

Juice Jacking Defender

**Dr. Vaibhav Gandhi¹, Sasyareeth Malyala², Aditi Panchal³,
Obili Yashwanth Reddy⁴, Rajesh Panigrahi⁵**

Director and Faculty of Computer Science Engineering¹
Students, Department of Computer Science Engineering^{2,3,4,5}
Parul University, Vadodara, Gujarat, India

Abstract: *In an increasingly digital world, the proliferation of mobile devices has led to a growing dependence on public charging stations. However, these ubiquitous amenities also present a hidden danger: the threat of juice jacking. Juice jacking occurs when unsuspecting users connect their devices to compromised charging ports, inadvertently exposing their sensitive data to malicious actors. The “Juice Jacking Defender” project emerges as a proactive response to this pressing security concern. Through meticulous research, design, and development, this initiative seeks to create a robust defense mechanism against juice jacking attacks. By leveraging innovative technology, including portable devices or software solutions, the project aims to empower users with the means to detect and prevent potential security breaches while charging their devices in public spaces. Key components of the project include comprehensive analysis of existing juice jacking vulnerabilities and attack vectors, the creation of user-friendly interfaces for seamless interaction, and the implementation of sophisticated security measures to safeguard user data and device integrity. Rigorous testing ensures the effectiveness of the solution across diverse charging environments and device configurations. Moreover, the “Juice Jacking Defender” project extends beyond mere technical implementation. It places a strong emphasis on user education and awareness, striving to inform individuals about the risks associated with public charging stations and promote best practices for secure charging habits. Additionally, the project fosters collaboration with industry stakeholders, device manufacturers, and cybersecurity experts to advocate for improved security standards and regulations governing public charging infrastructure. Through continuous evaluation, feedback integration, and future enhancements, the “Juice Jacking Defender” project aims to evolve alongside emerging threats and technological advancements. By championing innovation, education, and collaboration, it seeks to establish a safer charging environment, thereby ensuring user confidence and privacy in an increasingly interconnected world.*

Keywords: Juice Jacking, USB Security Data Isolation, Public Charging Risks, Data Theft Prevention, USB Data Blocker, Mobile Device Protection, Public Charging Stations, Malware Defense, USB Data Isolation, IoT Security, Unauthorized Data Access, Cyber Attack Mitigation, Security Patch Analysis