Video#40: How safe is contactless payment? || How does RFID & NFC work? || EB#40

Understanding RFID and NFC Technologies

Introduction to Contactless Payment

In today's world, contactless payment methods, such as Google Pay, have become increasingly popular. These methods allow users to make payments without using cash, simply by holding their card or mobile device near a payment terminal. Contactless payments rely on technologies such as RFID (Radio Frequency Identification) and NFC (Near Field Communication), which enable wireless communication between devices. However, security concerns always arise when dealing with money transactions.

Introduction to RFID and NFC

RFID and NFC are the underlying technologies used in contactless payments. RFID is a wireless communication technology that enables data transfer using radio waves, while NFC is a specialized subset of RFID that operates over short distances and is commonly used for secure transactions like contactless payments.

Common RFID Reader ICs

When searching for RFID readers for Arduino on platforms like eBay, three popular ICs emerge:

1. **RDM6300** – Operates at a low frequency (125 KHz).

2. **PN532** – Operates at a high frequency (13.56 MHz).

3. **RC522** – Also operates at a high frequency (13.56 MHz).

To explore these modules, all three readers were tested, each of which came with an RFID tag or card.

Connecting an RFID Reader to Arduino

The RC522 board was connected to an Arduino UNO according to the wiring scheme provided in the dump_in_full example sketch of the RC522 Arduino library. After establishing the

connections and uploading the example code, the serial monitor displayed data when an RFID tag was brought near the board.

How RFID Works

RFID stands for **Radio Frequency Identification** and enables wireless communication. The RFID reader has an antenna, typically in the form of a coil, which generates a magnetic field when a sinusoidal current flows through it. The key concepts include:

- **Frequency Usage:**

  - High Frequency (HF): 13.56 MHz (used by PN532 and RC522).

  - Low Frequency (LF): 125 KHz (used by RDM6300).

- **RFID Tag Components:** An RFID tag consists of an antenna (coil) and an integrated circuit (IC), which stores data.

- **Wireless Energy Transfer:** When the RFID tag enters the magnetic field of the reader, it induces voltage in the tag's coil, powering its IC.
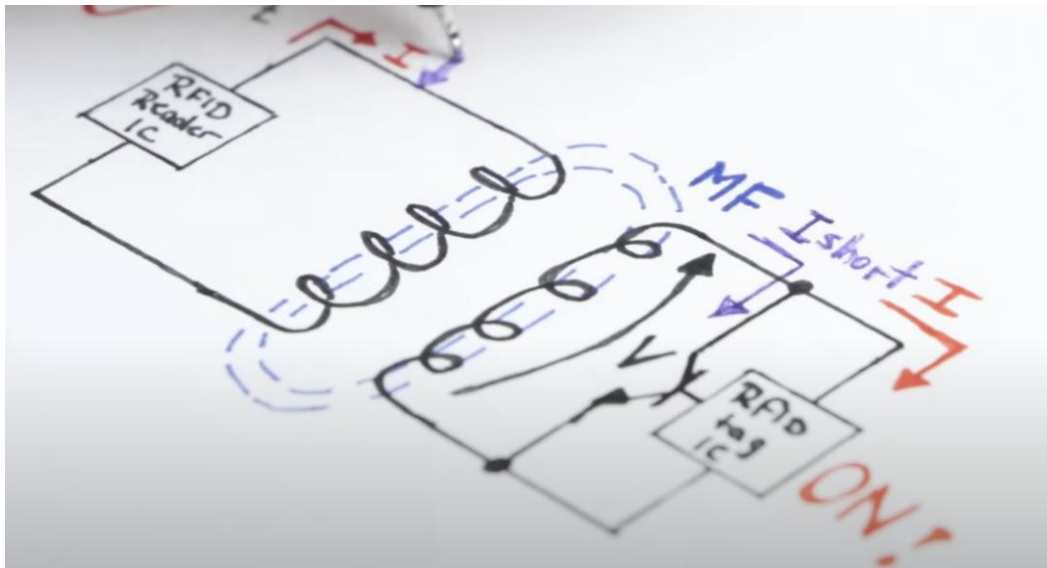

Fig: working principle of RFID

Communication Between RFID Reader and Tag

Once powered, the RFID tag transmits its stored data to the reader by modulating the amplitude of the received signal. This is achieved by shorting the coil inside the tag using a built-in transistor, which affects the carrier wave and allows data transmission.

NFC vs. RFID

Although NFC is based on RFID, there are some key differences:

- NFC is a subset of RFID and follows strict international standards such as ISO 14443, ISO 18092, and ISO 21481.

- NFC operates only at **high frequencies (13.56 MHz)** and requires close proximity between devices (a few centimeters).

- Unlike RFID, NFC allows both **reading and writing** of data, making it more versatile for secure transactions.

Using RFID in Arduino Projects

RFID readers can also write new data to RFID tags, enabling applications like security systems where RFID authentication is required to activate an action (e.g., turning on an LED). This makes RFID ideal for projects involving access control and authentication.

Security of Contactless Payment

To assess the security of contactless payment methods, experiments were conducted using the RC522 and PN532 readers. Neither was able to read data from a Girocard (a German bank card), indicating that such cards have security measures preventing unauthorized access.

Using NFC for Reading Data

Modern smartphones are equipped with NFC functionality. Using apps like **NFC Tools** or **NXP TagInfo**, users can scan and retrieve general information from RFID tags. When scanning a Girocard, it was recognized as an **ISO 14443-4 compliant tag**, but the stored memory was unreadable, likely due to encryption and security protocols.

Security Measures for Contactless Payments

- Contactless payments use **encryption techniques** to prevent unauthorized access.

- The requirement for close proximity between card and reader reduces risks.

- Payment limits often restrict the amount that can be transacted without authentication.

- **Anti-skimming cardholders**, made of metal, can block RFID signals and prevent unauthorized scanning.

Importance of RFID in Modern Technology

RFID technology is widely used beyond payment systems. For example, RFID-enabled cards can be used to access specific services, such as opening a YouTube channel when brought near a smartphone.

RFID and NFC are powerful wireless communication technologies with applications in payment systems, authentication, and security. While concerns exist regarding data security, encryption, proximity requirements, and additional protective measures make contactless payments relatively safe. RFID also opens up possibilities for various Arduino-based projects that involve data exchange and access control.