Preface

INTRODUCTION

It’s no secret that the smart phone has become one of the most important devices in our lives. We use it for interacting with each other, entertainment as well as for performing various day to day activities. There are now more mobile devices than people in the world. Mobility is also impacting business significantly and most enterprises are providing services to facilitate their mobile workforce. More of us are using mobile technologies at work. In fact, use of mobile in the enterprise is growing at about 25% per year (Markets and Markets, 2014).

THE DIFFERENT ASPECTS OF MOBILITY

Most mobile devices use one of the two dominant operating systems: Google-developed Android and the Apple-developed iOS. Market shares of other mobile platforms like Windows and Blackberry are diminishing. Users interact with the smart phones using various mobile applications. As expected in recent days mobile applications have become extremely popular - among consumers as well as in the enterprise. There are three types of mobile application:

- Native apps live on the device and are accessed through icons on the device home screen. They are developed specifically for one Operating System and can take full advantage of all the device features. Native apps are installed through an application store (such as Google Play or Apple’s App Store).
- Web apps are not real applications; they are really websites that, in many ways, look and feel like native applications, but are not implemented as such. They are run by a browser and typically written in HTML5.
- Hybrid apps are part native apps, part web apps. Like native apps, they live in an app store and can take advantage of the many device features available. Like web apps, they rely on HTML being rendered in a browser, with the caveat that the browser is embedded within the app.

The Mobile Application Lifecycle contains different stages from development of the application, to its testing and deployment. Creating mobile applications has some unique challenges. The developer first needs to decide whether to create native, web or hybrid app (Badiu, 2013). Research shows that out of the two dozen apps each of us have on our phones, we spend 80% of our time on just five of them
Preface

(Husson, 2015). Therefore the application has to provide a superior customer experience to be attractive to the end users. Some of the requirements are being user friendly, having superior performance and not draining the battery. Testing all aspects of the app before it is released is also essential. Moreover accessibility of the application - ensuring that every person is able to access information and perform tasks regardless of that person’s physical or cognitive capabilities - is another important requirement.

In these days we utilize the mobile phone to handle sensitive data; for example financial data from a banking app, corporate data from an enterprise app as well as medical data from a healthcare app. Moreover for most of us, our mobile device is within arm’s reach 90% of the time; therefore we sometimes use the applications even using an insecure connection. This makes the sensitive data on our phone extremely vulnerable. Thus mobile security is an extremely important topic. In the race for mobile mind share, it is tempting to prioritize speed over security. In fact, about 65% of companies admit that the security of mobile applications is sometimes put at risk to meet customer demand. But at any given moment, malicious code is infecting 11.6 million of our mobile devices (Ponemon Institute, 2015).

One of the advantages of the smartphone is that it enables the determination of the context of the user using sensors on the smart phones. For example the GPS can give us the location of the user while the accelerometer can give the state of the user (whether she is static or in motion). This enables the creation of various very innovative context-aware apps (Chen & Kotz, 2000). However consumer concerns about the privacy of their personal sensitive information are at an all-time high. Therefore ensuring the privacy of the user’s data is absolutely essential. In recent years regulators have increasingly turned a watchful eye to ensure the privacy of the mobile user (Bohorquez & Felz, 2016).

Once the application has been developed one needs to analyze the applications to determine how it is being utilized by the end user. Mobile Analytics can help determine the impact a mobile application has on a company’s business. Such analysis can discover any deficiencies in the application so that the problems can be quickly rectified. The analysis can also give insights on how to make the application more useful for the consumers. Predictive analytics can discover problems even before they occur. On the other hand Prescriptive analytics provide actionable insights that will move businesses forward by not only indicating exactly what the issues are, but also suggesting which measures need to be taken to correct them. A recent report by the Aberdeen Group found companies using mobile analytics saw an 11.6 percent increase in brand awareness while those without a mobile-specific analytics strategy had a 12.9 percent decrease (Minkara, 2014).

Most mobile applications need to interact with various backend services. For example Push notifications let an application notify a user of new messages or events even when the user is not actively using the application. In many cases these backend services are hosted in the cloud. Cloud services are a good match for supporting mobile devices. Mobile applications tend to have time variable usage patterns that are well handled by the scalability and elasticity of cloud computing - increasing and decreasing the backend resources to match the level of requests from the mobile devices. It is also characteristic of mobile applications to make use of server-side data. Thus the interaction of mobility and cloud is an important topic. The Cloud Standards Customer Council (CSCC) has developed Mobile Cloud Architecture (Cloud Standard Customer Council, 2015) to showcase the interaction of mobile devices and cloud services.

OBJECTIVE OF THE BOOK

This book covers important topics from the major areas of Mobility:
Mobile Application Development: We focus on the challenges of mobile application development, Mobile Testing and Accessibility.

Mobile Security: Since Mobile Security is an extremely important topic several chapters are dedicated to the different aspects of Mobile Security. We look at how security can be ensured by program analysis as well as various ways to control access to sensitive data.

Context-Aware Applications: We explain different techniques to track the location of the user. Some challenges of context-aware applications, especially ensuring privacy of the data, are also discussed. We also introduce an innovative participatory sensing application which makes use of mobile sensors.

Mobile Analytics: A comprehensive survey of Mobile Application and User Analytics is presented.

Mobile and Cloud: We discuss the synergy between Mobile and Cloud and explain the challenges and opportunities of Mobile Cloud Computing.

Some chapters survey important areas of Mobility while other chapters describe some key research challenges and present their solutions. This comprehensive publication aims to be an essential reference source and builds on the available literature in this field. Academicians, researchers, advanced-level students and mobile application developers will find this text extremely useful in furthering their research exposure to pertinent topics in this area that is becoming more and more popular and important.

ORGANIZATION OF THE BOOK

The book is organized into twelve chapters. A brief description of each of the chapters follows:

Chapter 1 discusses three key aspects Mobile application development:

1. Smart and incremental computation to improve battery consumption,
2. The trade-offs that can be made between accuracy and simplicity of the data-processing algorithms, and
3. Data storage and privacy aspects, i.e., which information should effectively leave the user’s smartphone.

The authors showcase the development of an efficient life-logging Android application, MEmoIt based on these three aspects.

Chapter 2 surveys a key aspect of Mobile Application development – the testing of the applications. It discusses three key forms of mobile testing. Functional testing is performed to ensure functionality, i.e. to test whether the application is performing the functions that it was designed for. Performance testing is conducted to determine how optimal the application is, in terms of its compute resource usage, battery usage and latency related issues. And finally, Usability and Accessibility testing aims to capture how easy it is for users to be able to work with the applications to execute the functions for which the application is designed.

Chapter 3 digs deeper into the important area of accessibility of the mobile applications. The mobile evolution has brought two areas of Accessibility closer together. People who rely on assistive technologies are able to participate in ways that have been historically unavailable to them. On the other hand,
as people are performing more tasks on devices that are smaller and using them in situations where they
may not be able to look at or hear the device, these individuals require assistive technologies that have
traditionally focused on people with severe disabilities.

Chapter 4 introduces Phoenix, a novel solution that combines static program analysis with machine
learning to ensure that no private information is exposed to unauthorized observers in a mobile applica-
tion. Phoenix uses relatively scalable static analysis to approximate possible program behaviors, and
then applies machine learning in order to identify programs exhibiting suspicious sequences of opera-
tions. This solution has been widely applied to mobile applications obtaining impressive results, with
low false-positive and false-negative rates.

To secure mobile devices, there has been increasing focus on Trust negotiation, a procedure whereby
two entities are able to establish a measure of mutual trust, even if no prior contact between either entity
has existed in the past. Adaptive trust negotiation refers to the ability to dynamically adjust security
parameters based on the level of trust established during the negotiation process. Chapter 5 explores the
feasibility and utility of adaptive trust negotiation and its suitability for a mobile healthcare application.

Chapter 6 also looks into the security aspects of mobile healthcare application. It presents the ben-
efit of utilizing role-based access control (RBAC) which allows the information owner to specify how
much access other users have on the information based on their roles. For example this enables patients
to grant access of their electronic health and fitness information to different individuals (e.g., primary
physicians, spouse, family, emergency medical providers, etc.) at varying levels of granularity. RBAC is
used by the mobile application to determine the ability of a user to view or modify medical information.

Chapter 7 proposes and discusses the Spatio-Situation-Based Access Control (SSBAC) model that
combines features from existing access control models (like Role-Based Access Control, Spatio-temporal
Access Control, Situation-Based Access Control, Workflow-Based Access Control, etc.) with new capa-
bilities for the dynamic enforcement of security as a user moves among various locations with his/her
mobile device and associated applications over time and distance. This concept is applied to a mHealth
application, to constrain access to different health IT systems as a medical provider moves in both space/
time and by the situation so that the application can dynamically adapt to the environments and allow
or deny the access to specific data.

Chapter 8 focuses on the work done in the Platys project for the privacy and security aspects of
context-aware mobile applications. It presents a fine-grained context driven access control mechanism
for the apps. Context in Platys is generated by leveraging capabilities of smartphones. This allows an
app on the phone to capture key elements of context: like the user’s location and, through localization,
characteristics of the user’s environment, etc. The context is represented using Semantic Web technologies
which allow handling of various data flow scenarios from and through users’ mobile devices. Access
control policies are then defined to reduce security and privacy risks.

Location-based services have become very popular both in the general public and enterprises, with
the advent of smartphones and other sophisticated mobile devices. While many people are accustomed
to using such services, knowledge of how they work, and which underlying technologies are most ap-
propriate for different types of use cases, remains limited even to experienced developers. Chapter 9
describes the different types of location tracking technologies, their advantages and disadvantages as
they relate to different use cases, as well as the challenges associated with the technologies and location
tracking in general.

Participatory sensing empowers citizens with sensor-embedded hand-held devices to contribute to
micro and macro-scale urban sensing applications. Chapter 10 focus on a novel Urban Sensing Platform
(USP) that aggregates data from an eco-system of data sources (e.g., mobile sensing data, social media, web-based public forums, as well as the civic agencies’ internal data) to derive valuable insights. Challenges in terms of architecting the platform to gather and aggregate data in a scalable manner are discussed. The aggregated data is then categorized to create meaningful summaries of reports gathered by the platform. This chapter also describes a data veracity framework that determines data veracity in participatory sensing systems. Finally, a case study of a participatory sensing deployment for developing regions is presented.

Chapter 11 is a comprehensive survey of Mobile Analytics. The chapter begins with a taxonomy of mobile analytics problems and then discusses the technical details of a typical mobile analytics solution. Scale, heterogeneity, dynamically changing environments, and diverse privacy requirements, pose challenges to collecting and processing data for such analysis. This chapter examines how analytics solutions handle these challenges. The core of the chapter consists of a technical section describing the general architecture of a mobile analytics solution, procedures to collect and process data, event monitoring infrastructure, system administration processes, and privacy management policies. Case studies of a number of analytics solutions available as commercial products or prototypes are introduced.

Chapter 12 focuses on Mobile Cloud Computing which can be defined as a combination of ubiquitous connectivity of mobile device and elastic resources of the cloud to enable a computing and storage platform for providing unrestricted mobility, personalization, storage, and computing on the go. The chapter discusses the core techniques and novel applications of mobile cloud computing as well as the challenges faced by mobile cloud systems. The chapter concludes by highlighting opportunities and future research areas in the field of mobile cloud computing.

Sougata Mukherjea  
IBM, India

REFERENCES


Preface

