



TECHNOLOGY FEATURE Technology Report

Unseen Waves: The Mechanics and Vulnerabilities of Modern RFID Systems

A look into the wireless technology powering our world and the critical security gaps that remain hidden in plain sight.

By **M Tauseef Haider** | University of Agriculture, Faisalabad | Published: June 2026

✉ tauseefhaider.dev@gmail.com | Position: Student / Computer Sciences

Introduction

Every one of us would have been wondered when using a card at some ATM or at some metro station and that is just a simple tap and a beep sounds and our operation is performed or even some people would have experienced some locking and unlocking mechanism at some labs and private places where the users just have simple key ring or some card to scan and the door lock is open. It feels like magic for a new person who sees it the very first time or to the person who is unaware of the technology behind it. The magic is the RFID which is fully denoted as radio frequency Identification which consists of electromagnetic waves that just travel between two mediums between the scanner and the RFID Chip and data is transferred between them. So, every RFID card or tag has some unique ID which is used to recognize that specific one at the time of scanning.

In the digital progress of Pakistan, everyone is using that in daily life, but a very short amount of people knows the science and the magic behind it. Even the people on the motorways just pay using their M-Tags, which are also the RFID tags which are scanned at the tolls and the amount from their account is deducted.

These unseen waves are a piece of dopamine for new people when they see it for the first time as a luxury but there is a downside of the RFID which demands the security concerns should also be focused as there are certain flaws in the systems which may cause the system to fail and get penalized later.

"RFID is the silent backbone of the Internet of Things; it bridges the physical and digital worlds, but a bridge without a gate is a vulnerability."

Technology Overview

Originally, an RFID system have two main components which play the vital roles in the whole data transfer and operation performance they are termed as the **Tag** the transponder which stored the information and the **Reader** the interrogator which provides the power wirelessly using the electromagnetic waves and gets the data stored in the card or a tag. All this data transfer happens just due to the hidden waves which are the main cause of the whole magic.

These waves have different kinds of ranges depending upon the frequency of the **Tag** and the **Reader**, so the frequency matching is also a vital phenomenon to make the data transfer happen successfully. So, the ones with the low frequency having the lowest range are having 125KHz Frequency, the high frequency having the middle range are having 13.56MHz and the ultra-high frequency are the ones which have frequency in range from 860MHz to 960MHz.



To perform a successful data operation there is the need for tag to be in the range of the reader, and the range depends upon the frequency as already stated above the three waves with different frequencies have ranges 1-10cm, 1meter and 12 meters respectively.

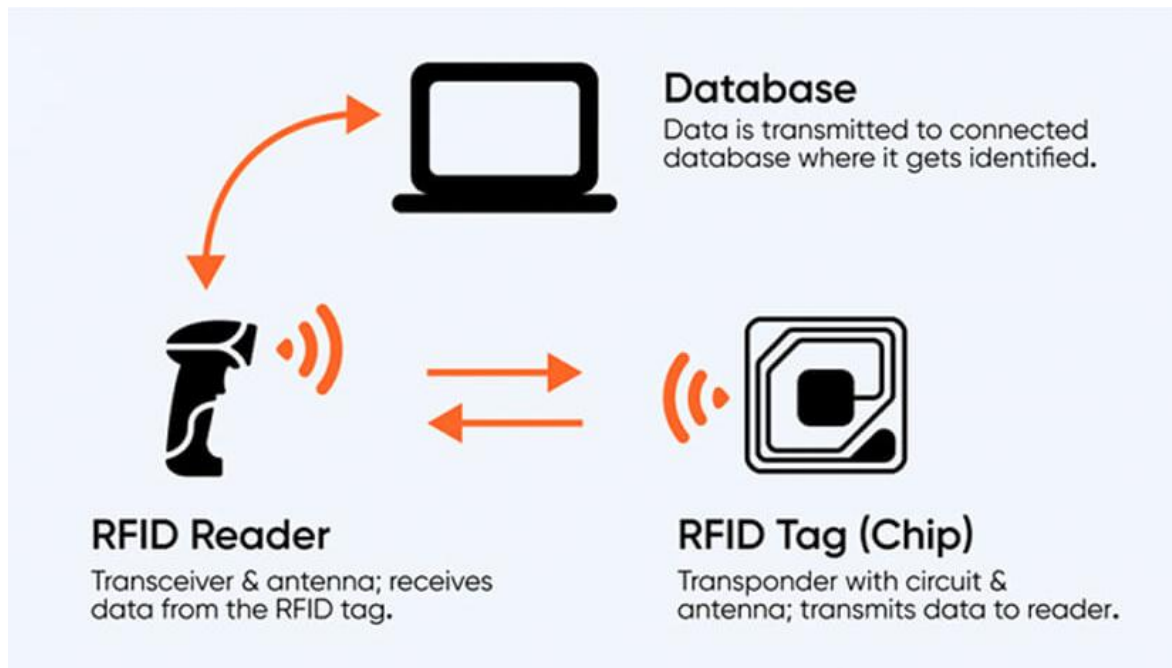


Figure 1: What is RFID technology. Credit: rfidlabel.com

Here as stated in the illustration below that when the card comes in the range of the reader, the card's chip antenna gets activated and provides electricity to the chip and chip releases the electromagnetic waves and send the data to the reader and the whole transaction proceeds the same way for the both operations the read and the write ones.

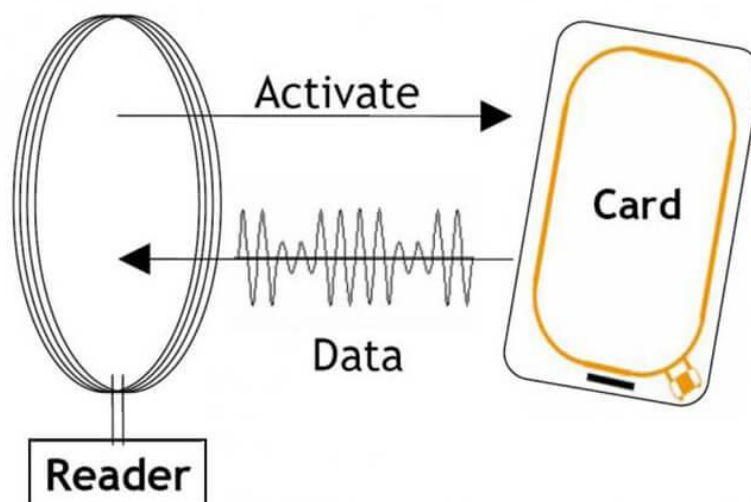




Figure 2: Working Principle of RFID Card. Credit: rfidlabel.com

Key Findings & Impact

The adoption of RFID brings a clear set of advantages, but they come with significant trade-offs:

The Pros:

- **Seamless Data Transfer:** The RFID technology takes an edge point on other competitors like the QR Code and the Bar Codes which are also scannable but the speed of scanning and amount of data store and transfer is fast in the RFID as compared to others as only one QR code or Barcode can be scanned at a time but in the antagonistic case a user can scan multiple or hundreds of cards at a time to transfer data and also has some higher data storage capacity.
- **Industrial Suitability:** In industries where the wear and tear is the main concern where a simple QR or Barcode scanner can get eroded due to the dust and smoke factors and can cause to stop working as they work on camera based sensors which need a proper clear vision to scan the data properly can be easily replaced by the RFID card can tags which can be embedded in the employees ID card which needs to be scanned only once and there is no chance of error in scanning due to the dust or smoke or other blocking factors and the scanner can scan even closed in the opaque box where there is no visibility so it gives the long lasting effect for the industrial use.
- **Complete Automation:** In inventory records where human errors are expected to come as humans can perform mistakes, but automated systems are no longer expected to perform any mistakes so automatic logistic management can be used to perform automated operations which can help keep proper track of later audit reports.
- **Digital Security:** In the bigger malls and markets where only human can not track all the goods to be paid before exiting the mall so to keep the track of such items the good are attached the RFID tags which are scanned at the payment counters and cleared from the data base and can be safely exited but if not then the exiting door scanner scans and check the tag info and beeps if the tag id is not marked as clear and it also have the edge point that the item can be scanned even if they are inside the bag of the customer.

The Cons and Security Concerns:

- **Data Theft and Cloning:** RFID tags have antennas which use the radio waves to communicate to the reader and if a person has some high gain antenna can read that data easily from a range and also the data or card can be cloned using the most famous device the Flipper Zero which is mostly used by most hackers to steal confidential information. So, it is susceptible to cloning which can be avoided using the RFID Blockers card holders or covers to protect unauthorized sensitive info tracking.
- **The Flaws of Unencrypted Channels:** In most of the RFID channels the data storage and transfer happens in the plain text instead of some encrypted or hashed form data so these data can also be read easily by some hackers using packet sniffing to radio waves capturing using antennas which can store even the confidential passwords or other IDs that should not be exposed. Also, most of the systems use the default password as by most manufacturers so it's easy to hack and write such cards so these should be changed before a hacker changes the password and the original user is blocked to use its card later.
- **System Integration Complexity:** As most of the developers are not well known of the IoT devices as the main focus by most of the developers is on other software systems so hardware and software integration



to update the database in real-time need proper expertise of such systems to handle the complex synchronized tasks to maintain the device scalability and the security to protect the end user from the later losses and regrets so to implement it there is the need of a proper developer who has deep knowledge for such IoT systems who can connect the devices to backends and also the sync that to the frontend data.

- **High Initial Capital Cost:** As the RFID needs proper hardware for setting up the whole system unlike the QR codes and the Barcodes which are simply printed and printing cost is less, needs the RFID tags, cards and scanners which cost much at the start so to setup the system the whole management cost can exceed some times for some organization's budgets as the developers who will setup such system will also demand the higher due to the lack of such people in the market.

For Pakistan's tech industry, the impact is double-edged. While RFID can revolutionize our logistics and agricultural supply chains, a lack of standardized encryption protocols could lead to a surge in identity theft and supply chain tampering.

What's Next?

Soon the Active Tags are to be used for better security and Blockchain technology can be there to help secure the systems from normal hackers so decrease the security flaws. Developers also need to study and have a proper home work on this to make such system robust in the future securing the systems making their implementation the hesitation free for the end user protecting the business firm from the economic and confidential losses just due to the RFID system flaws so needs to update the scanner and the chip to make an encrypted handshake instead of the simple one that can be tracked easily.

Next time if you are tapping your RFID card at some scanner, Metro Station the Bank ATM or the Door Lock, make sure to have a mind map of how the data is shared between these devices and helping the users to make their life convenient.

About the Author

M Tauseef Haider is a Computer Science Student at UAF with a primary focus on IoT and Embedded Systems. He can be reached at tauseefhaider.dev@gmail.com

Keywords: RFID; IoT; Cybersecurity; Wireless Communication; Pakistan Tech

References

- [1] Want, R. (2006). *An Introduction to RFID Technology*, IEEE Pervasive Computing, 5(1), pp. 25-33
- [2] Juels, A. (2006). *RFID security and privacy: a research survey*, IEEE Journal on Selected Areas in Communication, 24(2), pp.381-394.