DEVELOPMENT OF AN ELECTRONIC MAIL ENVIRONMENT WITH NFC TECHNOLOGY EXTENSION

KEREM OK

B.S., Information Technology Işık University, 2006

Submitted to the Graduate School of Science and Engineering
in partial fulfillment of the requirements for the degree of
Master of Science
in
Information Technology

IŞIK UNIVERSITY

2010

IŞIK UNIVERSITY

GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

DEVELOPMENT OF AN ELECTRONIC MAIL ENVIRONMENT WITH NFC TECHNOLOGY EXTENSION

KEREM OK

APPROVED BY:

Assist. Prof. Vedat COŞKUN _____
(Thesis Supervisor)

Assist. Prof. Hacı Ali MANTAR _____

Assist. Prof. Mehmet N. AYDIN _____

APPROVAL DATE: 12/01/2010

DEVELOPMENT OF AN ELECTRONIC MAIL ENVIRONMENT
WITH NFC TECHNOLOGY EXTENSION

Abstract

E-mail is one of today's widely used communication tools. Mobility, which is defined as being free from any geographical restrictions to make use of any service, is a very important requirement for the users to access e-mail data. The aim of this study is to develop a web based mail server application, and a mobile mail client application to provide an e-mail service for the users which gives the opportunity to reach their e-mails from anywhere they want. MailMoby webmail application enables users to reach their mailboxes from their browsers while they are on the Internet. On the other hand, MobileMoby, the mobile client application, enables access to mailbox using their Java-enabled smart phones.

Mobile technologies are growing fast to satisfy mobility requirements; one of these rapidly growing mobile technologies is NFC (Near Field Communication). In addition to the e-mail applications development, NFC is studied, and usability of an NFC application is tested through MobileMoby.

BİR ELEKTRONİK POSTA ORTAMININ GELİŞTİRİLMESİ
VE YAKIN SAHA İLETİŞİMİ UYGULAMASI

Özet

Elektronik posta günümüzde yaygın olarak kullanılan iletişim araçlarından bir tanesidir. Coğrafi kısıtlamalardan bağımsız olarak servis kullanımı olarak tanımlanan hareketlilik (taşınırlık), kullanıcıların elektronik postalarına ulaşabilmeleri için önemli bir gereksinimdir. Bu çalışmanın amacı internet tabanlı ve mobil tabanlı elektronik posta uygulamalarını geliştirerek, kullanıcılara elektronik posta hizmeti sağlamak ve elektronik postalarına istedikleri her yerden ulaşabilmelerini sağlamaktır. İnternet tabanlı MailMoby Uygulaması kullanıcıların tarayıcılarını kullanarak, internet üzerinden elektronik posta kutularına ulaşmalarını sağlamaktadır. Diğer taraftan, MobileMoby kullanıcıların Java destekleyen telefonları üzerinden elektronik postalarına ulaşmalarını sağlamaktadır.

Mobil teknolojilerin hızla geliştiği günümüzde, bu teknolojilerden biri de "Yakın Saha İletişimi"dir. Elektronik posta uygulamalarının geliştirilmesine ek olarak, bu teknoloji çalışılmış, araştırılmış ve bu teknolojiyi kullanan bir uygulamanın kullanılabilirliği MobileMoby uygulamasının da yardımıyla test edilmiştir.

Acknowledgements

I'm sincerely grateful to my supervisor Assist. Prof. Vedat Coşkun for his incredible guidance, support, encouragement and help through my thesis and my graduate study. I also thank him for his faith in me. I would also like to thank all of my faculty staff for their help through my graduate education.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

API	Application Programming Interface
CLDC	Connected Limited Device Configuration
CSS	Cascading Style Sheets
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IASTED	International Association of Science and Technology for Development
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
ISO	International Organization for Standardization
J2ME	Java Platform, Micro Edition
JSP	Java Server Pages
Kbit	Kilobit
MHz	Megahertz
MIDP	Mobile Information Device Profile
MTA	Mail Transfer Agent
MUA	Mail User Agent
NFC	Near Field Communication
OTA	Over The Air Transfer
POP3	Post Office Protocol
RFC	Request For Comments
RFID	Radio-frequency Identification
SMTP	Simple Mail Transfer Protocol
W3C	World Wide Web Consortium
WWW	World Wide Web

WYSIWYG	What You See Is What You Get
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language

Chapter 1

Introduction

Communication is one of the most important needs for human being. People need to communicate with each other in order to express their opinions, feelings, and thoughts. Developments in technology helped on this issue and offered new possibilities to improve the way that humans communicate. One of these communication technologies that is widely used in both social and business life is e-mail. E-mail is described as a method of exchanging digital messages [1]. It is a communication way that occurs in computer networks.

An e-mail environment requires especially two important components, namely MTA (Mail Transfer Agent), and MUA (Mail User Agent). MTA processes and stores user e-mails, and is the heart of the whole system. Users need MUA in order to send and receive e-mails. MUA can be either a client application that is installed on a local machine, or a webmail that works on a server and accessed via WWW (World Wide Web). In case of web based usage, web server prepares the pages to be displayed on client's web client.

In order to process e-mails of a client, such as sending or receiving e-mails, MUA communicates with the local MTA; on the other hand local MTA performs the transfer operations (sending and receiving) over computer networks with the remote MTAs.

A webmail web server enables sending, receiving, and additional processing services using a web client (browser) over a network, such as the Internet. By the rises in e-mail communication webmail usage is increased, and webmail interface and services became important to provide better and more services to people. Additional need for mobility is arisen for e-mail communication to send and receive e-mails without any geographical restriction.

In this study, we have analyzed the requirements, after which we have developed MailMoby webmail server application and MobileMoby client application. Webmail application provides an easy-to-use interface and additional services to users. It doesn't require additional software for computers; only a web browser installed on a client's computer is enough to access. Additionally a mobile application is developed to eliminate geographical restrictions, since it allows users to send and receive e-mails using mobile phones from wherever they want.

The motivations behind this study are as follows:

- Building a webmail application using Java technology, which includes advanced features, and has easy-to-use interface,
- Building a mobile client to provide mobile access to e-mails,
- Researching mobile technologies and integrating NFC technology in mobile applications.

The remainder of this document is organized as follows. Chapter 2 consists of background information of e-mail, and standards and tools used in MailMoby webmail server application and MobileMoby client application.

Chapter 3 consists of detailed information about MailMoby webmail server application.

Chapter 4 consists of MobileMoby client application and its features.

Chapter 5 consists of definition of an emerging technology NFC, and its usage areas and presents a study on this subject.

In chapter 6, developed remote electronic voting system using NFC and its usability is presented.

Finally conclusion of my thesis is presented in chapter 7.

Chapter 2

Background Information

2.1 Electronic Mail

Electronic mail, or abbreviated as e-mail, is a method of exchanging digital messages between a sender and one or more receivers over a computer network, traditionally the Internet. E-mail servers are based on a store-and-forward model in which, they accept, forward, deliver, and store messages [1].

An electronic mail message consists of two components, the message header, and the message body [2]. The message header contains control information, and the body contains the actual content to be sent. The body originally consisted of only text based content, standardized by RFC 2045 through RFC 2049, collectively called, Multipurpose Internet Mail Extensions (MIME) [3, 4, 5, 6, 7]. As of these standards, the body may also include multimedia content such as files and audio, video attachments. Currently available header fields are listed below.

- **From**: The e-mail address, and optionally the name of the author(s).
- **Sender**: Address of the actual sender acting on behalf of the author listed in the *from* field (secretary, list manager, etc.).
- **To**: The e-mail address(es), and optionally name(s) of the message's recipient(s).
- **Cc**: Carbon copy; many e-mail clients will mark e-mail in your inbox differently depending on whether you are in the To: or Cc: list.
- **Bcc**: Blind Carbon Copy; addresses added to the SMTP (Simple Mail Transfer Protocol) delivery list but not (usually) listed in the message data, remaining invisible to other recipients.
- **Subject**: A brief summary of the topic of the message.
- **Date**: The local time and date when the message was written.

- **Message-ID**: An automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To: (see below).
- **Content-Type**: Information about how the message is to be displayed, usually a MIME type.
- **Reply-To**: Address that should be used to reply to the message.
- **In-Reply-To**: Message-ID of the message that this is a reply to. Used to link related messages together.
- **Precedence**: used to indicate that automated "vacation" or "out of office" responses should not be returned for this mail, e.g. to prevent vacation notices from being sent to all other subscribers of a mailing list.
- **Received**: Tracking information generated by mail servers that have previously handled a message, in reverse order (last handler first).
- **References**: Message-ID of the message that this is a reply to, and the message-id of the message the previous was reply a reply to, etc.
- **X-Face**: Small icon.

2.2 Electronic Mail Architecture

A user may need to use an e-mail client, or more formally a MUA to access e-mail server, or more formally a MTA which handles actual exchange of the electronic messages. A MUA is either a desktop e-mail client application or a webmail which is intended to be accessed via a web browser. The desktop application may be a standalone application running on a computer, or running on a mobile device, such as a mobile phone. Electronic mail architecture, in which the sender uses a web based e-mail client, and the receiver uses a standalone e-mail client working on a mobile phone, is shown in Figure 2.1.

A scenario to include an e-mail exchange between the sender and the receiver can be summarized as follows. Please note that number of the items is also depicted in the related figure.

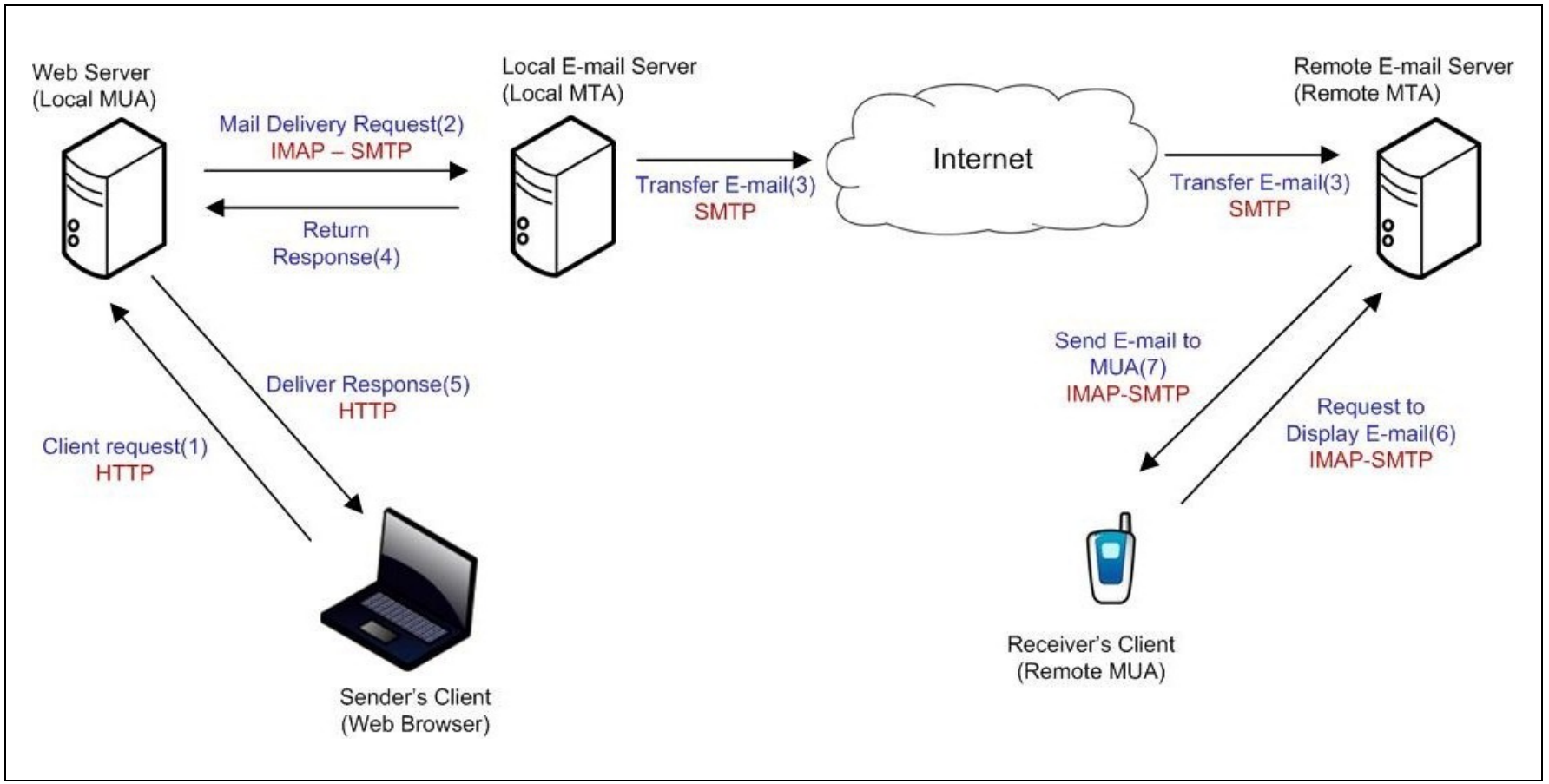

Figure 2.1. Electronic Mail Architecture

1. Sender composes the mail, after which she sends a request to the local MUA to transfer the mail.
2. Local MUA sends request to local MTA to transfer the mail to the remote MTA(s)
3. Local MTA tries to communicate with remote MTA after receiving the transfer request. The communication is performed as soon as the remote MTA becomes available. Both MTAs create a peer-to-peer connection for this purpose.
4. Local MTA returns response to local MUA about successful delivery of the mail.
5. Local MUA displays this notification to user via browser
6. Receiver requests to display the received mails
7. Remote MTA sends the mail to the remote MUA, after which the mail is displayed on the remote client.

2.3 Comparison of Desktop and Web Based E-mail Clients

E-mail clients display the received mails and related information as requested by the user. There are two different types of e-mail clients; Desktop applications and Webmail applications.

Desktop Applications: Executable codes of client applications are installed to, and executed on the client machine. It uses client's processing power to process e-mails. Some of the currently available examples are Microsoft Outlook, Mozilla Thunderbird, Eudora, and Windows Live Mail.

Webmail Applications: Webmail applications run on web servers and are accessed via web browser, such as Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, Netscape Navigator, and Opera. Client machine uses Internet connections to access the webmail server application. Main processing is performed at web server, after which the web client on the client machine is responsible only from displaying the results. Web server communicates with e-mail server and performs the required operations. Some of favorite webmail applications are Hotmail, Yahoo, Gmail, and AOL.

Desktop vs. Webmail Applications:

Desktop and webmail applications have different characteristics, which are compared at Table 2.1.

Table 2.1. Desktop Applications vs. Webmail Applications

Desktop Applications	**Webmail Applications**
Processing is performed at client	Processing is performed at web server
Application is needed to be installed on client's computer	No need for any software other than a web browser
E-mails can be stored at local device	E-mails have to be stored at e-mail server
Old e-mails can be accessed without Internet connection	Old e-mails cannot be accessed without Internet connection

2.4 Protocols and Standards Used to Develop MailMoby and MobileMoby Applications

HTTP (Hypertext Transfer Protocol) is used for MailMoby webmail client, whereas SMTP and IMAP (Internet Message Access Protocol) protocols are used for data exchange between MUAs and MTAs for MailMoby and MobileMoby mail clients.

HTTP: HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems [8]. The standards of HTTP are defined in RFC 2616. HTTP is a typical example of client server computing, in which client makes a request and server responds to this request. In our implementation HTTP protocol is used for accessing webmail and requesting webmail operations via web browser.

SMTP: SMTP is an e-mail transmission protocol and its standards are defined in RFC 5321 [9]. SMTP is capable of transporting e-mails. An e-mail message passes through gateways from sender to recipient. When a client wants to send e-mail from webmail, web server requests this SMTP operation from e-mail server, and e-mail server sends e-mail message using SMTP protocol. In mobile application, application directly sends SMTP commands to e-mail server.

IMAP: IMAP is one of the e-mail retrieval protocols. Its standards are described in RFC 3501 [10]. This protocol is used to access mail data at e-mail servers. IMAP's difference from POP3 (Post Office Protocol), which is another protocol for e-mail retrieval, is it is designed specifically for online use, whereas POP3 is designed for offline use. IMAP protocol doesn't download e-mail messages to the local computer and deletion of e-mail messages must be done manually. On the other hand in POP3 protocol, clients download e-mails to local machine and deletion of e-mails can be automated. IMAP's another most important feature is a user can reach all mailbox folders at the server more than INBOX, such as Sent, Drafts, Trash and user-defined folders. In our MailMoby Webmail Application and MobileMoby Mobile Application implementations, IMAP protocol is used to access e-mails. When a client requests to read an e-mail via webmail, web server requests e-mail from e-mail server using IMAP protocol and e-mail server returns the requested messages to web server. On the other hand, MobileMoby Mobile Application directly connects to e-mail server and request e-mails using this protocol.

2.5 Tools and Technologies Used to Develop MailMoby and MobileMoby Applications

As described before, development of MailMoby and MobileMoby client applications required following components:

- The web based MUA to communicate with the local MTA
- The desktop MUA to run on the mobile phone which communicates with the remote MTA
- An MTA to communicate with the MUAs and with the remote MTAs.
- A Web Server to execute the web based MUA

The developed system uses Qmail as MTA, JSP (Java Server Pages) and Java (Beans) as server-side programming language to develop web based MUA, Java ME to develop desktop MUA, and Apache Tomcat as web server. Figure 2.2 depicts the tools and technologies used in MailMoby webmail application. The components in blue are developed by us; the components in red are developed by third party.

2.5.1 Web Based MUA Development Environment

Every dynamic webpage needs a web server to process the source code of the page. In MailMoby project, Apache Tomcat Web server is used to host the web mail. Apache Tomcat is a Servlet and Java Server Pages container developed under the Apache License [11]. Apache Tomcat powers numerous large-scale web applications.

JSP: JSP is a server-side programming language that allows developers to develop dynamic web pages. *"As part of the Java technology family, JSP technology enables rapid development of Web-based applications that are platform independent."*[12]. JSP technology allows Java code to be embedded into XHTML (Extensible Hypertext Markup Language) pages. The Java programming language is a high-level language that can be characterized simple, object-oriented, multithreaded, robust, dynamic, and secure [12]. As an outcome, JSP uses the power of these Java programming language characteristics in dynamic web pages. In MailMoby Webmail Application implementation, JSP technology is used for programming the webmail.

Java Beans: A Java Bean is a software component that works with Java Technology [13]. It is consisted of a Java class that defines the class's properties. Its properties are accessed via getter and setter methods.

XHTML: XHTML is a XML (Extensible Markup Language) markup language used to code web pages, and its standards are developed by W3C (World Wide Web Consortium). XHTML provides ease to create new elements and element attributes by using XML. XHTML documents should contain an xml declaration and must contain doctype and xmlns declarations [14].

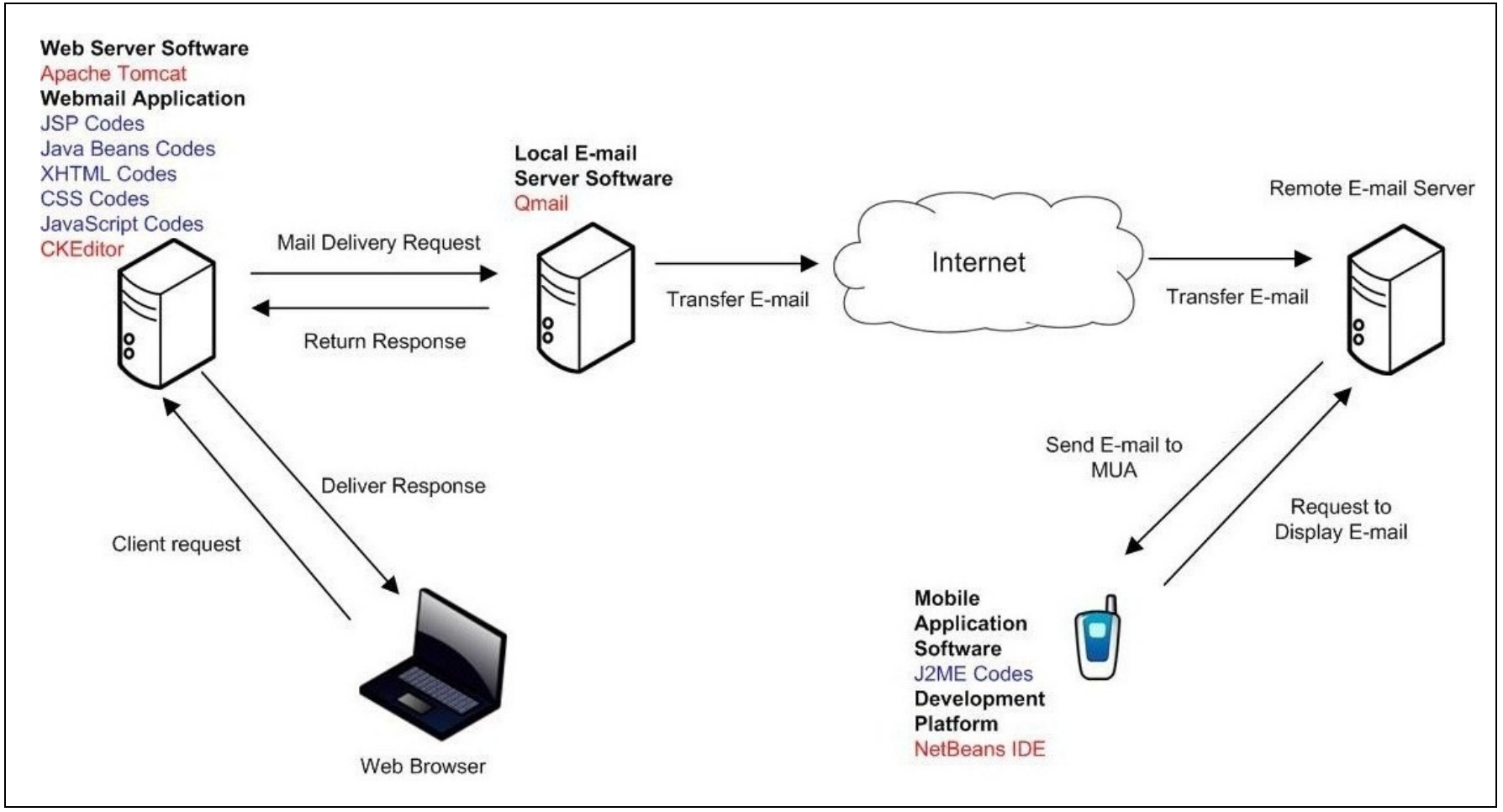

Figure 2.2. Tools and Technologies used in MailMoby and MobileMoby

CSS: CSS (Cascading Style Sheets) is a language to define how the elements are displayed at web page [15]. In MailMoby webmail application, CSS is used for giving style to webmail.

JavaScript: JavaScript is an object-oriented client-side scripting language, and is widely used in web applications [16].

CKEditor: CKEditor is a WYSIWYG (What You See Is What You Get) text editor to be used inside web pages. By using CKEditor, users can compose HTML (Hypertext Markup Language) enabled e-mails. Inserting and editing images, edition of font are some examples of HTML enabled composing [17].

XHTML, CSS, Javascript, JSP and JavaBeans codes are developed by us to build the web mail. CKEDitor is used for composing HTML e-mail messages.

2.5.2 Desktop MUA Development Environment

MobileMoby application is written using Java language. Java availability in almost all mobile phones was our motivation to write this program in Java programming language. Java programming language for mobile devices J2ME (Java Platform, Micro Edition) is used to code the mobile software [18]. Also software is developed on NetBeans IDE (Integrated Development Environment) [19]. Figure 2.2 shows the tools and technologies used in mobile application. Java ME technology is based on three elements as described in [18].

1. **CLDC:** CLDC (Connected Limited Device Configuration) is a configuration providing the basic libraries for application interfaces and virtual machine capabilities
2. **MIDP:** MIDP (Mobile Information Device Profile) provides APIs (Application Programming Interfaces) to write applications for mobile devices
3. **Optional Packages:** Optional packages are sets of specific APIs.

Chapter 3

MailMoby Webmail Application

3.1 MailMoby Webmail Application Description

MailMoby is a webmail implementation written in JSP programming language. It is designed to allow users to access it from anywhere and any computer they want while they are connected to the Internet. The only need is a web browser.

It allows users to make mail operations such as reading and composing e-mails, and provides additional services to users such as advanced search and address book. The details of MailMoby webmail services are explained in the following sections.

The goal of the MailMoby webmail is to provide easy access to webmail operations from anywhere. Identified goals for this purpose are:

- There shouldn't be any need for extra software, only a web browser is enough.
- It should be accessible from any internet-connected device, a computer or a mobile device with the required specifications.
- It should support popular browsers such as Mozilla, Internet Explorer, Netscape, Opera
- It should provide user-friendly interface for end users. Interface of MailMoby webmail is implemented using XHTML and CSS for this purpose.

MailMoby Webmail Application has standard features such as reading and composing, and management features such as address book and search. Following is the list of standard and management features of MailMoby Webmail.

Standard Features

- Reading an E-mail

- Composing
- Replying
- Forwarding
- Deleting

Management Features

- Address Book
- Search
    - Quick Search
    - Advanced Search
- Settings
- E-mail Sorting
- Mails per Page for Session

MailMoby webmail's interface is divided into two parts. Left part is mostly static, and consists of links to mail folders, address book, and searching. Right part is a more dynamic and its content changes after each click of the user. Right part is further divided into three sections. Top and bottom sections include the informative information about the content of the middle section, and some additional links for the user. Top section consisted of currently logged-in user's e-mail address, and links to "changing password", "settings page", and "sign out". Middle section changes more dynamically depending on the current content. An example Inbox page is given in Figure 3.1.

3.2 Read

Content of an e-mail message is displayed in HTML format when the subject part of an e-mail is clicked while Inbox page is being viewed. When an attachment is included, its link is given provided below the message and can be downloaded to local machine. Additional "Reply", "Reply All", "Forward", "Delete", and "Spam" buttons are displayed in the bottom section. When "Reply" button is clicked, browser displays "Compose" page with a new message form, and body is quoted with the sender's e-mail message. Also "Subject" field is filled with sender's email's subject prefixed with "Re:". An example "Reading an E-mail" page is given in Figure 3.2.

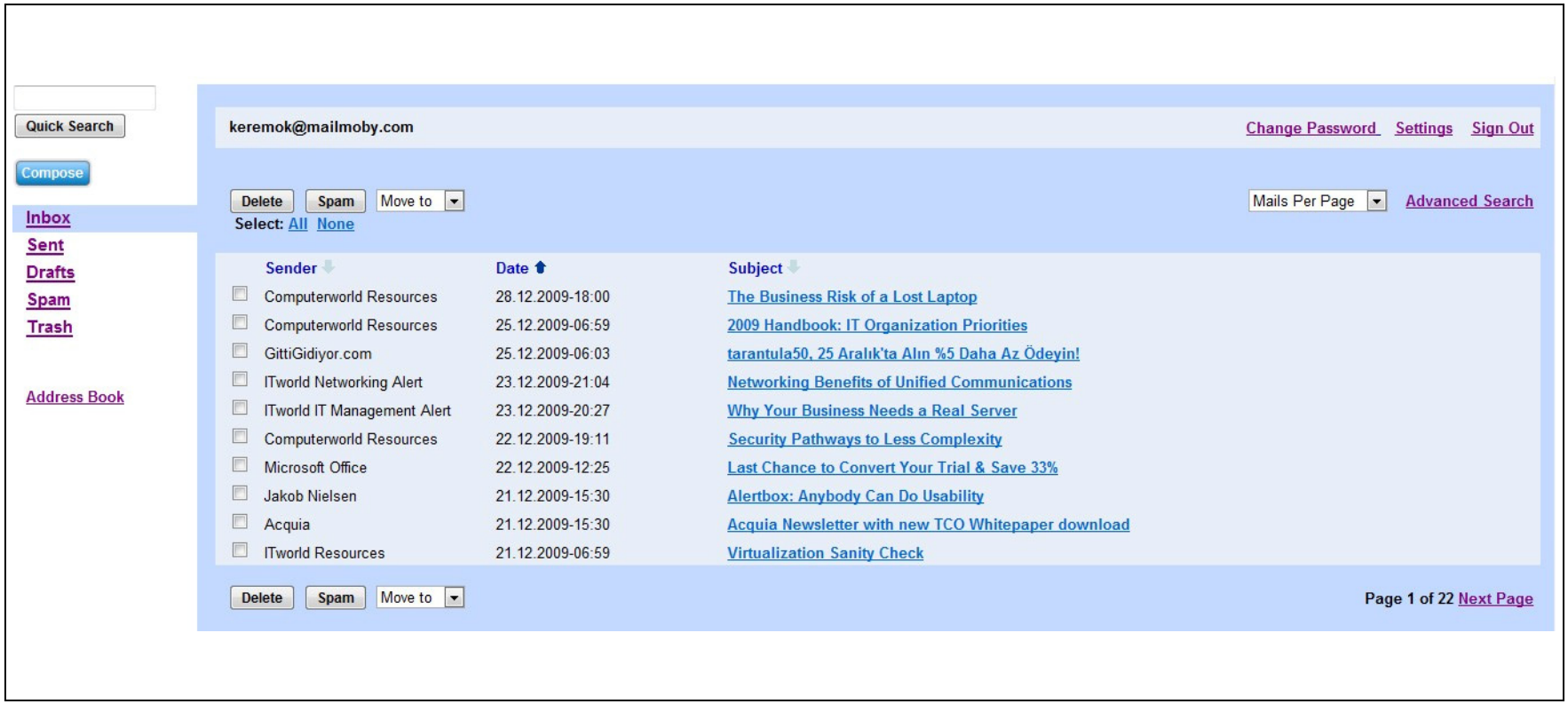

Figure 3.1. Inbox Page

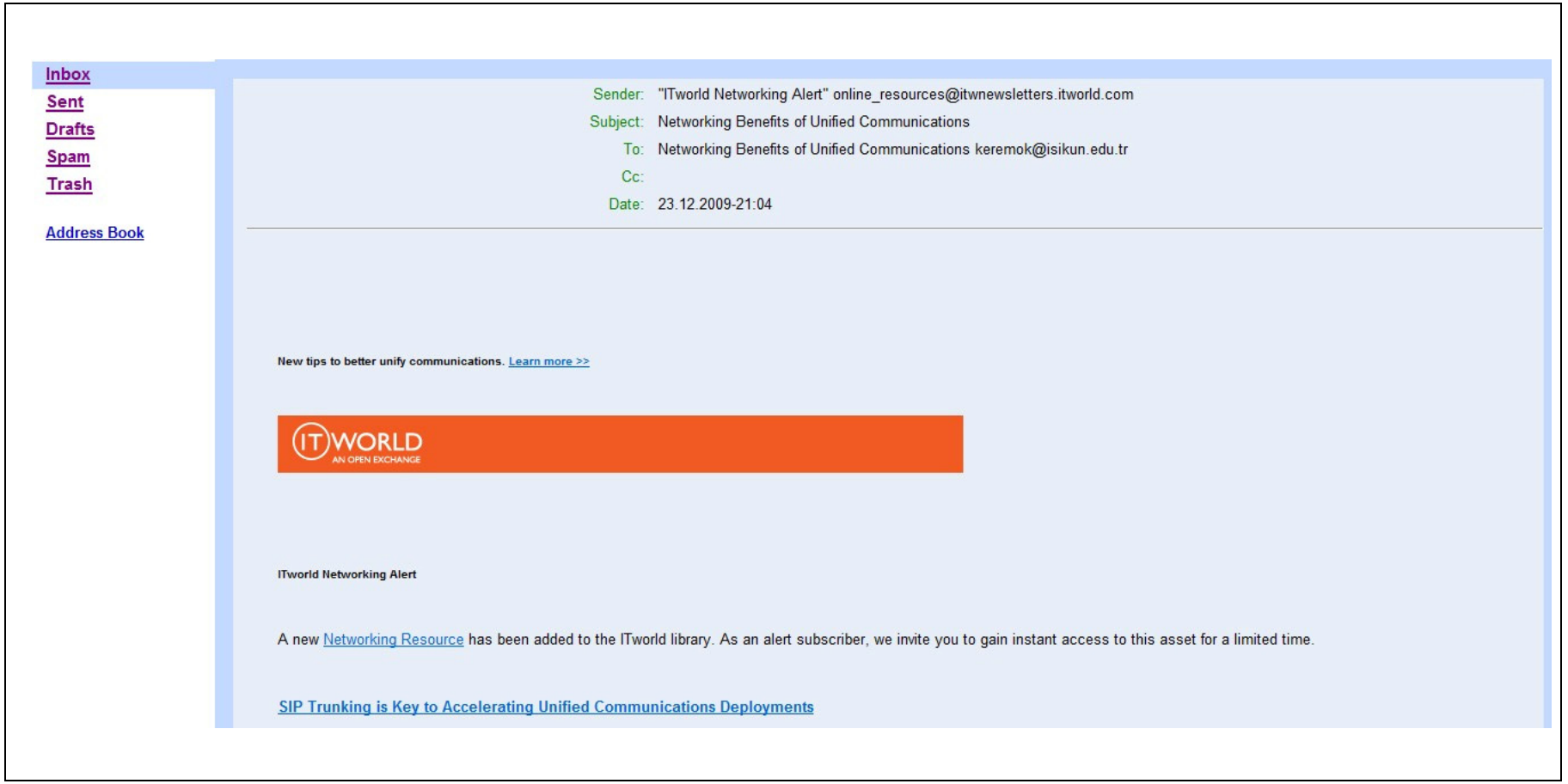

Figure 3.2. Reading an E-mail

3.3 Compose

“Compose” button is available on the left section, and linked to the compose page which gives opportunity to send HTML e-mails including file attachments. In the compose page, there are to, cc, bcc, and subject text fields to get input from user and buttons for user to submit.

At the top section there are four text fields; to, cc, bcc, and subject. To, cc, and bcc are address fields that e-mail will be sent. E-mail addresses are inputted to these fields and multiple addresses are separated with comma. E-mail addresses written in “to” field are sent directly to those e-mail addresses. On the other hand the copies of e-mails are sent to the addresses inputted to “cc”, and “bcc” fields, where the recipients will not see the inputted e-mail addresses in bcc field.

Below the address fields there is a subject field, which takes input from user, and sets as the subject of the sent e-mail.

Most of the page is filled with body of the email. This part is a text area, and user can input HTML messages from this field. To enable HTML enabled composing CKEditor is used [17].

At the bottom of the page, there are “Browse”, “Send”, “Save”, and “Cancel” buttons. By using “Browse” button user can upload attachments to e-mail. “Send” button posts the values of address fields, body field, and attachments (if any) and then posted page validates the values and sends the e-mail. “Save” button enables users to save an e-mail to be sent in the future. “Cancel” button discards the e-mail and returns to the previous page. An example “Compose” page is given in Figure 3.3.

3.4 Reply

Users can reply to e-mails that have been sent to them. While reading an e-mail message, “Reply” and “Reply All” button is shown above the message. When “Reply” button is clicked browser enters a compose page that body is quoted with e-mail body, and subject field is filled with e-mails subject appended with “Re: ” phrase. To field is filled with sender’s e-mail address. “Reply All” button differentiates at to and cc fields. When “Reply All” button is clicked, to field is filled with sender’s e-mail address, and cc field is filled with cc e-mail addresses.

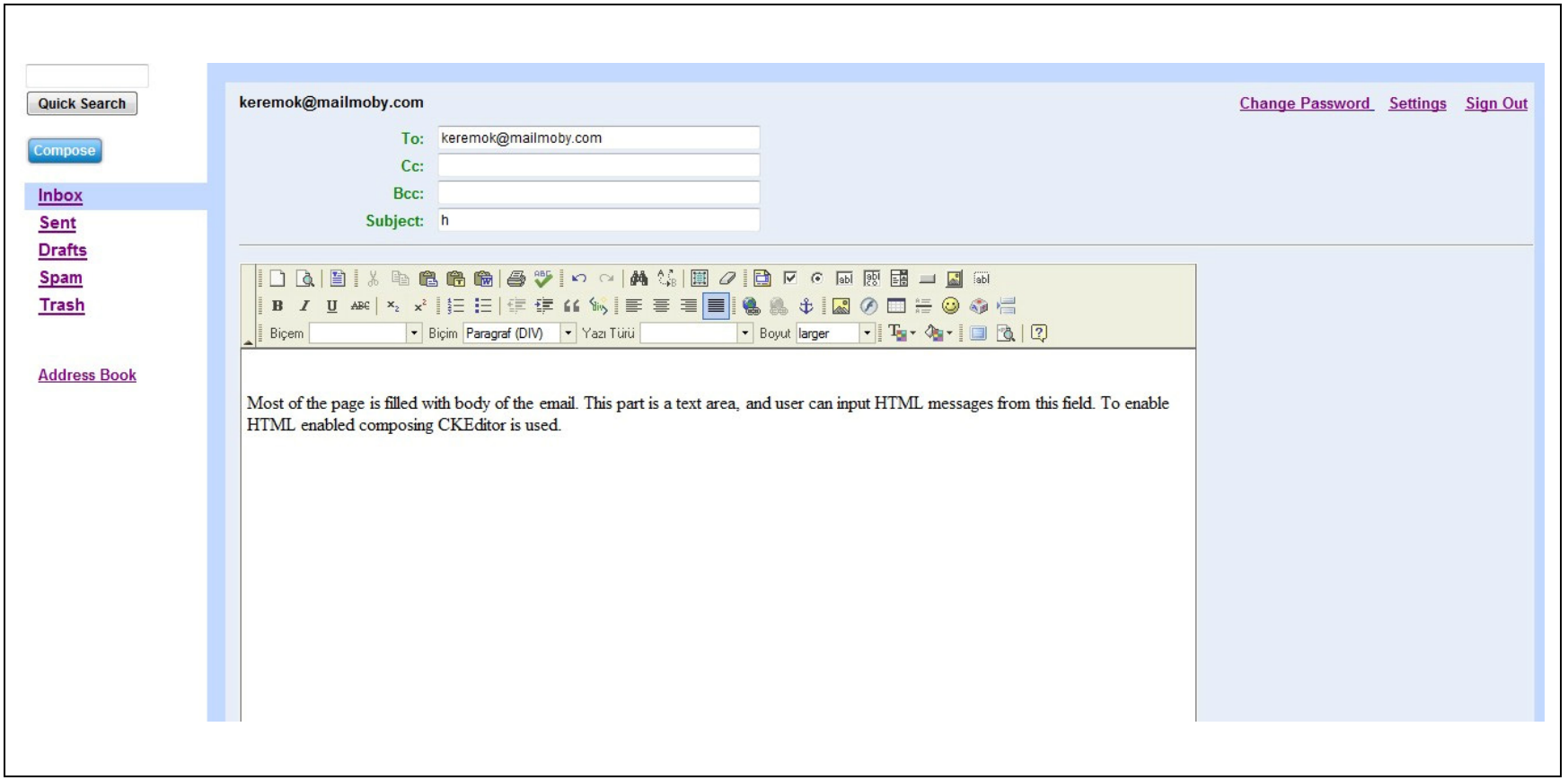

Figure 3.3. Composing an E-mail

3.5 Forward

Forward button enables users to forward e-mails to other users. When forward button is clicked, compose page is opened with body is quoted with e-mail body.

3.6 Delete

Delete button enables users to delete an e-mail. When delete button is clicked in an e-mail, e-mail is deleted and user is forwarded to previous page by the system.

3.7 Address Book

Address book link is available under folders. A user can add frequently used contact's information to this address book. This contact information includes title, name, surname, company, e-mail, mobile, home phone, work phone, and notes. "Address Book" page is given in Figure 3.4.

3.8 Search

There are two search options available. First one is "Quick Search" which is available on top left in main page. Users can enter a phrase from this text field and search mails. "from", "subject", and "body" fields of e-mails are searched inside e-mails and results are shown to the user.

The second search option is "Advanced Search", which's link is available in almost all pages' top right. Using this link user can enter "Advanced Search" page and search e-mails based on "from", "subject", "body", "date", and "folders".

3.9 Settings

Settings page is available at top-right of every page. Users can set "Display Name" and "Mails per Page" from this menu. "Display Name" is set as name of the sender of each e-mail and set "Mails per Page" number enables to display fixed number of e-mails at every page. They can also have the option to change their password from this page.

Figure 3.4. Address Book

3.10 E-mail Sorting

E-mails are sorted automatically based on sent or received date. But there are options to sort e-mails based on other criteria. These options include sorting by sender, date, and subject both backwards and forwards. As shown in Figure 3.1, current sort selection is colored and other sort selections are colorless.

3.11 Mails per Page for Session

As explained above, e-mails per page can be set through settings page. But there is an option to set e-mails per page for current session. “Mails per Page” drop-down menu is available in top-right of folders’ pages. Set “Mails per Page” is fixed for that session, but when user’s session is expired “Mails per Page” is set again to the value at “Settings” page.

Chapter 4

MobileMoby Mobile Application

4.1 MobileMoby Mobile Application Description

MobileMoby mobile application is written to be used in Java-enabled mobile devices to be used as e-mail client software to access e-mails from anywhere. A Java-enabled device can read and compose e-mails using this program by installing the MobileMoby Application software. While data rates of mobile communication is increasing, people tend to use mobile applications with eliminating geographical restrictions. So it is important to enable mobile access for users.

MobileMoby Mobile Application enables users to send and receive e-mails using their mobile devices. To send and receive e-mails, mobile phone should be accessible to Internet. Figure 4.1 shows the screenshot of MobileMoby Mobile Application's Index (Main Menu) page.

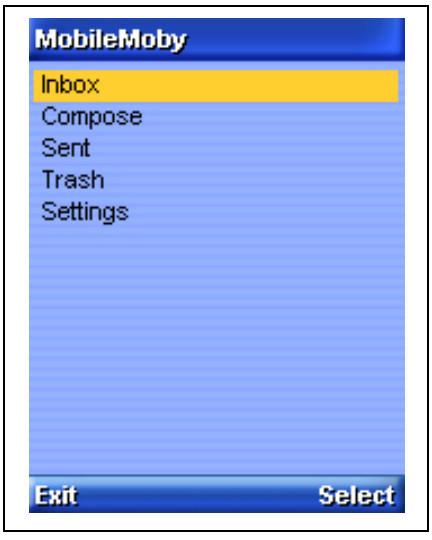

Figure 4.1. Index page of MobileMoby Mobile Application

4.2 Reading E-mails

Users can read their e-mails using the application. When “Inbox” is clicked in “Main Menu”, application enters to “Inbox” page. At Inbox page 10 e-mails are listed with subject and sender information, ordered by date. User can reach older e-mails using “Next Page” button, and newer e-mails using “Prev. Page” button under the “Menu” item.

When an e-mail is selected to read, additional header information such as sender’s name, sender’s e-mail address, sent date, subject, and message is displayed. Also “Delete Mail” link is given to delete that e-mail and “Back” link is given to go back to “Inbox”. Figure 4.2 shows the screens of Inbox and reading an e-mail.

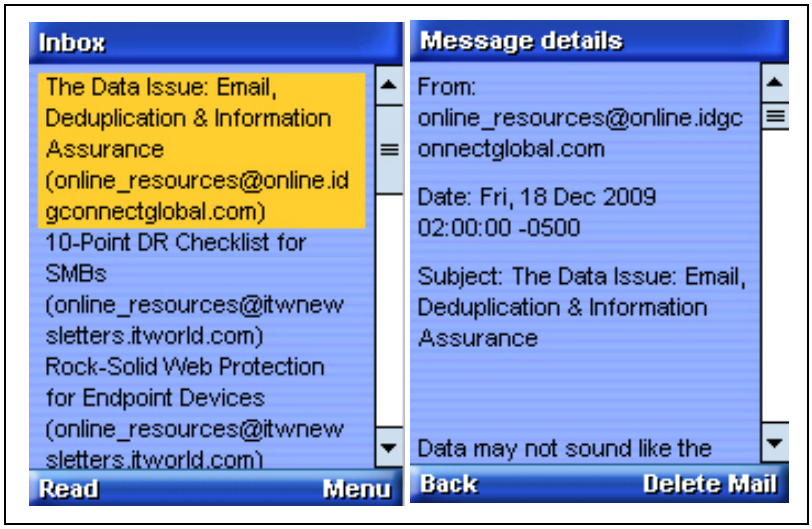

Figure 4.2. Inbox and Reading e-mail using MobileMoby Mobile Application

4.3 Sending E-mails

Users can compose an e-mail using “Compose” button at “Main Menu”. In the compose menu there are four textboxes which are “to”, “subject”, “cc”, and “bcc”. When textboxes are filled and “Next” button is pushed, body textarea is displayed. When user fills the body of the e-mail and pushes “Send Mail” button, e-mail is sent and an information message is displayed to the user. Screens of compose section is given in Figure 4.3.

In addition to “Compose” option there are “Reply” and “Forward” options. When a user is reading an e-mail, “Reply” and “Forward” buttons are displayed under the

"Menu" item, which is given in Figure 4.4. Using "Reply" and "Forward" buttons, user can reply to the e-mail or forward the e-mail to another person.

Figure 4.3. Composing e-mail using MobileMoby Mobile Application

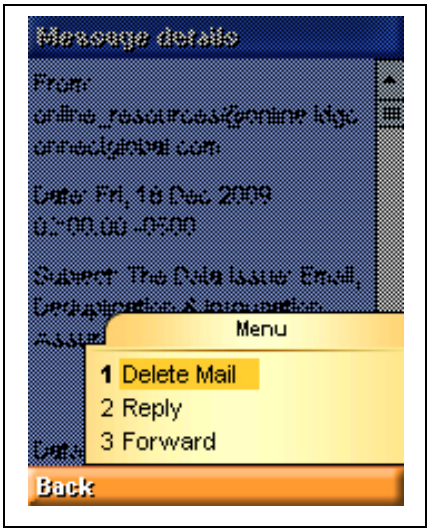

Figure 4.4. Reply and Forward Options in MobileMoby Mobile Application

4.4 Settings

Settings menu enable users to enter their login information. A user can reach "Settings" from "Main Menu". User should enter his/her login information for once,

and application saves it for further use. Screenshot of Settings page is given in Figure 4.5.

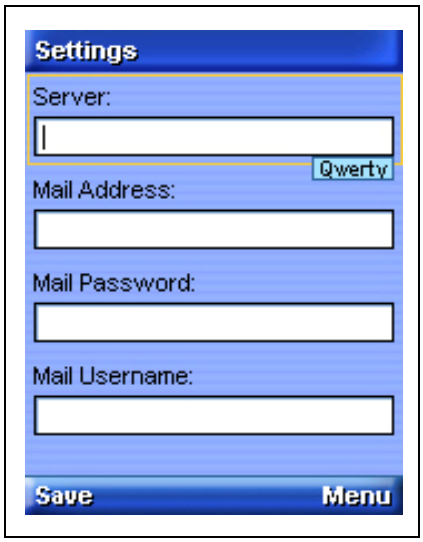

Figure 4.5. Settings Page of MobileMoby Mobile Application

Chapter 5

An Emerging Mobile Technology: NFC

5.1 Near Field Communication

Near-field Communication is a short range radio communication technology. It enables communication between two NFC-compatible devices when they are brought together within less than four centimeters. Hence, the communication in NFC is peer-to-peer communication. It operates at 13.56 MHz (Megahertz) and can transfer data up to the speed of 424 Kbits (Kilobits) per second [20]. The attractive part of NFC technology is mobile phones can be built in NFC-enabled. Since mobile phones are easy to use communication equipments, and most of the people carry those most of the time, NFC becomes important and has the opportunity to easiness our lives. Researchers indicate that, by 2011 NFC-enabled mobile phones will reach to 500 million worldwide [21]. This favors that NFC can become one of our daily life technology in the future.

As we said there are two parties at the communication. Parties share a single RF band, and the communication is half-duplex, in which when a party is receiving a signal, it must wait until it stops. In other words, one party should transmit signal if the transmission isn't detected from the other party [22].

The two parties in the communication named initiator and target. Initiator is the device which starts the communication. On the other hand target device is responsible to make responses that are made by initiator. Initiator is an active device which must have an energy component such as a mobile phone. Target can be an active device or a passive device, and it doesn't need to have an energy component [20, 22].

There are unique features of NFC technology that doesn't exist in other technologies.

- One of the most important features of this technology is its short range communication, because it brings ease of use and inherent security. The communication is terminated when the devices move out of range.

- Establishing communication is very familiar to people. The only thing for a person to do is to make a physical contact between the devices.

- NFC is compatible with widely used contactless smart cards such as Felica and Mifare. These smart cards can be placed as target devices and hold data to be read from an initiator.

- NFC devices can be used either as an initiator or as a target. For example NFC-enabled mobile phones can be used as initiator but also can be used as target instead of a card or NFC tag.

In order to standardize and to advance the use of NFC technology, NFC-Forum is formed at 2004. NFC-Forum defines three operating modes; peer-to-peer, reader/writer, and Card Emulation [20].

Peer-to-peer mode: In peer-to-peer mode, two devices can exchange data at link-level. This mode is standardized on the ISO/IEC 18092 standard, and allows data speed up to 424 Kbit/sec [20].

Reader/Writer mode: In Reader/Writer mode NFC devices can act as reader/writer for RFID (Radio-frequency Identification) tags. NFC device acts as an initiator and passive tag is the target. Passive tag doesn't need any source of power. Active NFC device creates magnetic inductive coupling and transfers energy to smart card when it gets close enough. After the smart card is powered, communication starts. In this mode of communication the data speed is up to 106 Kbit/sec [20, 22].

Card Emulation mode: In Card Emulation mode NFC device acts as an NFC tag and other NFC devices can read data from this NFC device. The advantage of this mode is that there isn't any need for any NFC tag or a smart card [20].

5.2 NFC Applications

The main property of NFC is using mobile communication over short distance, which injects a secure convenience technique. Convenience is provided because bringing the mobile to a reader is a very trivial action. Security is provided because only a reader within 4 cm. can communicate with the mobile device. Additional security measures such as cryptography are also to be provided to enhance security.

Recent studies in NFC technology showed that many real-life applications can be developed to give different opportunities to users. Some of these studies are; a meal service system [23], an electronic data capture system [24], mobile coupons to promote products [25], a system to encourage outdoor physical activities [26], a sales data management system of chain enterprises [27], an NFC infrastructure to use a location-based wiki [28].

Various applications using NFC technology are developed so far, all of which make use of convenience, and most of them make use of security. The following list is some of the potential applications that can be created in the near future.

- **Mobile Payments:** Users will be able to pay using their mobile phones, in which their credit card information embedded.
- **Information Kiosks:** Users can download information to their mobile phones from information kiosks.
- **Ticketing:** Tickets can be bought and received to NFC-enabled devices, and then checked out touching the device to a turnstile.
- **Exchanging Electronic Business Cards:** By touching NFC-enabled devices to each other, users can exchange their business cards.

As a part of my thesis, a remote electronic voting system is developed with NFC, and evaluated the system's usability. It will be presented in "The IASTED International Conference on Software Engineering 2010", and its content is also given in Chapter 6.

Chapter 6

Usability of Mobile Voting with NFC Technology

In this chapter, paper of "Usability of Mobile Voting with NFC Technology" is presented, which is published in the proceedings of IASTED International Conference on Software Engineering 2010. Followings are the information on the paper.

Paper Title: USABILITY OF MOBILE VOTING WITH NFC TECHNOLOGY

Authors: Kerem Ok, Vedat Coşkun, Mehmet N. Aydın

Conference: The IASTED International Conference on Software Engineering 2010

Conference Date: 16-18 February 2010

Conference Place: Innsbruck, Austria

Conference Web Site: http://www.iasted.org/conferences/home-677.html

6.1 Background Information of Electronic Voting

Voting is described as a method for a group such as a meeting or an electorate to make a decision or express an opinion-often following discussions, debates, or election campaigns in [29]. In traditional voting systems, people go to specific voting locations and cast their vote using paper ballots.

After the extensive implementations of traditional voting for many centuries, as the advances in technology promised some help on this issue, electronic voting systems are developed giving the opportunity to people cast their votes using electronic devices. Electronic voting has several benefits and solves many problems of traditional voting [30]. It further enables voters to vote almost anywhere without geographical restrictions [31].

Electronic voting systems are classified as poll-site voting, kiosk voting, and remote electronic voting [30].

Poll-site voting: This is similar to traditional voting systems. A voter goes to a specific place to cast her vote, generally through touch screen voting terminals. The voter identifies himself using her ID card [30].

Kiosk Voting: Voting machines are placed to convenient locations such as libraries and schools. The voting platforms are controlled by election officials to ensure security and privacy [30].

Remote Electronic Voting: A voter may vote from any location and her vote is transmitted over Internet. In this method, the voter can vote using electronic devices such as notebooks, mobile phones, or PDAs. The voter is identified via remote verification mechanisms such as digital signature, biometrics, and PIN codes [30].

While it is clear that electronic voting systems must still satisfy the requirements of traditional voting systems, it demands some additional requirements. The additional requirements mentioned in various study are accuracy [31, 32, 33], democracy [31, 32, 33], privacy [31, 32, 33], verifiability[31, 32, 33], mobility[31, 32], convenience[32], flexibility[32], simplicity[31], uncoercibility[31], and no unauthorized proxy[33]. Clearly, some of these requirements overlap, and some are very much related to each other.

After analyzing requirements of classical voting systems and the requirements set by the referenced works, we summarize the requirements for an electronic voting as follows:

1. *Accuracy*: (i) A vote should not be altered. (ii) An invalid vote should not be counted in the final tally. (iii) It should not be possible to eliminate a validated vote from the final tally.
2. *Democracy*: (i) Only eligible voters should be able to vote. (ii) All eligible voters may vote only once.
3. *Anonymity* (*Privacy*): A ballot should not be linked back to the voter who casted it.
4. *Verifiability*: Each voter may verify that her vote is counted.
5. *Mobility*: A voter may vote anywhere without any geographical restrictions.
6. *Usability*: A system may be used by intended users to achieve specific goals.

We investigate the use of NFC-enabled devices in voting, namely NFC voting, which extends electronic voting process. We analyze the requirements of NFC voting, by taking into account the requirements of traditional and electronic voting as well. While exploring the requirements of electronic voting system using Near Field Communication (NFC) technology, we specifically consider the usability of NFC based voting. Usability of electronic voting systems can be measured by three metrics; *effectiveness*, *efficiency*, and *satisfaction* [34]. The first two metrics are objective, whereas the last one is a subjective metric. Effectiveness is about an extent to which the goals of using the system are achieved in terms of its accuracy and completeness. Effectiveness can be measured by completion rates, errors, and assists. Efficiency is the relationship between the level of effectiveness achieved, and the amount of resources expanded. It can be measured by the time spent to achieve the task. Satisfaction can be defined as the user's pleasure whilst using the system. In the context of voting, it can be measured by subjective responses of voters. Satisfaction is assured when a voter is pleased with her voting experience, confident with her vote to be counted, and she thinks that her anonymity is preserved [34, 35].

The NIST reports standardized instruments to test user satisfaction in "Common Industry Format for Usability Test Reports" in [34]. One of these instruments is the

SUS (System Usability Scale). It is a simple, ten-item scale giving a global view of subjective assessments of usability. It investigates various aspects of usability and should be used immediately after giving the opportunity to evaluate the system to the participants. In the SUS assessment model, ten five-point items are asked to the participants. The ratings for the items are calculated in a particular manner and a score between 0-100 is produced. A higher score indicates higher usability and lower score indicates the opposite [36].

We study the viability of the emerging technology, NFC, in the context of electronic voting to improve its usability. To evaluate the usability of NFC in mobile voting, we create a test bed by applying an experimental student council voting in our university. Furthermore, we compare the usability of our model with web-based voting, which is the current method of casting votes at our university. Moreover we investigate if the requirements can be satisfied in the proposed system.

6.2 Background Information of Near Field Communication Technology

Voting technology and the usability of these technologies in the context of voting actually can influence the voters' response to the system and directly influence the election results [37]. The usability of electronic voting systems is not deeply studied, and it still preserves its obscurity. Remote electronic voting is the only option to eliminate geographical constraints in the context of voting. So, current and promising technologies which can be used in remote electronic voting have the potential to increase voters' satisfaction.

NFC is one of these promising technologies. It is a short range radio communication technology based on Radio Frequency Identification (RFID). It enables communication between two NFC-compatible devices when they are brought together within less than four centimeters apart, or even by touching themselves. Short range communication within short distance is the major feature of this technology, because it brings ease of use and inherent security. It operates at 13.56 MHz and can transfer data up to 424 Kbits per second [20].

In NFC model, Radio Frequency (RF) communication is performed between two NFC-enabled devices: an *initiator*, and a *target*. Initiator starts the communication,

where the target responses to the request made by the initiator. An initiator is an active device which has embedded energy component, where a target may be either an active or a passive device such as an RFID tag. An RFID tag, also called as an NFC tag, is a passive device, since it does not include any energy source. It holds data that can be read only by an active NFC device [22].

One of the important aspects of NFC technology is its inherent security, because communication is started by bringing two devices very close to each other. Separating devices over a limit terminates the communication. The range is so short that, if any hacker device comes close, it will be clearly noticed [21].

One of the most important advantages of this technology is that NFC enabled devices are easy to use, since its technical process is already integrated to the NFC enabled phones during manufacturing. The required software can also be downloaded and installed easily by the technique named as OTA (Over The Air Transfer) transfer. Mobile phones are today's easy to use and comfortable communication equipments, and it is expected that the NFC-compatible mobile phones will reach to 500 million by 2011 [21]. This encourages NFC to be one of our daily life technologies in the near future.

Innovation of NFC technology and NFC built-in mobile phones offer new possibilities for many real-life applications. In [23] a meal service system based on NFC is studied. An application that allows making daily meal orders by touching NFC-enabled mobile phones to an NFC-enhanced menu is tested. In [24] an Electronic Data Capture system for patients is developed. Patient's blood pressure, heart rate, stroke volume and other related data are read by patients' NFC-enabled mobile phone and transferred to the hospital's server system over Internet. In [25] mobile coupons are used to promote products and services. In this way, users can download mobile coupons to their mobile devices, using the NFC tag attached to a poster or a newspaper. After the download, the coupons can be used at the cashier. In [38] several NFC scenarios are studied and tested. First, a person sees a poster on the street and downloads the information about a movie to her NFC-enabled mobile phone by scanning the NFC tag which is embedded into the poster. She buys a ticket for the movie with her mobile phone, so that cost will be paid through the phone bill

later. Then she enters to the theatre by waving her mobile phone to turnstile. After the show, she may also scan a taxi company's poster by the theater entrance to call a taxi. In [26] a prototype system using NFC to support and encourage the outdoor physical activities is presented.

6.3 Proposed Model

We propose an electronic voting model which uses NFC-enabled devices. We have selected our university's student council election for verification and evaluation of our model. Our university currently uses an in-house developed web-based system for this purpose. After testing the model, it became possible to request comparison of our model with the current model from the student voters.

In our model, three applications will be used: *voting midlet* running on the mobile phone to enable secure voting, *validator servlet* running on the validator server to authenticate the votes, and the *tallier servlet* running on the tallier server to count the legitimate votes. Voting midlet will be installed to the NFC-enabled mobile phone, whereas the servlets will be installed on two separate servers. In order to satisfy some requirements mentioned in the earlier parts of this chapter, the votes will be encrypted by the midlet, and will be decrypted by the servlets. The midlet as well as the required encryption keys will initially be loaded to the mobile phones. A voter student further can touch her mobile phone to an NFC tag of her favorite candidate in order to start voting process. The student must then enter the pin code to enable the midlet retrieve the encryption keys to be used in encrypting the vote. To send the vote to the validator server, mobile phone should have internet access through Wi-Fi, WiMax, or another mobile data service such as GPRS, EDGE, or HSDPA. After the mobile phone sends the encrypted vote to the validator server, the decryption process is executed and the valid votes are further counted by the tallier server. The details of the process occurred in backend servers are explained further in the following section. After performing this process, midlet displays a confirmation message on the screen giving information about the result of the voting process. Some screen shots of the execution of the midlet are given at Figure 6.1.

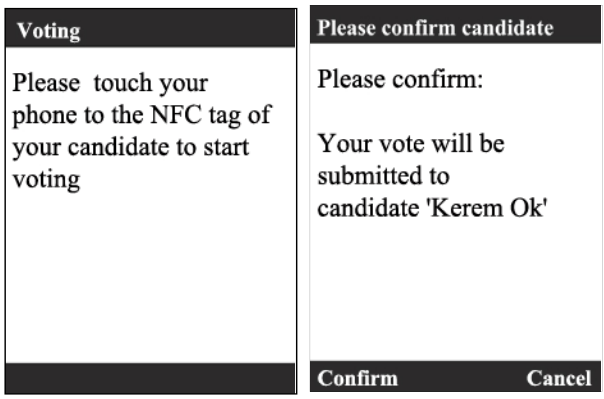

Figure 6.1. Mobile Phone Displays

6.3.1 Details of the Model

Important phases of electronic voting are validating each vote to enable only authorized users vote, and then counting already validated votes. In order to validate and count the votes appropriately we have used two servers; *Validator Server* to validate the received votes, and *Tallier Server* to count validated votes. Validator server must ensure that only and all eligible voters can vote, and they can vote at most once; it keeps the list of the eligible students for this purpose. During the registration of the eligible voters, validator server is also responsible for generating public & private key pair of students, and keeping the students' public keys at its database. For counting the votes we need another server, namely Tallier Server. This server is responsible for counting the validated votes, by using appropriate methods so that anonymity is also satisfied at the same time.

$$\text{Vote} = D(K_{R_t}, D(K_{U_v}, E(K_{R_v}, E(K_{U_t}, \text{Vote}_{\text{user}})))) \qquad (6.1)$$

Technical details of the voting are depicted in Figure 6.2, whereas the model architecture is depicted in Figure 6.3. We used public-key algorithms for secure data transfer between the mobile phone and the servers, as shown in Equation 6.1. During the voting process, voting midlet encrypts the vote twice; first using tallier server's public key (K_{Ut}) and then using voter's own private key (K_{Rv}). After the encryption process, voting midlet creates a packet which includes the encrypted vote together with the voter's id, and later sends the packet to the validator server. Validator server extracts the voter identification number from the packet's header. It first searches the list of registered voters from its database. If it finds the student's identification

number within the list, it further searches the voted users list until then. If a student's identification number doesn't exist in the voted users list, it decrypts the data using student's public key. If it can't find the student's identification number in the registered voters list or if it finds the identification number in the voted users list, it returns error message to midlet. Otherwise the vote needs to be added to the used vote list, and hence validator server sends the decrypted data to Tallier server. Tallier server decrypts the data using its own private key (K_{Rt}) and increments the related candidate's vote count. After a successful final, tallier server notifies the validator server, and the validator server notifies the mobile about the successful final.

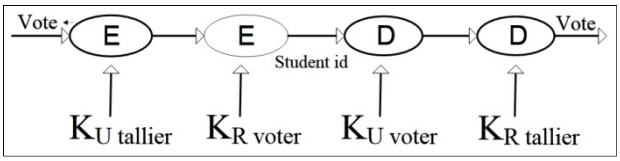

Figure 6.2 Vote Authentication and Counting Process

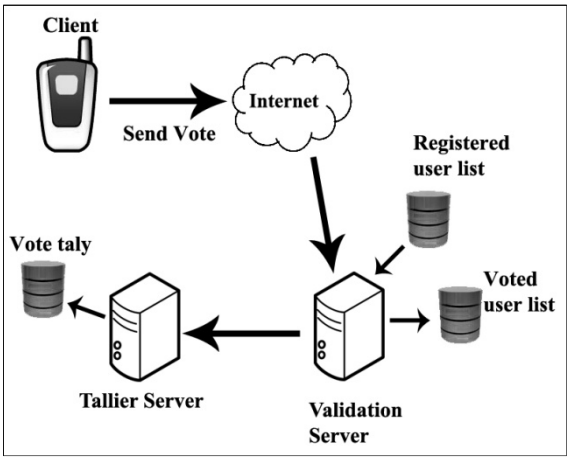

Figure 6.3 Model Architecture

Students need to complete the registration process prior to voting. Registration process includes registering voters and installing the midlet together with the keys to the mobile phone. It involves face-to-face meeting of the voter with the registrar to determine eligible voters. For this purpose the eligible voter goes to voting registrar's office and shows her student identity card to registrar. Registrar verifies the identity of the student and generates a public-private key pair (K_{Uv}, K_{Rv}) which is unique for that specific voter. After the key pairs are generated, the registrar installs the private key of the voter together with public key of tallier server (that is only created once

and stored by the registrar) to the student's mobile phone by conveniently using NFC. Public key of the voter (K_{Uv}) is saved on the validator server at this time. Validator server adds student's identification number to its list of registered user list during this process. Note that Registered User List will be used in voting process, as shown in Figure 6.3.

6.3.2 Voting Scenarios

NFC tags are to be prepared for each candidate. During this process, candidate's election id is to be integrated into the NFC tag, which possibly will be attached to a form that contains human readable candidate information. We propose three scenarios for student council voting. Each scenario provides different features and usage opportunities to voters. Each student can vote using any one of the scenarios in our model.

Voting Room Scenario (#1): In this scenario, voter should cast her vote inside the voting room. The room should be prepared accordingly prior to the voting. In the room stands may be used to include replaceable candidate information, papers, and candidate NFC tags. NFC tags are prepared by the registrar to include candidate information prior to the Election Day as described above. When a voter enters to the voting room, he approaches to the plastic stand and touches her phone to the tag of her favorite candidate. Then the processes described in the section 6.3.1 will occur.

Promotional Product Scenario (#2): In this scenario, the candidates may prepare promotional products (e.g. pencil, keychain) with their NFC tags attached. Within the election week, the candidates may reserve some period at the conference room to meet with the students. A 30 to 60 minutes period may be appropriate for this purpose. At the meeting candidate can talk about her plans about the next academic year to convince the voters. After this meeting, candidate distributes her promotional product to students. Students can vote by using this promotional product whenever and wherever they want, since NFC tags are already embedded into them. For example; when voter arrives home, he touches her phone to the NFC tag on the promotional product. And then the processes described in section 6.3.1 will occur.

Poster Scenario (#3): In this scenario each candidate prepares her poster together with the tags attached on it. During the election period candidates hang their posters to different places in university (e.g. cafeteria, gym). When a student sees a poster, she can vote making her phone close to the tag on the poster. As she touches the phone to the tag, the processes described in section 6.3.1 will occur.

6.4 Experiment

For the experimental purpose, a real-time environment is prepared for each of the three scenarios. To use as the test area for voting room scenario (#1), we prepared plastic stands (Figure 6.4) and candidate fliers. Stands included advertorial documents those contain candidate descriptive information. These stands are further placed into the voting room. Papers on the stands include the data such as candidate's photo, name and surname, student number, e-mail address, faculty, department, and class information. On the paper, a space is allocated for the NFC tag. For the promotional product scenario (#2), we prepared promotional pens with NFC tags attached. For the poster scenario (#3), we obtained posters, and onto the posters we have attached the NFC tags.

50 students (31 boys and 19 girls) have attended to the prototype testing. All attendees were university students who actually have voted in the previous web-based student council election. Attendees were 19-26 years old. Since NFC is a rather new technology and most people did not know much about this technology, brief explanation of the NFC technology and how to vote using our model required 2 to 3 minutes. After the scenarios are explained, all students were requested to choose one of the three available scenarios and vote using that chosen scenario. After the voting is completed, the attendees were asked to fill out a survey to test the system's usability. This survey includes SUS survey of NFC-voting and web based voting to test the satisfaction, a subjective usability metric. SUS is formed by 10 questions, each of which is rated between 1 and 5, which contributes with its score value to the overall system usability. Items 1, 3, 5, 7, 9 are positive items and the score contribution of these items is scale position minus 1. Items 2, 4, 6, 8 and 10 are negative items and, score contribution of these items is 5 minus scale position. Then to calculate the overall value of SUS, total value of score contribution is multiplied

by 2.5. Obtained SUS score ranges from 0 to 100. Higher score indicates higher usability.

Figure 6.4 Plastic Stands

In addition to SUS, some additional questions are asked in the survey to receive information about participants and scenarios.

6.5 Experiment Results and Discussion

6.5.1 Experiment Results

Our survey consisted of two parts. The first part is about attendees and scenario selections. In [20], NFC technology's major intentions are listed as *simplicity* and *ease of use*. On the other hand a voting system must definitely preserve user's *anonymity*. Thus privacy and ease of use are considered as two primary factors in choosing a scenario. So we asked participants whether the criteria to choose their scenario were privacy or ease of use. After first part, the ease of use term is tested with SUS usability survey.

In the first part, *technology usage of attendees* is asked to students to learn the familiarity with technology. In Table 6.1 the distribution of the answers is presented. The distribution of chosen scenarios is presented in Table 6.2.

Table 6.1 Frequency of Technology Usage of Attendees

Technology Usage	Count	Percentage
I try to use new technologies	33	66
I use new technologies when I need	11	22
I use new technologies when I have to	6	12

Table 6.2 Frequency of Chosen Scenario

Chosen Scenario	Count	Percentage
Voting Room	20	40
Promotional Product	11	22
Poster	19	38

60% of students those have chosen *Voting Room Scenario* stated their reason of scenario selection as *privacy*. All of the students those have chosen *Poster Scenario* and 73% of students those have chosen *Promotional Product Scenario* stated their reason of scenario selection as *ease of use*. The distribution of scenario selection reason is presented in Table 6.3.

We asked the planned place for voting to the students who have chosen promotional product scenario. Five students stated that they would vote anywhere; three students stated that he will vote at home, and three students stated that she will vote immediately after she gets the promotional product.

Table 6.3 Frequency of Scenario Selection

Scenario Selection Reason	Privacy		Ease of Use		Other	
	#	%	#	%	#	%
Voting Room	12	60	7	35	1	5
Promotional Product	3	27	8	73	0	0
Poster	0	0	19	100	0	0
Total	15	30	34	68	1	2

Table 6.4 shows the scores of the SUS survey. Figure 6.5 shows the overall SUS score of *web based voting* and NFC-voting which is calculated by SUS survey's

score. Overall SUS score of web-based voting is 78.50, and overall SUS score of NFC voting is 82.75.

6.5.2 Experiment Discussion

6.5.2.1 Survey Discussion

Figure 6.5 shows that NFC voting gained a higher usability than web based voting. We argue that the main reason for high usability of NFC voting may depend on the population who performed voting. These 50 students are university students and have high technology adaption as shown in Table 6.1. Also the sample size needs to be considered as an important factor to generalize the findings. It should be performed on a larger and homogeneous group of people to get more detailed findings.

Table 6.4 Scores of SUS Survey

Ratings and Scores of (*Web-based Voting* / NFC Voting)							
	5	**4**	**3**	**2**	**1**	**Average Score**	**Average Score Contribution**
Q1: System use	*28* / 35	*13* / 12	*2* / 1	*1* / 0	*6* / 2	*4.12* / 4.56	*3.12* / 3.56
Q2: Complexity	*5* / 1	*4* / 2	*2* / 3	*8* / 12	*31* / 32	*1.88* / 1.56	*3.12* / 3.44
Q3: Ease of use	*31* / 38	*10* / 6	*4* / 3	*3* / 0	*2* / 3	*4.30* / 4.52	*3.30* / 3.52
Q4: Need for support	*2* / 6	*7* / 3	*6* / 11	*8* / 7	*27* / 23	*1.98* / 2.24	*3.02* / 2.76
Q5: Integrity	*28* / 35	*10* / 10	*3* / 3	*4* / 1	*5* / 1	*4.04* / 4.54	*3.04* / 3.54
Q6: Inconsistency	*7* / 1	*4* / 4	*2* / 3	*8* / 4	*29* / 38	*2.04* / 1.52	*2.96* / 3.48
Q7: Ease of learning to use	*27* / 31	*11* / 5	*6* / 10	*3* / 2	*3* / 2	*4.12* / 4.22	*3.12* / 3.22
Q8: Cumbersome to use	*4* / 3	*1* / 1	*4* / 1	*6* / 6	*35* / 39	*1.66* / 1.46	*3.34* / 3.54
Q9: Confidence	*28* / 25	*15* / 15	*4* / 7	*0* / 0	*3* / 3	*4.30* / 4.18	*3.30* / 3.18
Q10 :Learning a lot of things to get going with system	*2* / 7	*5* / 2	*7* / 6	*9* / 11	*27* / 24	*1.92* / 2.14	*3.08* / 2.86
SUS Score:(Total Score Contribution * 2.5)							*78.50* / 82.75

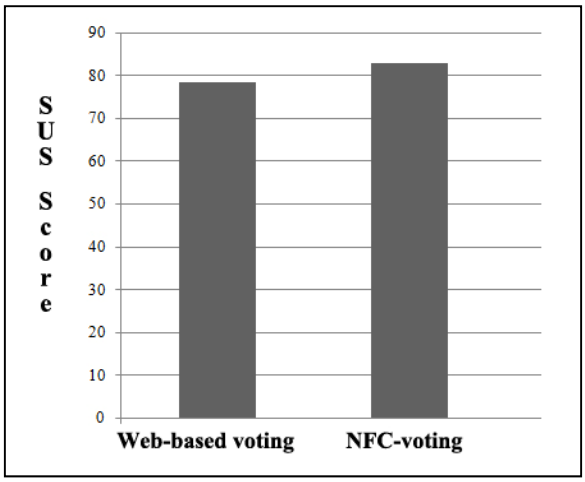

Figure 6.5 Overall SUS Score

The three proposed scenarios differ in terms of ease of use and privacy. In this regard, the voting room scenario (#1) satisfies privacy better, but it definitely requires extra time for the voters to arrive a specific voting place, hence satisfying worse ease of use. So it is expected that voting room scenario would be mostly preferred when privacy is the main concern, and it should be less preferred in terms of ease of use. On the contrary, poster scenario satisfies ease of use better, however it does not satisfy privacy property, since anyone can see a voter's selection easily. Promotional product usage may satisfy privacy in various degree based on where and how the voting is performed using the product. If a voter votes in a private place such as home, it satisfies privacy; but if she votes in a public place, it may not satisfy. So if a participant has selected the poster scenario, she is not expected to have concerns about the privacy issue, rather she is expected to care about ease of use.

All participants those have chosen poster scenario stated their reason as ease of use. On the other hand, 60% of the participants who have chosen voting room scenario stated their reason as privacy. 73% of participants who have chosen promotional product scenario stated their reason as ease of use, 27% percent stated their reason as privacy. These findings suggest that people who go for ease of use may not consider privacy with high priority. On the other hand, those people who care about their privacy, ease of use may not be so much important for their selection.

For the usability testing, NFC-voting's SUS score gave a total value of 82.75, whereas web-based voting gave a score of 78.50. At the outset, NFC-voting has

generally good usability than web-based voting. The fact that NFC-voting has a higher usability is not much surprising. It is developed to provide ease of use, but in the context of voting, NFC's usability is measured, and its high usability is attractive.

Analyzing some of the scores shows important results. The answer to the 2nd question shows that NFC-voting is less complex than web-based voting. The contribution of 3rd question shows that NFC-voting is easier to use. The result of the 6th question shows that people see less inconsistency in NFC-voting.

Questions 4, 7, and 9 can be analyzed as a group. The score of the 7th question meant that NFC model is easier to learn, 4th question meant that NFC model needs more support, and 9th question meant that voters feel less confident with NFC model. After a preliminary analysis, the results may be seen as conflicting, but it is not so. Although the people tend to apply NFC model easily, they are still suspicious about the potential problems that may occur because of immature new technologies, hence they assume that more support is required with NFC than web based known model. They also have less confidence to NFC for the same reason. But we may also comment on this, since as time passes and NFC technology becomes more recognized, and with the rise of NFC usage in daily life, the usability score of NFC may grow up in the very close future.

From our findings we contend that the usability of NFC at the context of voting is high enough, and it will increase when NFC is used more frequently in our daily life. Overall we can evaluate that, NFC-voting satisfies the student voters in university environment.

6.5.2.2 Voting Requirements Discussion

Notice that we have listed six voting system requirements; namely accuracy, democracy, anonymity, verifiability, mobility, and usability in section 6.1. In this section, we will investigate whether these requirements are actually satisfied or not.

As also explained in section 6.3, a voter encrypts her vote first using the tallier server's public key, and then using her private key and further sends the encrypted data to the validator server. The validator server checks the incoming data to make sure that the voter is registered and haven't voted before. Then it forwards data to the

tallier server. The tallier server decrypts the data with its own private key and records the vote, which is depicted in Figure 6.2. These processes prevent unauthorized users to vote and authorized users to vote more than once. So democracy requirements, namely *only eligible voters to vote* and *all eligible voters to vote only one time* are satisfied. This process also satisfies the *anonymity/privacy* requirement; a *ballot cannot be linked back to the voter who cast it*.

Also the *mobility* criterion is satisfied by enabling voting via mobile phones. Although there are some geographical constraints in voting room scenario and poster scenarios, promotional product scenario doesn't have any geographical constraints. A student can vote using the promotional product at her dormitory, home or wherever he wants.

In the contrary, *accuracy* and *verifiability* requirements couldn't be satisfied in our proposed system. In the future we will try to satisfy these properties and assess this systems objective usability.

6.5.2.3 Discussion on Related Work

In the context of voting, some usability studies are performed earlier. In [35] subjective usability together with objective usability of arrow ballot, bubble ballot, punch card, and lever machine are investigated, and it is found that bubble ballot provides higher subjective usability than the other three. In [37] the usability of DRE systems are investigated and it is found that only %10 of the voters have significant concerns. These studies investigated the usability of electronic voting systems but not remote electronic voting. On the other hand remote electronic voting is the only voting system that satisfies mobility requirement. It has the potential to increase users' satisfaction, but the usability of such systems isn't investigated. So our efforts to investigate the usability of remote electronic voting are a progress toward the goal, but there is still much work to done.

Chapter 7
Conclusions

In this study, MailMoby webmail server application and MobileMoby mobile application are developed. These two developments together provided mobility to users for processing their e-mails.

In order to create an implementation regarded with mail issue, but also to perform a further study on Mobile Communication and Near Field Communication technology, a conference paper is written which is accepted to be presented in IASTED (International Association of Science and Technology for Development) Software Engineering Conference.

These studies together with my graduate study earned me incredible benefits. These studies will form my research areas for the future, and shape my future research.

In my near future researches, I will try to extend the paper of "Usability of Mobile Voting with NFC Technology", in which I will investigate the system's subjective usability together with objective usability. NFC is rather a new technology and its usability is wondered by industry and academia. Its usability studies in different contexts will help this technology's development. I also want to develop different usable applications using NFC technology and investigate this technology's usability in different contexts.

References

[1] Email-Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Email.

[2] RFC 5322-Internet Message Format, http://tools.ietf.org/html/rfc5322.

[3] RFC 2045-Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, http://tools.ietf.org/html/rfc2045.

[4] RFC 2046-Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, http://tools.ietf.org/html/rfc2046.

[5] RFC 2047-MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text, http://tools.ietf.org/html/rfc2047.

[6] RFC 2048-Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures, http://tools.ietf.org/html/rfc2048.

[7] RFC 2049-Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples, http://tools.ietf.org/html/rfc2049.

[8] RFC 2616-Hypertext Transfer Protocol, http://tools.ietf.org/html/rfc2616.

[9] RFC 5321-Simple Mail Transfer Protocol, http://tools.ietf.org/html/rfc5321.

[10] RFC 3501-Internet Message Access Protocol, http://tools.ietf.org/html/rfc3501.

[11] Apache Tomcat,
http://tomcat.apache.org/.

[12] JavaServer Pages Technology-Developers Source for Java Technology,
http://java.sun.com/products/jsp/.

[13] Java Beans-Sun Developer Network,
http://java.sun.com/javase/technologies/desktop/javabeans/index.jsp

[14] XHTML-World Wide Web Consortium,
http://www.w3.org/TR/xhtml1/.

[15] Cascading Style Sheets-World Wide Web Consortium,
http://www.w3.org/Style/CSS/.

[16] JavaScript-Wikipedia, the free encyclopedia,
http://en.wikipedia.org/wiki/Javascript.

[17] CKEditor Official Web Site,
http://ckeditor.com/.

[18] Java ME-Sun Developer Network,
http://java.sun.com/javame/index.jsp.

[19] NetBeans Official Web Site,
http://netbeans.org.

[20] NFC-Forum Home Page,
http://www.nfc-forum.org/home.

[21] M. Csapodi, A. Nagy, New applications for NFC devices, *Proceedings of 16th IST Mobile and Wireless Communications*, Budapest, HUNGARY, 2007, 245-249.

[22] Ecma International, *Near Field Communication - White Paper*, 2005, Ecma/TC32-TG19/2005/012, http://www.ecma-international.org/.

[23] E. Siira, J. Haikio, Experiences from near-field communication (NFC) in a meal service system, *Proceedings of 1st RFID Eurasia Conference*, Istanbul, TURKEY, 2007, 273-278.

[24] J. Morak, V. Schwetz, D. Hayn, F. Fruhwald, G. Schreier, Electronic Data Capture Platform for Clinical Research based on Mobile Phones and Near Field Communication Technology, *Proceedings of 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Vancouver, CANADA, 2008, 5334-5337.

[25] S. Dominikus, M. Aigner, mCoupons: An Application for Near Field Communication (NFC), *Proceedings of 21st International Conference on Advanced Networking and Applications Workshops/Symposia*, Niagara Falls, CANADA, 2007, 421-428.

[26] O. Rashid, P. Coulton, W. Bird, Using NFC to Support and Encourage Green Exercise, *Proceedings of 2nd International Conference on Pervasive Computing Technologies for Healthcare*, Tampere, FINLAND, 2008, 203-206.

[27] X. Yiqun, H. Zhenzhen, W. Longjun, Sales data management system of chain enterprises based on NFC technology, *Proceedings of 2nd International Conference on Anti-counterfeiting, Security and Identification*, 2008, 455-458.

[28] E. Siira, T. Tuikka, V. Tormanen, Location-Based Mobile Wiki Using NFC Tag Infrastructure, *Proceedings of 1st International Workshop on Near Field Communication*, Hagenberg, AUSTRIA, 2009, 56-60.

[29] Email-Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Near_Field_Communication.

[30] A.E. Keshk, H.M. Abdul-Kader, Development of remotely secure E-voting system, *Proc. ITI 5th International Conf. on Information and Communications Technology*, Cairo, EGYPT, 2007, 235-243.

[31] L. Chun-Ta; H. Min-Shiang; L. Yan-Chi, A Verifiable Electronic Voting Scheme Over the Internet, *Proc. 6th International Conf. on Information Technology: New Generations*, Washington DC, USA, 2009, 449- 454.

[32] L.F. Cranor, R.K. Cytron, Sensus: A security-conscious electronic polling system for the Internet, *Proc. 30th Hawaii International Conf. on System Sciences*, Wailea, HI, USA, 1997, 561-570.

[33] I. Ray, I. Ray, N. Narasimhamurthi, An Anonymous Electronic Voting Protocol for Voting Over The Internet, *Proc. 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems*, San Jose, CA, USA, 2001, 188-190.

[34] Industry Usability Reporting Project. (2001). *Common industry format for usability test reports (ANSI/INCITS 354-2001)*.

[35] M.D. Byrne, K.K. Greene, S.P. Everett, Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines, *Proc. Conf. on Human Factors in Computing Systems*, San Jose, CA, USA, 2007, 171-180.

[36] J. Brooke, SUS: A “quick and dirty” usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester & A. L. McClelland (Eds.), Usability Evaluation in Industry, 1996, 189-194.

[37] B.B. Bederson, B. Lee, R.M. Sherman, P.S. Herrnson, R.G. Niemi, Electronic voting system usability issues, *Proc. SIGCHI Conf. on Human factors in computing systems*, Florida, USA, 2003, 145 – 152.

[38] O. Falke, E. Rukzio, U. Dietz, P. Holleis, A. Schmidt, Mobile Services for Near Field Communication, *Technical Report LMU-MI-2007-1*, 2007, ISSN: 1862-5207.

Curriculum Vitae

Kerem Ok was born in 2 November 1984, in Istanbul. He received his BS degree in Information Technology in 2006 from Işık University, Istanbul. He is currently working as a teaching and research assistant at the department of Information Technology of Işık University. His research interests include web technologies, mobile technologies, and near field communication.