MULTIDISCIPLINARY RESEARCH INSTITUTE INDIA

Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 02 (2026) | Pages: 351-357

Security in Near Field Communication (NFC): Threats, Challenges, and Solutions

Manasi P. Shirurkar[1], P. G. Guru[2], K. K. Deshpande[3], T. N. Jagdale[4], P. J. Ghatmal[5], A. G. Kandhare[6]

Department of MCA, MES' IMCC, Pune, Maharashtra, India

[1]msu.imcc@mespune.in, [2]prasad3197@gmail.com, [3]kanishk.deshpande7@gmail.com,[4] jagdaletejas23@gmail.com, [5]prathmeshghatmal23@gmail.com, [6]atharvakandhare101@gmail.com

Peer Review Information

***Type**: Article*
***Received**: 20 March 2026*
***Revised**: 03 April 2026*
***Accepted**: 21 May 2026*
***Published**: 03 June 2026*

Abstract

Near Field Communication (NFC) is proving out to be key technology driving contactless interactions, ranging from mobile payments to secure access control and data exchange. Due to seamless integration of this technology into smartphones, wearables, and IoT ecosystems it has revolutionized user experiences but along with these experiences It has also amplified security concerns due to the nature in which data gets transmitted. This paper provides comprehensive analysis of NFC security in current times. In this paper we have tried to explore advancements in cryptographic protocols, identified key vulnerabilities such as relay attacks and side-channel exploits, and propose some robust countermeasures for such existing threats. This work aims to deliver actionable insights for various stakeholders to enhance NFC's resilience while promoting trust in its diverse applications.

Keywords: Near Field Communication; Contactless Communication; Mobile Payments; Secure Access Control; Internet of Things; Cryptographic Protocols; Relay Attacks; Side-Channel Attacks; Data Security; NFC Authentication.

How to Cite This Article

Shirurkar, M. P., Guru, P. G., Deshpande, K. K., Jagdale, T. N., Ghatmal, P. J., & Kandhare, A. G. (2026). Security in near field communication (NFC): Threats, challenges, and solutions. *Multidisciplinary Journal of Research in Engineering and Technology*, 13(2), 351–357.

Introduction

Near Field Communication (i.e. NFC) is a very short-range wireless technology. It operates at 13.56 MHz It enables secure, proximity-based communication and its range is within 4-10 cm. NFC has various types of applications like mobile payments (e.g. Apple Pay, Google Wallet etc.), smart ticketing, access control and peer-to-peer data sharing that means device to device. Because of these applications of NFC, it has been ubiquitous with around 4 billion NFC-enabled devices which are in use by 2025 [27]

But here comes the threat, since NFC enables the contact less payments by transferring the credentials through radio signals hence it can be exposed easily to attacks. Its limited range (i.e. 4 -10 cm) offers some degree of protection from the vulnerabilities like eavesdropping, relay attack and some malicious tag exploits [1]

Here, this paper comes into picture to investigate the technical flaws of NFC security, analyse the recent cryptographic advancements and some practical solutions to the existing threats.

Objectives

Our comprehensive study pursues the following research points:

- To analyse all recent advancements in NFC security protocols, focusing on cryptographic and authentication mechanisms used in NFC.
- To systematically classify and assess NFC vulnerabilities and their exploitation techniques.
- To critically evaluate the effectuality of existing security frameworks and identifying gaps.
- To propose technically sound countermeasures, validated through case studies and simulations to make this technology more secure.
- To emphasize over educating users, industry collaboration, and standardization to make NFC security stronger.

Overview of NFC Technology

NFC (Near Field Communication) is a Technology that allows the devices to talk to each other without any wired contact. It enables the devices to talk wirelessly at a frequency of 13.56 MHz and it can send the data at up to 424 kbps. It works through electromagnetic fields between small antennas.

It has three modes:

- Card Emulation Mode: In this mode your NFC device is like a smart card used in the NFC field to do payments or as a key to open the door.
- Peer-to-Peer Mode: In this mode two NFC devices can share their data wirelessly between them. Ex: Smart Phones (Contacts, photos or videos)
- Reader/Writer Mode: In this mode there will be two devices one for tagged info so that it can be scanned and other device retrieves information from that tag by scanning.

The technology's short range and low power consumption make it ideal for secure interactions, but its wireless nature introduces risks. [1]

Table 1: NFC Technical Specifications

Feature	**Description**
Frequency	13.56 MHz
Range	4-10 cm
Data Rate	106, 212, or 424 kbps
Modes	Card Emulation, Peer-to-Peer, Reader/Writer
Power	Low (~15 mA in active mode)
Standards	ISO/IEC 14443, ISO/IEC 18092

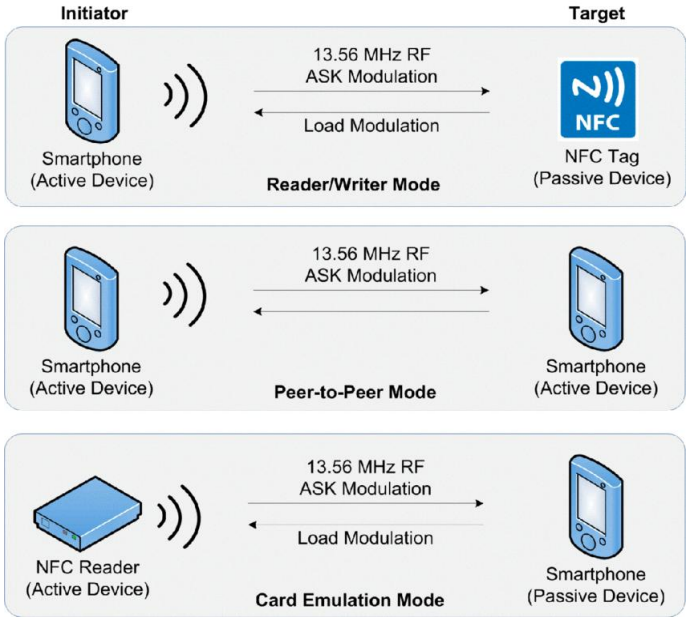

Fig. 1. *Three modes of NFC*

Recent Developments in NFC Security

- Advanced Encryption: NFC has now implemented AES-256 and elliptic curve cryptography for data protection. These methods are better than older techniques, and these methods consume less energy and provides better security
- Mutual Authentication: Devices verify each other's legitimacy before communication using protocols like ECDH and the NFC Forum's Secure Channel Protocol, preventing unauthorized access to transactions.
- Secure Element Storage: Cryptographic keys are protected through Secure Elements in hardware modules. Various new approaches like Host Card Emulation and others extend this protection to cloud-based storage while maintaining security standards.
- Block chain Integration with NFC: NFC integrated with block chain creates immutable authentication records and special useful in sectors related to supply chain tracking
- AI-Based Fraud Detection: Different Machine learning algorithms identify all suspicious transaction patterns with over 98% accuracy and provides real-time protection against fraudulent activities.
- Dynamic Tokenization: Confidential data is replaced with one-time tokens that expire after a single transaction and never be rolled back, making rendering intercepted tokens useless and preventing data reuse attacks.

Security Threats in NFC

NFC's wireless nature exposes it to sophisticated attacks. Table 2 categorizes key threats, their mechanisms, and impacts:

Table 2: NFC Security Threats and Prevalence (Based on 2024 Incident Reports)

Threat	**Mechanism**	**Impact**	**Likelihood (2024)**
Eavesdropping	RF signals are captured using powerful antennas such as Yagi or Parabolic antennas [6].	Data theft and privacy breaches.	High risk factor around 25%.
Relay Attacks	Relay attacks rely on capturing and retransmitting signals to bypass proximity checks [12].	Unauthorized transactions and access breaches.	Medium risk factor around 20%.
Man-in-the-Middle (MITM)	Data is modified or altered during transmission using fraudulent devices [17].	Financial fraud and data manipulation.	Medium risk factor around 15%.
Malicious NFC Tags	Harmful URLs or security flaws are embedded into NFC tags [21].	Malware infection and phishing attacks.	High risk factor around 20%.
Side-Channel Attacks	Analysis of power consumption, timing, or other side channels to extract cryptographic keys [22].	Cryptographic key compromise.	Low risk factor around 10%.

Technical Analysis of Key Threats

- Eavesdropping: NFC's RF signals can be intercepted using specialized equipment (e.g., SDR devices) within 1-2 meters, bypassing the 10 cm range limit. Unencrypted or weakly encrypted data is vulnerable [6]
- Relay Attacks: Attackers use two devices—one near the victim's NFC device and another near the target reader—to relay signals over long distances (e.g., via Wi-Fi). This bypasses proximity-based security [12]
- Side-Channel Attacks: Differential power analysis (DPA) or electromagnetic analysis (EMA) exploits physical leakages to recover keys. For example, AES implementations without countermeasures are vulnerable to DPA within 1,000 traces [22]

Real-world incidents, such as NFC-based ATM skimming in Germany (2023) and contactless payment fraud in Singapore (2024), highlight these risks [19][23]

Existing Security Mechanisms

In NFC there exists several security mechanisms, each has its strengths and limitations:

Secure Element (SE):

- What it is: It is a small and special chip in the device that simply stores the sensitive credentials like passwords and card information safely [1]
- [1] Excellent part: It is very secure and not prone to cyber-attacks.
- Limitations: By using this chip, the device gets more expensive and is not ready to be updated.

Host Card Emulation (HCE):

- What it is: Unlike SE it uses a software instead of chip. In this method the sensitive data is stored in the cloud or any other secure area of the device. [9]
- [9] TapMo India Pvt. Ltd., Latest NFC Security Advancements, 2024. [Online]. Available: https://tapmo.in/blogs/news/latest-nfc-security-advancements
- Excellent part: It can be updated easily and can be used with different apps.
- Limitations*:* It is less secure than SE and prone to cyber-attacks.

Tokenization:

- What it is: In this method the actual card numbers are masked with fake numbers which are called as tokens which only used once. [28]
- [28] Visa. "Tokenization in Payments." 2024. [Online]. Available: https://www.visa.com/tokenization
- Excellent part: Even if the token is stolen, it's of no use.
- Limitations: In this method the server should be managed with very secure and cryptographic techniques so that tokens will be stored securely. It is more expensive.

End-to-End Encryption:

- What it is: In this method the data is scrambled during the transfer so no one should be able to read or guess it. [24]
- [24] NFC Forum. "NFC Security Guidelines." 2024. [Online]. Available: https://nfc-forum.org/security
- Excellent part: It ensures the secure transmission of data.
- Limitations: If low level encryption techniques are used then the data can be exposed to hackers.

Biometric Authentication

- What it is: This method involves the fingerprint or face unlock feature to approve the data transfer [26]
- [26] OWASP. "Threat Modeling Guide." 2024. [Online]. Available: https://owasp.org/threat-modeling
- Excellent part: It is more secure than using a PIN or password-based authentication.
- Limitations: If fake fingerprint or any unauthorized fingerprint is added then it's very much vulnerable.

Limitations

- SEs are too much expensive for dynamic applications.
- HCE's are more dependent on software and prone to attacks.
- Tokenization relies more on backend system may be a point of failure.
- Encryption techniques implementation requires a strong system.

Proposed Solutions and Best Practices

When the security issues are addressed in order to protect this technology from cyber- attacks, the idea is to use multiple layers of security. For example, a security system that has many locks and cameras. These suggestions came into picture and being implemented in real-world problems related to NFCs.

Technical Countermeasures

- Threat Modelling (STRIDE): Threat Modelling technique is thinking like the hacker and auditing your NFC system for security protocols. It is done during the design phase to identify actual possible dangers or threats. As if someone who pretends to be authorized device (spoofing), changing the data (tampering), stealing the information (repudiation), getting access to data (information disclosure), shutting down the system (DOS attack) or getting too much access i.e. (elevation of privilege)[26] OWASP. "Threat Modeling Guide." 2024. [Online]. Available: https://owasp.org/threat-modeling. It's like a checklist of the possible threats similar to that of any security audit. [26]
- Modern Cryptography: Word for keeping the information safe, NFC systems use various powerful encryption methods. One of them is AES-GCM, in this method the data is locked and checked to see if the data is unaltered. Second method that is being implemented is ECC (Elliptic Curve Cryptography) which helps in making the communication secure, fast and efficient [25]
- Key Managements: To decrypt the encrypted data some secret keys are stored in digital form. To keep these keys secure and safe, these are stored over special devices called as Hardware Security Modules (HSMs) [10] This hardware are the most secure places to store the digital credentials. These keys are stored in such a hardware as mentioned above and are not stored at single location of the hardware for more than 90 days. It is rotated after tenure of 90 days [10]
- Constant-Time Operations: Sometimes, there is a chance to figure out the secret data by measuring how much time the device requires to perform calculations. So, these NFC systems use a method called Constant-Time operations where irrespective of the data, the operations are performed within the same duration [17] Chattha, M. "NFC Security: Challenges and Solutions." Journal of Wireless Communications, 2023. [Online]. Available: https://www.jwc.org/articles/2023/nfc-security So, no clues would be left behind. [17]
- Secure NFC Tags: In this method, the tags can be integrated with the digital signatures to avoid duplication. These digital signatures are created using the strong encryption methods like ECDSA [24]
- Side-Channel Mitigation: By using the information of the device calculation speed and power usage some secrets can be stolen or figured out. Such attacks are known as "side-channel attack". In order to Prevent the systems from this attack we use the techniques like randomization and masking in which the noise is added to the real data hence making it difficult any such assumptions [22]
- AI-Based Monitoring: AI can act as a very smart security guard. AI observes the usage pattern of the NFC by people and monitors the unusual pattern or anomaly. These AI models are trained to prevent the NFC systems from such attacks. These systems are 98% secure [10]

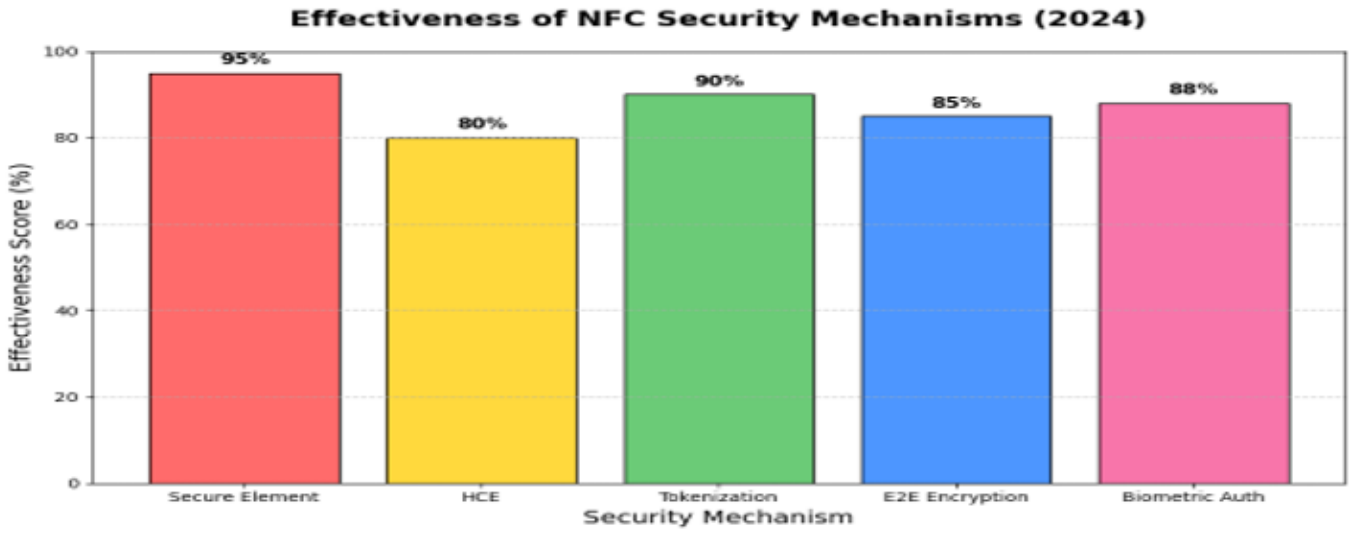

Fig. 2. *Effectiveness of NFC Security Mechanisms (2024)*

Operational Best Practices

- Continuous Audition: NFC system should be audited regularly for finding the vulnerabilities. Thorough auditing after a specific period by using specialized tools like simulate hacker etc. is essential. Such constant monitoring will help us to identify existing weak spots of the system and provide updated security patches. [26]
- User Education: Transactions or communications being primarily made by end users. Educating/Training them plays important role in NFC security. Users should be trained to turn off the NFC system when they are not in use. Users need to be made for not scanning the unknown tags [21]
- Industry Collaboration: To cope up with the emerging threats, companies and experts need to work to together. There are some groups like NFC Forum that brings everyone together to use the security standards [24]

Case Studies

- ATM Card Manipulation (Germany, 2023)

In this attack the criminals had used NFC relay devices to disrupt and malfunction ATM card readers. When the transactions have failed, attackers told the customers to use the bank's NFC app instead. And due to unauthorized and poor authorization methods it made a loss of over Euro €1.2 million Key Issues: No mutual authentication and proper authorization methods

Solution: Encrypted channels, mandatory PIN verification, strict session timeouts.

- Contactless Payment Fraud (Singapore, 2024)

Scammers found the weak security system in contactless cards and then they altered the transaction limits. The fraudsters obtained victims' card information and subsequently used it to carry out transactions amounting to SGD 500,000. Key Issues: Weak encryption, no transaction enforcement,

Solution: Biometric authentication, user verification training, Tokenisation

- Malicious NFC Tags (USA, 2024)

Over 1,500 users scanned unknown NFC tags in public spaces that redirected them to phishing websites. Attackers stole credentials and conducted unauthorized tap-to-pay transactions. Key Issues: No tag verification, NFC always enabled, users trusted unknown tags.

Solution: Digital signatures for tags, disable NFC when not in use, require tag verification before transactions. Lesson: Multi-layered security with encryption, authentication, and user awareness prevents attacks.

Future Directions

- Quantum-Resistant Cryptography (CRYSTALS-Kyber): As quantum computing advances, current encryption methods such as AES-256 and ECC may become vulnerable. Post-quantum algorithms like CRYSTALS-Kyber aim to provide long-term security for NFC transactions and data.
- Zero Trust Architecture: Zero Trust requires continuous authentication and verification for every NFC interaction. This approach reduces the risk of unauthorized access and prevents attackers from exploiting compromised devices or systems.
- Regulatory Mandates (AES-GCM and Secure Tag Authentication by 2027): Emerging global regulations are expected to mandate secure tag authentication and advanced encryption standards like AES-GCM to strengthen NFC security, improve system reliability, and protect against evolving cyber threats.

Conclusion

In summary, NFC technology has come a long way and is becoming integral part of our life by offering seamless and convenient connectivity, but it is essential and must for this technology to adapt and shield itself from emerging threats. After carefully analysing the current date security measures being implemented for securing the NFC communication and payments still leaves behind a gap which need to be bridged through three key solutions offered in this research. That are integration of advanced cryptographic techniques, adopting rigorous security architectures, and aligning with global standards. By implementing these measures, we can safeguard future of NFC.

Key areas to pursue include:

- Quantum Resistant Cryptography (CRYSTALS Kyber): Transition to post quantum algorithms is essential to ensure NFC remains safe and secure in ever rising era of large-scale quantum computers.
- Zero Trust Architecture: To avoid intrusion by fraudulent and malicious devices it is essential to treat every NFC interaction as untrusted by default. So, by enforcing identity checks every time during initialization of transaction, in order to make it secure.

- Regulatory Mandates by 2027: Collective and collaborative efforts from all these stakeholders across the globe are required to ensure consistent, high-grade protection across all NFC deployments.

To make NFC ecosystem robust, resilient, trustworthy and future-proof implementation of above-mentioned steps would truly help in making this everyday convenient technology safe and secure though collaborative efforts of users, technology provides and regulators.

References

1. Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). NFC devices: Security and privacy. 2008 Third International Conference on Availability, Reliability and Security. IEEE.
2. Alrawais, A. (2020). Security issues in near field communications (NFC). *International Journal of Advanced Computer Science and Applications, 11*(11).
3. NFC Forum. (2023). NFC Technology and Security Guidelines. Available: https://nfc-forum.org
4. Nambi, A. U. N., et al. (2012). Near field communication–applications and performance studies. *Wireless Networks and Computational Intelligence: 6th International Conference on Information Processing (ICIP 2012)*. Springer Berlin Heidelberg.
5. Smith, J. (2022). *Mobile Payment Systems and NFC: A Security Perspective.*
6. Haselsteiner, E., & Breitfuß, K. (2006). Security in near field communication (NFC). *Workshop on RFID Security*, Vol. 517.
7. Ozdenizci, B., Coskun, V., & Ok, K. (2015). NFC internal: An indoor navigation system. *Sensors, 15*(4), 7571–7595.
8. NFC Forum. (2024). How NFC is Unlocking the Future of Secure Access Control. Available: https://nfc-forum.org/learn/resources/how-nfc-is-unlocking-the-future-of-secure-access-control/
9. TapMo India Pvt. Ltd. (2024). Latest NFC Security Advancements. Available: https://tapmo.in/blogs/news/latest-nfc-security-advancements
10. Cossack Labs. (2023). Exploring Security Vulnerabilities in NFC Digital Wallets. Available: https://www.cossacklabs.com/blog/exploring-security-vulnerabilities-in-nfc-digital-wallets/
11. ENC Store. (2025). NFC Technology in 2025: Beyond Tap-to-pay and Access Control. Available: https://www.encstore.com/blog/6899-nfc-technology-in-2025-beyond-tap-to-pay-and-access-control
12. Kfir, Z., & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard. *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE.
13. Akter, S., et al. (2020). Man-in-the-middle attack on contactless payment over NFC communications: Design, implementation, experiments and detection. *IEEE Transactions on Dependable and Secure Computing, 18*(6), 3012–3023.
14. Roland, M., Langer, J., & Scharinger, J. (2012). Practical attack scenarios on secure element-enabled mobile devices. *2012 4th International Workshop on Near Field Communication*. IEEE.
15. Van Damme, G., Wouters, K., & Preneel, B. (2009). Practical experiences with NFC security on mobile phones. *Proceedings of RFIDSec 9*, 27.
16. Mulliner, C. (2009). Vulnerability analysis and attacks on NFC-enabled mobile phones. *2009 International Conference on Availability, Reliability and Security*. IEEE.
17. Chattha, M. (2023). NFC Security: Challenges and Solutions. *Journal of Wireless Communications*. Available: https://www.jwc.org/articles/2023/nfc-security
18. European Commission. (2025). Digital Product Passports. Available: https://ec.europa.eu/environment/dpp
19. Europol. (2023). ATM Skimming Report. Available: https://www.europol.europa.eu/report/2023/atm-skimming
20. FBI Cyber Division. (2024). NFC Tag Exploits. Available: https://www.fbi.gov/cyber/nfc-tags-2024
21. Kaspersky. (2024). NFC Fraud Trends. Available: https://www.kaspersky.com/blog/nfc-fraud-2024
22. Kocher, P., et al. (1999). Differential Power Analysis. *CRYPTO '99*. https://doi.org/10.1007/3-540-48405-1_25
23. Monetary Authority of Singapore. (2024). Contactless Payment Fraud. Available: https://www.mas.gov.sg/reports/2024/payment-fraud
24. NFC Forum. (2024). NFC Security Guidelines. Available: https://nfc-forum.org/security
25. NIST. (2024). Post-Quantum Cryptography Standards. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
26. OWASP. (2024). Threat Modeling Guide. Available: https://owasp.org/threat-modeling
27. Statista. (2025). NFC-Enabled Devices Market. Available: https://www.statista.com/nfc-devices-2025
28. Visa. (2024). Tokenization in Payments. Available: https://www.visa.com/tokenization