Cryptanalysis of RFID Based Authentication Protocol (RSEAP2) for VCC

Vikas Kumar* and Rahul Kumar

Department of Mathematics, SSV College Hapur, Uttar Pradesh, India

*Corresponding Author

ABSTRACT

A technology that supports the Internet of Things (IoT) is RFID (Radio Frequency Identification). In RFID, any physical object can be linked to the Internet of Things. Security and privacy issues are inevitable when RFID is widely used, and adoption rates are rising. Security risks include interference with, manipulation of, and replay of the wireless broadcast channel between the tag and the reader. Unverified tags or readers send messages that are not reliable. A reliable and secure RFID authentication solution is needed for IoT. We evaluate the security of the hash-based and ECB-based RSEP2 authentication protocol, both of which were recently developed by Safkhani et al. According to our security study, RSEAP2 has significant security flaws such mutual authentication, session key agreement, and denial of service attacks. Therefore, RSEAP 2 is not secure in VCC.

Keywords: RFID, IoT, RSEAP2, VCC.

DOI: 10.21467/abstracts.138 ISBN: 978-81-957605-2-7 (eBook)