TECHNICAL SCIENCES

APPLICATION OF NFC-BASED ATTENDANCE SYSTEMS, CHALLENGES AND SOLUTIONS

Jafarov N.
Associate Professor of the Department of "Computer Technologies" of Azerbaijan Technical University
ORCID: https://orcid.org/0009-0002-0667-8819
Gasimli T.
Azerbaijan Technical University - Master's student
Rahmanov J.
Azerbaijan Technical University - Master's student
Mahmudov V.
Azerbaijan Technical University - Master's student
https://doi.org/10.5281/zenodo.15102675

Abstract

The application of NFC technology has become popular in many areas. Also, the optimal implementation of NFC-based attendance verification systems in the education system is a pressing issue. The article discusses the advantages of applying the NFC system for student attendance records, the collection of attendance data in the database, and the possibilities of integration into the university system.

Keywords: NFC technology, NFC mobile application, advantages of NFC technology, difficulties of NFC technology, NFC-based attendance system, NFC system architecture

Introduction. Near Field Communication (NFC) is a short-range wireless communication technology that enables secure data exchange between devices within a distance of less than 10 cm. NFC-enabled systems in the education system allow students to mark attendance by tapping their NFC-equipped student card or smartphone on a reader device, automating data collection and reducing errors caused by manual processes. The card reader captures unique identification data from the NFC tag and records attendance in a centralized database. The application of NFC technology has gained popularity in many areas. Additionally, methods for the optimal implementation of NFC-based attendance verification systems in the education system are reflected in this article. The article discusses the advantages of implementing the system, the collection of attendance data in the database, and the possibilities of integration into the university system.

Traditional attendance verification methods pose several challenges, which can be overcome and automated by integrating the NFC system into the university's student attendance system:

- **Time-consuming:** Manual attendance processes can consume significant teaching time.
- **Prone to errors:** Manually entered data may lead to inaccuracies in attendance records due to human errors.
- **Fraudulent practices:** Traditional methods are vulnerable to proxy attendance, where one student marks attendance on behalf of another.
- **Inefficient data management:** Paper-based systems make it difficult to store, retrieve, and analyze attendance data efficiently.

The main objectives of implementing NFC-based attendance systems include:

- **Enhancing efficiency:** Automating attendance processes reduces the time spent on manual methods and allows for more efficient operations.
- **Improving accuracy:** NFC technology minimizes human errors, ensuring accurate and reliable attendance records.
- **Preventing fraud:** NFC-based systems enhance security by reducing the potential for fraudulent attendance practices.
- **Real-time data transmission:** These systems provide immediate access to data, facilitating timely interventions and decision-making.
- **Integration capability:** NFC-based attendance systems can be integrated with existing university management software, improving overall operational efficiency.

From the above points, it is evident that implementing NFC-based attendance systems eliminates the shortcomings of traditional methods by offering a more efficient, accurate, and secure approach to attendance management. [1,2]

The implementation of an NFC-based student attendance tracking system requires several key components to ensure seamless operation, data accuracy, and integration with university servers. The key components include NFC readers, NFC tags (or student cards), and servers for data processing and storage:

1. **NFC Readers:** NFC readers serve as the primary interface for scanning student identification cards and capturing attendance data. These readers interact with NFC tags, retrieve student data, and send it to the system for processing. Installed in classrooms or lecture halls, the NFC reader connects to a computer running attendance tracking software. When a student taps their NFC-enabled card on the reader, the reader extracts a unique identifier and verifies their presence in real time.
2. **NFC Tags (Student Cards):** NFC tags act as digital identifiers assigned to each student. These tags contain unique identification numbers corresponding to student records stored in the database. If the system

supports NFC-based data reading via mobile phones, NFC-enabled smartphones can also serve as virtual tags, replacing physical cards.

3. **Servers:** The backend infrastructure of the system consists of university servers responsible for processing, storing, and managing attendance records.

- **Database Server:** Stores student data, attendance records, and class schedules.
- **Application Server:** Manages data processing, authentication, and integration with university systems.
- **Integration with the Electronic Education System:** Attendance data is transferred to the university's "Electronic Education System" for recording absences and participation. [3]

Proper structuring of data flow and processing mechanisms in NFC-based attendance systems is crucial for their effectiveness and reliability. This technology facilitates real-time user identification by offering low-latency and fast data exchange capabilities. The main stages of data transmission in NFC-based systems include:

1. Data Collection

At this stage, NFC reader devices collect data from cards or tags. One of the most important elements here is the **UID (Unique Identifier),** which is the unique identification code assigned to each NFC tag.

- **ISO/IEC 14443 and ISO/IEC 15693 protocols** define the data transmission standards for NFC cards and readers.
- **Difference between RFID and NFC:** NFC enables close-range (less than 10 cm) data transmission, increasing its security advantage.
- **Active and Passive NFC Tags:** While active tags have an internal power source, passive tags derive power from the electromagnetic waves generated by the NFC reader. When a user brings an NFC card close to the reader, the system retrieves the UID stored on the tag, initiating the identification process.

2. Data Processing

The UID and other user data retrieved by the NFC reader are sent to the **Data Processing Server.** These servers perform the following key functions:

- **Authentication & Authorization** – Verifies whether the user is registered in the system. If the UID exists in the database, the system records attendance.
- **AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) encryption** methods can be used to enhance data security during transmission.
- **API and Web Services Integration** – NFC-based systems can integrate with existing organizational databases, allowing them to work in sync with HRM (Human Resource Management) and ERP (Enterprise Resource Planning) systems.

3. Data Storage & Utilization

Collected and processed data is archived in servers or cloud systems for long-term storage.

- **SQL and NoSQL databases** are used for storing structured and unstructured data (e.g., MySQL, PostgreSQL, MongoDB).
- **Backup and Redundancy Systems** – To prevent data loss, automatic backup systems (Backup Servers) and RAID (Redundant Array of Independent Disks) technology can be employed.
- **GDPR (General Data Protection Regulation) and ISO/IEC 27001** – Compliance with international standards for data security and privacy is essential.

4. Real-time vs. Offline Processing

NFC-based attendance systems can process data using two main methods:

- **Real-time Processing:** Data is immediately transmitted to the server, and attendance records are updated instantly. This method is faster and more efficient but requires a continuous internet connection.
- **Offline Processing:** The NFC device temporarily stores data locally and transfers it to the server at a later time. This method is useful in areas with poor internet connectivity. [4,5,6]

Role of Mobile Applications. Mobile devices and applications play a crucial role in NFC-based attendance systems. These applications allow users to participate in the attendance process conveniently through their mobile devices without the need for physical cards or identification tools. The functionality of mobile applications not only enhances user convenience but also ensures the system operates more flexibly and efficiently.

The primary roles of mobile applications in NFC-based attendance systems should be evaluated based on the following aspects:

1. **Identification and Authentication** – Mobile applications should function as NFC readers. This enables users to be identified directly via their smartphones without requiring physical cards. Unique identifiers (UID) or cryptographic keys are used in this process to perform authentication.
2. **Real-time Data Transmission and Synchronization** – Mobile applications should establish real-time communication with the attendance system's server and automatically update user data. This prevents delays and maximizes data reliability. Additionally, through the user interface, employees or students can access real-time information about their attendance status.
3. **Cloud-based Data Management** – NFC-based attendance systems are often integrated with cloud technologies to ensure system continuity and accessibility. Mobile applications should transmit attendance data to cloud servers, ensuring secure storage and remote management. This facilitates organizations' and institutions' access to attendance records anytime and anywhere.
4. **Expanded Functionality and Notifications** – Mobile applications should offer more than just attendance registration. For example, if the system records delays or attendance issues, the mobile application should notify the user. Additionally, users should be able to access their attendance records, manage missed days, and submit leave requests through the application.

The use of mobile applications in NFC-based attendance systems increases technology's flexibility and convenience while reducing the need for physical infrastructure. Such applications help organizations automate workflows and manage attendance more efficiently. [7]

Implementation Challenges. The implementation of NFC-based attendance systems inevitably encounters various challenges. These challenges manifest in technical, security, and user acceptance aspects. Below are the key technical challenges:

1. **Device Incompatibility**

- **Devices Without NFC Support:** Some older or lower-end mobile devices do not support NFC functionality, limiting users' access to the system.
- **Cross-platform Incompatibility:** The varying implementations of NFC functions across different operating systems (e.g., Android and iOS) complicate the integration process.

2. **Interface and Protocol Incompatibility**

- **Diversity of Standards:** The presence of different protocols and standards in NFC technology can lead to compatibility issues between devices.
- **Software Incompatibility:** The use of different firmware versions across various manufacturers' devices can create integration difficulties.

3. **Infrastructure Limitations**

- **Challenges in Integration with Existing Systems:** Integrating NFC-based attendance systems with existing databases and management systems may be complex.
- **Network Connectivity Constraints:** Real-time data transmission requires a stable and high-speed network connection, which may not always be available in certain locations.

4. **Energy Consumption and Battery Life**

- **High Energy Demand:** Continuous use of NFC functionality may reduce mobile device battery life, potentially affecting user satisfaction.
- **Energy Efficiency Issues:** Devices with low energy efficiency may face problems during prolonged usage. [6,7]

NFC-based attendance systems process personal and sensitive data, making them vulnerable to various cybersecurity risks. To protect data, security measures must be implemented at both software and hardware levels:

1. **Unauthorized Data Interception (Eavesdropping)**

Since NFC technology operates over short distances, third parties can intercept data transmissions. Attackers can steal user data by listening to electromagnetic waves. To prevent this:

- **AES-128 or AES-256 encryption methods** should be applied.
- **Secure communication methods** such as Diffie-Hellman key exchange should be used.

2. **Replay Attacks**

Attackers can capture signals transmitted during NFC communication and later resend the same signal to the system. To prevent this:

- **One-Time Passwords (OTP)**
- **Timestamp validation**
- **Cryptographic nonces (random number generators)** should be used.

3. **Man-in-the-Middle (MITM) Attacks**

During data transmission between NFC devices, third parties may intercept and alter the communication. To mitigate this:

- **Mutual authentication** should be implemented.
- **TLS (Transport Layer Security) and SSL (Secure Sockets Layer) encryption protocols** should be used.

4. **Privacy Violations and Personal Data Protection**

NFC-based attendance systems collect students' or employees' personal data. To comply with GDPR (General Data Protection Regulation) and other data security regulations:

- **Data minimization** should be applied (only essential data should be stored).
- **Pseudonymization and anonymization techniques** should be used.
- **Data retention periods** should be limited, and an automatic data deletion policy should be implemented. [8,9]

Solutions and Recommendations:

1. **Standardization and Compatibility Testing.** To ensure interoperability between different NFC devices, compliance with international standards such as **ISO/IEC 14443, ISO/IEC 18092, and ISO/IEC 21481** must be ensured.

2. Standardization should also be supported by **NFC Forum's tag and device compatibility tests.** For example:

- Devices supporting **NFC-A, NFC-B, and NFC-F** protocols should be tested.
- **Verification tests** should be conducted to confirm the accuracy of identification data (UID).

3. **Implementation of Security Protocols.** The following protocols should be applied to enhance data security:

- **TLS 1.3 or TLS 1.2 Protocols**

NFC-based attendance systems should use TLS 1.3 or TLS 1.2 when transmitting data to servers to prevent data interception by third parties.

- **HMAC (Hashed Message Authentication Code) and SHA-256 Hashing**

To prevent data tampering, **HMAC-SHA256** authentication methods should be applied to every communication process.

- **Elliptic Curve Cryptography (ECC) and RSA 4096**

Using **ECC-256 or ECC-384** cryptography for NFC devices enhances both speed and security.

- **Near Field Communication Secure Element (NFC-SE)**

Implementing a **Secure Element (SE)** within NFC chips ensures secure data storage within the device. **Embedded Secure Element (eSE)** or **SIM-based Secure Element** options can be used.

User Training and Awareness Campaigns

1. **Security Training for Users**

Users should be educated on best security practices when using NFC-based attendance systems.

2. **Raising Awareness of Potential Risks**

Informing users about security threats such as data interception, unauthorized access, and phishing attacks is essential.

3. **Integration of Security-Enhancing Hardware and Software**

Organizations should implement additional security measures, such as **biometric authentication, multi-factor authentication (MFA), and intrusion detection systems.** [5,6,8]

References:

1. McHugh, S., & Yarmey, K. (2014). What Is NFC? In S. McHugh & K. Yarmey (Eds.), NearFieldCommunication: Recent Developments and Library Implications (pp. 5–13). Springer International Publishing. https://doi.org/10.1007/978-3-031-02036-0_2
2. https://www.researchgate.net/publication/300791064_A_Review_of_Student_Attendance_System_Using_Near-Field_Communication_NFC_Technology
3. https://www.researchgate.net/publication/377914273_Attendance_Data_Collection_Using_NFC_Tags
4. ISO/IEC 14443 & ISO/IEC 15693 Standards for Contactless Smart Cards. https://www.iso.org
5. Coskun, V., Ozdenizci, B., & Ok, K. (2013). A Survey on Near Field Communication (NFC) Technology. Wireless Personal Communications, 71(3), 2259-2294. https://doi.org/10.1007/s11277-012-0935-5
6. Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). NFC Devices: Security and Privacy. Proceedings of the Third International Conference on Availability, Reliability and Security, 642-647. https://doi.org/10.1109/ARES.2008.155
7. Ondrus, J., & Pigneur, Y. (2007). An Assessment of NFC for Future Mobile Payment Systems. Proceedings of the International Conference on the Management of Mobile Business (ICMB), 43-43. https://doi.org/10.1109/ICMB.2007.9
8. NFC Forum Technical Specifications. https://nfc-forum.org