IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 1, September 2025

Impact Factor: 7.67

Study on Wi-Fi De-authentication Attacks: Execution, Impact, and Ethical Detection

Karthick N[1], Vignesh G[2], Dharaneesh S R[3]

Assistant Professor[1]

BCA Students[2,3]

Sri Krishna Arts and Science College Coimbatore

karthickn@skasc.ac.in, vigneshg23bca065@skasc.ac.in, dharaneeshsr23bca017@skasc.ac.in

Abstract: *Radio Frequency Identification (RFID) is a rapidly growing wireless communication technology that enables automatic identification and tracking of objects using radio waves. It is widely used in various sectors such as transportation, healthcare, logistics, retail, and security systems. RFID offers advantages like fast scanning, automation, and contactless interaction, making it a preferred choice for modern systems. However, as the adoption of RFID increases, so do the concerns regarding its security and vulnerability to attacks. Many RFID systems are not properly secured, making them susceptible to exploitation by attackers using relatively simple tools.*

This journal aims to provide a detailed study on RFID hacking and the security mechanisms that can be used to prevent unauthorized access and data breaches. RFID systems typically consist of three main components: tags, readers, and backend databases. These components communicate wirelessly, often without the knowledge of the user, and this opens the door to several potential attacks such as eavesdropping, skimming, cloning, spoofing, and denial-of-service attacks. In particular, attackers can use off-the-shelf equipment to capture RFID signals from a distance, and in some cases, they can even modify or duplicate the information on RFID tags to impersonate legitimate users.

Understanding how these attacks work is crucial for improving the security of RFID-based systems. This study not only covers the various types of attacks but also investigates real-world scenarios where RFID systems were compromised. For example, RFID access cards used in office buildings and hotels have been cloned to gain unauthorized entry. Similarly, RFID-enabled passports and credit cards have been skimmed to steal personal and financial data. These cases demonstrate the importance of implementing robust security measures to protect sensitive information.

Several security solutions are discussed in this journal, including encryption techniques, mutual authentication protocols, and secure tag-reader communication. Newer technologies like blockchain-based RFID and machine learning-based intrusion detection systems are also explored as future directions. The goal is to evaluate how effective these solutions are in mitigating different types of threats and how organizations can adopt them without compromising usability or performance..

Keywords*: RFID*

DOI: 10.48175/568