**Multidisciplinary Journal of Research in Engineering and Technology**
ISSN: 2348-6953
Volume 13 Issue 2 (2026) | Pages: 199-204

# Security of NFC Transactions

Ashwini Patil[1], Prathmesh Joshi[2], Piyush Chikhalkar[3], Devanshu Joshi[4], Kartikey Konge[5], Buddhabhushan Dhale[6]

[123456]MCA, MES IMCC, Pune, Maharashtra, India
[1]asp.imcc@mespune.in, [2]prathmeshjoshi60580 @gmail.com, [3]chikhalkarpiyush@gmail.com, [4]joshi.drj23@gmail.com, [5]kongekartikey007@gmail.com, [6]bhushandhale2020@gmail.com

**Peer Review Information**

***Type**: Article*
***Received:** 19 March 2026*
***Revised:** 11 April 2026*
***Accepted:** 12 May 2026*
***Published:** 01 June 2026*

**Abstract**

Near Field Communication, or NFC, is paid for making payments smoother and faster than ever you merely tap your card or phone and you're done [4]. But just as this tech becomes more entrenched in our day-to-day living, so are the concerns surrounding just how secure it is. This piece sees more closely into the security behind NFC payments and looks at traditional threats like eavesdropping, relay attack, and tampering with messages [1], [5].
By looking into real cases, expert researches, and updated security measures, we determine areas where NFC systems are doing things right and where they need more work. All technologies like encryption, tokenization, and biometric authentication indeed help, yet we found out that both technology and consumer tendencies still have improvements to make [2], [4]. We also compare NFC to other contactless payment technologies like Bluetooth-based payments and QR codes to see how each of them stacks up on security. The goal is to give consumers, developers, and businesses a better idea of the dangers and allow them to make better informed decisions in this hectic, tap-to-pay world.

**Keywords:** Near Field Communication, Contactless Payments, Relay Attacks, Data Security, Biometric Authentication**.**

**How to Cite This Article**

Patil, A. Joshi, P. Chikhalkar, P. Joshi, D. Konge, K. Dhale, B. (2026). Security of NFC Transactions. *Multidisciplinary Journal of Research in Engineering and Technology*13(2), 199–204.

## Introduction

*What is NFC?*

Near Field Communication (NFC) is a form of wireless communication where two devices that are compatible can exchange information when they are placed very close to each other—typically a distance of 10 cm [1]. It uses the same technology as RFID (Radio Frequency Identification) but is used for efficient, secure, and fast communication. NFC works in two modes: active, where a device generates its own radio signal, and passive, where it uses the other device's signal. Because of its low power usage and ease of integration, NFC is employed widely in smartphones, contactless cards, smartwatches, and other consumer products, mainly for purposes such as tap-to-pay transactions and digital access [4].

Table 1

| | | Device A and Device B |
|---|---|---|
| Active | Passive | Only Device A generates the RF field |
| Passive | Active | Only Device B generates the RF field |

NFC specification details are available in ISO 18092 [1]. The most prominent feature of NFC is that it is a wirelessly connected user interface with a functional range of about 10 cm. The interface is operable in various modes. Modes are defined based on whether a device generates its own RF field or not, and whether a device extracts the power from the RF field a device has generated or not. If the device generates its own field, the device is referred to as an active device, or alternatively referred to as a passive device. Active devices will typically include a power source, passive devices will not (e.g. contactless Smart Card). If two devices are communicating with each other there are three possible arrangements. These are outlined in

Table 2: *Communication Configurations*

| **Device A** | **Device B** | **Description** |
|---|---|---|
| Active | Active | When a device sends data, it generates an RF field. When receiving data, a device does not generate an RF field. Thus, the RF field is alternatively generated by. |

This study isn't just about listing vulnerabilities (though we will list those as well). It's about asking: How do we get NFC as secure as it is convenient? We'll explore real- world attacks—like how thieves skim data off contactless cards or take over mobile wallets—and why current defenses occasionally fail [5]. More importantly, we'll explore how to build a stronger, more unified security framework that keeps up with both the technology and the threats. Because in an era where a single tap can unlock your car, your office, and your bank account, security can't be an afterthought.

## Background and Literature Review

*History and Development of NFC*

NFC technology evolved from RFID systems during the early 2000s as a two-way communication method [2]. The technology was standardized by Sony, Philips, and Nokia in the NFC Forum in 2004. Initial applications were focused on the exchange of basic data between devices.

The technology entered mainstream after its adoption in smartphones, beginning with Google Nexus S in 2010. It enabled innovative contactless applications like mobile payments (Apple Pay/Google Pay), access control, and public transit [4].

Whereas NFC's convenience brought with it swift deployment, its security framework suggests original design priorities favoring convenience at the expense of strict protection. Such is the reason for the vulnerabilities of today as the technology evolves to meet today's security needs.

*Technologies Applied in NFC Systems*

The NFC transaction process is based on a highly coordinated combination of a variety of distinct technologies. These all work together to enable secure, easy, and quick device-to-device communication. The technologies at the core include NFC readers, NFC chips, and secure elements [1].

*NFC Chips*

At the center of all NFC gadgets is the NFC chip. Inside, tiny, tiny microchips that make phones, watches, and contactless cards communicate with each other when they are in close contact—usually no further than 10 cm apart [1]. The chip does the radio

frequency communication and may be active mode (its own radio signal emitter) or passive mode (it picks up a signal given out by another gadget). Its low power consumption and compact size make it a suitable candidate for use in a wide range of consumer devices and payment applications.

*NFC Readers*

NFC readers are generally installed in payment points, ATMs, ticketing machines, and security access systems. They function as initiators of an NFC communication transaction, actively transmitting a signal to seekSecure Elements (SE)

NFC technology has secure elements—specialized parts for safe storage and processing of confidential data when protecting sensitive personal and financial information [3]. A tamper-proof element can store payment credentials, cryptographic keys, and other security-critical data. The secure elements occur in many forms:

- Embedded SE: Integrated directly into the device hardware (a feature on modern smartphones).
- SIM-based SE: Deployed inside the SIM card, managed by mobile network operators.
- Host Card Emulation (HCE): A cloud storage or operating system-based solution that enables emulation of the secure element.

All of these categories of secure elements have their own security model, and a choice is usually made depending on the application and how much control the service provider requires.

external and communicate with proximate NFC chips. The reader has an important function in authenticating the user and managing transaction information. For those applications concerned with money, NFC readers must comply with rigorous security requirements in an effort to provide secure data transfer.

*Research on NFC Vulnerabilities to Date*

Since NFC technology is being used more and more in normal payments, its security has been questioned by researchers [1], [4]. While the mode of operation that NFC communications are limited to within a short distance—generally less than 10 cm— may have suggested that it's secure by design, a number of studies have indicated that this isn't always so. The vulnerabilities may be due to both technical limitations inherent to NFC or how it's been implemented on various devices.

*Eavesdropping: Hearing at a Distance*

One of the most contested threats to NFC communication is, perhaps, eavesdropping [1]. At first glance, one might think that it would not be possible—well, devices must be layered on top of each other. Yet research by Alrawais (2020) and Van Damme et al. has shown that hostile individuals with sensitive antennas can receive NFC signals from 10 meters away if the transmitter device is powered on. In passive mode, the range is shortened to about 1 meter—but it is still a risk, especially in crowded public environments.

*Relay and Man-in-the-Middle (MITM) Attacks*

The second significant threat is relay attacks, which deceive systems into believing that there's an original NFC card when in reality a distant attacker substitutes it [5]. This has been demonstrated in most studies, such as the study by Korhonen (2017) and Alrawais (2020), where two smartphones were employed to relay the NFC signal— basically permitting an attacker to "tap" his victim's card remotely.

Man-in-the-middle attacks, though more difficult to execute because of NFC's quick and near-field nature, can still be executed. There have been demonstrations by some researchers on how delay or synchronization gaps can be used to intercept and modify communication between two devices.

*Denial of Service (DoS): Crashing and Disrupting Devices*

In some tests, scientists have shown that NFC phones can be hijacked through specially crafted tags [5]. For instance, a phone can crash or freeze simply by tapping it with an empty or malicious tag. In one test, repeatedly scanning a malformed tag caused the phone to reboot automatically, something that could be exploited to destroy trust in NFC services.

*Data Manipulation and Injection*

NFC messages are also subtly manipulated [5]. A simple example is manipulating smart posters with NFC tags sending links so that the user unknowingly accesses a spoof site. Collin Mulliner (2009) discovered that attackers are able to manipulate message display, concealing malicious data with formatting tricks such as inserted whitespace. In certain instances, even payload length manipulation of a message can cause the device to crash.

*Malware and Application Vulnerabilities*

The application side of NFC also does not go without its set of problems— particularly on operating systems such as Android [5]. Various research identified the way malicious applications which have NFC privileges can be employed in order to mount attacks. For example, Korhonen (2017) demonstrated how phishing attacks might be conducted by deploying imposter NFC tags in public areas, which would cause users to download malware or enter personal details unwittingly. On rooted devices, the attackers can proceed by cracking Secure Elements (SE) and stealing information from them.

*How NFC Compares to Other Technologies*

Unlike other wireless payment technologies such as Bluetooth or RFID, NFC has disadvantages as well as advantages [2], [4]. Its proximity constraint makes accidental attacks unlikely and easier to use. On the other hand, unlike with Bluetooth, NFC doesn't

have inherent strong security attributes—so the responsibility lies with app developers and service providers to lock down the communication. Bluetooth links are pair and encrypt by default otherwise.

**Methodology**

This research is entirely literature-based, focusing on analysing existing work rather than conducting new experiments or surveys. The goal was to understand how secure NFC (Near Field Communication) technology really is, especially when used in digital payments.

*Literature Review*

To investigate this, we reviewed a large corpus of literature that consisted of research papers, journal articles, technical whitepapers, and actual security reports. Sources were obtained from academic websites which are reliable such as IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. Of interest was the awareness of known existing vulnerabilities in NFC systems—relay attacks, eavesdropping, and data tampering—and how researchers have suggested ways of countering them [1], [5].

This review enabled us to have a clear picture of how NFC operates, its limitations, and how security technologies like encryption and secure elements are being utilized to manage risk [3], [4].

*Case Study Analysis*

In addition to theoretical studies, we also explored actual demonstration samples and case study reports. Demonstrations encompass hands-on demonstrations of attacks, e.g., relay attacks on two phones, and how NFC tags can be used to crash devices or direct users to sites that are intended to cause harm [5].

By applying such common examples, we were able to bridge what the research suggests with how things really work in real life. This enabled us to understand better both the positives and negatives of existing NFC security.

*Scope of the Study*

This study has no experiments, user surveys, or interviews. Instead, our concern was to gather, compare, and analyze what others have studied and documented previously. In doing so, we aim to gain a clear concept of where NFC security is now and point out where further research or improvement is still needed.

*Security Analysis – Vulnerabilities in NFC's*

*Eavesdropping* NFC eavesdropping is covert because it exploits our confidence in proximity contactless payments [1]. You think you're tapping in security when tapping your phone or card, but the wrong individuals with the appropriate equipment can snoop on that information from up to 20 cm away, particularly in densely populated areas like train stations or queues outside shops. Older NFC systems are particularly dangerous, because some transmit card information unencrypted, so it's simple for the one who happens to be standing there to steal your information and you'll never realize. Even some newer systems that have encryption are not totally safe, and as eavesdropping is traceless, many don't discover until they notice something odd. While technologies such as EMV tokenization are in place to prevent it, interaction between legacy infrastructure and new forms of hacking ensures that eavesdropping is a continuing issue [4]. The best defense? Encryption and understanding where and when to make a contactless payment.

*Relay attacks* is among the digital pickpocketing—just more subtle [5]. Imagine someone standing near you in crowded place, like shopping mall or market, with a hidden device that silently steals the signal from your NFC card or phone. Meanwhile, another of their accomplices is waiting at payment terminal somewhere else, using that signal to make a purchase which is impersonating you. Your card never leaves your pocket, and your money's still gone. That's the scary part: you don't even know it's happening. Such a theft is made possible because NFC isn't always checking how close the device really is—it only finds a proper signal [5]. While newer technology like fingerprint checks and distance measurements are helping, not all systems support them yet. So, though tapping to pay is actually quite handy, it's a good idea to keep your wits about you, especially in crowded spaces where a person could get close enough to perform a relay without you ever noticing.

*Device theft* Theft of the device is a simple but real risk [4]. If your phone or your contactless payment card is stolen, the thief can then access your money—especially if there is no protection or lock screen. A little like losing your purse or wallet but with the danger that your electronic wallet is easily available to tap-and-go spend immediately.

Luckily, modern phones now have a fingerprint unlock, face ID, or PINs that can leave thieves stuck—but only if you take advantage of them [2]. Contactless cards, on the other hand, don't need any PIN for small purchases, so they are more open to misuse if it is stolen.

The take-home message? Treat your card or phone like cash. Lock your phone, turn on tracking features in case it gets lost, and immediately report your card lost if you lose it. A couple of simple steps can make all the difference when it comes to protecting your money.

*Proposed Contributions and Suggestions*

While existing security mechanisms like tokenization and biometric authentication have significantly improved NFC security, there is still room for improvement [2], [4]. Based on our analysis, we propose a few practical enhancements that can make NFC transactions safer in real-world scenarios.

One of the biggest concerns today is relay attacks, which work almost like digital pickpocketing [5]. Even though the user's card or phone never leaves their pocket, attackers can still misuse it. To address this, we suggest implementing distance bounding techniques that can verify how close the device actually is, instead of just trusting the signal. This would make it much harder for attackers to trick the system from a distance.

Another area that needs attention is authentication. Right now, many small transactions happen without any verification, which makes misuse easier if a device is lost or stolen [4]. A better approach would be adaptive authentication, where the system asks for fingerprint or PIN not just based on amount, but also on unusual behavior—like multiple quick transactions or a change in location.

We also believe that NFC systems can benefit from smarter fraud detection. Instead of reacting after fraud happens, systems should be able to detect suspicious activity in real time. For example, if multiple taps are happening in a short span or from different places, the system should automatically flag or block the transaction. This is where AI-based monitoring can play a major role.

Another practical issue is fake or malicious NFC tags, especially in public places [5]. Users often tap without thinking, which can lead to phishing or malware attacks. To reduce this risk, NFC tags should include some form of digital verification so that devices can confirm whether the source is trusted before opening links or performing actions.

In addition, stronger encryption should be enforced across all NFC systems. While modern systems are more secure, older or poorly implemented systems still leave gaps [1]. Ensuring end-to-end encryption without fallback to weaker modes can help reduce risks like eavesdropping.

User awareness is equally important. Many attacks succeed not because of weak technology, but because users are unaware of risks. Simple measures like showing instant transaction alerts or warning users when tapping in risky environments can make a big difference.

Finally, instead of fixed transaction limits, systems can adopt dynamic limits based on risk level. For example, transactions in a trusted environment can have higher limits, while suspicious situations can automatically reduce the allowed amount or require additional verification.

Overall, these suggestions aim to bridge the gap between existing security mechanisms and real-world threats. By combining stronger technology with smarter systems and better user awareness, NFC transactions can become not just convenient, but also significantly more secure.

*Risk Mitigation Techniques*

*Tokenization* is one of the smartest ways to secure your payment information during an NFC transaction [4]. Instead of passing on your actual credit card number when you tap to pay, the system passes on a single-use-only, one-of-a-kind code—a token. That token stands in for your real information and can't be reused even if an attacker manages to catch it.

Think of it like a one-time fake key. So, even if the hacker gets that token, it won't work in any other transaction except that one. That way, your actual card number is kept secret and secure. Most of these mobile wallets like Apple Pay, Google Pay, and Samsung Pay are already tokenizing by default, so tap-to-pay every day becomes much safer [4].

*Biometric verification* places a strong layer of individual security on NFC transactions by making sure that you're the one verifying the transaction [2]. Instead of just tapping your card or phone and hoping it's safe, programs now often ask for a fingerprint, facial scan, or even a voice scan to make sure it's really you.

It's like carrying your fingerprint as the password—something that everyone else doesn't have but you. This is quite difficult for other people to open your gadget, even in the event that it gets lost or stolen. Biometric identification arrives as a capability on various current smartphones as well as cash payment apps to ensure that single tapping does not equal an effortless goal for intruders [2].

*Transaction limits* are a simple but efficient way to limit fraud risk in NFC payments [6]. In essence, they limit the amount of cash that can be spent on a single transaction without further authentication—like fingerprint or PIN recognition.

For example, the majority of NFC systems allow you to pay for a fixed amount of money (usually a few dollars) without any additional security. If you try to pay for something more expensive, the system will ask for confirmation. You won't lose much in this case if your phone or card is stolen. Even if they succeed in tapping and making an instantaneous payment, they won't be able to drain your account in one go. It's as if there's a transaction limit on a debit card—you attempt to swipe beyond a certain limit, you're halted. Transaction limits protect NFC buys, even when you have your phone or card sitting unsecured [6].

## Conclusion

Near Field Communication (NFC) has made payment a quicker and touchless process, but growing reliance upon it forms ever-mounting security threats. It is our observation from this literature review that even though NFC has been contemplated for use in near-field communication to limit threat, it remains vulnerable to existing threats such as eavesdropping, relay attacks, and hijacking of the device—especially with legacy system presence or lack of user focus.

Despite all these dangers, the advent of tokenization, biometric verification, and payment caps is in the right direction towards security. New smartphones and mobile wallets are leading the way through secure contactless transactions.

In short, the future of NFC is one of security and convenience in harmony. Secure deployment, regular system updating, and end-user education are the secret to safeguarding against new threats without compromising the advantages of contactless technology.

**References**


1. "NFC Devices: Security and Privacy" - G Madlmayr, J Langer, C Kantner… - … Reliability and Security, 2008 - ieeexplore.ieee.org.
2. "Current benefits and future directions of NFC services" - Kerem Ok; Vedat Coskun; Mehmet N. Aydin; Busra Ozdenizci, 10.1109/ICEMT.2010.5657642
3. "Security in near field communication (NFC)" - Philips Semiconductors Mikronweg 1, 8101 Gratkorn, Austria.
4. "NFC and NFC payments: A review" - Nahar Sunny Suresh Shobha; Kajarekar Sunit Pravin Aruna; Manjrekar Devesh Parag Bhagyashree; Kotian Siddhanth Jagdish Sarita, IEEE *Xplore*.
5. "NFC Payment & Security Threats" - Niko Korhonen - Bachelor's Thesis Degree Programme in Business Information Technology 2017.
6. "Secure NFC Based Loyalty Management System with Payment Module" - International Journal of Innovative Science and Research Technology ISSN No: - 2456- 2165.