated system whose integrity is vulnerable to cyberattacks [10].

SISU Sense: Concussion-sensing mouthpiece by SISU Mouthguards is an overview of a high-profile AI-driven wearable. It investigates devices that collect highly sensitive biometric and injury data. This source supplements the theory: how the security of data flow is crucial for preventing exploitation or unauthorized leaks [11].

Artificial Intelligence Security: Threats and Countermeasures by Yupeng Hu identifies common AI threats. They highlight model poisoning, adversarial inputs, and privacy attacks as high-priority threats. It is important to be able to identify these threats to prevent tampering with computer-vision officiating and poisoning concussion detecting models [2].

Generative AI/Cybersecurity in F1 by Sports Business Journal provides an industry perspective on how teams use AI to simulate game scenarios. This is an example of how organizations view AI as both a tool and a risk [5].

NFL Next Gen Stats by NFL Operations is an example of large-scale AI integration into sports. This is a process used by the NFL to provide in-depth real-time analytics on football performance [6]

Concussion Rates by Sport by Complete Concussions is a research article that assists in justifying research into concussion-sensing technology by showing which sports have the highest concussion risks. This quantifiable data emphasizes the gravity of protecting concussion data and device integrity [7]. This source is coupled with *Effects of Repetitive Sub-Concussive Head Impacts* by Kawata et al. This article provides clinical reports on the effects of head trauma. With this research, consequences of concussion device failure or manipulation are able to be seen [8].

Stanford Engineering - Most Sensors Produce Inaccurate Data provides research on real-world limitations of sensor accuracy. This assists in emphasizing how sensor unreliable might produce exploitable vulnerabilities or harmful mis-decisions [12].

IV. Results

A. Survey Results

Quantifiable data is necessary to make a proper analysis of findings. There were two surveys made in order to collect this data: a survey for computer science professionals and students, and a survey for athletes and sports professionals. This survey was a Google Form posted on Reddit, Instagram, Facebook, and campus buildings. After leaving the form up for a couple weeks, the survey for athletes received 230 participants and the survey for computer scientists received 219 participants.

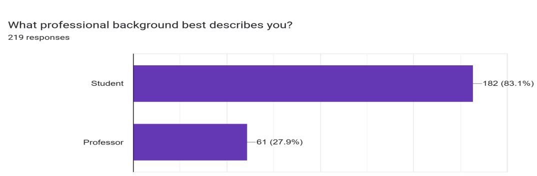

Figure 1: Professional background of participants in computer science survey

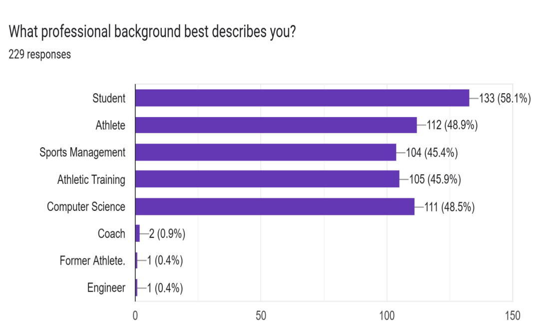

Figure 1.1: Professional background of participants in athletic survey

The purpose of the first questions in the survey was to illustrate credibility and diversity of the population. Ideally, a diverse population will cause a reduction in biases. The questions following the introductory questions asked participants how they use AI personally.

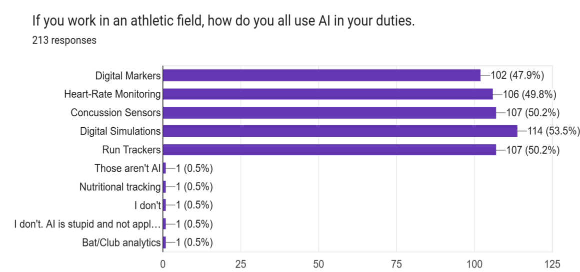

Figure 2: There are many AI tools on the market in the athletic field right now. Digital simulations seem to be the most common tool used by athletes and sports professionals.

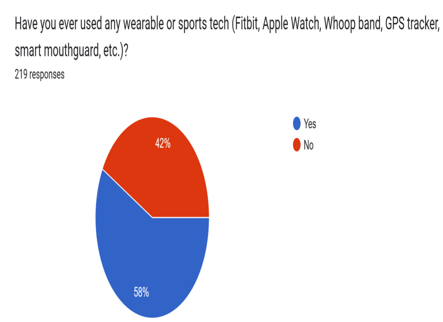

Figure 2.1: 58% of computer scientists use wearable or sports technology.

Now that it is known that a majority of participants use AI in their duties and personal life, it is important to note their familiarity with it and how comfortable they feel about its integration into the athletic domain.

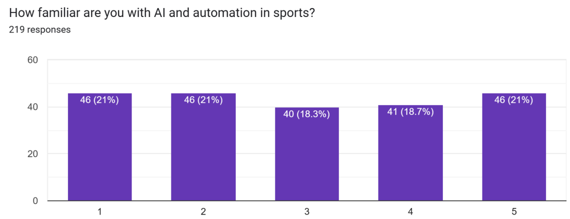

Figure 3.1: Computer scientists vary in familiarity of AI and automation usage in sports.

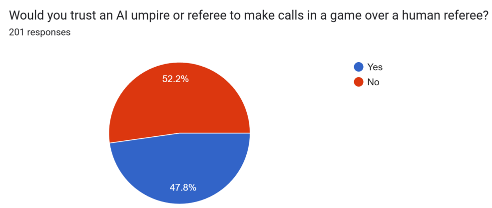

Figure 3.2: 52.2% of athletic participants don't trust the integration of AI into sports officiating.

It has been illustrated that a majority of participants use AI in their personal and professional lives. Following that, it was found that participants do not really understand how AI and automation are used in sports but they do not trust it to officiate games. Since it is stated that AI and automation isn't trusted in officiating, it is important to note why they don't trust it.

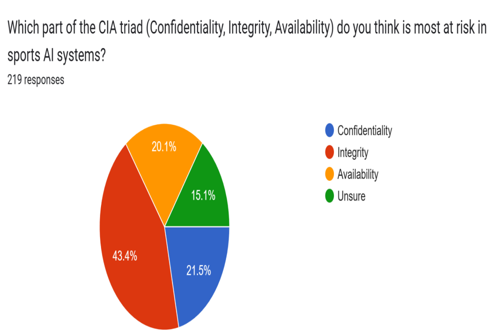

Figure 4.1: Computer scientists highlight integrity as the most at risk sector in the Confidentiality, Integrity, and Availability (CIA) triad (43.4%).

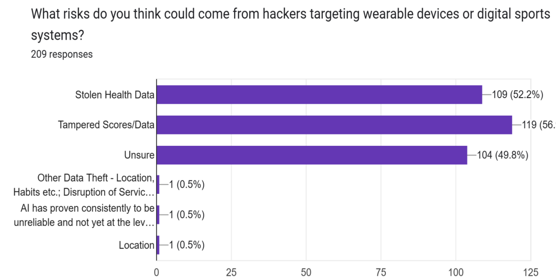

Figure 4.2: Athletic professionals believe hackers will want to steal health data (52.2%) or tamper scores/data (56.9%).

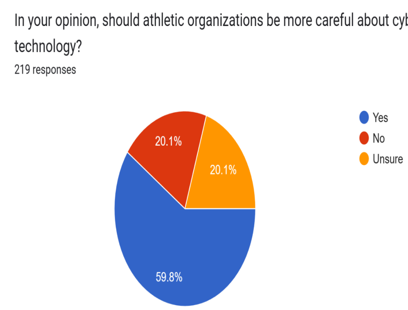

Figure 4.3: Participants feel AI is a delicate tool in sports, and organizations should be very careful in using it (59.8%).

A firm understanding of participants comprehension, usage, and opinion of AI and automation in sports is now organized. Since risks have been identified, mitigation techniques must also be identified. When prompted, athletes stated data accuracy and integrity is the biggest concern with AI and automation integration in sports. Computer scientists recommended for human oversight and policies to be put into place to mitigate this risk.

B. Literature Results

Research papers and articles were analyzed to identify existing knowledge regarding the integration of AI and automation in sports. The findings were synthesized to identify current usages and vulnerabilities, past mitigation techniques, and future trends.

First, the current usages of AI and automation in sports should be highlighted. The NFL uses a plethora of technologies to enhance the experience for players, coaches, and fans. Since 2014, their Next Gen Stats system uses radio-frequency identification (RFID) tags placed in players' shoulder pads, officials, pylons, and footballs [6]. A tracking system in every NFL captures location, speed, distance traveled, and other data at a rate of 10 times per second. This process generates over 200 new data points on every play [6].

Sports also rely on AI and automation for officiating and measuring. Hawk-eye technology is the most widely used and Statcast is one of the most notable subfunctions of it[14]. Hawk-eye technology is a ball-tracking system that uses multiple fast cameras to analyze a ball's trajectory then generates a 3D ball route model [14]. It is commonly used in baseball and tennis to make split-second decisions, especially when it deals with line calling. Baseball combines the Hawk-eye system with Statcast. This process uses 12 high-frame-rate cameras per ballpark that are dedicated to track pitching, hitting, running, and fielding data [15]. In the 2023 season, from Opening Day through the end of the World Series, more than 725,000 pitches and more than 125,000 batted balls were tracked by Statcast [15]. The NFL uses the Hawk-eye virtual measurement system for first downs by using six 8k cameras for optical tracking. The NFL believes this process is an efficient alternative to traditional chain management, especially because it is up to 40 seconds faster than the manual process. However, they keep the traditional chain crew on the field for oversight. NFL coaches, players, and staff use the data collected by these systems on league-provided tablets throughout the games and practices to make decisions. The integration of these services provide the ability to communicate, review high-resolution images of offensive and defensive formations, and access near-real-time game stats [6].

The third domain of AI and automation integration in sports is player safety. There are 4 million concussions in sports in the USA every year and half of them are undiagnosed. These concussions result in over 1 million ER visits and significant socio-economic stigma to athletes that have to live with traumatic brain injury, adding up to a total cost to society of $60B/year [11]. Concussion rates are a major concern. Mixed Martial Art (MMA) has the highest reported amount of concussions among organized sports (nearly 1 in 7 fights results in a concussion), Aussie Rules Football was in second, and rugby in third [7]. It is important to highlight this because repetitive mild frontal head impacts disrupt oculomotor processes. This can cause an athlete to feel disoriented for a minimum of 24 hours after a collision [8]. The NFL has adopted advanced pads and helmets, such as Riddell's Precision-Fit helmets, to manage data on player health. This specific helmet uses personalized, 3D-printed padding contoured to an athlete's head to manage impact energy [9]. Another technology used for player safety is the SISU Sense concussion-sensing mouthguard. This tool uses an embedded microchip sensor to give accurate acceleration readings when an impact occurs. The mouthpiece comes with an app that allows users to instantly view data from specific days or months [11].

The implementation of AI and automation increases efficiency, fairness, and accuracy, but it comes with risks. A research paper covering the threats and countermeasures of AI stated the data collection and pre-processing phase are vulnerable to sensor spoofing and scaling attacks [1]. In addition, the training and inference phases of the AI model are subject to poisoning attacks and adversarial attacks [1].

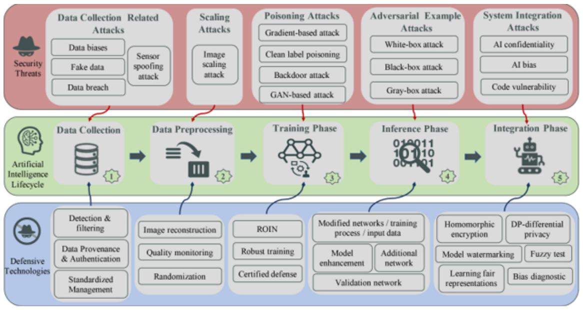

Figure 5: The overall framework of attack and defense strategies for the AI systems [1].

Data integrity and accuracy are also at risk. Research at Stanford University found that many commonly used head impact sensors produce inaccurate data. The reasoning behind this is because sensors mounted to flexible soft tissue, like a skin patch or skull cap, can move upon impact and overpredict the acceleration of the impact by up to 500 percent compared to skill motion. This error makes it difficult to interpret measurements for injury risk predictions. In addition, the researchers found that devices attached to the teeth, like the previously highlighted SISU mouthguard, or sensors inside the ear canal perform better [12].

Wearable sensors collect vast amounts of personal data that can be processed by AI algorithms to profile individuals without explicit consent [3]. This can lead to invasive targeted advertising, increased insurance premiums based on health data, or even surveillance [3].

Figure 6: the technical process by which data from wearable sensors is transformed into structured datasets for AI and ML model development tends to overlook transparency but prioritizes data collection.

Ideally, organizations would not implement these systems knowing the risks without implementing the proper mitigation techniques. Earlier Hu highlighted the data collection and pre-processing phase for being vulnerable to sensor spoofing and scaling attacks. They suggest detection and filtering, data provenance and authentication, and standardized management to mitigate these risks. In addition, image reconstruction uses selective median and random filters to identify altered pixel points; this process has been used to defend against scaling attacks without modifying the original neural network [1]. Another risk is found in computer vision. It has been found that computer vision faces challenges such as similarities between players and frequent occlusions, difficulty in jersey number recognition due to massive jerseys with sharp contours, false positives because of fans wearing jerseys, and lack of cross-compatibility of AI algorithms [4]. Play area estimations and specialized AI algorithms have been shown to reduce the impact of these risks [4].

V. Analysis

The implementation of AI and automation in sports is a double-edged sword. In its current state, developers need to prioritize security before it is implemented. The survey highlights divergences and consensuses in security priorities. Athletes explicitly state they're primarily concerned with tampered scores/data (56.9%) and stolen health data (52.2%), and computer scientists add to this by stating they believe integrity is the most important vulnerability in the CIA triad(43.4%). This agreement draws the conclusion that integrity and accuracy is paramount for the deployment of AI and automation.

Hawk-eye and Statcast are great representations of applications of AI in automated officiating by providing benefits to efficiency and accuracy of measurements in sports when compared to manual methods. Though they have proven themselves effective, participants do not prefer AI officials over humans(52.2%). This lack of trust is partly justified. Reuters highlights these systems are vulnerable to cyberattacks such as model poisoning and adversarial inputs that can alter the outcome of computer-vision officiating. Participants in the survey agreed with the industry standard of using human oversight as a mitigation technique that addresses accountability and accuracy.

Since systems collect health data on users, their security is critical. An exploitation of these systems could enable exploitation or unauthorized leaks. The broader ethical concerns are privacy issues such as invasive targeted advertising and increased insurance premiums. In addition to it being vulnerable to attacks, its accuracy is invaluable to validate. Hu suggests implementing detection and filtering and data provenance and authentication to ensure data is reliable. Also, when it comes to wearable concussion sensors, it is best to have the sensors stored in the users mouth or ear canal compared to their skin or tissue.

VI. Conclusion

The integration of AI and automation in the sports industry has improved fairness, accuracy, and player safety. Technologies like the NFL's Next Gen Stats, Hawk-Eye officiating, and SISU Sense mouthguards are actively transforming training, fan experience, and player health management. However, it has been found that the mass adoption of AI and automation has outpaced the adoption of cybersecurity measures. This introduces risks to athlete data, match outcomes, and device reliability. The core challenge identified is a vulnerability in data integrity, especially data tampering and theft from hackers. Threat vectors include sensor spoofing, scaling attacks, and model poisoning. These risks are exceptionally high in the massively used wearable devices.

In the future, developers should focus on security in addition to their already present innovations. Developers should implement detection and filtering protocols, data provenance, and authentication to ensure trustworthiness and accuracy of all sensor data. In addition, human oversight and policy build confidence in accuracy and allow for accountability.

By emphasizing security over creativity, AI and automation can safely improve fairness, efficiency, and accuracy of sports.

References

[1] Yupeng Hu, Wenxin Kuang, Zheng Qin, Kenli Li, Jiliang Zhang, Yansong Gao, Wenjia Li, and Keqin Li. (January 2023). Artificial Intelligence Security: Threats and Countermeasures. ACM Comput. Surv. 55, 1, Article 20, 36 pages.

https://dl.acm.org/doi/pdf/10.1145/3487890?casa_token=waanfcph69AAAAAA:6aILytn1bRM97LD6GHmFc6Ly873GvYVKtQaIb0tKLE3sjCEAWC0baCPvfJh3uGumb6wRilFfbV9p

[2] Naik, B. T., Hashmi, M. F., & Bokde, N. D. (2022). A Comprehensive Review of Computer Vision in Sports: Open Issues, Future Trends and Research Directions. Applied Sciences, 12(9), 4429. https://doi.org/10.3390/app12094429

[3] Radanliev P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. Frontiers in digital health, 7, 1431246. https://doi.org/10.3389/fdgth.2025.1431246

[4] Naik, B. T., Hashmi, M. F., & Bokde, N. D. (2022). A comprehensive review of computer vision in sports: Open issues, future trends and research directions. Applied Sciences, 12(9), 4429.

[5]Schaefer Rob. (2023). Generative AI plays on both sides of cybersecurity issue. Sports Business Journal. https://www.sportsbusinessjournal.com/Articles/2023/12/04/ai-cybersecurity/

[6] National Operations. (n.d.). NFL Next Gen Stats. https://operations.nfl.com/gameday/technology/nfl-next-gen-stats/

[7] Complete Concussions. (2025). https://completeconcussions.com/2018/12/05/concussion-rates-what-sport-most-concussions/

[8] Kawata, K., Tierney, R., Phillips, J., & Jeka, J. J. (2016). Effect of repetitive sub-concussive head impacts on ocular near point of convergence. International journal of sports medicine, 37(05), 405-410.

[9] NFL helmets Riddell. (n.d.). Precision-Fit helmets brochure. https://precisionfit.riddell.com/wp-content/uploads/files/Riddell_Precision_Fit_Brochure.pdf

[10] Reuters. (2025). NFL implementing Hawk-Eye system to measure first downs. https://www.reuters.com/sports/nfl-implementing-hawk-eye-system-measure-first-downs-2025-04-01/

[11] SISU Mouthguards. (n.d.). SISU Sense: Concussion-Sensing Mouthguards. https://www.sisuguard.com/sisusense/

[12] Stanford University. (2021). Most sensors designed to measure head impacts in sports produce inaccurate data. https://engineering.stanford.edu/news/most-sensors-designed-measure-head-impacts-sports-produce-inaccurate-data-stanford.

[13] NFL Operations. (n.d.). TECHNOLOGY AND THE GAME. https://operations.nfl.com/gameday/technology/technology-and-the-game/

[14] Gray Bren. (2024). Electronic Line Calling: Hawk-Eye Technology Explained. https://www.tennisnerd.net/articles/electronic-line-calling-hawk-eye-technology-explained/39915#:~:text=The%20Evolution%20and%20Origin%20of,What%20is%20this?

[15] MLB. (n.d.). Statcast. https://www.mlb.com/glossary/statcast