As a library, NLM provides access to scientific literature. Inclusion in an NLM database does not imply endorsement of, or agreement with, the contents by NLM or the National Institutes of Health.
Learn more: PMC Disclaimer | PMC Copyright Notice

Sensors (Basel). 2015 Jun 5;15(6):13348–13405. doi: 10.3390/s150613348

The Survey on Near Field Communication

Vedat Coskun [1,*], Busra Ozdenizci [1], Kerem Ok [1]

Editor: Fabrizio Lamberti[1]

Author information Article notes Copyright and License information

PMCID: PMC4507650 PMID: 26057043

Abstract

Near Field Communication (NFC) is an emerging short-range wireless communication technology that offers great and varied promise in services such as payment, ticketing, gaming, crowd sourcing, voting, navigation, and many others. NFC technology enables the integration of services from a wide range of applications into one single smartphone. NFC technology has emerged recently, and consequently not much academic data are available yet, although the number of academic research studies carried out in the past two years has already surpassed the total number of the prior works combined. This paper presents the concept of NFC technology in a holistic approach from different perspectives, including hardware improvement and optimization, communication essentials and standards, applications, secure elements, privacy and security, usability analysis, and ecosystem and business issues. Further research opportunities in terms of the academic and business points of view are also explored and discussed at the end of each section. This comprehensive survey will be a valuable guide for researchers and academicians, as well as for business in the NFC technology and ecosystem.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 1 of 84

Keywords: Near Field Communication, NFC survey, Internet of Things, ubiquitous computing, Wireless Body Sensors, NFC ecosystem, NFC security, NFC applications, secure element, NFC usability

1. Introduction

Near Field Communication (NFC) is a short range wireless communication technology that emerged only a decade ago, but which has rapidly gained appreciation as a significant contributor to several technologies such as Internet of Things (IoT), Ubiquitous/Pervasive Computing (Ubicomp) and Smart Environment, Ambient Intelligence (AmI), Wireless Sensor Networks (WSN), and Cloud Computing (CC).

NFC fulfills the need to provide secure, short-distance, and implicit paired communication capability in smartphones. The strength of NFC technology arises from its ease of use by triggering the communication just with a simple touch in a short distance, and terminating the communication immediately as the devices detach. One of the most important aspects of NFC technology is its inherent security, since the communication range is extremely short. In NFC communication, bringing two devices very close to each other starts communication and separating the devices beyond a certain limit terminates the communication immediately.

NFC technology invalidates many other devices, components, materials, and items so that only a smartphone used as an integrated everyday life object would be sufficient to realize all daily activities [1,2]. Smartphones could be used to lock/unlock the house, car, and office doors, pay for the newspaper, exchange business cards, pay for public transportation, tip a doorman, help disabled or elderly people cope with their daily life, and much more.

NFC not only brings simplicity to our lives, but also creates additional opportunities for entrepreneurs as well. Mobile Network Operators (MNOs), financial institutions, transportation authorities, device manufacturers, and Service Providers (SPs) are increasingly aware of the NFC technology since its ecosystem creates promising business opportunities. As of today, most smartphones are sold with an integrated NFC hardware module, and almost all smartphone/Mobile Operating Systems (MOSs) have NFC support, which are important evidence of its popularity and usefulness through the dissemination of the technology.

NFC is compatible with the existing infrastructure spawned for Radio Frequency Identification (RFID) technology such as passive RFID tags and contactless ISO 14443 compatible readers. In

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 2 of 84

order to engage in an NFC interaction, a user needs to touch her smartphone alternatively to an NFC tag, another smartphone, or an NFC reader. The smartphone communicates with each mentioned device in a different fashion. When touched to an NFC tag, the smartphone reads/writes data from/to the tag. When touched to another smartphone, they exchange data. When touched to an NFC reader, the reader reads the data stored in the Secure Element (SE) of the smartphone. An operating mode name is given to each interaction: reader/writer mode to the tag interaction, peer-to-peer mode to the smartphone interaction, and card emulation mode to the reader interaction.

The pioneering work on NFC began about a decade ago, as covered by our previous review on the topic [3]. We observed the growing momentum in the technology, including technical aspects, application development efforts, SE alternative proposals, and new ecosystem models, which motivated us to provide an up-to-date study. The main objective of our current study is to provide insights into what has been happening in all aspects of NFC technology and address open research areas for further improvement.

This survey is based on articles in journals and mostly conference proceeding papers. We exclude some writings published as editorials, news reports, book reviews, or white papers. The literature search was based on two descriptors: “NFC” and “Near Field Communication”. The search for papers was conducted using electronic databases such as IEEE/IEE Electronic Library, Association for Computing Machinery, ISI Web of Knowledge, Academic Search Complete, Computer and Applied Science Complete, Science Direct and Emerald Full Text.

Sometimes the abstract, but mostly the full text of each article was read to identify whether the article had high relevance to NFC. The literature review strategy followed for this study was an iterative process, hence, we tried to find and add new studies about NFC to the survey.

In conjunction with the above-mentioned objective, the remainder of this study is organized based on the major research areas of NFC technology: in Section 2, we present the NFC technology, NFC communication, and related studies. In Section 3, SE essentials, SE management issues, and related studies are reviewed. Section 4 contains the applications and services making use of NFC technology. In Section 5 security and privacy issues regarding NFC technology are discussed, and Section 6 provides usability studies on NFC technology. In Section 7 ecosystem and business models for NFC technology are reviewed. Concurrently, we provide useful guidelines and mention open research issues for the reader at the end of each section.

2. NFC Technology Essentials

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 3 of 84

NFC technology is a short-range half duplex communication, which was jointly developed by Philips and Sony in late 2002 for contactless communications. NFC relies on the inductive coupling principle between transmitting and receiving devices, and differs from far field RF communication, which is used for longer-range wireless applications. We provide an account of NFC technology in this section.

2.1. NFC as a Contributor Technology

A sensor is a device that aims to detect some event or characteristics of its environment. Analogous to the Internet of computers, sensor technology has the capability to provide a large network of sensors with the ability to obtain data from the environment and process it afterwards [4] in areas including air, ground, water, and even underwater [5,6]. The idea of IoT arose in this way, as being the concept of variety of things, which interact with each other to reach some common goals [7]. Currently such IoT include RFID and NFC tags, barcodes, sensors, actuators, and smartphones, *etc*., which may potentially include additional items in the future.

UbiComp refers to the next level of interaction between human and computers, where computing devices are completely integrated into our everyday life and objects around. UbiComp is a model in which human beings do not design their activities according to the machines, instead, machines change their forms to adjust to human behaviors [8].

AmI also has a crucial role in UbiComp, especially in living environments such as homes. It is defined as an information technology paradigm that makes use of context-sensitive digital environment by being adaptive and responsive to people's needs, habits, gestures, and emotions. By embedding technology into objects, AmI establishes effortless interaction and enables information to be accessed anywhere and anytime [9]. Ubiquitous communication including NFC technology is also one of the primary technologies that promote AmI [10]. IoT, UbiComp, Smart Environment, and AmI are some conceptual responses those are provided by the scientists in response to the public need to simplify their lives to technology. Herein, NFC technology plays an important role in promoting almost all of those concepts. NFC technology brings ease of use, provides physical object elimination, enables implicit coupling, and much more.

Needless to say, NFC is a major contributor technology for the promotion of IoT and context-aware Smart Environment. The authors of [4] provide a good example that integrates NFC technology into the IoT concept. Each smart classroom is equipped with NFC tags and readers to collect real-time information and to manage these smart classrooms accordingly. Another study [11] defines the education system called NFC Mobiquitous—mobile and ubiquitous—Learning

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 4 of 84

System (MoLS) where course contents are accessible by anyone, anytime, and anywhere with a simple interaction of NFC tags and smartphones.

Another important technology that also promotes IoT is WSNs, which are composed of sensor nodes deployed in an area [5]. WSNs are used in a variety of areas such as forest fire detection, healthcare monitoring, natural disaster prevention, and so on. In addition to using passive components (sensors) in the network, active devices (actuators) are added to perform some action, in which case the network is known as a Wireless Sensor and Actuator Network (WSAN). The gathered data are first transmitted to a base station to transfer it to a final location over the Internet, which enables execution of applications including health care, diagnosis, emergency treatment and so on [12]. Another notable specific form of WSN is the Wireless Body Area Network (WBAN), which is a wireless network of wearable computing components placed on the body to collect data. WBANs have arisen increasingly to meet the needs of growing markets such as health monitoring, emergency assistance, video games, and smart clothes [13]. Another study [14] provides a good example of the benefits of NFC technology in WBANs. The authors introduce a smart mobile system that collects sensor data via Bluetooth, uses NFC as a facilitator for establishing Bluetooth connection, and streams data simultaneously to a central server via the Internet.

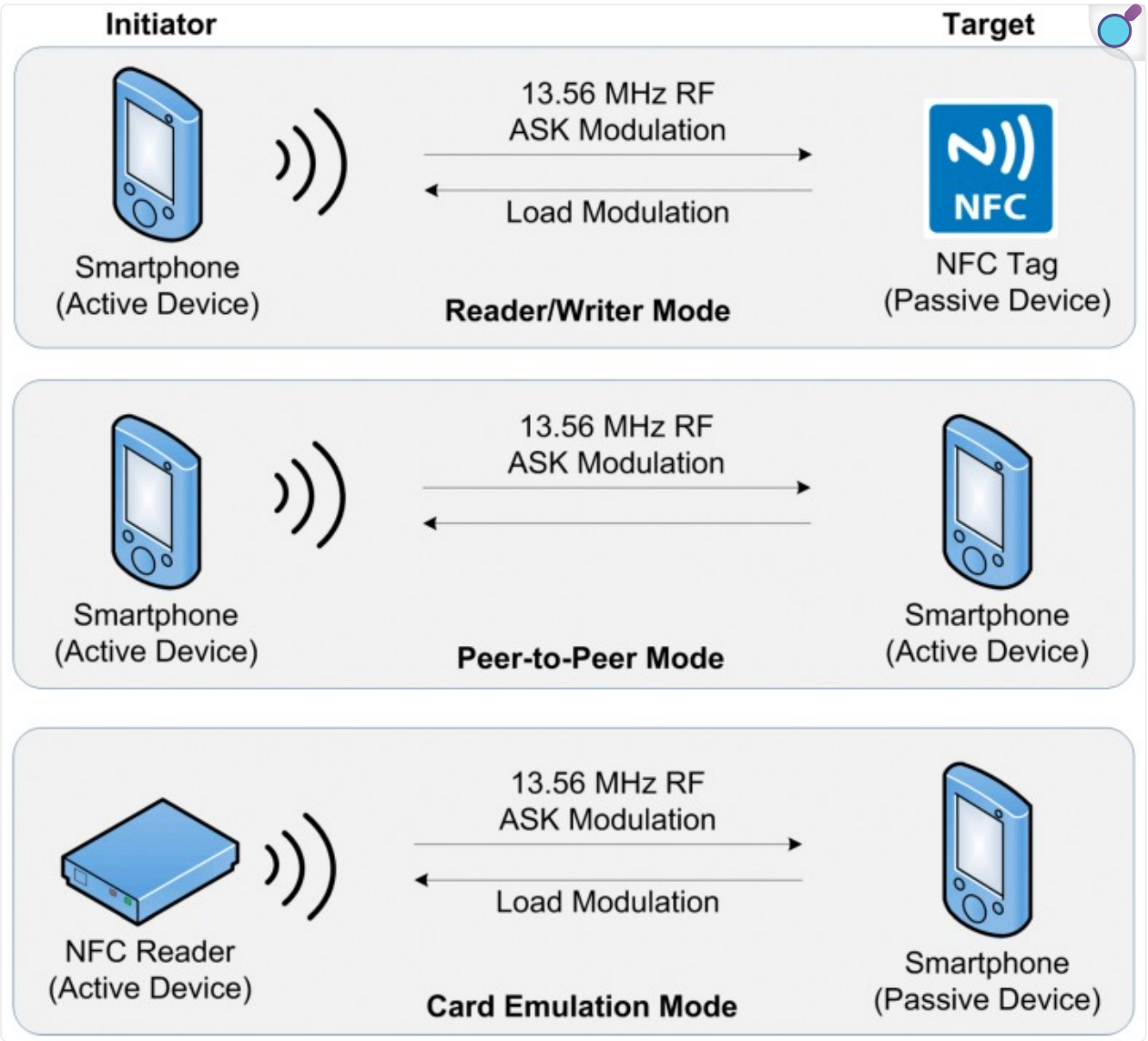
NFC technology also provides important contributions to the development of CC services. In particular, storing private data on the Cloud instead of on smartphones is an important recent development; and several significant studies on Cloud-based NFC services exist [15,16,17] which are further discussed in Section 3.

2.2. NFC Communication

NFC communication occurs between two NFC compatible devices placed within a few centimeters of each other using the 13.56 MHz operating frequency (Figure 1). It provides easy communication between various NFC devices on ISO/EC 18000-3 air interfaces, with transfer rates of 106, 212, and 424 Kbits per second. The device that starts the communication is called the initiator, while the respondent is known as the target. NFC smartphone and NFC readers uses their own power, hence are active devices, whereas an NFC tag uses the power of the other party, and hence is called a passive device. All initiator devices are usually active devices, however a target device can be either active or passive, depending on the operating mode.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 5 of 84

Figure 1.



Open in a new tab

NFC interaction styles and operating modes.

Three types of NFC devices are involved in NFC communication: smartphones, NFC tags, and NFC readers. The possible interaction styles among NFC devices provide three different operating

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 6 of 84

modes as shown in Figure 1: reader/writer, peer-to-peer, and card emulation operating modes where communication occurs between a smartphone on one side, and an NFC tag, another smartphone, or an NFC reader on the other side, respectively [8,18].

Each operating mode uses its own communication interfaces and standards; ISO/IEC 18092 NFCIP-1 [19], ISO/IEC 21481 NFCIP-2 [20], JIS X 6319-4/Felica [21] and ISO/IEC 14443 [22] contactless smart card standards (referred to as NFC-A, NFC-B and NFC-F, respectively) in the NFC Forum specifications on RF layers. Moreover, each operating mode has different technical, operational and design requirements (see the next sections).

The NFC protocol occurs using two communication modes: active and passive mode [19]. In active communication mode, both devices use their own energy to generate their RF field to transmit the data. In the passive communication mode, only the initiator generates the RF field while the target device makes use of the energy that is already created.

In NFC communication that occurs from an active device to a passive device, the Amplitude Shift Keying (ASK) modulation technique is used at all possible data rates. In the case of communication from a passive device to an active device, the load modulation technique is used. In terms of coding schemes, it uses Non-Return-to-Zero Level (NRZ-L), Manchester, or Modified Miller coding techniques, which depend on the data rates and standards used on the RF interface (*i.e.*, JIS X 6319-4/Felica and ISO/IEC 14443 contactless smart card standards).

There exist several studies on improving the efficiency of NFC communication through novel modulation techniques. One study [23] deals with the increase of data rates for proximity coupling of NFC devices at 13.56 MHz, and compares the performance of the ASK and PSK modulation schemes in a real environment. It concludes that PSK performs 23% better than ASK in terms of field strength requirements and energy efficiency. Another study [24] focuses on a highly efficient 13.56 MHz NFC transmitter to improve the efficiency of ASK modulation.

Some authors have proposed a modulation technique called Active Load Modulation (ALM) to overcome the limitations of using passive load modulation [25]. Another study [26] handles the load modulation bottlenecks and provides ALM concepts, which enhances the card emulation mode operation.

The authors of [27] focus on high-speed NFC transmissions based on Extended Binary Phase Shift Keying (EBPSK) modulation and they present its advantages over the existing NFC system. The authors of [28] present a multi-level Phase Shift Keying (PSK) modulation to increase the data rate

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 7 of 84

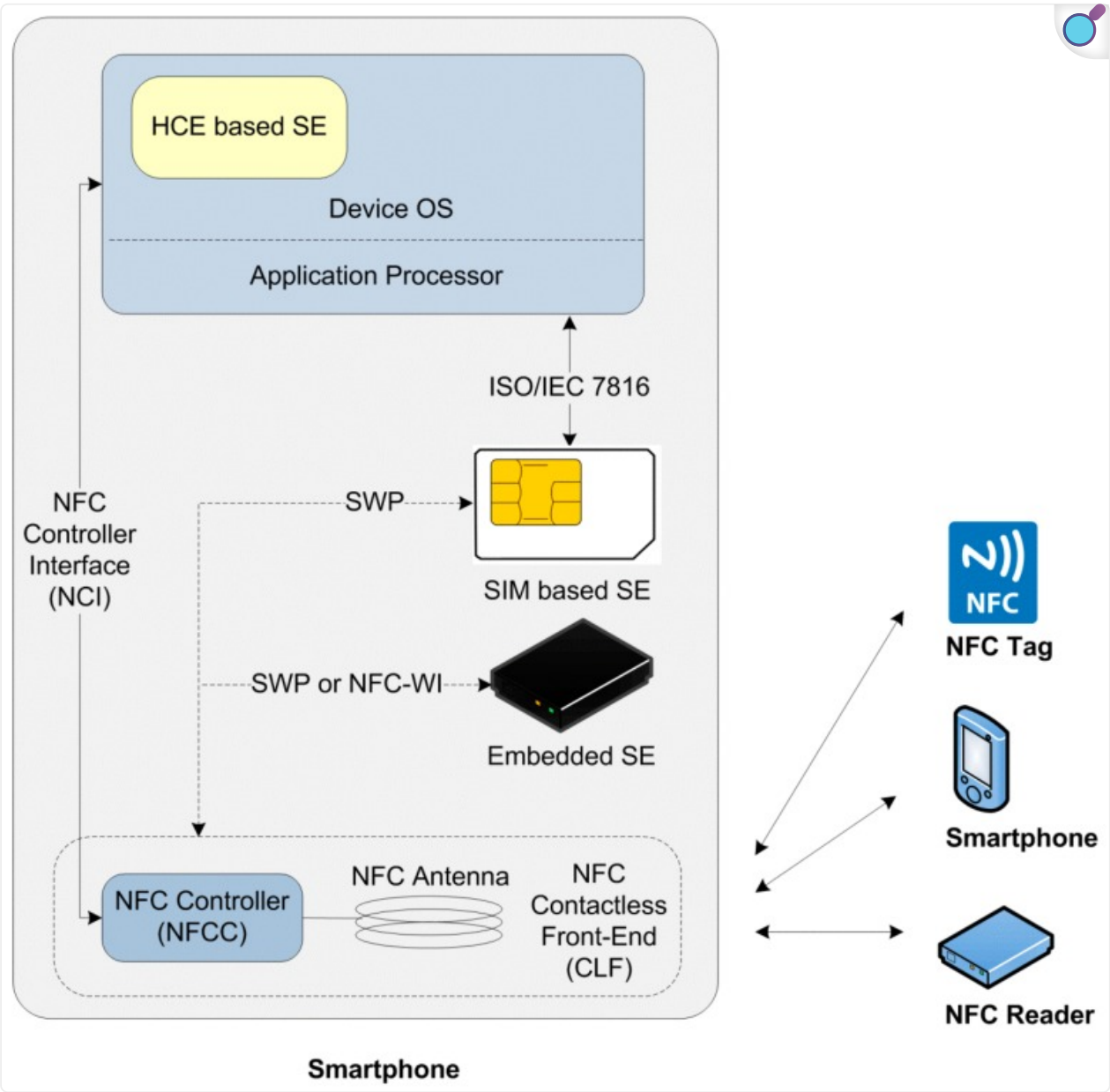
of 13.56 MHz inductively coupled systems. The authors of [29] examine Quadrature Phase Shift Keying (QPSK) in which modulation with additional data transmission is studied to enhance NFC transactions. The authors of [30] propose a Direct Antenna Modulation (DAM) technique to increase the performance of NFC link since most NFC systems operate at low RF frequencies.

2.3. NFC Smartphones

NFC smartphones are the irrevocable component of NFC communication, which is typically composed of various integrated circuits such as the NFC communication module depicted in Figure 2. The NFC communication module is composed of an NFC Contactless Front-end (NFC CLF), an NFC antenna and an integrated chipset referred to as an NFC Controller (NFCC) whose function is to manage the emission and reception of the signals, and modulation/demodulation.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 8 of 84

Figure 2.



Open in a new tab

General architecture of a NFC smartphone.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 9 of 84

A variety of studies have been performed to improve the NFC module and NFC antenna. Many studies [31,32,33,34,35,36,37,38,39,40] focus on optimization of NFC antenna design for enhancing the performance and operating distance of the NFC antenna, as well as for impedance adjustment issues.

Inkjet printed antennas [41,42] for passive components such as NFC tags are another popular NFC antenna design approach. Antenna design formulas optimizing bandwidth and power transfer efficiency [43], evaluation of eavesdropping range depending on the antenna design [44], development of mutual coupling of NFC antennas and coupling models for system performance estimation [45,46,47], resonant coupling method for enabling high quality NFC system [48,49] have also been studied extensively.

The mutual inductance on NFC antennas is another popular research area, which affects impedance matching and transmission efficiency for NFC applications. Some studies [50,51] provide Equivalent Circuit Analysis for inductively coupled NFC antennas to examine the mutual inductance parameters.

Moreover, novel NFC transceiver and chipset design approaches have been studied [52,53,54,55,56] for improving communication quality and security. Adaptive tuning strategies for NFC transmitter module to compensate receiver influence [57], quadrature carrier cancelling receiver to solve the self-jamming problem and increasing the sensitivity of NFC receivers [58] are other important issues for NFC system design.

Optimization of power requirements and energy saving interface models in NFC chipset design are proposed in studies such as NIZE [59] and PTF Determinatior [60]. Adaptive and dynamic field strength scaling methodologies are studied for energy saving purposes [61,62].

The SE of NFC technology enables secure storage and secured transactions among NFC devices [63]. Currently, the promising SE alternatives for NFC transactions are embedded hardware-based SE, SIM-based SE, and Host Card Emulation (HCE). For the embedded hardware-based SE option, the NFC Controller is connected to the SE through either Single Wire Protocol (SWP) [64] or NFC Wired Interface (NFC-WI, ECMA 373, S2C) [65]. SWP is the most adopted protocol between an NFC Interface and SE, which can be used in all SE form factors, and provides optimal interoperability with several protocols [66].

Another important NFC smartphone component is the NFC Controller Interface (NCI) which is a standard defined by the NFC Forum [67]. NCI is the interface between the NFCC and a device's

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 10 of 84

main application processor, *i.e.*, its host controller [68]. NCI enables the integration of chipsets manufactured by different chip manufacturers, and defines a common level of functionality and interoperability among the components within an NFC device.

In one study [69], the authors indicate that mobile device manufacturers expect NFC systems to be operating system (OS) independent, hardware independent, and OS application framework adaptive. Actually in today's smartphones, NFC stacks hardly meet all these requirements due to business model-related issues. In addition, the authors of [69] propose a new NFC stack architecture for mobile devices by analyzing OS services, ETSI standards and NFC Forum standards. The proposed NFC stack runtime environment is also validated on the Android and Windows Phone OSs.

2.4. NFC Operating Modes

NFC technology benefits from various elements such as smart cards, smartphones, NFC tags, and card readers. Various standardization bodies define how NFC technology should be integrated into smartphones and other related devices in all layers. The common vision of all NFC standardization bodies includes the ease of access, interoperability, and security.

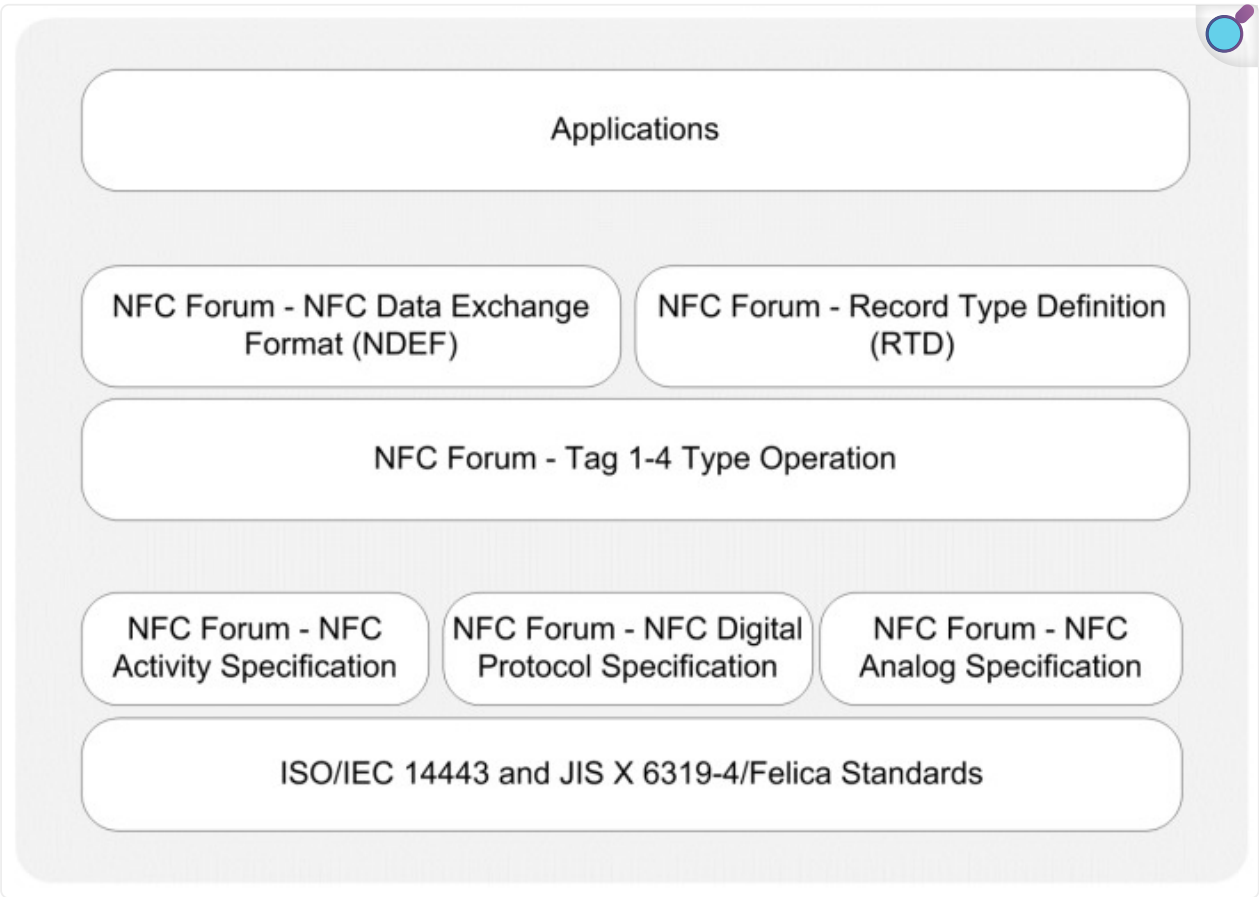
The most important association that focuses on developing and improving NFC technology is the NFC Forum [67]. It is a non-profit Standard Setting Organization (SSO) that was established with the initial aim of enabling NFC technology, and promoting it globally thereafter. Up to now, NFC Forum has provided diverse specifications such as Logical Link Control Protocol (LLCP) [70], NFC Tag Types [71,72,73,74], NFC Data Exchange Format (NDEF) [75], NFC Record Type Definitions (RTDs) [76,77,78,79,80] and so on. Three NFC communication modes are defined based on the paired NFC devices. The communication protocols and standards are defined as operating mode specific.

2.4.1. Reader/Writer Mode Communication Essentials

In reader/writer operating mode, a smartphone initiates the communication as an active device, and can both read from and write to an NFC tag. NFC tags are some form of passive RFID tags. Figure 3 provides a protocol stack illustration for reader/writer mode.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 11 of 84

Figure 3.



Open in a new tab

Protocol stack of reader/writer operating mode.

Physical Layer: The RF layer of the NFC communication is based on the ISO/IEC 14443 and JIS X 6319-4 Felica contactless smart card standards. Depending on these existing standards, the NFC Forum defined additional specifications for the physical layer, which are the analog specification, digital protocol specification, and activity specification. The analog specification is related to the RF characteristics of NFC devices and determines the operating range of devices [81]. The digital protocol specification refers to the digital aspects of ISO/IEC 18092 and ISO/IEC 14443 standards, and defines building blocks of communication [82]. The activity specification defines the required

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 12 of 84

activities which set up communication in an interoperable manner based on the digital protocol specification such as polling cycles or when to perform collision detection [83].

Data Link Layer: In this operating mode, a smartphone is capable of reading NFC Forum-mandated tag types, which are Types 1–4, as defined by the Tag 1–4 Type Operation Specifications [71,72,73,74]. These specifications indicate the commands and instructions used by smartphones to operate the NFC Forum mandated tags.

The NFC Forum also defines standardized NDEF, the data exchange format between two NFC devices [75]. The NFC Forum mandated tag-enabled read and write operations on the data link layer by using the NDEF and Record Type Definitions (RTDs) from/to a tag. NDEF has a binary message format that encapsulates one or more application specific payloads into a single message [75]. NDEF is also defined as a standardized format for storing formatted data on NFC tags and for transporting data across a peer-to-peer NFC link [84].

An NDEF message contains one or more NDEF records. Records can be chained together to contain large payloads. A record is the unit for carrying a payload within an NDEF message. Each NDEF record contains values describing its payload, payload length, and payload type. The length of NDEF records is variable, and definitions of NDEF record fields can be found in the specifications [75,76]. The most important one is the Type Name Format (TNF) field, which indicates the structure of the NDEF record. The NFC Forum provides various record types for NDEF messaging format such as smart poster, text, URI, signature [77,78,79,80].

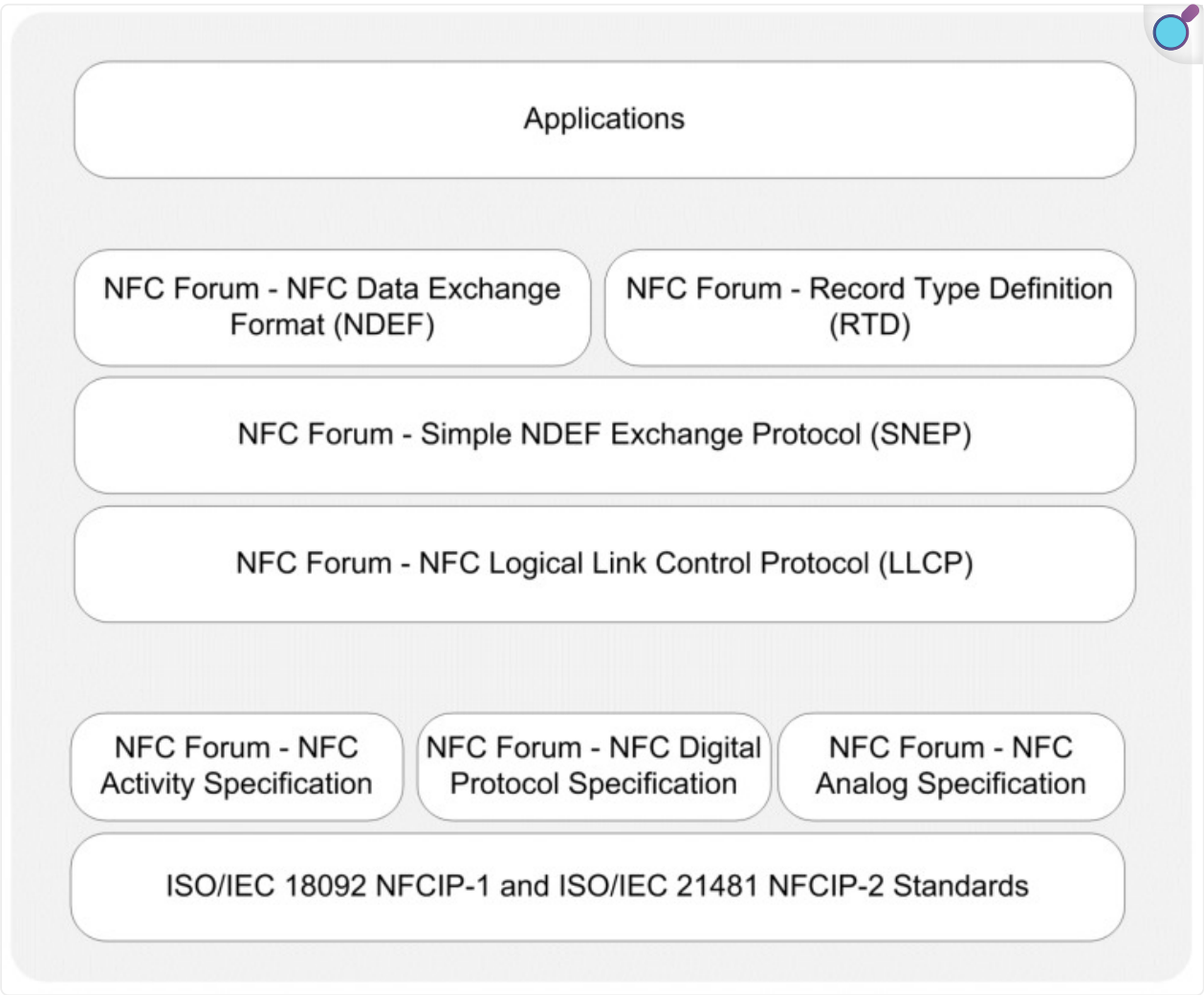
Application Layer: Smartphone applications in reader/writer mode may create their own data exchange format, or may also optionally use NDEF. Smart poster applications are examples of NDEF-based applications and handle the tag data based on NDEF specifications. On the contrary, non-NDEF-based vendor-specific smart poster applications are also possible.

2.4.2. Peer-to-Peer Mode Communication Essentials

In peer-to-peer mode, two smartphones establish a bidirectional connection to exchange data. In this mode, smartphones can exchange any kind of data such as business cards, digital photos, or any data specific to an application. Figure 4 provides a protocol stack illustration for peer-to-peer mode.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 13 of 84

Figure 4.



Open in a new tab

Protocol stack of peer-to-peer operating mode.

Physical Layer: The RF interface is standardized by ISO/IEC 18092 as NFCIP-1 and ISO/IEC21481 as NFCIP-2, which enables request-response model between two active devices [32], and also ISO/IEC 21481 as NFCIP-2, which detects and selects the communication protocol that will be used in peer-to-peer communication [20].

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 14 of 84

According to one study [85], the NFCIP-1 protocol allows error handling, provides an ordered data flow, and performs reliable and error free communication in the link layer. In another study [86], a simulation model for the NFCIP-1 over the network simulator is presented. The study indicates that NFCIP-1 protocol needs to be supported with other techniques such as flow control mechanisms. Another study [87] presents realization of an IP link by tunneling over the NFCIP-1 protocol, which enables devices to exchange data over the network easily. Such a tunneling implementation may bring new possibilities for peer-to-peer mode applications.

In addition to NFCIP-1 and NFCIP-2, the NFC Forum has the defined analog specification, digital protocol specification, and activity specification for the physical layer in peer-to-peer communication [81,82,83].

Data Link Layer: To support peer-to-peer communication between two NFC-enabled devices, the NFC Forum has standardized LLCP [70,87]. LLCP provides a solid ground for peer-to-peer mode applications and enhances the basic functionalities provided by the NFCIP-1 protocol. According to the NFC Forum, LLCP provides five important services: connectionless transport, connection-oriented transport, link activation, supervision and deactivation, asynchronous balanced communication, and protocol multiplexing [70].

As mentioned in [88], NFCIP-1 makes use of an initiator-target paradigm that defines the initiator and target devices prior to starting the communication. However, LLCP makes peer-to-peer transactions smoother since the devices are identical in LLCP communication [88]. After the initial handshake, the decision to assign initiator and target functions to each device is made by the application running in the application layer. Another study [89] presents a short comparison between NFCIP-1 and LLCP through a social networking application. Both NFCIP-1 and LLCP are tested during the application development. By using LLCP, users can easily perform peer-to-peer communication; they do not need to agree beforehand about the identity of the initiator and the target.

In some studies [90,91], a secure version of the LLCP is defined as LLCPS (*i.e.*, the Logical Link Control protocol secured by TLS), which protects the transactions in peer-to-peer mode. The protocol is validated by two experimental platforms and provides strong mutual authentication, privacy, as well as integrity.

Another important protocol in this layer is the Simple NDEF Exchange Protocol (SNEP) [92] that allows an application on an NFC-enabled device to exchange NDEF messages with another device

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 15 of 84

in peer-to-peer mode. The protocol makes use of the LLCP connection-oriented transport mode to provide a reliable data exchange [92].

In accordance with peer-to-peer protocols, one study [88] analyzes available peer-to-peer protocols and presents OPEN-NDEF Push Protocol (NPP) as an open source library. NPP is a simple protocol built on top of LLCP, which is designed by Google to push an NDEF message from one device to another on Android devices [88]. In another study [93], the authors present OPEN-SNEP library as an update to NPP, and analyze technical details of the OPEN-SNEP solution. The main differences between NPP and SNEP from a developer point of view are presented with use cases as well.

Similar to the reader/writer mode applications, peer-to-peer mode applications also use the standardized NFC Forum's NDEF messaging format and RTDs.

Application Layer: Peer-to-peer mode applications may optionally run over SNEP or other protocols. Up to now, diverse applications have been performed in peer-to-peer mode due to its highly standardized nature and various use case scenarios such as printing a file from a smartphone, business card exchange, *etc*. It is also possible to see some novel applications that combine NFC and Bluetooth technologies to create secure peer-to-peer applications such as secure money transfer between mobile devices [94].

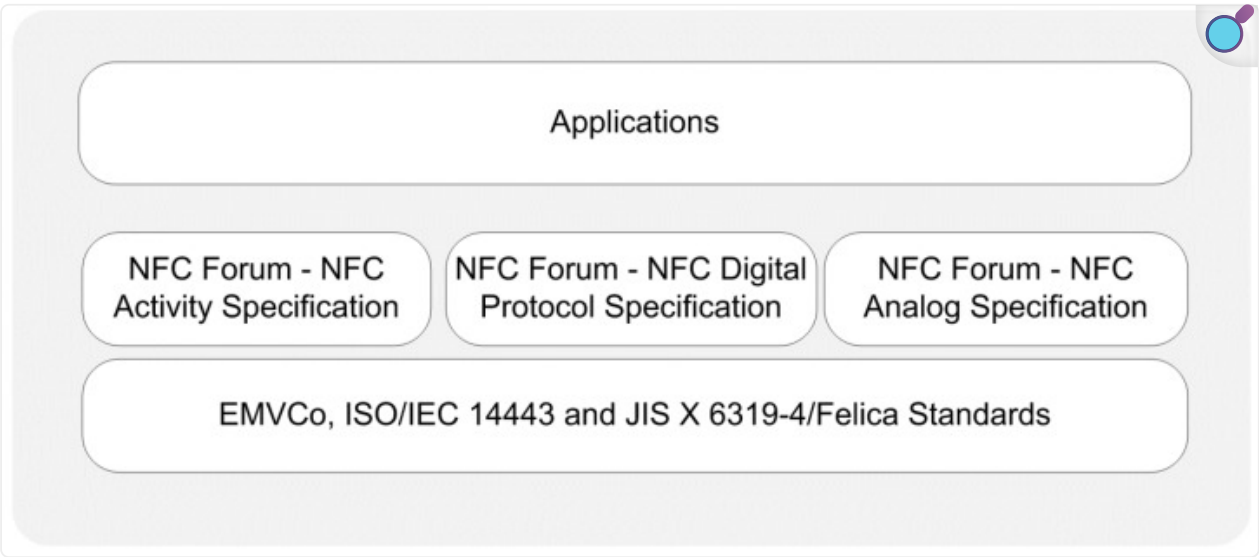
The NFC Forum also provides Reference Application Specifications to promote NFC-based applications and services such as Personal Health Device Communication [95] for the acquisition of personal health data from personal health devices using NFC and Connection Handover [96] to establish an alternative wireless communication such as Wi-Fi or Bluetooth between two NFC-enabled devices. A variety of applications can be enabled by using the Connection Handover protocol, such as printing to an NFC + Bluetooth printer, or streaming video to an NFC + WLAN television set.

2.4.3. Card Emulation Mode Communication Essentials

In card emulation mode, as the user touches a smartphone to an NFC reader, the smartphone behaves like a standard smart card; thus, the NFC reader interacts with the SE directly. Figure 5 provides a protocol stack illustration for card emulation mode.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 16 of 84

Figure 5.



Open in a new tab

Protocol stack of card emulation operating mode.

Physical Layer and Data Link Layer: The RF layer of the NFC communication is based on both ISO/IEC 14443 Contactless Smart Card and JIS X 6319-4 Felica standards. It uses digital protocol and analog techniques similar to smart cards, and it is completely compatible with the smart card standards based on ISO/IEC 14443 Type A, Type B and Felica. Moreover, it uses the NFC Forum's analog, digital protocol, and activity specifications for the physical layer, which are already mentioned above [81,82,83].

Application Layer: Card emulation mode includes proprietary contactless card applications such as payment, ticketing, and access control. These applications are based on the ISO/IEC 14443 Type A, Type B and Felica communication interfaces.

2.5. Further Research Opportunities

Technically, peer-to-peer communication can be performed between any two NFC active devices such as smartphones and NFC readers; but up to now only communication between two

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 17 of 84

smartphones has been studied in the literature. Various possibilities for research into NFC technology exist for academicians and researchers. Some of the challenging studies on technological essentials are listed below.

- Development of alternative protocols for NFC additional to SNEP for promoting P2P transactions.
- Extended investigation of LLCP with a simulation model.
- Exploration of low-power modulation schemes.
- Design of new modulation and coding techniques for NFC.
- Analysis of low energy consumption models on NFC readers.
- Development of simulation models for NFC tags as transponders.
- Examination of NFC Dynamic Tags which enable dynamic data, rather than NFC Static Tags.
- Integration of NFC technology with OS and novel NFC Stack Architecture models.
- Development of Quality of Service mechanisms in NFC context.

3. Secure Element

As smart cards have been used for storing private information, additional issues including where to save multiple applications and their credentials, how to provide authentication and identification, and how to satisfy PIN management and signatures have arisen. These issues have forced major standard providers to define a new concept known as SE, which is defined as the concept of storing and processing sensitive data on mobile components such as smartcards and smartphones. Creation of an SE requires a secured and controlled environment so that security requirements such as secrecy, authentication, or signature can be satisfied.

3.1. SE Essentials and Alternatives

An SE is built into secure crypto chips on the smart card where private data (e.g., credit and debit card numbers, mobile signature credentials, *etc*.) and corresponding smart card applications are saved and kept secure [8].

In most SEs, a Virtual Machine (VM) exists and it is associated with an executable VM called Security Domain (SD). A SD is a protected area on the card, which securely stores cryptographic keys [97]. Traditional SEs comprise CPU for processing, Read Only Memory (ROM) for storing the operating system, Non-Volatile Memory (NVM) for storing applications and related data, and Random Access Memory (RAM) [98]. SEs cannot trigger any application themselves; rather they

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 18 of 84

receive data requests from applications, and return responses. The commands they use are standardized by the ISO7816 standard [15,98].

As both smartphones and cellular communication technology have been improved in recent decades, smart cards have also became a major component of smartphones. Smart cards used in smartphones are known as Universal Integrated Circuit Cards (UICCs), also referred to as Subscriber Identity Module (SIM). Despite the fact that its aim was to identify the phone subscriber correctly, it also includes a SE for additional usage. UICCs are compliant with smart card standards and support the hosting of multiple applications on the same card [99].

SE is an important asset in mobile technology, since new business models and partnerships should be established with the party that owns the SE. Because of the incredible potential for high-value monetary transactions in NFC, the ecosystem actors (*i.e.*, banks, MNOs, or handset manufacturers) have tried to impose a specific model through which they could benefit most. The ad hoc model was to use UICC as the home of SE, which obviously creates a great advantage for the MNO, the manager of the SIM. Other actors in the game did not accept the UICC-based SE ownership model, and the efforts of other actors have initiated the creation of different SE alternatives.

The next option was to use embedded SE, which obviously delighted smartphone manufacturers. This chip is integrated into the smartphone during the manufacturing process and can be personalized after the device is delivered to the end user [99].

Other SE alternatives have also been proposed to enable secure storage and management of private data and card applications, but most of them were abandoned after a while due to inadequate attention and support from stakeholders.

The Secure Digital card was initially promoted in order for the users to increase the storage capacity of smartphones. Lately, it appeared to be a brilliant idea to use Secure Digital cards as the place for facilitating SE. Having this option in smartphones delighted Service Providers since they would neither be dependent on either MNOs (as in the UICC-based SE case) nor the manufacturers (as in the embedded SE case). Nevertheless, this option ended up being a disappointment for several reasons. After the decrease in the costs of embedded storage units of smartphones, there was not much need to provide external storage options such as Secure Digital. Additionally, not all Secure Digital cards, but only the ones that were manufactured accordingly could be used as alternatives to SE, hence the users who wished to use SE had to buy specific Secure Digital card models anyway, and they had to pay more to do so, due to the higher cost of SE-enabled Secure Digital cards. Secure Digital-based SE is no longer an alternative [98].

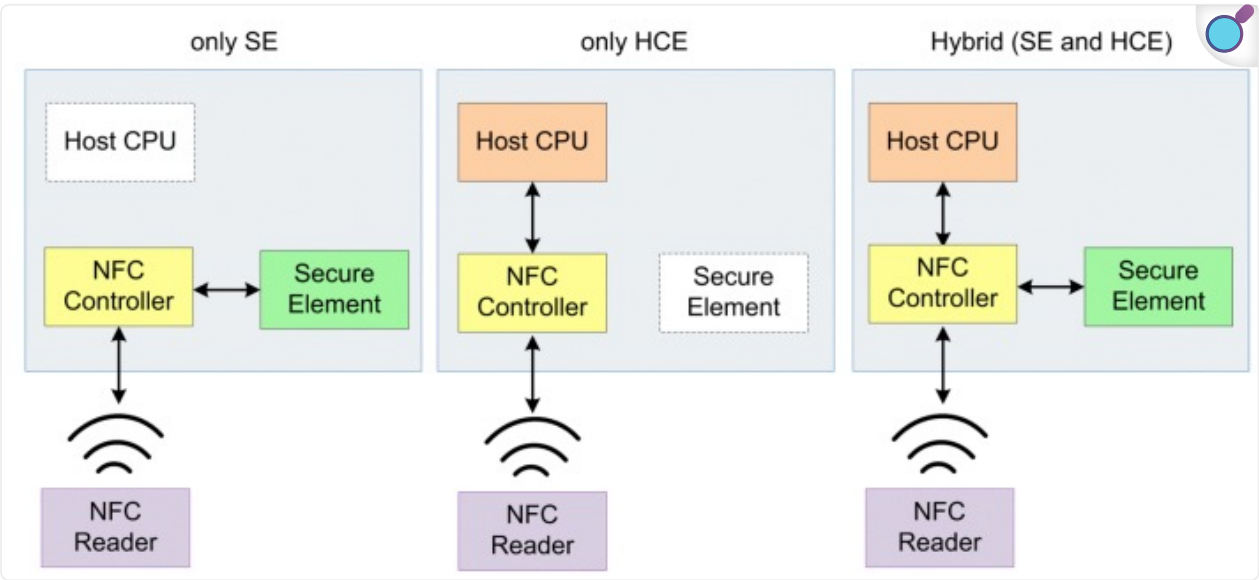
Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 19 of 84

Software-Based SEs, also known as Trusted Mobile Base (TMB), became interesting for a while. TMB was hosted at the root of the smartphones. It was defined as a secure isolated section on the Core Processor Units of the smartphones [100], but it also lost its popularity.

NFC Stickers with embedded NFC antenna were produced in order to launch pilot studies and deploy NFC services quickly by both providing a SE and providing NFC functionality to non-NFC-enabled smartphones [100]. However the integration of NFC into almost every smartphone diminished its preference.

Host Card Emulation (HCE) is the latest and most significant approach to store, access and manage private data, which separates the card emulation mode function of the smartphone from SE. The smartphone still performs card emulation mode functions, but the private data is stored in a different location such as on the smartphone or Cloud. HCE has its own protocols and standards to create and manage secured areas (Figure 6).

Figure 6.



Open in a new tab

SE and HCE architecture comparison.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 20 of 84

HCE provides more independence to SPs, but a drawback of Cloud-based HCE case is that poor user experience occurs if network latency exists [101]. Moreover, a smartphone may not connect to the Internet during the transaction for some reason, and thus cannot communicate with the SE on the cloud. In a study that includes a cloud-based HCE approach [16], the data is retrieved from the virtual SE on the cloud to the smartphone's internal SE in encrypted format. The contactless terminal reads data from SE and performs required operations such as a credit card authorization afterwards. In this model, the internal SE serves as a secure temporary storage.

Since HCE technology and Cloud-based HCE are new concepts, only a few studies for different architectures have been performed. In one of these studies, a remote server of SEs is proposed and named Cloud of Secure Elements (CoSE). In that study; a Smartphone remotely uses a SE that is hosted on the servers by establishing a secure TLS channel, and the system is able to solve trust issues for Internet users, mobile applications, and virtual machines environments [15]. In another proposed solution [16], Cloud-based SE securely stores personal data such as credit or debit card information, user identification number, loyalty program data, payment applications, PINs and personal contacts securely. Furthermore, UICC in the smartphone stores authentication data such as keys, certificates, protocols, and cryptographic mechanisms. In this case, SE in the smartphone is only used for authentication, and the data is stored on the Cloud [16]. As a result, the only remaining promising SEs as of today are UICC-based SE, embedded SE, and HCE.

3.2. SE Management

SEs can be remotely managed using Over-the-Air (OTA) technology that enables remote installation of applications, activation and deactivation, remote service management, lifecycle management of applications, and other online services [8]. SEs are managed according to the GlobalPlatform specifications [102]. As a result of these specifications; SD provides storage for applications and cryptographic keys, which are protected by mutual authentication using symmetric keys [98]. In one study [103], a new SE management named Over-the-Internet is proposed which transmits the SE management commands over a TCP connection.

SEs are managed by the SE Issuer by default, but they can also be managed by a Trusted Third Party (TTP) called Trusted Service Manager (TSM). TSM manages all or part of a SE and applications' lifecycle on behalf of SE Issuers, MNOs, and SPs using OTA infrastructure. Currently most MNOs are capable of providing OTA solutions by using their infrastructure and may even act as TSMs [104,105].

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 21 of 84

Management of SE can also be performed by multiple TSMs collaboratively by storing configuration data containing management rules and a description of the card content in the SE [105]. In order to manage an application in the SD, TSM requires keys for the SD, which are generally provided by the SE Issuer according to pre-defined business and technical agreements [104].

Controlling access to the SE is yet another important part of SE management. Smartphone applications may face some security vulnerabilities. Use of keyed authentication can be sniffed and storing PIN hash values inside the application would make it vulnerable to attacks that reuse the hash values. Thus, instead of enforcing the SE access control by the smartphone OS, it should be enforced by SE itself [97].

3.3. Further Research Opportunities

SE is a significant asset used in card emulation mode applications. SE options have lessened in the recent years by focusing on HCE and UICCs. The open research areas that can be examined, improved, and evaluated by academicians, researchers, and practitioners of SE are indicated below:

- Secure communication protocols for Cloud-based HCE transactions.
- Cloud-based reliable HCE architectures.
- Use cases and prototype implementations of Cloud-based HCE (e.g., access control, ticketing).
- Performance analysis of Cloud-based HCE.
- SE access control models for Smartphone Oss.
- Alternative models for HCE.
- Methods to enhance HCE security.
- Performance and security comparisons of UICC, embedded SE and HCE.
- Connectivity between Cloud-based HCE and Smartphone.
- Cloud based HCE's off-line running models.

4. NFC Applications in Service Domains

NFC technology covers a wide range of applications [106]. In this part, we analyze many NFC technology application domains including healthcare, location, finance, social networking, entertainment, education *etc*. In this section open research areas are clarified separately in each section as well.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 22 of 84

4.1. Healthcare Applications

The health ecosystem consists of a variety of actors including individuals such as patients, doctors, nurses, and pharmacists; organizations such as hospital administrative management and drug reservoirs; and materials such as drugs and medical devices. NFC can facilitate effective interaction among patients and other stakeholders such as doctors, pharmacies, and even enable the monitoring of drugs. Accurate data exchange between patients and doctors promises proper treatment; accurate data exchange between patients and pharmacies helps efficient and proper drug purchases; accurate data exchange involving patient-drug interaction can manage the risks such as Adverse Drug Event (ADE) and Adverse Drug Reaction (ADR), or overdosing.

There have already been affirmative studies on health applications up to now, but greater effort is still needed to create more satisfactory results. The domain of health can potentially benefit from NFC technology in the following issues:

(a) Healthcare Management Systems.
(b) Diagnosis and Medication by Professionals.
(c) Specific applications for the Disabled, Elderly, and People with Chronic Diseases.
(d) Self-Diagnosis and Medication.

4.1.1. Healthcare Management Systems

The use of NFC in healthcare management systems is reported to some extent in the literature. In one of the studies [107], check-ins at doctors' offices and hospitals, staff management, at-home diagnostics, fitness performance, emergency connections after injuries, and pharmacy-related operations are used along with NFC technology. In another study [108], a partial management system is presented in which a technical concept for NFC-based medication and related services are presented.

Medical and health cards have also been studied. Some authors offer a model that includes dissemination and usage of health cards during examination in hospitals or other healthcare centers [109]. The paper proposes using either an NFC tag or a smartphone to embed the health card, and also explains usage of both card emulation and peer-to-peer operating modes for use cases. The study also examines advantages, disadvantages and technical details of each such option.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 23 of 84

Another study on health cards [110] proposes an infrastructure where patient data is stored on central servers, portable carriers (*i.e.*, smartphones and tablet devices) or electronic health cards (eHC). For the patient appointment, an NFC-based system is proposed [111] and the latter deals with the medication phase as well [112].

4.1.2. Diagnosis and Medication by Professionals

Effective medication is another promising area, where NFC can be used for successful results. A model for clinical data acquisition based on NFC technology is studied in [113]. The authors of [114] examined the use of NFC tags to create information spots, pertaining to a comprehensive healthcare environment and described how nurses can use their smartphones to treat the patient with appropriate medication, medication amount, and timing. Another study [115] discusses the viability of NFC technology and NDEF structure for electrocardiograms (ECGs) and the authors optimize the data format so that low bandwidth capacity of NFC technology can be used efficiently.

In another study [116], an alternative Inpatient Medication System using NFC technology is proposed which aims to guard against adverse medication administration in hospitals. The proposed protocol authenticates doctors and nurses using the system, and matches them with the hospital equipment appropriately. The system aims to decrease the medication errors and identification of the source, place and time of the error are also recorded.

4.1.3. Applications for Disabled, Elderly, and People with Chronic Diseases

NFC technology can also be used for the disabled, the elderly and people with chronic diseases. In [117], an NFC-based model that enables interaction of a blind person with the environment through voice-augmented objects is presented. An NFC tag containing voice-based descriptions is attached to each object within the user's surroundings, and the user can make use of a smartphone to scan the surrounding augmented objects to verbalize their identity and characteristics. Similarly, another study [118] proposes using NFC technology at bus terminals for the safe movement of visually impaired people. Some researchers also propose expanding the transportation system with NFC technology for visually impaired pedestrians [119].

Assistance systems to help visually-impaired pedestrians already exist in many modern living areas; some of them create unexpected results contradicting the design parameters however. At road intersections where many crosswalks exist, the information from multiple beacons is

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 24 of 84

transmitted and the sounds broadcast from such systems can confuse visually-impaired pedestrians. Some researchers propose a model to prevent this chaos by making use of NFC technology [119].

In a study that focuses on Alzheimer's Disease [120], an application is proposed that aims to rehabilitate patients by using NFC tags attached to objects such as drawers and doors. In another study [121], the authors also propose a system for Alzheimer's Disease patients that aims to enhance and stimulate the cognitive abilities of patients. A patient uses a smartphone as well as tangible user interfaces those are equipped with NFC tags to improve the patient's performance in real-life situations.

A further study consists of a smart poster application that is offered for the elderly and for people with impaired fine motor skills [122]. The proposed application allows patient monitoring, electronic acquisition of well-being data from the patient's home, and real time representation of patient data.

4.1.4. Self-Diagnosis and Medication

Some studies on self-diagnosis and medication are also performed using NFC. In [123], the authors present an electronic data capture system based on NFC that makes use of smart posters and allows patients to assess their health status. The poster consists of pre-set questions about possible problematic areas towards the diagnosis of illness, which can be answered by the home-care patients using their smartphones. Medication errors that occur during medication administration stage are a serious issue in healthcare. In [124,125], the authors propose a solution that uses NFC technology for nurses to administer the right medication to the right patient in the right dose at the right time and via the right route during the medication administration stage.

In another study [126], a remote monitoring solution was developed to record patient's medication intake by using NFC-enabled smart medication blisters and a smartphone. Another study [127] also explores self-medication processes and offers a model that implements the lifecycle of prescription preparation, getting the drugs from the drugstore, and applying medication properly based on the directives of the doctor. In another study [128], a patient terminal concept with NFC technology was developed for patients suffering from chronic diseases and their attending physicians. The system was used in a number of proof-of-concept projects with hospitals and health insurance companies and in clinical trials.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 25 of 84

Some authors present an approach for ubiquitous/pervasive access to guidance and decision support services for medication safety with an intended audience of patients/citizens and even healthcare professionals [129]. The proposed model helps patients become aware of ADE effects from potential misuse risks such as risky drug-drug interactions or inappropriateness of a specific drug to their current medical, physical, or mental condition. It may also be used as a decision support system for preventing ADE conditions in this manner. In another study [130], the authors present a model so that NFC can be applied in a pharmaceutical system to examine drugs in order to detect cases of ADR.

In a study on dieting [131], a scenario is presented where the dieter uses a smartphone to get data about food nutrition just before consumption, and the application aggregates daily amounts to check the acceptability of food just before consumption, acting like a decision support system.

Researchers have studied the integration of WSNs with NFC in recent years, especially in healthcare monitoring systems. Attaching and embedding sensors to the human body is one of the deployment alternatives. A low-power wearable biosignal monitoring system is studied that can communicate with smartphones to check vital signs such as heart rate [132].

In [133], the authors propose a system where sensors are deployed on the human body. The data from sensors are collected by an intermediate device that uses ZigBee technology and then the data are transferred to the smartphone afterwards with NFC.

It is true that the power consumption of such wearable systems must be reduced and components need to be miniaturized to make them easier to carry [134]. The same paper offers wearable sensors and other health monitoring devices that switch to standby mode in order to reduce power consumption.

Empowering NFC-enabled medical devices also increases the usage of NFC technology in healthcare systems. In a study on NFC-enabled medical devices [135], the authors propose integrating a blood pressure meter and a pedometer on an NFC reader to receive the corresponding data and further transfer them to the database on the server it is connected to.

In [136], two medical wireless sensors—pulse meter and ECG—are attached to the patient's body for monitoring the activity of the heart, which is further transferred to the patient's smartphone, and then transferred to hospital's database when a medical assistant touches her smartphone to patient's Smartphone. In another study [137], the authors developed an interface that can be

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 26 of 84

attached to an existing sensor or measurement device, and enables monitoring and control of these devices using NFC technology and a cellular data network.

4.1.5. Further Research Opportunities

A significant number of health-related NFC studies have been performed in the literature. Nonetheless, there are still open research areas in the healthcare domain which may potentially integrate NFC technology with health applications:

- A complete healthcare management system by NFC and prototype implementation.
- Access control of doctors and health institutions to patient records on SEs of smartphones.
- Managing medical data (*i.e.*, how and where to store which part of the information).
- Medical data structure and format.
- Medical care of patients at home.
- NFC based healthcare system requirements for elderly and disabled people.
- Re-designing NFC capable medical devices (*i.e.*, a smartphone could easily get the measured data, or the device can get the patient data from the smartphone, *etc.*).
- Cloud HCE based health card applications and prototype implementations.

4.2. Location Based Services

Location-based services (LBSs) are key technologies in the mobile sector [138]. In this manner, smartphones are used in diverse environments such as buildings, outdoor areas, vehicles, and even underground settlements. This diversity makes it necessary to integrate different localization technologies to provide sufficiently accurate estimation of location in the majority of vicinities.

Using the geographical position of users' smartphones enables proposing many LBSs which include services like tracking, navigation, routing, identification, access control, and so on. Several studies have already been performed which combine LBSs and NFC technology.

4.2.1. Tracking Applications

In one study [139], integration of LBSs with NFC technology is performed to track users' behavior and to improve user experiences. Cities like Frankfurt and Oulu are examples of tagged environments enabling smartphones to retrieve location specific data from available tags [140]. The tags may be attached to park meters, bus stops, street lamps, or some other locations; and may

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 27 of 84

create an infrastructure for users to seek information about the local services. After addressing such examples, the authors of [141] offer the creation of a location-based mobile Wiki. Moreover, real time location data may enhance social networking, where the proposed LocaTag system uses instant messaging tools, location data, and NFC technology.

The authors of [142] analyze the basic requirements for trusted location data and propose a smartphone-based solution, which allows users to assure their current location, and Service Providers to obtain reliable information on users' location.

In another study [143], an NFC check-in system is presented, which benefits from Implied Location Based Services (ILBS), smartphones, and NFC tags. In order to enable a specific action, the user has to physically be at a specific location; allowing more intimate interaction. Advantages of the implied NFC check-in service with respect to manual check-ins (*i.e.*, Facebook, Foursquare and so on) are presented in the same study.

4.2.2. Navigation and Routing Applications

Other significant NFC-based LBSs are routing, guidance and navigation services. It is known that cellular-based positioning systems do not perform well in indoor environments. There exist valuable NFC-based navigation applications for indoor environments including shopping malls, hospitals, university campuses, museums and so on [144,145,146,147,148].

The authors of [144,145] present an NFC-based navigation system they call NFC Internal, which orients the user by touching a smartphone to NFC tags those are spread inside the building. A prototype implementation for a shopping mall is also performed and performance evaluation of the system is conducted in terms of several parameters, including security, privacy, cost, accuracy, performance and robustness. Another study [146] proposes an NFC/Inertial Navigation System (INS) localization system which reads the NFC tags are previously placed on the floor of the building. The accuracy of using NFC technology for localization in indoor environments is guaranteed due to the fixed positions of the NFC tags [145,147].

4.2.3. Identification and Access Control Applications

Location-based identification and access control services making use of NFC technology are also reported in the literature. An access control system based on two-factor authentication is provided that utilizes a smartphone (*i.e.*, something that the user has) and user's photo that has

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 28 of 84

embedded hidden password (*i.e.*, something that the user knows) to overcome the disadvantages exhibited by access control systems using access cards [149]. The proposed system combines NFC technology with an information hiding technique, steganography. In another study [150], the authors provide a two-factor access control system for unlocking a door where biometric fingerprint recognition is used for authentication, and NFC is used to transmit the authentication data to the computer controlling the door. In another study [151], an overall identification and utility system for Hajj pilgrims is also described which includes pilgrim identification, prepaid services, lost pilgrims, e-purse and so on.

Another important application area of LBSs is location-based attendance and identification that is especially useful in schools. Innovative NFC identification and attendance services [152,153,154] have been tested and implemented to simplify attendance monitoring and tracking in education. Another study of note presents a NFC-equipped smart classroom to automate attendance management, locate students, and provide real-time feedback [155]. NFC-enabled attendance management systems conserve time and reduce paper work since students use their NFC smartphones to register their attendance automatically.

4.2.4. Further Research Opportunities

The LBS area needs more application-related studies than theoretical ones; hence, solid use cases would be appreciated. There are still some open research areas, which are listed hereunder:

- Integrating wireless sensors with NFC for tracking user behavior and enabling valuable services.
- Identification and access control use cases and prototype implementations in diverse areas.
- Usability studies of LBSs.

4.3. Financial Applications

One major motivation for technological developments is obviously their prospective economic impact. For example, research and development efforts on NFC-based payment services always gain remarkable support since payment services immediately affect monetary benefits. Ticketing, coupons, and loyalty are additional financial services in this area.

4.3.1. Payment, E-Money and E-Wallet Applications

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 29 of 84

In the last decade, Card Issuers (CIs) have introduced contactless credit and debit cards which can be used very intuitively and seamlessly. NFC technology enables smartphones to be used for contactless payment instead of credit or debit cards.

A payment protocol, named as MobiTag [156], enriches the EMV protocol to upgrade it from a payment protocol to a complete transaction protocol. Mobitag enables using, redeeming and acquiring other valuables representing vouchers, coupons, or tickets. The authors of [157] present a system that collects tolls using NFC technology. Another study [158] emphasizes the importance of the agreement between the actors in the NFC ecosystem for enabling beneficial payment services.

Most of the existing payment schemes are either user-centric or institutional-centric; either a person or an institution may purchase goods or services. Some authors [159] propose a model that enables cars to make payments by using pre-paid accounts.

E-wallets are yet another concept for increasing the efficiency of monetary processes. An e-wallet is analogous to traditional wallets which store credit cards, debit cards, gift cards, loyalty cards, and so on. Currently, two popular electronic wallets (e-wallets) exist in the market: Google Wallet [160] and Apple Pay [161].

4.3.2. Ticketing Applications

In parallel to the integration of computers into our life, electronic tickets (e-tickets) have largely replaced the classical form of tickets. With the introduction of NFC into ticketing services, many studies have been realized to create NFC-based ticketing models, prototypes, and projects. An e-ticket prototype that implements NFC technology has been developed [162] and the usability of the prototype is also demonstrated in the same study. Another project [163] made use of NFC technology in e-ticket-related activities. According to the report, a user can purchase tickets, link the tickets to his/her e-wallet, buy items at the food and drinks stands in the hall, and perform similar actions.

In a study [164], a scenario for the integration of an NFC-based e-ticket model into a public transport system is introduced. The model is pretty much flexible, so that the user may travel using any form of public transportation vehicle such as trains, trams, or buses, and may transfer between different kinds of vehicles during the journey. The vehicles may be operated by different companies, and the journey may even include different countries. In another study [165], a

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 30 of 84

prototype implementation of NFC-based ticketing application is presented. Another NFC ticketing system that is provided by OTA provisioning and off-line authentication using public key cryptography is also proposed in [166].

Some authors [167] have proposed an NFC-based e-invoice (electronic invoice) remitting scheme using NFC peer-to-peer communication and discuss how it fulfills major security requirements including authenticity, integrity, and non-repudiation. The proposed system is also implemented and tested in Taiwan's e-invoicing system. In another study [168], the authors present a solution where a smartphone in reader/writer mode interacts with a ticketing system in card emulation mode.

4.3.3. Coupon Applications

Using coupons is an option for companies to promote their products or services. The customer benefits from coupons by a discount or rebate during redemption, whereas the company benefits from customer loyalty. Electronic coupons (e-coupons) and mobile coupons (m-coupons) have been the subject of many studies. In studies on m-coupons [169,170,171], the authors propose a model for enabling m-coupons, which can be downloaded from a smart poster or a newspaper that contains NFC tags. The user can then redeem the m-coupon at the cashier during checkout.

In a study termed WingBonus [172], an NFC-based model is defined; and its dissemination, distribution, supply, validation, and management of vouchers, loyalty point cards, *etc*. are further explained. WingBonus can also be used as a platform for advertising products and managing market research. The coupons can be managed through both its web site, or by a mobile phone. WingBonus was later extended to include QR codes [173] and is claimed to be fully adaptable to the requirements of marketing campaigns, voucher providers, shop or retailer infrastructures and mobile devices and purchasing habits. The security of the voucher is also studied within the same work as well.

4.3.4. Loyalty Applications

Some authors [174,175,176,177] have proposed NFC Loyal to manage data interaction and sharing among payment and loyalty applications. NFC Loyal initially stores the information provided by the payment applications, and then shares them with the loyalty applications through a secure communication model; hence loyalty firms benefit from these valuable data and provide loyalty services for users. The immediate outcome of NFC Loyal is the increase in purchase frequency of

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 31 of 84

customers; as well as a better business plan among payment firms, loyalty firms, and improved conditions for the user.

4.3.5. Further Research Opportunities

Financial application studies so far are mostly commercial, and only a few academic studies exist in the literature. Security of financial applications has been studied in detail, and we handle those issues in Section 5. The open research areas in terms of financial applications are as follows:

- E-Wallet use cases and implementations including loyalty cards and coupons.
- HCE based financial applications and prototype implementations.
- Usability studies of NFC-based financial applications and their comparison with non-NFC alternatives.

4.4. Social Networking Applications

Recently social media applications have been attempting to apply obligatory rules to tether virtual identities to the actual person, so that the declared properties would be real. NFC can be used in that kind of unobjectionable case to bind the real and virtual identities to improve functionality. This phenomenon is studied by taking conference attendance as a case [178]. In this study, each attendee uses a smartphone programmed to expose his/her Social Network Service Identity (SNS ID). The proposed model aims to bind an actual identity to the SNS ID of the participant. Smartphones get in touch with NFC tags and use cellular data network to communicate with the conference database server when some data is to be exchanged. The expected outcome of the study is improved communication between participants, as proposed by the authors. A similar work [179] has been performed as well, where authors propose a participant management system for meetings. The system promotes social networking of participants by binding SNS IDs and NFC tags of participants.

Updating status or profile on social networks using NFC is another studied area. In one study [180], NFCSocial is developed that allows a user to update her position automatically, as well as her current mood manually, by selecting it from the provided list. Another study that presents placing project specific NFC tags to each location, termed 'Hot in the City' [89], also allows the users to synchronize their location data on the social network.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 32 of 84

An application called All-I-Touch [181] helps users to share a product that they wish to buy with their social network by touching the tag that is placed on the product package. In another interesting study [182], the authors propose an application that aims to create a trusted social network, in which a user builds its own online social space through physical contacts. Users touch their smartphones with another person's smartphone to initiate a relationship or friendship on a social network. Unlike current social networks, the proposed model integrates real life friendship with the online social space.

NFC technology can also be used to gather information. Crowdsourcing is the process of getting the required knowledge—or in broader terms, a service—from volunteer contributors. Crowdsourcing systems face four key challenges; how to recruit contributors, what they can do, how they combine the contributions, and how to manage abuse [183].

Some authors [184] propose a platform that uses NFC tags on urban infrastructure, allows citizens to make public participatory reports to identify problems, and eventually improves maintenance strategies and urban conservation. The platform makes use of social networks by publishing data to increase participation of citizens.

Another study [185] presents a system that gets the musical preference of people inside a music arena and play mostly voted songs. The system also allows people linking their social network accounts such as Twitter, Facebook and Foursquare to increase the dissemination of social information around all networks.

Further Research Opportunities

As summarized, some social networking applications using NFC technology are already developed. However, more studies can be performed when compared to the attention given to social networking in recent decades. The open research areas include:

- Usability of NFC in profile and status updates on social networks.
- Information dissemination using NFC technology.
- Requirements for building NFC-based social network systems.
- Conservation of privacy on social networks.

4.5. Entertainment Applications

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 33 of 84

Smartphones will eventually become an all-in-one device as already discussed in Section 1. We will perform most of the activities that we do today by only using smartphones in the very near future; entertainment is no different. As an example, smartphones can already replace remote television controllers. McDonald's has launched an NFC campaign in Singapore that turns dining tables into interactive racing tracks [186]. Another game, whack-a-mole, is adapted to smartphones by the authors of [187]. In another interesting game that simulates location-based treasure hunting, tasks are stored in NFC tags, after which they are concealed within a natural setting [188]. Players of the game first find a tag, and must perform the task on the tag. A similar multiplayer ubiquitous strategy game based on NFC is studied in [189]. Still another location-based adventure game is proposed in [190]. In the game, players have to solve quests and find checkpoints in different locations by touching their smartphones to previously placed NFC badges.

Another multiplayer game is also developed in [191] which makes use of NFC peer-to-peer mode. Some authors [121] propose two interactive and collaborative games to be used by people suffering from Alzheimer's Disease. The games aim to enhance and stimulate the cognitive abilities of these patients. An entertainment case on sharing music experiences is developed in [192] by using NFC tags. Finally, a technically similar case [185] examines how the musical preferences of concert-goes are included on the concert playlist, based on the preference ratings.

Further Research Opportunities

Games combining geographic locations and NFC are also widely studied since touching an NFC tag provides assurance of the user's physical location. The research on games and entertainment areas might be extended to study:

- Pleasure gained by playing NFC enabled games.
- Privacy concerns in peer-to-peer games.
- Technical requirements for NFC-based games.
- Learning systems by NFC-based games.

4.6. Education Applications

It is seen from the surveyed studies that NFC is potentially related with education and training. After the development of NFC technology, the existing mobile computing and application development courses in universities were devoted to NFC technology in varying proportions, with

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 34 of 84

entire courses on NFC subsequently developing. Some papers [193,194,195] accordingly comment on education applications of NFC.

Smart school and university environments implemented using NFC technology and NFC- equipped classrooms for course enrollment, attendance and registration control, information gathering and related cases have been developed. In one study [195], an anonymous assessment of exam papers using NFC technology is presented. According to the model, each student has NFC tags, which consist of user identification data such as name and a number. As the student fills in the exam paper, she attaches a tag to the exam sheet, and submits it to the exam supervisor. During grading of exam papers, the evaluating teacher does not see any hint of the identity of the student. In another study [196], authors offered a Smart University project that aims to utilize NFC technology in a university environment. The project consists of smartphones, several NFC tags, NFC readers, and servers for enabling different use cases such as class attendance control and registration fee payment.

NFC technology can be used to improve the capability of students towards learning process for educational content. The Bologna process is recognized as the major motivation for integrating NFC technology into universities [194]. NFC technology is applied to a set of university scenarios for the development of the smart university environment. In another study [11], a learning system is developed that enables educational content to be accessible without time and location dependence. The proposed system integrates NFC and home automation technologies and enhances learning process at home. Students use their smartphone's NFC capability to display educational content, such as slides and videos, on large TV screens/displays. In another study [197], usage of a ubiquitous NFC-based game in learning is proposed. The game makes use of an open course management system that helps educators create on-line learning communities. Some authors [198] developed an NFC-enabled learning environment that supports Japanese conversation practice. Students interact with the system using their smartphones and download learning materials. Moreover, students are able to share the materials among themselves using NFC peer-to-peer mode. In another study that is conducted for easy access to bibliographic sources [199], a pervasive system is proposed to students for accessing, reading, and reviewing necessary bibliographic sources.

Further Research Opportunities

Several NFC based education and teaching models exist that have focused on partial issues. However, a complete technological education solution that also integrates NFC technology is beneficial.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 35 of 84

4.7. Miscellaneous NFC Applications

Further NFC applications which cannot be included in a specific section above discussed in this section. Dynamic NFC Display is an approach to touch-based mobile interaction between smartphones and NFC-tagged large screens. The Dynamic NFC Display concept is studied in [200,201]. A smart poster model [202] is also studied in which the authors switch the role of NFC tag and reader for the implementation of smart posters.

Sme authors [203] have reviewed applications of NFC technology in the tourism field. NFC-enabled tour guiding [204], NFC services in tourism farm [205], NFC smart tourist cards [206] are some of the substantial applications developed in this domain.

In a study of an NFC-enabled shopping process [207] several different processes were implemented including shopping list management, basket management, coupon redemption and payment. In parallel to the promotion of IoT, the Smart Home concept is making use of current technology to improve residential life. The authors of [208] have designed and developed a smart home environment that makes use of NFC.

NFC-enabled environments for museum visitors [209,210], NFC-based dining experience [211], NFC in industrial manufacturing plants [212], automatically connecting to a Wi-Fi access point using NFC tags [213], a car parking model that utilizes NFC for efficiency in finding the way back to car [214], a complete and innovative smart car parking system which also integrates the valet service electronically [215], NFC-based voting [216] are further implemented applications.

5. NFC Security

NFC services are subject to store and manage users' private and monetary information, so NFC services must be able to provide a secure framework to reassure users and thereby motivate demand. The security of NFC technology can be analyzed in the following domains:

- Security of NFC Tags.
- Security of NFC Readers.
- Security of Secure Elements.
- Security of NFC Communication.

5.1. Security of NFC Tags

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 36 of 84

NFC tags are used in the reader/writer mode of NFC. Two use cases are typical: the smartphone may read data from a previously loaded NFC tag, or the smartphone may write/overwrite to a tag. Read and write permissions of tags are important here; unauthorized read or write functions are unwelcome, of course. Physical security of the tags, unwitting actions weakening the system, as well as threats aiming to damage the system are potential risks of NFC tag security.

The aim of an attacker is potentially find a way to manipulate the data stored on the tag such as overwriting malicious data onto the original one, deleting the content of the tag, or even cloning the tag and impersonating it thereafter. An attacker may inject a worm-URL into the tag, eventually causing the smartphone that reads tag to become infected. Denial of Service (DoS) attack is another risk for the tags [217].

It is possible for an attacker to alter data in an NFC tag and hence create a new malicious tag that leads to malicious content sharing with the attacker [217,218,219]. Using NFC Forum's Signature Record Type Definition in NDEF messages [80] initially seemed to be a good counter, however, vulnerabilities were later discovered in these record types [84,218]. According to the results of these studies, Signature Record Type Record needs improvement for to create secure NDEF records.

As a prevention mechanism, read and write privileges can be defined for the tags, so that only the authorized users can make use of the service. For checking authorization, authentication mechanisms are required, and there are two main authentication categories that a tag can perform. The first option is off-line authentication, which is performed between the smartphone and the tag. When there is no previously shared secret—such as password or a key—between the smartphone and the tag to build a secure communication, off-line authentication is a challenging process since the tags have a low computational power. In on-line authentication techniques, the smartphone connects to a server that contains a database of secrets. After obtaining a tag's secret from the server, it ascertains whether it matches with the secret on the tag or not [219,220].

Recent studies have examined authentication and encryption on tags. One of these demonstrated a cryptographic challenge-response protocol is executed between the smartphone and the tag that is based on Public Key Cryptography (PKC) and Public Key Infrastructure (PKI) [221]. The protocol successfully detects illegal modification and cloned tag cases. In another recent study [222], a security-enabled passive NFC tag is designed and implemented which supports authentication using symmetric cryptography. The tag is also able to digitally sign the data using asymmetric cryptography. These recent studies provided authentication and encryption/decryption on tags and eventually overcame the challenges faced in off-line authentication. However, studies on new

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 37 of 84

authentication protocols and analysis of recently developed tags are still required to eliminate obstacles on off-line and on-line authentication of NFC tags.

5.2. Security of NFC Readers

NFC readers have the central role in card emulation mode, though they have the potential to act in peer-to-peer mode as well. NFC readers can be wired or wirelessly connected to the backend server. All card emulation mode services process sensitive data such as credit card credentials; hence, the communication between readers and the servers must be secured via encryption. Potential attacks may be realized towards either the NFC reader itself, or towards the communication between NFC reader and smartphone. There are few significant studies in the literature on this topic thus far. Furthermore, since NFC readers are almost identical to RFID readers, NFC readers can be subject to destruction or removal [223].

5.3. Security of SEs

SE is an essential part of the NFC card emulation mode as explained above. Security of SE is vastly important, since the whole purpose of creating SEs is to handle sensitive data. Consequently, strong keys are used in encryption to protect SE-related data; and applications would be installed to an SE only after authorization. SDs as part of the SE are also embedded with secret keys to secure the communication with Service Providers.

Since SE security is the crux of all NFC-based financial services; security of SEs and countermeasures are well studied by MNOs, financial institutions, and other SPs. Moreover, GlobalPlatform performs standardization on SE security.

Some studies exist in the literature which analyze SE security, and some of them propose new frameworks. In a study in the literature [224], several possible attack scenarios on the SE are presented and studied. The first attack was DoS attack. After authentication tries and failures on a SD, the card's state is changed to TERMINATED. As a result of the state change, new applets cannot be installed or existing applets cannot be removed; nevertheless, all pre-installed applets could still operate. It can be argued that, in this case DoS attack was partially successful. The study also indicates that every application can make an authentication attempt to the SD, thus a malicious code can be injected into a smartphone application that performs a DoS attack and easily put an SD into a TERMINATED state. In the same study, a relay attack is performed by installing a malicious application to the user's smartphone. The communication with the SE is relayed across a

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 38 of 84

network to a card emulator. Using such means, this card emulator performs card emulation with the remote SE.

The applets installed on SEs may also cause vulnerabilities if erroneous code exists; hence prevention mechanisms are required. In one study [225], the authors propose a genetic algorithm that searches for vulnerabilities in SE applets. Another study [226] also examines a SE applet—Google Wallet—for vulnerabilities in software-based relay attacks. The communication between smartphone application and SE applet, as well as the interaction between NFC reader and SE are analyzed. It is found that the applets were not sufficiently protected from the smartphone applications and hence were vulnerable to software-based relay attacks. Moreover, it is seen that the PIN protection which is controlled by smartphone application can be bypassed by sending lock and unlock commands to the applet. The study also notes that Google fixed the software-based relay attack in the next version of the application. In another study [227], the security of tickets stored on SEs is discussed and a new protocol is proposed that performs ticketing process between two entities which do not trust each other. It is seen that at the usage stage, ticket cloning can be prevented by online verification.

Using Personal Identification Numbers (PINs) to secure the SE is a trivial option, and several other biometric techniques including fingerprint, voice recognition and face recognition can be used as well.

An intelligent authentication framework benefiting from various authentication methods is developed in one study [228]. The security framework defines security zones and their minimum requirements, and determines the security level of device, based on user's previously performed activities. When a transaction is requested, if the corresponding application's required security level meets the current security level of the device, the transaction is allowed without any authentication. However, if the security level does not meet the criteria, the framework uses an authentication method such as fingerprint, voice recognition, face recognition, password, or PIN. Another study on authentication for access control systems [229] makes use of steganography, cryptography and graphical password to deploy a secure two-factor authentication system. The developed system enables users to use their Smartphone as a key for access control securely.

The security of developed protocols can be further analyzed using security analysis software. A study analyses an existing NFC coupon protocol using the Casper/FDR tool and discovers an attack that enables an intruder to cash a coupon even if she is not allowed to do so [230]. Also, a mutual authentication between the user and the cashier is proposed in the study, which counters the attack.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 39 of 84

5.4. Security of RF Communication

Since NFC uses wireless communication, a variety of attacks is possible on the communication between two NFC devices. The short range of NFC is an advantage to maintain secure communication, but several other attacks such as eavesdropping, MIM attacks, data corruption, data modification, and data insertion are still possible. As a matter of fact, several countermeasures are already proposed in the literature.

Eavesdropping is possible by using a receiver, suitable antenna, and RF signal decoder [231]. The attacker can use a high capacity powerful antenna and intercept the communication between NFC devices over a greater distance [231,232]. In order to be protected from eavesdropping, a secure communication channel needs to be maintained [231,232,233]. NFC-SEC protocol (NFCIP-1 Security Services and Protocol) is promoted to exchange a secret key between NFC devices for symmetric key encryption [231,234]. To prevent eavesdropping, a scheme is also proposed that leverages the noisy wireless channel to obtain provable secrecy for both card emulation and peer-to-peer modes [235]. The scheme distributes the key on multiple frames in the communication, and the passive eavesdropper becomes completely blind when she misses at least one frame.

Modifying the data in NFC communication may cause Data Corruption. If the attacker converts the data to an unrecognized format, the action may cause a DoS attack since the receiver will not be able to recognize the incoming data and will not be able provide the intended service thereafter. In order to counter data corruption, active NFC devices may check the RF field strength of the communication. Since the attacker needs to produce a higher amount of power than the typical RF field power, the active NFC device will detect this high RF field power caused by the attack [232,233].

To cause a Data Modification attack, the attacker may replace the original data with a valid one that a receiver may understand and accept. In a study [233], it is stated that a data modification attack is feasible for certain bits in modified Miller Amplitude Shift Keying (ASK) and for all bits in Manchester coding with 10% ASK. However, the attacker needs expertise in the radio communication field, and should be able to handle amplitude modulations of the transmission [232]. There are several methods to counter data modification attacks. The first option is to decrease the Baud rate to 106k in active mode; this option potentially makes the communication vulnerable to eavesdropping, however. Another method is to counter the attack by monitoring RF field continuously for such an attack, and cease the communication in case an attack is detected. The third and last method to counter data modification attack is using a secure communication channel [231,232].

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 40 of 84

In the case of Data Insertion attacks, unwanted or falsified data can be inserted into the actual data transmitted during the communication. The success of a data insertion attack depends on the response time of the target device. If the target device needs a long time to respond, data insertion may be possible. Various methods exist to counter data insertion attacks. The first option is for the target to respond immediately; the second option is continuous monitoring of the channel by the target; and the third option is to use a secure communication channel [231,232].

Since NFC operates in a very short distance, a Man-in-Middle (MIM) Attack is very hard to execute at such a communication distance [231,233]. Even so, using active-passive communication mode is recommended as an additional countermeasure. Moreover, if an active device monitors the RF Field while sending the data, the attacker would be detected easily [231,232]. It is also stated in a study [236] that a relay attack is possible on communication and usage of nonce prevents MIM attacks.

In order to prevent relay attacks, the temperature data of the temperature-enabled tags are used [237]. The surface temperature of the tag is measured both by the tag itself and by the smartphone, and they both use distance-based validation. Both of the measured temperatures should be very close to each other, and verifying the physical proximity of tags by using measured temperatures is used to prevent relay attacks.

Most attacks in RF communication can be prevented by establishing a secure channel between NFC devices. Diffie Hellman-based key exchange protocol or Ecliptic Curve Cryptography (ECC) can be used to establish a secret key; and the generated key then can further be used in a symmetric encryption protocol such as 3DES [233] to enable channel security.

Authentication protocols are one of the most studied issues in NFC communication security. One study has developed a Needham-Schroeder-based secure mutual authentication protocol which aims to guarantee authentication and confidentiality between SE and NFC readers in card emulation mode [238]. The protocol enables devices to share a session key, which will be used for secure transactions thereafter. It uses a trusted entity termed as Authentication Server, which verifies reliability of entities, authentication of SE to NFC reader, and authentication of NFC reader to SE. Another mutual authentication protocol for reader/writer mode communication is proposed in [239]. The protocol uses ECC, and provides mutual authentication and a secure environment for demanding transactions. An additional mutual authentication protocol that is designed for mobile payment is also presented [240], which deals with card cloning, skimming, downgrading terminal and relay attacks. The protocol mutually authenticates the customer, smartphone, NFC reader, and bank before the transaction; and uses one time password (OTP) to

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 41 of 84

generate session keys for encryption purposes. The study also analyses the protocol using Casper security analysis software. Some authors [236] propose a high-speed processing of authentication and key agreement for NFC payment, and also present a method to perform secure communication. In a further study, two authentication protocols that also ensure mutual authentication between two devices are proposed [241].

One-way authentication protocols are also studied in the literature. A lightweight ECC based authentication protocol taking into account resource constraints of system such as smart cards is submitted [242]. A new mobile payment protocol, EMV-TLS, based on modified EMV chip has also been developed [243]. The protocol solves the issue of trustworthy remote use of a chip by using an NFC smartphone that currently has an Internet connection.

Privacy is an important topic in NFC security, however, there are not many studies on preserving user privacy in NFC communication. In one of the few studies on this subject, protection methods are proposed for users to protect their privacy. The proposed methods try to hide the user's identity, but the user's identity can still be confirmed by the TSM whenever required [231]. Another study [244] investigates privacy issues of NFC payment services; and a specific framework is designed and applied to perform the analysis. In another study [245], an anonymous car rental protocol is proposed where a TTP knows the users' real identity, however car hiring SP and malicious users are unable to break users' anonymity. The developed protocol also counters replay and MIM attacks; and provides anonymity, confidentiality and secrecy at the same time. We provide in Table 1 a brief summary of all possible security vulnerabilities and attacks of NFC-based systems and the corresponding countermeasures.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 42 of 84

Table 1.

Vulnerabilities, attacks and countermeasures.

	Vulnerabilities and Attacks	Countermeasures
NFC Tags	Tag Manipulation (*i.e.*, NFC Worms, Phishing, DoS Attacks)	• Digitally Signing Tags • Using Tag Authentication
	Tag Cloning and Tag Impersonation	• Digitally Signing Tags
	Tag Replacement and Tag Hiding	• Protecting Tags with a Physical Shield
RF Communication	Eavesdropping	• Using Secure Communication Channel
	MIM Attack	• Attack is nearly impossible • Using active-passive communication mode (RF field is continuously generated by one of the valid parties) • Listening RF field when sending data
	Relay Attack	• Using nonce • Using physical proximity based information (e.g., temperature)
	Data Corruption	• Checking the power of RF Field
	Data Modification	• Changing Baud rate • Monitoring RF Field • Using Secure Communication Channel
	Data Insertion	• Response with no delay from answering device • Listening the channel by answering device

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 43 of 84

	Vulnerabilities and Attacks	Countermeasures
		• Using Secure Communication Channel
SE	DoS Attack	• Solutions needed
	Relay attack	• Disabling internal mode communication
	By passing the applet PINs those controlled by Smartphone applications	• Two-factor authentications • New solutions needed
	Vulnerabilities in applets caused by erroneous codes	• Genetic algorithms to search for vulnerabilities in applets • Formal security analyses
	Cloning an asset (e.g., ticket, coupon)	• Online verification before usage

Open in a new tab

5.5. Further Research Opportunities

From the technical point of view, some security issues in NFC technology are already solved and standardization is mostly provided as well. However, there are still unsolved security issues. Related with analyzed studies, the following open research topics are identified to be a helpful guide for the academicians and researchers with an interest in NFC security issues:

- Studies on new authentication protocols and analysis of recently developed tags for eliminating obstacles on off-line and on-line authentication of NFC tags.
- Creating new protocols/mechanisms on off-line and on-line authentication of NFC tags.
- Analyzing security of off-line and on-line authentication of NFC tags.
- Development of security mechanisms for protecting NDEF records within a tag.
- Formal security analysis of proposed applications.
- Experimental security analysis of HCE.
- Security analysis of protocols that makes use Cloud-based HCE.
- Preventing DoS attacks on SEs.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 44 of 84

- Experimental comparison of SE alternatives in terms of vulnerability.
- Mechanisms to prevent relay attacks on SEs.
- Mechanisms for preventing the PIN bypass of SE applets that are controlled by smartphone applications.
- Proposal of NFC specific alternative key exchange protocols to prevent various attacks on RF communication.
- Mechanisms to provide user's privacy.
- Exploration of various NFC service domains in terms of privacy, sensitivity and ethical issues.

6. Usability

As science and technology improve, some options explode, while others vanish. The lifetime of new technologies does not merely prove or disprove the technological superiority of the exploded models, and *vice versa*. There are some additional parameters, which affect success of the emerging technologies. One major parameter that determines the survivability of the emerging technology is its acceptance by users. Usability, in this sense, is the ease of use and learnability of the methodology it offers; in this sense NFC technology is not privileged at all.

The communication paradigm between a smart object and the smartphone is known as a mobile interaction technique, and the currently available techniques are Touching, Pointing, and Scanning [246]. By using the Pointing interaction technique, the user can select a smart object by pointing it with the mobile device. Scanning interactions allow the user to get a list of nearby smart objects by using a wireless mechanism, and then select one of them afterwards. Touching is also NFC's communication paradigm, and occurs when a mobile device is touched to a nearby smart object. Touching is a natural and possibly the simplest interaction technique, since all that a user needs to do is to touch the mobile device to the smart object.

Some usability studies on the Touching paradigm have already been performed in the literature. One study presents a usability analysis of the interaction techniques in general; 134 people participated in the test, though the results are not encouraging for a Touching paradigm [246], as based on the given responses, only 25% of the volunteers enjoyed using it. When they were asked to select one of the provided interaction alternatives, a paltry 13% of the attendees selected Touching as their preferred option. In a usability study [247], the user experience of mobile interactions with the dynamic NFC display is investigated in both single user and multi-user contexts. The study with single user context showed the high appreciation of the interaction. In case of multi-user context, interactions were also appreciated, however users seem to prefer single user interactions to multi-user options.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 45 of 84

Several interaction methods are discussed by some authors and NFC-based touch-driven interaction is suggested [248]. According to the authors, touch-driven interaction provides users with full controllability, fine-grain accuracy and high usability. Another work [9] points out the advantages of touch-based interaction in terms of controllability and accuracy. It considers NFC touching as a differentiator between RFID and NFC. With traditional RFID technology, the server controls the process, because the RFID antennas are placed all over the environment, and they detect RFID tags as the user navigates around them. On the contrary, in NFC, users decide when to activate NFC interaction themselves. Additionally, behavior monitoring and extracting by sensors is inaccurate, intrusive, and difficult to control. The authors also argue that modeling user behavior using explicit user action—such as touching devices or putting smartphones together—achieves better accuracy and gives user full control of the system.

6.1. Overall Usability of NFC Services

For usability analysis, several analysis models such as Unified Theory of Acceptance and Use of Technology (UTAUT), Strengths, Weaknesses, Opportunities, and Threats (SWOT), Analytical Hierarchy Process (AHP), and Technology Acceptance Model (TAM) have been used in the literature.

The UTAUT model is used for user acceptance analysis of NFC in one study [249]. As stated in the paper, the main purpose of the study was to explore the key factors that influence the Behavioral Intention to use smartphone-based services. The authors gathered 189 valid responses from respondent of various genders, ages, education levels, professional occupations, and prior experience with NFC. The results indicate that Effort Expectancy (the degree of ease that is associated with the use of the system) has a positive effect on Performance Expectancy (the degree to which an individual believes that using the system will help her to attain gains in job performance). Also, Performance Expectancy and Social Influence (the degree to which an individual perceives the importance of others' belief to use the new system) have a positive effect on Attitude Toward Use of Technology, but Anxiety has a negative effect on it. Finally, Attitude Toward Use of Technology is more significant than Facilitating Conditions (the degree to which an individual believes that sufficient organizational and technical infrastructure exists to support use of the system) in affecting Behavioral Intention.

SWOT analysis is a model to critique strengths and weaknesses of a system. In a study [250], telecommunication professionals with prior knowledge about NFC filled out 23 questionnaires. The findings indicate that the positive factors (strengths and opportunities) associated with NFC

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 46 of 84

are potentially more important than the negative factors (weaknesses and threats). According to the authors, this indicates the potential benefits of NFC-based projects.

Another study analyses a rather detailed technical and user feedback in order to compare paper-based and NFC-based tickets [163]. The study searches for answers to the questions such as: is an electronic ticketing system that much faster than a paper-based system; will customers agree with the vision that a single compact card is easier to use than many regular tickets; will event organizers be convinced by a system that provides protection against reselling vouchers, but does not provide a physical proof of vouchers exchanging hands at the time, *etc*. The study performs the tests based on TAM, which models how affirmatively users accept a new technology. The model suggests that when users encounter a new technology, two major factors influence their decision: perceived usefulness (PU) which presents provided performance increase by the new technology; and perceived ease-of-use (PEOU) which presents ease of use of the new technology. The same study shows that when PU is strongly lower than PEOU, the behavioral intention to use NFC is low as well. Technical study showed that using NFC ticketing requires slightly more time than the traditional paper-based alternative.

NFC-based electronic voting is an alternative to the traditional version, but no satisfactory improvement in this topic has been implemented yet. A study performed on voting [216] created a prototype for using NFC in voting and obtained the feedback of 50 voters towards the usage of the new technology in the voting process. The voters also compared the usability of web-based voting with NFC voting and according to the results NFC voting affords insignificantly better usability.

The results of a usability study show that user experiences on the NFC service were moderately positive, though there were mixed results considering the performance effects of NFC service usage [251]. The potential usefulness of proposed future NFC service functionalities was considered quite high.

In another study [252], user preferences between audio-haptic and visual-haptic alternatives were analyzed. In the study, users tap their smartphones to the NFC tags on the products in the grocery store, and the application on the smartphone creates audio and visual alerts to the user if the food contains a high enough amount of sugar to threaten the user's health condition; the threshold is based on the user's diet. The study showed that the participants preferred haptic-visual feedback, which was faster than the audio-haptic feedback, whose long vibration patterns were less suitable as an indication of the amount of sugar in products than the visual representation of the haptic-visual feedback. The participants rated haptic-visual feedback as more helpful, easier to learn, and more pleasant to use. These quantitative results were also confirmed by the qualitative results of

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 47 of 84

the questionnaire. Some results also indicated that purely haptic feedback with various patterns (e.g., vibration intensity) could provide an added value, e.g., for visually impaired users.

A pilot test of an application that preserves anonymity of the students during exam paper evaluation by the instructors, was conducted with 28 students [195]. After all students had turned in the exam papers, they were asked to fill out a satisfaction survey. The survey consisted of 12 questions on the privacy feeling by using the application and the process; and the satisfaction rate was realized as 4.22/5. The authors then concluded that students wished to maintain their anonymity during the exam process, and NFC is a leading candidate to ensure this.

6.2. Usability of NFC Based Financial Services

The rapid evolution of mobile technologies and the increasing diffusion of smartphones have provided significant opportunities for innovative companies to offer NFC-based payment solutions and value-added services to their customers.

One of the earlier studies that investigated the acceptance of NFC by European retailers was conducted between October 2007 and April 2008 [253]. According to the questionnaire results, the usage of NFC payment was more promising than other options such as NFC Loyalty, NFC Smart Posters, or NFC Coupons. The responders agreed that NFC-based payment had the potential to speed up the payment part of the check-out process at the cashier.

NFC payment is a significant opportunity to turn smartphones into digital wallets. Some authors [254] provide guidelines for the adoption of NFC-based mobile payments, by proposing a research framework to provide a profound understanding of factors facilitating or impeding this. The study focuses on:

(a) product-related factors (perceived usefulness, perceived ease of use, compatibility, perceived security and privacy risk, perceived cost of use, trialability, and additional value of NFC mobile payment);
(b) personal-related factors (personal innovativeness in new technologies, absorptive capacity);
(c) trust based factors; and
(d) attractiveness of alternatives. The authors made use of five academic and 10 practitioner customers. The authors conclude that:
    - Customers are unlikely to adopt NFC mobile payments unless Service Providers shed some light on the outstanding characteristics and differentiation of NFC-based mobile

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 48 of 84

payment.

- It is beneficial for the entrepreneurs and Service Providers to classify the market into different segmentations, customize, promote and offer services to suit the specific needs of consumers.

The performance and security issues of NFC-based payment solutions with the classical ones have been compared in one study [255]. The paper concludes by claiming that traditional models are more secure, whilst NFC-based solutions are more functional. Another effort [256] performs a study with 1001 users and 13 professionals, working for various NFC payment actor organizations. The conclusions of the study states that the users emphasized the importance of security; the users prefer to use PIN codes to feel secure; and they prefer double-tap (once to learn the payment amount, and then to approve the payment).

Another study [257] analyzed acceptance of NFC payments in detail. The authors applied a questionnaire to 262 respondents with varying demographic properties with respect to sex, age, educational level, professional area, and credit card usage. The study examined the preference of NFC-based payment by using TAM models. The authors conclude that there is a significant and direct relationship between both PEOU and PU on Intention to Use (IU) while Trust (TR) and Personal Innovativeness in Information Technology (PIIT) have significant indirect effects on IU.

In an additional study [156], the MobiTag protocol containing both customer and merchant interfaces is presented, and user acceptance tests are performed as well. The authors collected 34 answers: nine from participants in the laboratory pilot, eight from merchants, and 17 from customers that participated in the experimental pilot tests. The major identified problem was the performance of NFC connection, which made the users find tapping their smartphones slow and complicated, Transactions are sometimes not completed and must be reinitiated. The pilot users performed 10 different tasks and evaluated the tasks as easy to perform. The attitude of customers and merchants were generally very positive regarding the usage of NFC. Authors asserted that the people are generally open to new possibilities offered by mobile payments such as NFC payment and are willing to experiment with it.

Finally, the design, usability, and user experience of user interactions on dynamic NFC-enabled displays have been investigated [248]. The authors conducted two complementary user studies with the prototypes they created. The first study was carried out with single users to assess the overall performance, usability, and user acceptance of the interaction. The second study was carried out with groups of users to evaluate their behavior during the interaction with NFC-based interactive surfaces together with other users. The responders consisted of 11 students and

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 49 of 84

researchers. The users reported satisfaction with the usage of the system overall, and found it easy to use.

6.3. Usability of NFC Based Healthcare Services

There is a variety of actors in health-related services including individuals such as patients, doctors, nurses, and pharmacists, organizations such as hospital administrative management and drug reservoirs, and materials such as drugs. The authors of one study developed an NFC-based system to help nursing students to perform patient care tasks with simple interactions, including medication administration, clinical tests, and vital signs supervision, among others [124]. The authors also evaluated the system in two nursing schools. Sixty-two nurses were engaged in the tests and the results assert that about two-third of the attendees found the NFC-based system useful enough.

In another study [127], an NFC-based system was developed to enable self-reporting of instant health status of the user, to represent and analyze real time patient data and to allow direct medical intervention by physicians. The results of a field test indicated that NFC usage is almost as simple as filling out a paper-based questionnaire, as indicated by the authors. Further, NFC technology was perceived as very intuitive and the information quality of each patient's health status could be improved using NFC technology.

Usability of NFC technology for the elderly, disabled, and immature individuals is rather important. One study [258] consisted of a field experiment which used NFC smartphones as a user interface element so as to enable home-dwelling elderly people to choose their meals to be delivered by means of a home care service. The authors focused on examining the suitability of a touch-based user interface in the everyday life activities of elderly users. The eight-week experiment showed that the touch-based user interface was easy to learn and adopt and the users were able to successfully use it regardless of their physical or cognitive weaknesses.

6.4. Further Research Opportunities

NFC technology is generally thought as easy to use and in parallel, and the results of most of the usability studies indicate the same result. However, we also need to mention that users generally experience a wow effect at first time of NFC usage, but when the time passes this passionate desire to use the technology decreases. Moreover, many usability studies concentrate on the usability of the applications with usage of the NFC technology a secondary focus at best. Relating to the

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 50 of 84

reviewed studies, the following open research areas on NFC usability issues are identified as a guide for the researchers:

- Usability analysis of NFC interaction in various service domains.
- Comparisons of the usability of NFC operating modes.
- Analysis of the NFC wow effect.

7. NFC Ecosystem and Business Models

NFC technology is made up of several components, which makes it part of a large business environment, cutting across boundaries of many organizations from diverse business sectors. Its large value-chain includes several industries and organizations such as MNOs, banking and payment services, device manufacturers, software developers, other supplementary merchants including transport operators and retailers [8,18]. All stakeholders in the NFC ecosystem have already experienced and agreed on the fact that NFC services to end users cannot be provided by a dominant single actor; so collaboration of the participants is vital.

The standardization of NFC technology is already achieved and valuable developments have occurred, creating a considerable increase in commercially available NFC-enabled smartphones. According to a forecast by IHS Technology, NFC will be included in 64% of the smartphones shipped in 2018, up from 18.2% in 2013 [259]. Moreover, researchers predict that global shipments of NFC-enabled smartphones in 2018 will be four times higher than in 2013 which means most of the smartphone manufacturers have begun to adopt NFC technology in their products as a *de facto* standard [259].

As also mentioned in [260], the business cases and models in NFC ecosystem are still unclear due to lack of common understanding and vision in NFC technology among participating organizations and industries. It is expected that companies shall cooperate with each other to create the added value first, and compete with each other to take the biggest share of it afterwards [261]. A mutually beneficial business model in the financial services could not have been formed yet.

A study examining the deficiencies of NFC services collaborating with existing contactless and smart card standards in a comprehensive approach and categorizes the problems in two aspects: technology and business related [262]. In terms of technology-related problems, some important issues to be considered are:

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 51 of 84

- Although NFC technology warrants the separation of various applications on the same SE with a high security and minimal risk of interference, certain security specifications prohibit this coexistence. Thus, the management of multiple applications on the same chip is also an unresolved issue.
- OTA service provisioning is a great benefit of mobile technology, which is used to manage SEs without being physically connected to it [263]. However, diverse technical OTA solutions exist with different capabilities that are not interoperable with each other.
- Currently, different SE alternatives are available in the market, hence different NFC service options exist; each actor proposes a different business model that brings more advantage to that actor than others. For example MNO's propose SIM-based models, since they can control these cards and hence can receive more profit if this model is used, whereas a mobile handset manufacturer provides embedded hardware-based SE models and NFC services to gain more control in the NFC business environment.

In terms of business and managerial problems, the revenue to be shared is enormous; this creates a failure in common understanding and vision in working with suitable business models in the NFC ecosystem. Furthermore, each participating ecosystem organization is powerful in its own sector; causing it to become arrogant and expect the other parties to respect its subjective demands [262].

To enable a beneficial business model and manage Business-to-Business (B2B) relations efficiently, some profitable models and proposals such as User Centric Smart Card Ownership Model (UCOM) [261], Consumer Oriented Trusted Service Manager (CO-TSM) as a TSM deployment model [264], StoLPan's Host Application Model as a transparent and uniform platform for managing multiple services [265], Platform Manager Model [260], and Role Based Ecosystem Model [266] are already provided.

In all proposed models so far, the main goal is to achieve a successful business model. It is important to drive cooperation of the partners in the ecosystem and also to enable customer acceptance. Currently there is a tremendous amount of work on organizing the contributions and interests of all entities, and better governance of the overall ecosystem.

From the technical point of view, to create sustainable business models for NFC services, some issues need to be solved completely from all involved parties' perspective. Secure elements play an important role in defining the business model and ecosystem. In the case of SE elements (e.g., UICC, embedded hardware), three components, namely the SE and SE issuer, SE Platform Manager and OTA Provider determine and structure the business model for an NFC service.

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 52 of 84

As a matter of fact, practical implementation of such proposed SE-based NFC applications and ecosystem related studies are mostly missing in the literature. Some literature reviews [267,268] also indicate that only 9.46% of the NFC literature focuses on NFC ecosystem and business issues. There is a clear need for rigorous NFC research papers to provide a high level of research [268]. Business models of NFC technology need to be clearly considered with methodologies and design principles that have theoretical proof.

HCE, as a new approach in SE, is an important advance in NFC technology which is referred as a "game changer" in the NFC ecosystem [269]. HCE-based NFC solutions completely eliminate the need for an SE Issuer, TSM and MNO to enable NFC services. On the contrary, HCE Solution Provider (HSP) and Token Service Provider (TSP) as new actors, engage with the ecosystem depending on the HCE solution alternative which can be either cloud-based HCE solutions or tokenization-based HCE solutions [269]. We assume that HCE-based business models will create considerable changes in the NFC ecosystem in the near future.

Further Research Opportunities

There are still some challenging research areas related with the NFC ecosystem. The following open research topics may be of interest to academicians and researchers:

- Development of sustainable ecosystem model alternatives for NFC services including revenue-cost analysis, SE usage, competency and feasibility analysis.
- Examination of proposed NFC applications' business impacts and models based on various theoretical frameworks.
- Exploration of HCE-based NFC services business models.
- Analysis of business and economic performance of complex NFC applications such as NFC payment, ticketing and transportation.
- Exploration of business case opportunities based on demography, regulation, market structure, and infrastructure readiness *etc*.
- Identification of liability issues, customer care, and division of other related roles and responsibilities between key stakeholders.

8. Conclusions

NFC is one major emerging technology of the last decade. Even though it remains a comparatively newborn technology, NFC has become an attractive research area for many researchers and

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 53 of 84

practitioners due to its exponential growth and its promising applications and related services. In this survey, we have covered all aspects of NFC and put special stress on the academic and innovative issues. We have provided a comprehensive, up-to-date review of NFC technology including academic studies as well as some valuable white papers of industry pioneers within the NFC ecosystem. We believe that this survey study will provide a beneficial source to understand the current status of NFC research. There is a clear need for more rigorous publications to address the issues that have been highlighted in the research opportunities sections. Academicians and researchers should focus on these recommended research issues, perform high quality research and disseminate their findings in order to maintain the advancement of knowledge in NFC research and to identify the gaps between theory and practice.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Ok K., Coskun V., Aydin M.N., Ozdenizci B. Current Benefits and Future Directions of NFC Services; Proceedings of the IEEE International Conference on Education and Management Technology; Cairo, Egypt. 2–4 November 2010; pp. 334–338. [Google Scholar]

2. Ok K., Aydin M.N., Coskun V., Ozdenizci B. Exploring Underlying Values of NFC Applications; Proceedings of the Third International Conference on Information and Financial Engineering; Singapore. 2011. pp. 290–294. [Google Scholar]

3. Coskun V., Ozdenizci B., Ok K. A Survey on Near Field Communication (NFC) Technology. Wirel. Personal Commun. 2013;71:2259–2294. doi: 10.1007/s11277-012-0935-5. [DOI] [Google Scholar]

4. Palma D., Agudo J.E., Sánchez H., Macías M.M. An Internet Of Things Example: Classrooms Access Control Over Near Field Communication. Sensors. 2014;14:6998–7012. doi: 10.3390/s140406998. [DOI] [PMC free article] [PubMed] [Google Scholar]

5. Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E. A Survey on Sensor Networks. Commun. Mag. 2002;40:102–114. doi: 10.1109/MCOM.2002.1024422. [DOI] [Google Scholar]

6. Tezcan H., Cayirci E., Coskun V. A distributed scheme for 3D space coverage in tactical underwater sensor networks; Proceedings of the Military Communications Conference (MILCOM); Monterey, CA, USA. November 2004; pp. 697–703. [Google Scholar]

7. Atzori L., Lera A., Morabito G. The Internet of Things: A Survey. Comput. Netw. 2010;54:2787–2805. doi: 10.1016/j.comnet.2010.05.010. [DOI] [Google Scholar]

8. Coskun V., Ok K., Ozdenizci B. Near Field Communication (NFC): From Theory to Practice. 1st ed. John Wiley and Sons; London, UK: 2012. [Google Scholar]

9. Bravo J., Hervas R., Nava S.W., Chavira G., Sanchez C. Towards Natural Interaction By Enabling Technologies: A Near Field Communication Approach; Proceedings of the Workshops of the First European Conference on Ambient Intelligence; Darmstadt, Germany. 7–10 November 2007; pp. 338–351. [Google Scholar]

10. Chen M.Y. Context-Aware for Smartphone Sensing in Over-the-Counter Market: Ambient Intelligence in Mobile Stock Markets; Proceedings of Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS); Taichung, Taiwan. 3–5 July 2013; pp. 641–646. [Google Scholar]

11. Cheong S.N., Chai I., Logeswaran R. Near Field Communication Mobiquitous Learning System; Proceedings of the International Conference on Advanced Computer Science Applications and Technologies (ACSAT); Kuching, Malaysia. 23–24 December 2013; pp. 490–494. [Google Scholar]

12. Lai X., Liu Q., Wei X., Wang W., Zhou G., Han G. A Survey of Body Sensor Networks. Sensors. 2013;13:5406–5447. doi: 10.3390/s130505406. [DOI] [PMC free article] [PubMed] [Google Scholar]

13. Fahier N, Fang W. An Advanced Plug-and-Play Network Architecture for Wireless Body Area Network Using HBC, Zigbee and NFC; Proceedings of the IEEE International Conference on Consumer Electronics—Taiwan (ICCE-TW); Taipei, Taiwan. 26–28 May 2014; pp. 165–166. [Google Scholar]

14. Yi W.J., Saniie J. Smart Mobile System for Body Sensor Network; Proceedings of the IEEE International Conference on Electro/Information Technology (EIT); Rapid City, SD, USA. 9–11 May 2013; pp. 1–4. [Google Scholar]

15. Urien P. Cloud of Secure Elements: An Infrastructure for the Trust of Mobile NFC Services; Proceedings of the 10th International Conference on Wireless and Mobile

Computing, Networking and Communications (WiMob); Larnaca, Cyprus. 8–10 October 2014; pp. 213–218. [Google Scholar]

16. Pourghomi P., Saeed M.Q., Ghinea G. Trusted Integration of Cloud-Based NFC Transaction Players; Proceedings of the 9th International Conference on Information Assurance and Security (IAS); Gammarth, Tunisia. 4–6 December 2013; pp. 6–12. [Google Scholar]

17. Coskun V., Ozdenizci B., Ok K., Alsadi M. NFC Loyal System on the Cloud; Proceedings of the 7th International Conference on Application of Information and Communication Technologies (AICT); Baku, Soviet Azerbaijan. 23–25 October 2013; pp. 1–5. [Google Scholar]

18. Coskun V., Ok K., Ozdenizci B. Professional NFC Application Development for Android. 1st ed. John Wiley Sons, Wrox; London, UK: 2013. [Google Scholar]

19. ECMA 340: Near Field Communication Interface and Protocol 1 (NFCIP-1), ECMA International. [(accessed on 13 April 2015)]. Available online: http://www.ecma-international.org/publications/standards/Ecma-340.htm .

20. ECMA 352: Near Field Communication Interface and Protocol 2 (NFCIP-2), ECMA International. [(accessed on 13 April 2015)]. Available online: http://www.ecma-international.org/publications/standards/Ecma-352.htm .

21. Felica. [(accessed on 13 April 2015)]. Available online: http://www.sony.net/Products/felica/

22. ISO/IEC14443, Identification cards—Contactless integrated circuit cards—Proximity cards. [(accessed on 13 April 2015)]. Available online: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39693 .

23. Gossar M., Stark M., Gebhart M., Pribyl W., Soser P. Investigations to Achieve Very High Data Rates for Proximity Coupling Devices at 13.56 MHz and NFC Applications; Proceedings of the 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 71–76. [Google Scholar]

24. Park S., Park S., Park J., Baek D. Design of 13.56 MHz ASK Transmitter for Near Field Communication Using a DLL Architecture; Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS); Seoul, Korea (South). 20–23 May 2012; pp. 1760–1762. [Google Scholar]

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 56 of 84

25. Al-Kadi G., van de Beek R., Ciacci M., Kompan P., Stark M. A 13.56 Mbps PSK Receiver for Very High Data Rate 13.56 MHz Smart Card and NFC Applications; Proceedings of the IEEE International Conference on Consumer Electronics (ICCE); Las Vegas, NV, USA. 13–16 January 2012; pp. 180–182. [Google Scholar]

26. Gebhart M., Wobak M., Merlin E., Chlestil C. Active Load Modulation for Contactless Near-Field Communication; Proceedings of the IEEE International Conference on RFID-Technologies and Applications (RFID-TA); Nice, France. 5–7 November 2012; pp. 228–233. [Google Scholar]

27. Man F., Shuqiang X., Lenan W. Research on High-Speed NFC Transmission Based on High-Efficiency EBPSK Modulation; Proceedings of the 5th International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2013); Beijing, China. 22–25 November 2013; pp. 119–122. [Google Scholar]

28. Stark M., Gebhart M. How to Guarantee Phase-Synchronicity in Active Load Modulation for NFC and Proximity; Proceedings of the 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

29. Kang E., Won Hong S., Seog Han D. Improved Speed NFC with Rotated QPSK Constellation and Hidden Data Transmission; Proceedings of IEEE International Symposium on the Broadband Multimedia Systems and Broadcasting (BMSB); Seoul, Korea. 27–29 June 2012; pp. 1–2. [Google Scholar]

30. Azad U., Wang Y.E. Direct Antenna Modulation (DAM) For Enhanced Capacity Performance of Near-Field Communication (NFC) Link. IEEE Trans. Circuits Syst. I Regul. Pap. 2014;61:902–910. doi: 10.1109/TCSI.2013.2283995. [DOI] [Google Scholar]

31. Brown T.W.C., Diakos T. On the Design of NFC Antennas for Contactless Payment Applications; Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP); Rome, Italy. 11–15 April 2011; pp. 44–47. [Google Scholar]

32. Gebhart M., Szoncso R. Optimizing Design of Smaller Antennas for Proximity Transponders; Proceedings of the IEEE Second International Workshop on Near Field Communication; Monaco. 20 April 2010; pp. 77–82. [Google Scholar]

33. Ohmura N., Takase E., Ogino S., Okano Y., Arai S. Optimize Pattern of Magnetic Sheet Attached on NFC/HF-RFID Antenna; Proceedings of the International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS); Naha, Japan. 12–15 November 2013; pp. 627–631. [Google Scholar]

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 57 of 84

34. Smierzchalski M., Collardey S., Mahdjoubi K. A novel metamaterial-based RFID antenna with efficient of operating distance; Proceedings of the 6th European Conference on Antennas and Propagation (EUCAP); Prague, Czech. 26–30 March 2012; pp. 3038–3041. [Google Scholar]

35. Lee B., Kim B., Harackiewicz F.J., Mun B., Lee H. NFC Antenna Design For Low-Permeability Ferromagnetic Material. IEEE Antennas Wirel. Propag. Lett. 2014;13:59–62. [Google Scholar]

36. Gebhart M., Baier T., Facchini M. Automated Antenna Impedance Adjustment for Near Field Communication (NFC); Proceedings of the 12th International Conference on Telecommunications (ConTEL); Zagreb, Yugoslavia. 26–28 June 2013; pp. 235–242. [Google Scholar]

37. Ohmura N., Takase E., Ogino S., Okano Y., Arai S. Material Property of On-Metal Magnetic Sheet Attached on NFC/HF-RFID Antenna and Research of Its Proper Pattern and Size on; Proceedings of the International Symposium on Antennas Propagation (ISAP); Nanjing, China. 23–25 October 2013; pp. 1158–1161. [Google Scholar]

38. Tanabe Y., Chang T., Yeh A., Poon A. A Small Dual-Band Asymmetric Dipole Antenna for 13.56 MHz Power and 2.45 GHz Data Transmission. IEEE Antennas Wirel. Propag. Lett. 2014;13:1120–1123. doi: 10.1049/el.2014.0858. [DOI] [Google Scholar]

39. Lee W.S., Kim D.Z., Yu J.W. Multi-Functional High-Isolation Dual Antenna for Controllable Wireless Charging and NFC Communication. Electron. Lett. 2014;50:912–913. doi: 10.1049/el.2014.0858. [DOI] [Google Scholar]

40. Gebhart M., Neubauer R., Stark M., Warnez D. Design of 13.56 MHz Smartcard Stickers with Ferrite for Payment and Authentication; Proceedings of the 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 59–64. [Google Scholar]

41. Mujal J., Ramon E., Díaz E., Carrabina J., Calleja A., Martínez R., Teres L. Inkjet Printed Antennas for NFC Systems; Proceeding of the 17th IEEE International Conference on Electronics, Circuits, and Systems (ICECS); Athens, Greece. 12–15 December 2010; pp. 1220–1223. [Google Scholar]

42. Pachler W., Grosinger J., Bosch W., Holweg G., Popovic K., Blumel A., List-Kratochvil E.J. A Silver Inkjet Printed Ferrite NFC Antenna; Proceedings of the Antennas and Propagation

Conference (LAPC); Loughborough, UK. 10–11 November 2014; pp. 95–99. [Google Scholar]

43. Warnick K.F., Gottula R.B., Shrestha S., Smith J. Optimizing Power Transfer Efficiency and Bandwidth for Near Field Communication Systems. IEEE Trans. Antennas Propag. 2013;61:927–933. doi: 10.1109/TAP.2012.2220325. [DOI] [Google Scholar]

44. Brown T.W., Diakos T., Briffa J.A. Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards; Proceedings of the 7th European Conference on Antennas and Propagation (EuCAP); Gothenburg, Sweden. 8–12 April 2013; pp. 3525–3528. [Google Scholar]

45. Chen Y.S., Chen S.Y., Li H.J. Analysis of Antenna Coupling in Near-Field Communication Systems. IEEE Trans. Antennas Propag. 2010;58:3327–3335. doi: 10.1109/TAP.2010.2055782. [DOI] [Google Scholar]

46. Muehlmann U., Gebhart M., Wobak M. Mutual Coupling Modeling Of NFC Antennas By Using Open-Source CAD/FEM Tools; Proceedings of the IEEE International Conference on RFID-Technologies and Applications (RFID-TA); Nice, France. 5–7 November 2012; pp. 393–397. [Google Scholar]

47. Schober A., Ciacci M., Gebhart M. An NFC Air Interface Coupling Model for Contactless System Performance Estimation; Proceedings of the 12th International Conference on Telecommunications (ConTEL); Zagreb, Yugoslavia. 26–28 June 2013; pp. 243–250. [Google Scholar]

48. Yoon S.K., Kim S.J., Kwon U.K., Lee J.C. Advanced Near Field Communication with Resonant Coupling; Proceedings of the IEEE 11th Consumer Communications and Networking Conference (CCNC); Las Vegas, NV, USA. 10–13 January 2014; pp. 269–274. [Google Scholar]

49. Menghin M., Druml N., Kipperer B., Steger C., Weiss R., Bock H., Haid J. Energy Efficiency By Using Field Strength Scaling for Multi-Transponder Applications; Proceedings of the 12th International Conference on Telecommunications (ConTEL); Zagreb, Yugoslavia. 26–28 June 2013; pp. 263–270. [Google Scholar]

50. Wang M., Guo Y.X., Wu W. Equivalent Circuit Analysis of Inductively Coupled NFC Antennas; Proceedings of the IEEE Antennas and Propagation Society International Symposium (APSURSI); Memphis, TN, USA. 6–11 July 2014; pp. 1540–1541. [Google Scholar]

51. Bauernfeind T., Renhart W., Schemthanner S., Gebhart M., Preis K. Equivalent Circuit Parameter Extraction for Controlled Detuned NFC Antenna Systems Utilizing Thin Ferrite Foils; Proceedings of the 12th International Conference on Telecommunications (ConTEL); Zagreb, Yugoslavia. 26–28 June 2013; pp. 251–256. [Google Scholar]

52. Cho J.H., Cole P.H., Kim S. An NFC Transceiver Using an Inductive Powered Receiver for Passive, Active, RW and RFID Modes; Proceedings of the International SoC Design Conference (ISOCC); Busan, Korea. 22–24 November 2009; pp. 456–459. [Google Scholar]

53. Roland M., Witschnig H., Merlin E., Saminger C. Automatic Impedance Matching for 13.56 MHz NFC Antennas; Proceedings of the 6th International Symposium on Communication Systems, Networks and Digital Signal Processing; Graz, Austria. 25 July 2008; pp. 288–291. [Google Scholar]

54. Li D., Shen M., Huangfu J., Long J., Tao Y., Wang J., Ran L. Wireless Sensing System-On-Chip For Near-Field Monitoring of Analog and Switch Quantities. IEEE Trans. Ind. Electron. 2012;59:1288–1299. doi: 10.1109/TIE.2011.2148676. [DOI] [Google Scholar]

55. Zhang L., Xu H., Dai Y., Min H. An NFC System with High Sensitivity Based on SDR; Proceedings of the IEEE 10th International Conference on ASIC (ASICON); Shenzhen, China. 28–31 October 2013; pp. 1–4. [Google Scholar]

56. Li W., Zhou D., Li M., Nguyen B.P., Zeng X. Near-Field Communication Transceiver System Modeling and Analysis Using Systemc/Systemc-AMS with the Consideration of Noise Issues. IEEE Trans. Large Scale Integr. (VLSI) Syst. 2013;21:2250–2261. doi: 10.1109/TVLSI.2012.2231443. [DOI] [Google Scholar]

57. Dieng M., Azais F., Comte M., Bernard S. Study of Adaptive Tuning Strategies for NFC Transmitter Module; Proceedings of the 19th International Mixed-Signals, Sensors and Systems Test Workshop (IMS3TW); Porto Alegre, Brazil. 17–19 September 2014; pp. 1–6. [Google Scholar]

58. Zhang L., Xu H., Min H. NFC Quadrature Carrier Cancelling Receiver Design and Implementation; Proceedings of the 12th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT); Guilin, China. 28–31 October 2014; pp. 1–4. [Google Scholar]

59. Druml N., Menghin M., Basagic R., Steger C., Weiss R., Bock H., Haid J. NIZE-A Near Field Communication Interface Enabling Zero Energy Standby For Everyday Electronic Devices; Proceedings of the IEEE 8th International Conference on Wireless and Mobile Computing,

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 60 of 84

Networking and Communications (WiMob); Barcelona, Spain. 8–10 October 2012; pp. 261–267. [Google Scholar]

60. Menghin M., Druml N., Steger C., Weiss R., Bock H., Haid J. The PTF-Determinator: A Run-Time Method Used to Save Energy in NFC-Systems; Proceedings of the Fourth International EURASIP Workshop on RFID Technology (EURASIP RFID); Torino, Italy. 27–28 September 2012; pp. 92–98. [Google Scholar]

61. Druml N., Menghin M., Steger C., Weiss R., Genser A., Bock H., Haid J. Adaptive Field Strength Scaling: A Power Optimization Technique for Contactless Reader/Smart Card Systems; Proceedings of the 15th Euromicro Conference on Digital System Design (DSD); İzmir, Turkey. 5–8 September 2012; pp. 616–623. [Google Scholar]

62. Menghin M., Druml N., Steger C., Weiss R., Bock R., Haid J. NFC-Dynfs: A Way to Realize Dynamic Field Strength Scaling during Communication; Proceedings of the IEEE 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

63. Madlmayr G., Dillinger O., Langer J., Scharinger J. Management of Multiple Cards in NFC Devices; Proceedings of 8th IFIP WG 8.8/11.2 International Conference (CARDIS 2008); London, UK. 8–11 September 2008; pp. 149–161. [Google Scholar]

64. ETSI TS 102 613, Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics, Technical Specification, ETSI TS. [(accessed on 13 April 2015)]. Available online: http://www.etsi.org/deliver/etsi_ts/102600_102699/102613/07.03.00_60/ts_102613v070300p.pdf .

65. ECMA 373: Near Field Communication Wired Interface (NFC-WI), ECMA International. [(accessed on 13 April 2015)]. Available online: http://www.ecma-international.org/publications/standards/Ecma-373.htm .

66. NFC Stepping Stones 2011, SIM Alliance, White Paper. [(accessed on 13 April 2015)]. Available online: http://simalliance.org/nfc/nfc-technical-releases/

67. NFC Forum. [(accessed on 13 April 2015)]. Available online: http://www.nfc-forum.org/

68. NFC Controller Interface (NCI), NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 61 of 84

69. Xiao K., Luo L. A Novel Mobile Device NFC Stack Architecture; Proceedings of the 11th International Conference on Dependable, Autonomic and Secure Computing; Chengdu, China. 21–22 December 2013; pp. 169–173. [Google Scholar]

70. NFC Logical Link Control Protocol LLCP, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

71. Type 1 Tag Operation, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

72. Type 2 Tag Operation, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

73. Type 3 Tag Operation, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

74. Type 4 Tag Operation, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

75. NFC Data Exchange Format (NDEF), NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

76. NFC Record Type Definition (RTD), NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

77. RTD Smart Poster Record Type Definition, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

78. RTD Text Record Type Definition, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

79. RTD URI Record Type Definition, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

80. RTD Signature Record Type Definition, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

81. NFC Analog, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

82. NFC Digital Protocol, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

83. NFC Activity, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

84. Roland M., Langer J. Digital Signature Records for the NFC Data Exchange Format; Proceedings of the Second International Workshop on Near Field Communication (NFC); Monaco. 20 April 2010; pp. 71–76. [Google Scholar]

85. NFC Connection Handover, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

86. Touch the Future with a Smart Touch, VTT, White Paper. [(accessed on 13 April 2015)]. Available online: http://www.vtt.fi/inf/pdf/tiedotteet/2009/T2492.pdf .

87. Ali W., ElKilani W., Hadhoud M. Simulation of NFCIP-1 Protocol over NS-2; Proceedings of the 7th International Conference on Informatics and Systems (INFOS); Cairo, Egypt. 28–30 March 2010; pp. 1–6. [Google Scholar]

88. Grunberger S., Langer J. Analysis and Test Results of Tunneling IP Over NFCIP-1; Proceedings of the First International Workshop on Near Field Communication; Hagenberg, Austria. 24 February 2009; pp. 93–97. [Google Scholar]

89. Lotito A., Mazzocchi D. OPEN-NPP: An Open Source Library to Enable P2P over NFC; Proceedings of the 4th International Workshop on Near Field Communication (NFC);

Helsinki, Finland. 13 March 2012; pp. 57–62. [Google Scholar]

90. Siira E., Tormanen V. The Impact of NFC on Multimodal Social Media Application; Proceedings of the Second International Workshop on Near Field Communication (NFC); Monaco. 20 April 2010; pp. 51–56. [Google Scholar]

91. Urien P. LLCPS: A New Security Framework Based on TLS for NFC P2P Applications in the Internet of Things; Proceedings of the Consumer Communications and Networking Conference (CCNC); Las Vegas, NV, USA. 11–14 January 2013; pp. 845–846. [Google Scholar]

92. Urien P. LLCPS: A New Secure Model for Internet of Things Services Based on the NFC P2P Model; Proceedings of the IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP); Singapore. 21–24 April 2014; pp. 1–6. [Google Scholar]

93. Simple NDEF Exchange Protocol, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

94. Lotito A., Mazzocchi D. OPEN-SNEP Project: Enabling P2P over NFC using NPP and SNEP; Proceedings of the 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

95. Monteiro D.M., Rodrigues J.J., Lloret J. A Secure NFC Application for Credit Transfer among Mobile Phones; Proceedings of International Conference on Computer, Information and Telecommunication Systems (CITS); Amman, Jordan. 14–16 May 2012; pp. 1–5. [Google Scholar]

96. NFC Forum Personal Health Device Communication, NFC Forum, Technical Specification. [(accessed on 13 April 2015)]. Available online: http://nfc-forum.org/our-work/specifications-and-application-documents/

97. Anwar W., Lindskog D., Zavarsky P., Ruhl R. Redesigning Secure Element Access Control for NFC Enabled Android Smartphones Using Mobile Trusted Computing; Proceedings of the International Conference on Information Society (i-Society); Toronto, ON, Canada. 24–26 June 2013; pp. 27–34. [Google Scholar]

98. Urien P., Kiennert C. A New Cooperative Architecture for Sharing Services Managed By Secure Elements Controlled by Android Phones with IP Objects; Proceedings of the

International Conference on Collaboration Technologies and Systems (CTS); Denver, CO, USA. 21–25 May 2012; pp. 404–409. [Google Scholar]

99. Reveilhac M., Pasquet M. Promising Secure Element Alternatives for NFC Technology; Proceedings of the First International Workshop on Near Field Communication; Hagenberg, Austria. 24–26 February 2009; pp. 75–80. [Google Scholar]

100. Alternatives for Banks to Offer Secure Mobile Payments, White Paper, Mobey Forum. [(accessed on 13 April 2015)]. Available online: http://www.mobeyforum.org/Press-Documents/Press-Releases/Alternatives-for-Banks-to-offer-Secure-Mobile-Payments .

101. Host Card Emulation, A Smart Card Alliance Mobile NFC Council White Paper. [(accessed on 13 April 2015)]. Available online: http://www.smartcardalliance.org/publications-host-card-emulation-101/

102. GlobalPlatform Card Specification, GlobalPlatform. [(accessed on 13 April 2015)]. Available online: http://www.globalplatform.org/specificationscard.asp .

103. Sabt M., Achemlal M., Bouabdallah A. Over-The-Internet: Efficient Remote Content Management for Secure Elements in Mobile Devices; Proceedings of the First Conference on Mobile and Secure Services; Gainesville, FL, USA. 20–21 February 2015; pp. 1–5. [Google Scholar]

104. Alimi V. A Novel Scheme for On-Demand Distribution of Secure Element Keys; Proceedings of the World Congress on Computer and Information Technology; Sousse, Tunisia. 22–24 June 2013; pp. 1–5. [Google Scholar]

105. Alimi V. An Ontology-Based Framework to Model a Globalplatform Secure Element; Proceedings of the 4th International Workshop on Near Field Communication (NFC); Helsinki, Finland. 13 March 2012; pp. 25–30. [Google Scholar]

106. Ozdenizci B., Alsadi M., Ok K., Coskun V. Classification of NFC Applications in Diverse Service Domains. Int. J. Comput. Commun. Eng. (IJCCE) 2013;2:614–620. doi: 10.7763/IJCCE.2013.V2.260. [DOI] [Google Scholar]

107. Gune A., Bhat A., Pradeep A. Implementation of NFC Based Healthcare Management System; Proceedings of the IEEE Symposium on Industrial Electronics and Applications (ISIEA); Kutching, Malaysia. 22–25 September 2013; pp. 195–199. [Google Scholar]

108. Engel T., Koennings M., von Heydebrand N., Goswami S., Krcmar H. A NFC-based Concept for Medication Related Patient Services; Proceedings of the European Conference

on Smart Objects, Systems and Technologies (SmartSysTech); Erlangen/Nuremberg, Germany. 11–12 June 2013; pp. 1–10. [Google Scholar]

109. Sethia D., Gupta D., Mittal T., Arora U., Saran H. NFC based secure mobile healthcare system; Proceedings of the IEEE Sixth International Conference on Communication Systems and Networks (COMSNETS); Bangalore, India. 6–10 January 2014; pp. 1–6. [Google Scholar]

110. Dunnebeil S., Kobler F., Koene P., Leimeister J.M., Krcmar H. Encrypted NFC Emergency Tags Based on the German Telematics Infrastructure; Proceedings of the IEEE 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 50–55. [Google Scholar]

111. Mey Y.S., Sankaranarayanan S. Near field communication based patient appointment; Proceedings of the IEEE International Conference on Cloud Ubiquitous Computing Emerging Technologies (CUBE); Pune, India. 15–16 November 2013; pp. 98–103. [Google Scholar]

112. Sankarananrayanan S., Wani S.M.A. NFC Enabled Intelligent Hospital Appointment and Medication Scheduling; Proceedings of the International Conference on Information and Communication Technology (ICoICT); Bandung, Indonesia. 28–30 May 2014; pp. 24–29. [Google Scholar]

113. Morak J., Hayn D., Kastner P., Drobics M., Schreier G. Near field communication technology as the key for data acquisition in clinical research; Proceedings of the IEEE First International Workshop on Near Field Communication (NFC'09); Hagenberg, Austria. 24 February 2009; pp. 15–19. [Google Scholar]

114. Fontecha J., Hervas R., Bravo J., Villarreal V. An NFC approach for nursing care training; Proceedings of the IEEE 3rd International Workshop on Near Field Communication (NFC'11); Hagenberg, Austria. 22 February 2011; pp. 38–43. [Google Scholar]

115. Jara A.J., Lopez P., Fern'ndez D., Ubeda B., Zamora M.A., Skarmeta A.F.G. Interaction of Patients with Breathing Problems through NFC in Ambient Assisted Living Environments; Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS); Palermo, Italy. 4–6 July 2012; pp. 892–897. [Google Scholar]

116. Özcanhan M.H., Dalkılıç G., Utku S. Cryptographically Supported NFC Tags in Medication for Better Inpatient Safety. J. Med. Syst. 2014;38:1–15. doi: 10.1007/s10916-014-0061-x. [DOI] [PubMed] [Google Scholar]

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 66 of 84

117. Ivanov R. Blind-Environment Interaction through Voice Augmented Objects. J. Multimodal User Interfaces. 2014;8:345–365. doi: 10.1007/s12193-014-0166-z. [DOI] [Google Scholar]

118. Jerabek M., Krcal J. Expansion of Information System with NFC Technology for Visually Impaired Passengers; Proceedings of the Second International Conference on Informatics and Applications (ICIA); Lodz, Poland. 23–25 September 2013; pp. 306–310. [Google Scholar]

119. Jerabek M., Krcal J., Zelinka T. Specification of Requirements for Visually Impaired Persons in Services in Transportation Electronic Information System. Syst. Cybern. Inform. 2014;12:59–63. [Google Scholar]

120. Zmily A., Abu-Saymeh D. Alzheimer's Disease Rehabilitation Using Smartphones to İmprove Patients' Quality of Life; Proceedings of the 7th International Conference on Pervasive Computing Technologies for Healthcare; Venice, Italy. 5–8 May 2013; pp. 393–396. [Google Scholar]

121. De la Guía E., Lozano M.D., Penichet V.R. Cognitive Rehabilitation Based on Collaborative and Tangible Computer Games; Proceedings of the 7th International Conference on Pervasive Computing Technologies for Healthcare Venice; Italy. 5–8 May 2013; pp. 389–392. [Google Scholar]

122. Prinz A., Menschner P., Altmann M., Leimeister J.M. inSERT—An NFC-based Self Reporting Questionnaire for Patients with Impaired Fine Motor Skills; Proceedings of the 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 26–31. [Google Scholar]

123. Prinz A., Menschner P., Leimeister J.M. Electronic data capture in healthcare-NFC as easy way for self-reported health status information. Health Policy Technol. 2012;1:137–144. doi: 10.1016/j.hlpt.2012.07.001. [DOI] [Google Scholar]

124. Alabdulhafith M., Sampangi R.V., Sampalli S. NFC-enabled smartphone application for drug interaction and drug allergy detection; Proceedings of the IEEE 5th International Workshop on on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

125. Alabdulhafith M., Sampalli S. NFC-based Framework for Checking the Five Rights of Medication Administration. Procedia Comput. Sci. 2014;37:434–438. doi: 10.1016/j.procs.2014.08.065. [DOI] [Google Scholar]

126. Morak J., Schwarz M., Hayn D., Schreier G. Feasibility of mHealth and Near Field Communication technology based medication adherence monitoring; Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC); San Diego, CA, USA. 28 August–1 September 2012; pp. 272–275. [DOI] [PubMed] [Google Scholar]

127. Vergara M., Díaz-Hellín P., Fontecha J., Hervás R., Sánchez-Barba C., Fuentes C., Bravo J. Mobile prescription: An NFC-based proposal for AAL; Proceedings of the Second International Workshop on Near Field Communication (NFC); Monaco. 20 April 2010; pp. 27–32. [Google Scholar]

128. Morak J., Schreier G. Design and Evaluation of Near Field Communication (NFC) Technology Based Solutions for mHealth Challenges. Mob. Health. 2015;5:813–838. [Google Scholar]

129. Koutkias V., Kilintzis V., Beredimas N., Maglaveras N. Leveraging medication safety through mobile computing: Decision support and guidance services for adverse drug event prevention; Proceedings of the EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth); Athens, Greece. 3–5 November 2014; pp. 19–22. [Google Scholar]

130. Jara A.J., Alcolea A.F., Alsaedy M., Zamora M.A., Gómez-Skarmeta A.F. Drugs interaction checker based on IoT; Proceedings of the Conference on Internet of Things (IoT); Tokyo, Japan. 20 November–1 December 2010; pp. 1–8. [Google Scholar]

131. Koene P., Köbler F., Leimeister J.M., Krcmar H. Touch'n'Document—A Nutrition Management System on an NFC-tagged TFT-display; Proceedings of the International Conference on Health Informatics; Rome, Italy. 26–29 January 2011. [Google Scholar]

132. Yamashita K., Izumi S., Nakano M., Fujii T., Konishi T., Kawaguchi H., Kimura H., Marumoto K., Fuchikami T., Fujimori Y., et al. 38 μA wearable biosignal monitoring system with near field communication; Proceedings of the IEEE 11th International Conference on New Circuits and Systems (NEWCAS); Paris, France. 16–19 June 2013; pp. 1–4. [Google Scholar]

133. Moon Y.J., Park J.H., Song W.C., Lee D.K., Choi D. NFC-based personal information management for U-health; Proceedings of the IEEE ICCE-China Workshop (ICCE-China); Shenzhen, China. 11–13 April 2013; pp. 39–20. [Google Scholar]

134. Izumi S., Kawaguchi H., Yoshimoto M., Fujimori Y. Normally-off technologies for healthcare appliance; Proceedings of the IEEE 19th Asia and South Pasific Design Automation Conference (ASP-DAC); Singapore. 20–23 January 2014; pp. 17–20. [Google Scholar]

135. Raffaeli L., Gambi E., Spinsante S. Smart TV based ecosystem for personal e-health services; Proceedings of the IEEE 8th International Symposium on Medical Information and Communication Technology (ISMICT); Firenze, Italy. 2–4 April 2014; pp. 1–5. [Google Scholar]

136. Zhang H., Li J. NFC in medical applications with wireless sensors; Proceedings of the IEEE International Conference on Electrical and Control Engineering (ICECE); Yichang, China. 16–18 September 2011; pp. 718–721. [Google Scholar]

137. Opperman C.A., Hancke G.P. A generic NFC-enabled measurement system for remote monitoring and control of client-side equipment; Proceedings of the IEEE 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 44–49. [Google Scholar]

138. Bittins B., Sieck J. Multimodal and collaborative localisation service for diverse environments; Proceedings of the IEEE 1st International Symposium on Wireless Systems (IDAACS-SWS); Offenburg, Germany. 20–21 September 2012; pp. 28–33. [Google Scholar]

139. Ho T., Chen R. Leveraging NFC and LBS technologies to improve user experiences; Proceedings of the IEEE International Joint Conference on Service Sciences (IJCSS); Tapei, Taiwan. 25–27 May 2011; pp. 17–21. [Google Scholar]

140. Siira E., Tuikka T., Tormanen V. Location-based mobile Wiki using NFC tag infrastructure; Proceedings of the IEEE First International Workshop on Near Field Communication; Hagenberg, Austria. 24 February 2009; pp. 56–60. [Google Scholar]

141. Köbler F., Koene P., Krcmar H., Altmann M., Leimeister J.M. LocaTag—An NFC-based system enhancing instant messaging tools with real-time user location; Proceedings of the Second International Workshop on Near Field Communication (NFC); Monaco. 20 April 2010; pp. 57–61. [Google Scholar]

142. Teufl P., Zefferer T., Kreuzhuber S., Lesjak C.M. Trusted Location Based Services; Proceedings of the IEEE International Conference for Internet Technology and Secured Transactions; Kuala Lumpur, Malaysia. 5–8 December 2010; pp. 185–192. [Google Scholar]

Telcom Ventures Exhibit No. 2012
Apple Inc. v. Telcom Ventures LLC
IPR2025-01236, U.S. Patent No. 11,770,756
Page 69 of 84

143. Nandwani A., Edwards R., Coulton P. Contactless check-ins using implied locations: A NFC solution simplifying business to consumer interaction in location based services; Proceedings of the IEEE International Conference on Electronics Design, Systems and Applications (ICEDSA); Kuala Lumpur, Malaysia. 5–6 November 2012; pp. 39–44. [Google Scholar]

144. Ozdenizci B., Ok K., Coskun V., Aydin M.N. Development of an indoor navigation system using NFC technology; Proceedings of the Fourth International Conference on Information and Computing (ICIC); Phuket Island, Thailand. 25–27 April 2011; pp. 11–14. [Google Scholar]

145. Ozdenizci B., Coskun V., Ok K. NFC Internal: An Indoor Navigation System. Sensors. 2015;15:7571–7595. doi: 10.3390/s150407571. [DOI] [PMC free article] [PubMed] [Google Scholar]

146. Edwan E., Bourimi M., Joram N., Al-Qudsi B., Ellinger F. NFC/INS integrated navigation system: The promising combination for pedestrians' indoor navigation; Proceedings of the International Symposium on Fundamentals of Electrical Engineering (ISFEE); Bucharest, Romania. 28–29 November 2014; pp. 1–5. [Google Scholar]

147. Hammadi O.A., Hebsi A.A., Zemerly M.J., Ng J.W. Indoor localization and guidance using portable smartphones; Proceedings of the 2012 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technology; Macau, China. 4–7 December 2012; pp. 337–341. [Google Scholar]

148. Lam K.Y., Ng J.K., Wang J.T. A Business Model for Personalized Promotion Systems on Using WLAN Localization and NFC Techniques; Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA); Barcelona, Spain. 25–28 March 2013; pp. 1129–1134. [Google Scholar]

149. Teh P.-L., Ling H.-C., Cheong S.-N. NFC Smartphone Based Access Control System Using Information Hiding; Proceedings of the IEEE Conference on Open Systems (ICOS); Kuching, Malaysia. 2–4 December 2013; pp. 13–17. [Google Scholar]

150. Derawi M.O., Witte H., McCallum S., Bours P. Biometric access control using Near Field Communication and smart phones; Proceedings of the 5th IAPR International Conference on Biometrics (ICB); New Delhi, India. 29 March–1 April 2012; pp. 490–497. [Google Scholar]

151. Mohandes M.A. Mobile Technology for Socio-Religious Events: A Case Study of NFC Technology. Technol. Soc. Mag. 2015;34:73–79. doi: 10.1109/MTS.2015.2396122. [DOI] [Google Scholar]

152. Fernández M.J.L., Fernández J.G., Aguilar S.R., Selvi B.S., Crespo R.G. Control of attendance applied in higher education through mobile NFC technologies. Expert Syst. Appl. 2013;40:4478–4489. doi: 10.1016/j.eswa.2013.01.041. [DOI] [Google Scholar]

153. Ervasti M., Isomursu M., Kinnula M. Experiences from NFC supported school attendance supervision for children; Proceedings of the Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM'09); Sliema, Malta. 11–16 October 2009; pp. 22–30. [Google Scholar]

154. Bucicoiu M., Tapus N. Easy attendance: Location-Based authentication for students integrated with moodle; Proceedings of the 11th Roedunet International Conference (RoEduNet); Sinaia, Romania. 17–19 January 2013; pp. 1–4. [Google Scholar]

155. Shen C.W., Wu Y.C.J., Lee T.C. Developing a NFC-equipped smart classroom: Effects on attitudes toward computer science. Comput. Hum. Behav. 2014;30:731–738. doi: 10.1016/j.chb.2013.09.002. [DOI] [Google Scholar]

156. Rodrigues H., José R., Coelho A., Melro A., Ferreira M.C., Monteiro M.P., Ribeiro C. MobiPag: Integrated Mobile Payment, Ticketing and Couponing Solution Based on NFC. Sensors. 2014;14:13389–13415. doi: 10.3390/s140813389. [DOI] [PMC free article] [PubMed] [Google Scholar]

157. Dias J., Nuno Matos J., Oliveira A. The Charge Collector System. Procedia Technol. 2014;17:130–137. doi: 10.1016/j.protcy.2014.10.220. [DOI] [Google Scholar]

158. Schamberger R., Madlmayr G., Grechenig T. Components for an interoperable NFC mobile payment ecosystem; Proceedings of the 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–5. [Google Scholar]

159. Coneland R., Crespi N. Wallet-on-wheels—Using vehicle's identity for secure mobile money; Proceedings of the 17th International Conference on Intelligence in Next Generation Networks (ICIN); Venice, Italy. 15–16 October 2013; pp. 102–109. [Google Scholar]

160. Google Wallet. [(accessed on 13 April 2015)]. Available online: https://www.google.com/wallet/

161. Apple Pay. [(accessed on 13 April 2015)]. Available online: https://www.apple.com/apple-pay/

162. Ghìron S.L., Sposato S., Medaglia C.M., Moroni A. NFC ticketing: A prototype and usability test of an NFC-based virtual ticketing application; Proceedings of the First International Workshop on Near Field Communication (NFC'09); Hagenberg, Austria. 24 February 2009; pp. 45–50. [Google Scholar]

163. Neefs J., Schrooyen F., Doggen J., Renckens K. Paper ticketing vs. Electronic Ticketing based on off-line system 'Tapango'; Proceedings of the Second International Workshop on Near Field Communication (NFC); Monaco. 20 April 2010; pp. 3–8. [Google Scholar]

164. Widmann R., Grunberger S., Stadlmann B., Langer J. System integration of NFC ticketing into an existing public transport infrastructure; Proceedings of the 2012 4th International Workshop on Near Field Communication (NFC); Helsinki, Finland. 13 March 2012; pp. 13–18. [Google Scholar]

165. Nasution S.M., Husni E.M., Wuryandari A.I. Prototype of train ticketing application using near field communication (NFC) technology on Android device; Proceedings of the 2012 International Conference on System Engineering and Technology (ICSET); Bandung, Indonesia. 11–12 September 2012; pp. 1–6. [Google Scholar]

166. Wu W.J., Lee W.H. An NFC E-ticket system with offline authentication; Proceedings of the 2013 9th International Conference on Information, Communications and Signal Processing (ICICS); Tainan, Taiwan. 10–13 December 2013; pp. 1–5. [Google Scholar]

167. Cha S.C., Joung Y.J., Tseng Y.C., Huang S.C., Chen G.H., Tseng C.T. Ensuring the integrity and non-repudiation of remitting e-invoices in conventional channels with commercially available NFC devices; Proceedings of the 2014 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD); Las Vegas, NV, USA. 30 June–2 July 2014; pp. 1–6. [Google Scholar]

168. Saminger C., Grunberger S., Langer J. An NFC ticketing system with a new approach of an inverse reader mode; Proceedings of the 2013 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–5. [Google Scholar]

169. Dominikus S., Aigner M. mCoupons: An application for near field communication (NFC); Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops Volume: 2; Niagara Falls, ON, Canada. 21–23 May 2007; pp. 421–428. [Google Scholar]

170. Hsiang H.C., Kuo H.C., Shih W.K. A secure mCoupon scheme using near field communication. Int. J. Innov. Comput. Inf. Control. 2009;5:3901–3909. [Google Scholar]

171. Hsiang H.C. A Secure and Efficient Authentication Scheme for M-Coupon Systems; Proceedings of the 2014 8th International Conference on Future Generation Communication and Networking (FGCN); Haikou, China. 20–23 December 2014; pp. 17–20. [Google Scholar]

172. Sánchez-Silos J.J., Velasco-Arjona F.J., Ruiz I.L., Gomez-Nieto M.A. An NFC-Based Solution for Discount and Loyalty Mobile Coupons; Proceedings of the 2012 4th International Workshop on Near Field Communication (NFC); Helsinki, Finland. 13 March 2012; pp. 45–50. [Google Scholar]

173. Borrego-Jaraba F., Garrido P.C., García G.C., Ruiz I.L., Gómez-Nieto M.Á. A Ubiquitous NFC Solution for the Development of Tailored Marketing Strategies Based on Discount Vouchers and Loyalty Cards. Sensors. 2013;13:6334–6354. doi: 10.3390/s130506334. [DOI] [PMC free article] [PubMed] [Google Scholar]

174. Ozdenizci B., Coskun V., Aydin M.N., Ok K. NFC loyal: A beneficial model to promote loyalty on smart cards of mobile devices; Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST); London, UK. 8–11 November 2010; pp. 1–6. [Google Scholar]

175. Ozdenizci B., Ok K., Coskun V. NFC Loyal for Enhancing Loyalty Services through Near Field Communication. Wirel. Pers. Commun. 2013;68:1923–1942. doi: 10.1007/s11277-012-0556-z. [DOI] [Google Scholar]

176. Coskun V., Ozdenizci B., Ok K., Alsadi M., Soylemezgiller F. Design and Development of NFC Enabled Loyalty System; Proceedings of the 6th International Conference of Advanced Computer Systems and Networks: Design and Application; Lviv, Ukraine. 16–18 September 2013; pp. 42–45. [Google Scholar]

177. Ozdenizci B., Ok K., Alsadi M., Coskun V., Soylemezgiller F. Development of NFC enabled loyalty application: Technical and business opportunities. Acad. J. Sci. (AJS) 2014;3:141–149. [Google Scholar]

178. Ninomiya H., Ito E., Flanagan B., HIrokawa S. Bridging SNS ID and User Using NFC and SNS; Proceedings of the 2012 International Conference on Anti-Counterfeiting, Security and Identification (ASID); Taipei, Taiwan. 24–26 August 2012; pp. 1–5. [Google Scholar]

179. Ninomiya H., Flanagan B., Ito E., Hirokawa S. Near friends communication encouragement system using NFC and SNS; Proceedings of the 2012 IIAI International Conference on Advanced Applied Informatics (IIAIAAI); Fukuoka, Japan. 20–22 September 2012; pp. 145–148. [Google Scholar]

180. Fressancourt A., Hérault C., Ptak E. NFCSocial: Social networking in mobility through IMS and NFC; Proceedings of the 2009 First International Workshop on Near Field Communication; Hagenberg, Austria. 24 February 2009; pp. 24–29. [Google Scholar]

181. Kneißl F., Rottger R., Sandner U., Leimeister J.M., Krcmar H. All-i-touch as combination of NFC and lifestyle; Proceedings of the 2009 First International Workshop on Near Field Communication; Hagenberg, Austria. 24 February 2009; pp. 51–55. [Google Scholar]

182. Gaito S., Quadri C., Rossi G.P., Zignani M. THINPLE-the new online Sociality is built on top of NFC-based Contacts; Proceedings of the 2012 IFIP Wireless Days (WD); Dublin, Ireland. 21–23 November 2012; pp. 1–5. [Google Scholar]

183. Doan A., Ramakrishnan R., Halevy A.Y. Crowdsourcing systems on the world-wide web. Commun. ACM. 2011;54:86–96. doi: 10.1145/1924421.1924442. [DOI] [Google Scholar]

184. Barron J.P.G., Manso M.A., Alcarria R., Gomez R.P. A mobile crowdsourcing platform for urban infrastructure maintenance; Proceedings of the 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS); Birmingham, UK. 2–4 July 2014; pp. 358–363. [Google Scholar]

185. Lochrie M., Burnett D., Coulton P. Using NFC check-ins to crowd curate music preferences; Proceedings of the 2013 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

186. McDonald's adds NFC games to restaurant tables. [(accessed on 13 April 2015)]. Available online: http://www.nfcworld.com/2013/07/15/324977/mcdonalds-adds-nfc-games-to-restaurant-tables/

187. Broll G., Graebsch R., Scherr M., Boring S., Holleis P., Wagner M. Touch to Play—Exploring Touch-Based Mobile Interaction with Public Displays; Proceedings of the 2011 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 15–20. [Google Scholar]

188. Christin D., Buttner C., Repp N. CachedSensing: Exploring and documenting the environment as a treasure hunt; Proceedings of the 2012 IEEE 37th Conference on Local

Computer Networks Workshops (LCN Workshops); Clearwater, FL, USA. 22–25 October 2012; pp. 973–981. [Google Scholar]

189. Garrido P.C., Miraz G.M., Ruiz I.L., Gomez-Nieto M.A. Near field communication in the development of ubiquitous games; Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions (ICITST); London, UK. 8–11 November 2010; pp. 1–7. [Google Scholar]

190. Brassai B., Varga B., Simon K., Torok-Vistai T. GeoQuesting: Mobile adventure game and web-based game editor; Proceedings of the 2014 IEEE 12th International Symposium on Intelligent Systems and Informatics (SISY); Subotica, Serbia. 11–13 September 2014; pp. 99–103. [Google Scholar]

191. Nandwani A., Coulton P. NFC mobile parlor games enabling direct player to player interaction; Proceedings of the 2011 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 21–25. [Google Scholar]

192. Idowu S., Hagos D.H., Tesfay W.B., Famurewa A., Rana J., Synnes K. NexTrend: Context-Aware Music-Relay Corridors Using NFC Tags; Proceedings of the 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS); Taichung, Taiwan. 3–5 July 2013; pp. 573–578. [Google Scholar]

193. Ebner M., Maierhuber M. Near Field Communication-Which Potentials Does NFC Bring for Teaching and Learning Materials? Int. J. Interact. Mob. Technol. (IJIM) 2013;7:9–14. doi: 10.3991/ijim.v7i4.3019. [DOI] [Google Scholar]

194. Miraz G.M., Ruiz I.L., Gómez-Nieto M.A. How NFC can be used for the compliance of European higher education area guidelines in European universities; Proceedings of the 2009 First International Workshop on Near Field Communication; Hagenberg, Austria. 24 February 2009; pp. 3–8. [Google Scholar]

195. Rios-Aguilar S., González-Crespo R., de-la-Fuente-Valentin L. Anonymous Assessment Information System for Higher Education Using Mobile Devices; Proceedings of the 2014 IEEE 14th International Conference on Advanced Learning Technologies (ICALT); Athens, Greece. 7–10 July 2014; pp. 157–161. [Google Scholar]

196. Bueno-Delgado M.V., Pavon-Marino P., De-Gea-Garcia A., Dolon-Garcia A. The smart university experience: An NFC-based ubiquitous environment; Proceedings of the 2012

Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS); Palermo, Italy. 4–6 July 2012; pp. 799–804. [Google Scholar]

197. Garrido P.C., Miraz G.M., Ruiz I.L., Gomez-Nieto M.A. Use of NFC-based pervasive games for encouraging learning and student motivation; Proceedings of the 2011 3rd International Workshop on Near Field Communication (NFC); Hagenberg, Austria. 22 February 2011; pp. 32–37. [Google Scholar]

198. Wang C.C., Wei C.R. The Implementation of a Context-Aware Mobile Japanese Conversation Learning System Based on NFC-enabled Smartphones; Proceedings of the 2014 IIAI 3rd International Conference on Advanced Applied Informatics (IIAIAAI); Kitakyushu, Japan. 31 August–4 September 2014; pp. 313–317. [Google Scholar]

199. Ruiz L. NFC solution for access to bibliographic sources; Proceedings of the 2012 IEEE Global Engineering Education Conference (EDUCON); Marrakech, Morocco. 17–20 April 2012; pp. 1–7. [Google Scholar]

200. Broll G., Vodicka E., Boring S. Exploring multi-user interactions with dynamic NFC-displays. Pervasive Mob. Comput. 2013;9:242–257. doi: 10.1016/j.pmcj.2012.09.007. [DOI] [Google Scholar]

201. Hardy R., Rukzio E., Wagner M., Paolucci M. Exploring expressive NFC-based mobile phone interaction with large dynamic displays; Proceedings of the 2009 First International Workshop on Near Field Communication; Hagenberg, Austria. 24 February 2009; pp. 36–41. [Google Scholar]

202. Volland D., Noyen K., Kayikci O., Ackermann L., Michahelles F. Switching the role of NFC tag and reader for the implementation of Smart Posters; Proceedings of the 2012 4th International Workshop on Near Field Communication (NFC); Helsinki, Finland. 13 March 2012; pp. 63–68. [Google Scholar]

203. Pesonen J., Horster E. Near field communication technology in tourism. Tour. Manag. Perspect. 2012;4:11–18. doi: 10.1016/j.tmp.2012.04.001. [DOI] [Google Scholar]

204. Hsieh M.Y., Wu T.Y., Tsai Y.T., Shih C.H., Li K.C. Interactive design using non-touch technologies for group trip; Proceedings of the 2012 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS); New Taipei, Taiwan. 4–7 November 2012; pp. 216–221. [Google Scholar]

205. Yan-Guang C., Ya-ming Z., Tao Z., Yi Y. A Hybrid Ontology Knowledge Integration for Farm-based Tourism with NFC; Proceedings of the Fourth International Conference on

Instrumentation and Measurement, Computer, Communication and Control; Harbin, China. 18–20 September 2014; pp. 548–553. [Google Scholar]

206. Basili A., Liguori W., Palumbo F. NFC Smart Tourist Card: Combining Mobile and Contactless Technologies towards a Smart Tourist Experience; Proceedings of the 2014 IEEE 23rd International WETICE Conference (WETICE); Parma, Italy. 23–25 June 2014; pp. 249–254. [Google Scholar]

207. Paradowski D., Kruger A. Modularization of mobile shopping assistance systems; Proceedings of the 2013 5th International Workshop on Near Field Communication (NFC); Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

208. De Luca G., Lillo P., Mainetti L., Mighali V., Patrono L., Sergi I. The use of NFC and Android technologies to enable a KNX-based smart home; Proceedings of the 2013 21st International Conference on Software, Telecommunications and Computer Networks (SoftCOM); Primosten, Croatia. 18–20 September 2013; pp. 1–7. [Google Scholar]

209. Di Rosa E., Benente F. “Excavate and learn”: Enhancing visitor experience with touch and NFC; Proceedings of the 2013 Digital Heritage International Congress (Volume: 2); Marseille, France. 28 October–1 November 2013; pp. 689–692. [Google Scholar]

210. Jara A.J., Skarmeta A.F., Parra M.C. Enabling Participative Marketing through the Internet of Things; Proceedings of the 2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA); Barcelona, Spain. 25–28 March 2013; pp. 1301–1306. [Google Scholar]

211. Argueta D., Lu Y.T., Ma J., Rodriguez D., Yang Y.H., Phan T., Jeon W. Enhancing the restaurant dining experience with an NFC-enabled mobile user interface. Mob. Comput. Appl. Serv. 2014;130:314–321. [Google Scholar]

212. Ramanathan R., Imtiaz J. NFC in industrial applications for monitoring plant information; Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT); Tiruchengode, India. 4–6 July 2013; pp. 1–4. [Google Scholar]

213. Lee S., Lee T., Kim K.H., Hong M. A fast and efficient wireless AP connection approach based on NFC Tag; Proceedings of the 2013 International Conference on ICT Convergence; Jeju, Korea. 14–16 October 2013; pp. 1076–1077. [Google Scholar]

214. Caimei H., Zhikun H., Yuefeng Y., Jian W., Ruonan Y. Design of reverse search car system for large parking lot based on NFC technology; Proceedings of the 26th Chinese Control and

Decision Conference; Changsha, China. 31 May–2 June 2014; pp. 5054–5056. [Google Scholar]

215. Ang J.T., Chin S.W., Chin J.H., Choo Z.X., Chang Y.M. iSCAPS-Innovative Smart Car Park System integrated with NFC technology and e-Valet function; Proceedings of the 2013 World Congress on Computer and Information Technology (WCCIT); Sousse, Tunisia. 22–24 June 2013; pp. 1–6. [Google Scholar]

216. Ok K., Coskun V., Aydin M.N. Usability of mobile voting with NFC technology; Proceedings of IASTED International Conference on Software Engineering; Innsbruck, Austria. 16–18 February 2010; pp. 151–158. [Google Scholar]

217. Mulliner C. Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones; Proceedings of the International Conference on Availability, Reliability and Security; Fukuoka, Japan. 16–19 March 2009; pp. 695–700. [Google Scholar]

218. Roland M., Langer J., Scharinger J. Security Vulnerabilities of the NDEF Signature Record Type; Proceedings of the 3rd International Workshop on Near Field Communication; Hagenberg, Austria. 22 February 2011; pp. 65–70. [Google Scholar]

219. Saeed M.Q., Walter C.D. Off-line NFC Tag Authentication; Proceedings of the International Conference Internet Technology and Secured Transactions; London, UK. 10–12 December 2012; pp. 730–735. [Google Scholar]

220. Lehtonen M., Staake T., Michahelles F. Networked RFID Systems and Lightweight Cryptography. Springer; Berlin/Heidelberg, Germany: 2008. From Identification to Authentication–A Review of RFID Product Authentication Techniques; pp. 169–187. [Google Scholar]

221. Saeed M.Q., Bilal Z., Walter C.D. An NFC Based Consumer-Level Counterfeit Detection Framework; Proceedings of the Eleventh Annual International Conference on Privacy, Security and Trust (PST); Tarragona, Spain. 10–12 July 2013; pp. 135–142. [Google Scholar]

222. Plos T., Hutter M., Feldhofer M., Stiglic M., Cavaliere F. Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography. IEEE Trans. Large Scale Integr. (VLSI) Syst. 2012;21:1965–1974. doi: 10.1109/TVLSI.2012.2227849. [DOI] [Google Scholar]

223. Mitrokotsa A., Rieback M.R., Tanenbaum A.S. Classification of RFID Attacks. J. Inf. Syst. Front. 2010;12:491–505. doi: 10.1007/s10796-009-9210-z. [DOI] [Google Scholar]

224. Roland M., Langer J., Scharinger J. Practical Attack Scenarios on Secure Element-Enabled Mobile Devices; Proceedings of the 4th International Workshop on Near Field Communication; Helsinki, Finland. 13 March 2012; pp. 19–24. [Google Scholar]

225. Alimi V., Vernois S., Rosenberger C. Analysis of Embedded Applications by Evolutionary Fuzzing; Proceedings of the International Conference on High Performance Computing Simulation (HPCS); Bologna, Spain. 21–25 July 2014; pp. 551–557. [Google Scholar]

226. Roland M., Langer J., Scharinger J. Applying Relay Attacks to Google Wallet; Proceedings of the 5th International Workshop on Near Field Communication; Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

227. Ceipidor U.B., Medaglia C.M., Marino A., Morena M., Sposato S., Moroni A., Morgia M.L. Mobile ticketing with NFC management for transport companies.Problems and solutions; Proceedings of the 5th International Workshop on Near Field Communication; Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

228. Abu-Saymeh D., Abou-Tair D.D., Zmily A. An Application Security Framework for Near Field Communication; Proceedings of 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications; Melbourne, Australia. 16–18 July 2013; pp. 396–403. [Google Scholar]

229. Cheong S.N., Ling H.C., Teh P.L. Secure Encrypted Steganography Graphical Password Scheme For Near Field Communication Smartphone Access Control System. Expert Syst. Appl. 2014;41:3561–3568. doi: 10.1016/j.eswa.2013.10.060. [DOI] [Google Scholar]

230. Alshehri A., Briffa J.A., Schneider S., Wesemeyer S. Formal Security Analysis of NFC M-Coupon Protocols Using Casper/FDR; Proceedings of the 5th International Workshop on Near Field Communication; Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

231. Eun H., Lee H., Oh H. Conditional privacy preserving security protocol for NFC applications. IEEE Trans. Consumer Electron. 2013;59:153–160. doi: 10.1109/TCE.2013.6490254. [DOI] [Google Scholar]

232. Chattha N.A. NFC-Vulnerabilities and Defense; Proceedings of the Conference on Information Assurance and Cyber Security; Rawalpindi, Pakistan. 12–13 June 2014; pp. 35–38. [Google Scholar]

233. Haselsteiner E., Breitfuß K. Security in Near Field Communication (NFC) Strengths and Weaknesses. [(accessed on 13 April 2015)]. Available online:

http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf .

234. ECMA 385: NFC-SEC (NFCIP-1 Security Services and Protocol), ECMA International. [(accessed on 13 April 2015)]. Available online: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-385.pdf .

235. Elbaoury A., Mohsen A., Ramadan M., Youssef M. Practical Provably Secure Key Sharing For Near Field Communication Devices; Proceedings of the International Conference on Computing, Networking and Communications; San Diego, CA, USA. 28–31 January 2013; pp. 750–755. [Google Scholar]

236. Jung M.S. A Study on Electronic-Money Technology Using Near Field Communication. Symmetry. 2014;7:1–14. doi: 10.3390/sym7010001. [DOI] [Google Scholar]

237. Urien P., Piramuthu S. Elliptic Curve-Based RFID/NFC Authentication with Temperature Sensor Input for Relay Attacks. Decis. Support Syst. 2014;59:28–36. doi: 10.1016/j.dss.2013.10.003. [DOI] [Google Scholar]

238. Ceipidor U.B., Medaglia C.M., Marino A., Sposato S., Moroni A. KerNeeS: A Protocol for Mutual Authentication between NFC Phones and POS Terminals for Secure Payment Transactions; Proceedings of the 9th International ISC Conference on Information Security and Cryptology (ISCISC); Tabriz, Iran. 13–14 September 2012; pp. 115–120. [Google Scholar]

239. Urien P., Piramuthu S. Framework and Authentication Protocols for Smartphone, NFC, and RFID in Retail Transactions; Proceedings of the IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing; Melbourne, Australia. 2–5 April 2013; pp. 77–82. [Google Scholar]

240. Abughazalah S., Markantonakis K., Mayes K. Secure Mobile Payment on NFC-Enabled Mobile Phones Formally Analysed Using CasperFDR; Proceedings of the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications; Beijing, China. 24–26 September 2014; pp. 422–431. [Google Scholar]

241. Thammarat C., Chokngamwong R., Techapanupreeda C., Kungpisdan S. A Secure Lightweight Protocol for NFC Communications with Mutual Authentication Based on Limited-Use of Session Keys; Proceedings of the International Conference on Information Networking; Siem Reap, Cambodia. 12–14 January 2015; pp. 133–138. [Google Scholar]

242. Druml N., Menghin M., Kuleta A., Steger C., Weiss R., Bock H., Haid J. A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems; Proceedings of the 17th Euromicro Conference on Digital System Design; Verona, Italy. 27–29 August 2014; pp. 372–378. [Google Scholar]

243. Urien P. EMV-TLS, A Secure Payment Protocol for NFC Enabled Mobiles; Proceedings of the 2014 International Conference on Collaboration Technologies and Systems; Minneapolis, MN, USA. 19–23 May 2014; pp. 203–21. [Google Scholar]

244. Vincent J., Alimi V., Plateaux A., Gaber C., Pasquet M. A Mobile Payment Evaluation Based on a Digital Identity Representation; Proceedings of the International Conference on Collaboration Technologies and Systems (CTS); Denver, CO, USA. 21–25 May 2012; pp. 410–418. [Google Scholar]

245. Luo J.N., Yang M.H., Yang M.C. An Anonymous Car Rental System Based on NFC; Proceedings of the International Symposium on Biometrics and Security Technologies; Chengdu, China. 2–5 July 2013; pp. 97–104. [Google Scholar]

246. Rukzio E., Leichtenstern K., Callaghan V., Holleis P., Schmidt A., Chin J. An Experimental Comparison of Physical Mobile Interaction Techniques: Touching, Pointing and Scanning; Proceedings of 8th International Conference (UbiComp 2006); Orange County, CA, USA. 17–21 September 2006; pp. 87–104. [Google Scholar]

247. Broll G., Vodicka E., Boring S. Exploring Multi-User Interactions With Dynamic NFC-Displays. Pervasive Mob. Comput. 2013;9:242–257. doi: 10.1016/j.pmcj.2012.09.007. [DOI] [Google Scholar]

248. Chen L., Pan G., Li S. Touch-driven Interaction between Physical Space and Cyberspace with NFC; Proceedings of the International Conference on and 4th International Conference on Cyber, Physical and Social Computing, Internet of Things; Dalian, China. 19–22 October 2011; pp. 258–265. [Google Scholar]

249. Chen K., Chang M. User Acceptance of 'Near Field Communication' Mobile Phone Service: An Investigation Based on the 'Unified Theory of Acceptance and Use of Technology' Model. Serv. Ind. J. 2013;33 doi: 10.1080/02642069.2011.622369. [DOI] [Google Scholar]

250. Mehmood F., Hassannezhad M., Abbas T. Analytical Investigation of Mobile NFC Adaption With SWOT-AHP Approach: A Case of Italian Telecom. Procedia Technol. 2014;12:535–541. doi: 10.1016/j.protcy.2013.12.526. [DOI] [Google Scholar]

251. Franssila H. User Experiences and Acceptance Scenarios of NFC Applications in Security Service Field Work; Proceedings of the Second International Workshop on Near Field Communication (NFC); Monaco. 20 April 2010; pp. 39–44. [Google Scholar]

252. Broll G., Palleis H., Richter H., Wiethoff A. Exploring Multimodal Feedback for an NFC-Based Mobile Shopping Assistant; Proceedings of the 5th International Workshop on Near Field Communication; Zurich, Switzerland. 5 February 2013; pp. 1–6. [Google Scholar]

253. Thomas J.P., Andreas S., Frédéric T., Elgar F. NFC Based Service Innovation in Retail: An Explorative Study; Proceedings of the 17th European Conference on Information Systems; Verona, Italy. 8–10 June 2009; pp. 1–9. [Google Scholar]

254. Pham T.T.T., Ho J.C. What Are The Core Drivers In Consumer Adoption of NFC-Based Mobile Payments? A Proposed Research Framework; Proceedings of the International Conference on Management of Engineering Technology (PICMET); Kanazawa, Japan. 27–31 July 2014; pp. 3041–3049. [Google Scholar]

255. Alshahrani A.M., Colchester U.K., Walker S. NFC performance in mobile payment service compared with a SMS -based solution; Proceedings of the International Conference on Green Computing, Communication and Conservation of Energy; Chennai, India. 12–14 December 2013; pp. 282–286. [Google Scholar]

256. Ceipidor U.B., Medaglia C.M., Opromolla A., Volpi V., Moroni A., Sposato S. A Survey about User Experience Improvement in Mobile Proximity Payment; Proceedings of the 4th International Workshop on Near Field Communication; Helsinki, Finland. 13 March 2012; pp. 51–56. [Google Scholar]

257. Leong L.Y., Hew T.S., Tan G.W.H., Ooi K.B. Predicting the Determinants of the NFC-Enabled Mobile Credit Card Acceptance: A Neural Networks Approach. Expert Syst. Appl. 2013;40:5604–5620. doi: 10.1016/j.eswa.2013.04.018. [DOI] [Google Scholar]

258. Häikiö J., Wallin A., Isomursu M., Ailisto H., Matinmikko T., Huomo T. Touch-Based User Interface for Elderly Users; Proceedings of the 9th International Conference on Human Computer Interaction with Mobile Devices and Services; Singapore. 11–14 September 2007; pp. 289–296. [Google Scholar]

259. Two In Three Phones to Come With NFC in 2018, NFC World. [(accessed on 13 April 2015)]. Available online: http://www.nfcworld.com/2014/02/12/327790/two-three-phones-come-nfc-2018/

260. Madlmayr G., Langer J., Scharinger J. Managing an NFC Ecosystem; Proceedings of the 7th International Conference on Mobile Business; Barcelona, Spain. 7–8 July 2008; pp. 95–101. [Google Scholar]

261. Akram R.N., Markantonakis K., Mayes K. Building the Bridges—A Proposal for merging different Paradigms in Mobile; Proceedings of the Eighth International Conference on Computational Intelligence and Security (CIS); Guangzhou, China. 17–18 November 2012; pp. 646–652. [Google Scholar]

262. Benyó B., Sódor B., Fordos G., Kovács L., Vilmos A. A Generalized Approach for NFC Application Development; Proceedings of the Second International Workshop on Near Field Communication; Monaco. 20 April 2010; pp. 45–50. [Google Scholar]

263. Aziza H. NFC Technology in Mobile Phone Next-Generation Services; Proceedings of the Second International Workshop on Near Field Communication; Monaco. 20 April 2010; pp. 21–26. [Google Scholar]

264. Akram R.N., Markantonakis K., Sauveron D. Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager; Proceedings of the 13th International Conference on Trust, Security and Privacy in Computing and Communications; Beijing, China. 24–26 September 2014; pp. 448–456. [Google Scholar]

265. Benyo B., Vilmos A., Kovacs K., Kutor L. NFC Applications and Business Model of the Ecosystem; Proceedings of the 16th IST Mobile and Wireless Communications Summit; Budapest, Hungary. 1–5 July 2007; pp. 1–5. [Google Scholar]

266. Ok K., Coskun V., Ozdenizci B., Aydin M.N. A Role-Based Service Level NFC Ecosystem Model. Wirel. Pers. Commun. 2013;68:811–841. doi: 10.1007/s11277-011-0484-3. [DOI] [Google Scholar]

267. Ozdenizci B., Aydin M.N., Coskun V., Ok K. NFC Research Framework: A Literature Review and Future Research Directions; Proceedings of the 14th International Business Information Management Association Conference on Global Business Transformation through Innovation and Knowledge Management; Istanbul, Turkey. 23–24 June 2010; pp. 23–24. [Google Scholar]

268. Ozdenizci B., Aydin M.N., Coskun V., Ok K. Design Science in NFC Research; Proceedings of IEEE International Conference for Internet Technology and Secured Transactions; London, UK. 8–11 November 2010; pp. 1–6. [Google Scholar]

269. The Host Card Emulation in Payments: Options for Financial Institutions, Mobey Forum, White Paper. [(accessed on 13 April 2015)]. Available online: http://www.mobeyforum.org/whitepaper/the-host-card-emulation-in-payments-options-for-financial-institutions/

Articles from Sensors (Basel, Switzerland) are provided here courtesy of **Multidisciplinary Digital Publishing Institute (MDPI)**