Chapter 9
Security Considerations in Generative AI for Web Applications

Siva Raja Sindiramutty
https://orcid.org/0009-0006-0310-8721
Taylor's University, Malaysia

Krishna Raj V. Prabagaran
Universiti Malaysia Sarawak, Malaysia

N. Z. Jhanjhi
https://orcid.org/0000-0001-8116-4733
Taylor's University, Malaysia

Mustansar Ali Ghazanfar
University of East London, UK

Nazir Ahmed Malik
https://orcid.org/0000-0002-0118-4601
Bahria University, Islamabad, Pakistan

Tariq Rahim Soomro
https://orcid.org/0000-0002-7119-0644
Institute of Business Management, Karachi, Pakistan

ABSTRACT

Protecting AI in web applications is necessary. This domain is a composite of technology and huge scope with good prospects and immense difficulties. This chapter covers the landscape of security issues with advancing generative AI techniques for integration into web development frameworks. The initial section is on security in web development—a conversation on the subtleties of generative AI-based methods. In a literal stance, the chapter offers 13 ways to approach it. Among the threats are those that introduce security issues related to generative AI deployments, which illustrate why it is vital for defenders and infrastructure owners to implement mitigation measures proactively. This chapter pertains to the security and privacy of data and lessons for securing and preventing vulnerability. The chapter explores attacks, model poisoning, bias issues, defence mechanisms, and long-term mitiga-

DOI: 10.4018/979-8-3693-5415-5.ch009

tion strategies. Additionally, Service A promotes transparency, explainability, and compliance with applicable laws while structuring a development methodology and deployment methods/operation. The text outlines how to respond and recover from incidents as it provides response frameworks for everyone involved in managing security breaches. Finally, it addresses trends, possible threats, and lessons learned from real-world case studies. In order to contribute to addressing these research needs, this chapter sheds light on the security considerations associated with AI for web development and suggests recommendations that can help researchers, practitioners, and policymakers enhance the security posture of popular generative AI advancements used in generating web applications.

INTRODUCTION TO SECURITY IN GENERATIVE AI FOR WEB ENGINEERING

Define the Importance of Security in Web Engineering and the Implications of Generative AI Techniques

Web development: Securing the web serves to protect assets and user privacy. As more usage is detected, security measures need to be in place. Per a study conducted by (Habbal et al., 2024), the context of security threats is ever-changing, making it tougher for web professionals. It would be best to implement security protocols to ensure that no one enters or can breach your data (Ahmadi, 2024). Artificial intelligence techniques are rising, bringing another layer to web security concerns. As highlighted by Liu et al. (2024), a new form of content creation and control involves text, images, or videos that highly accurate machines can manipulate. This development is an attractive opportunity for innovation but also raises fears regarding the misuse of AI-generated content (Kenwright, 2023; Sindiramutty et al., 2024).

Especially in web development, they have a safer internet because it secures the assets and privacy of users. Security is also essential, especially now with more and more activities happening around us. Research by Habbal et al. (2024) has observed that web professionals have to face challenges because cyber threats change daily. Our security proceeds related to access, data leakage and attacks are significant for being deployed against them (Ahmadi, 2024). That may result from the growing use of new UT web techniques or factoring in a fresh dimension field-based: more and automatising A Techniques, according to web security concerns. As highlighted by Liu et al. (2024), Generative AIs can produce and edit a wide range of content types, like text or images, with equal competency. An exciting technological evolution First and foremost, repurposing AI-generated content is a double-edged sword (Kenwright, 2023; Sindiramutty et al., 2024).