Preface

Do not worry about your difficulties in Mathematics. I can assure you mine are still greater. – Albert Einstein

The corresponding book publication summarizes the recent research papers on online banking security techniques, approaches and technologies and Case studies entitled, “Online Banking Security Measures and Data Protection.” This comprehensive and timely publication aims to be an essential reference source, building on the available literature in the field of e-banking security while providing for further research opportunities in this dynamic field. It is hoped that this text will provide the resources necessary for policy makers, technology developers and managers to adopt and implement security techniques and technologies in developing banks across the globe.

This book summarizes some current trends in the online banking security such as online banking security services, data protection techniques, applications and technologies, and explores one key area of growth: Online Banking. To illustrate the role of Applications and Services in the growth of online banking industries, a number of examples focusing on the learning, government, industry and security are used. Recommendations for future areas are presented.

This book is intended for researchers and practitioners who are interested in issues that arise from using technologies of online banking security advancements. In addition, this book is also targeted to anyone who wants to learn more about the online banking security measures and data protection research advancements in design and applications. For example, policy makers, academicians, researchers, advanced-level students, technology developers, bank officers and government officials will find this text useful in furthering their research exposure to pertinent topics in e-banking security and assisting in furthering their own research efforts in this field. Online banking security has become a hot topic in recent years and people at different levels in any organization need to understand online banking in different ways and different perspectives.
BOOK DESCRIPTION, MISSION, AND OBJECTIVES

Although the e-banking field has been found Information Systems literature since the mid-1990s, there is still a lack of advanced research into banking security adoption and associated organizational issues. In addition, there is a shortage in case studies surveying the real experience of firms and organizations in deploying e-banking security. As e-banking is an IT product for development and evolution, this sort of gap in the advanced research makes some sensitive issues and challenges for banking sector, particularly these that currently develop e-banking security because the weaknesses and actual limitations in subject to this field normally mean difficulties in planning and developing e-banking security measures and controls.

The use of the Internet as a main distribution channel raises the necessity of securing e-banking since it becomes a vital issue to the environment and could make organizations more vulnerable to system attacks and threats. Although there are several techniques and methods to security as a whole whose value is evident – there is an expectation that security can be more efficiently managed if the concentration goes beyond technical-oriented solutions.

E-banking can not only offer various benefits to customers in terms of ease and cost of transactions, but it also poses new challenges for banks in supervising their financial systems and in designing and implementing necessary security measures and controls. Therefore, understanding security communication in e-banking issues is important for senior management because it would assist them enhance their approach to e-banking security. This edited book addresses this issue by reporting exploratory case studies about developing and implementing security in e-banking. Particularly, this edited book of advanced research aims to explore how e-banking security measures and controls takes place within the bank, what are the standards and procedures that play an important role to the success of e-banking security and what key lessons come out of their experience which could be generalized.

This book also looks to discuss and address the difficulties and challenges that banks have faced in implementing security techniques, technologies and applications. The editor will seek chapters that address different aspects of e-banking adoption, ranging from Phishing of Banking Information, Pharming of Banking Websites, Adaptive Authentication in Banking, “Watering Hole” Attacks, Malware-Based Attacks, Zeus Trojan, Mobile Banking Security, Identity Theft, and Related Topics.

This book focuses on advanced research in the practical applications and the theoretical foundations of online banking security, through presentation of the most up-to-date advances and new directions of research in the field from various scholarly, professional, and practitioner perspectives. An interdisciplinary look at online banking, including engineering and business aspects, such book covers and
encourages high-quality research exposition on such topics as virtualization technologies for online banking, online banking security utilities, real case studies on online banking security vulnerabilities as well as data protection techniques, and business perspectives for online banking security.

The main mission of this book is to be the premier and authoritative source for the most innovative scholarly and professional research and information pertaining to aspects of online banking security measures and data protection. Such book presents advancements in the state-of-the-art, standards, and practices of online banking security, in an effort to identify emerging trends that will ultimately define the future of “the Cloud of Online Banking” and “the Gog of Online Banking”. The main topics are discussed through original papers, review papers, technical reports, case studies, and conference reports for reference use by academics and practitioners alike.

This book is intended to reflect new directions of research and report latest advances. It is a platform for rapid dissemination of high quality research / application / work-in-progress articles on Online Banking Security solutions for managing challenges and problems within the highlighted scope.

The objectives of this book are multi-folds, including:

1. Establish a significant channel of communication among Online Banking Security researchers, engineers, practitioners and IT policy makers;
2. Provide a space to publish and share the latest high quality research results in the area of Online Banking Security;
3. Promote and coordinate international collaboration in the standards of Cloud and Fog Computing of Online Banking to meet the need to broaden the applicability and scope of the current and future research of Online Banking Security.

Topics to be discussed in this book include the following:

- Techniques, technologies, and services
- Applications
- Architecture
- Standards
- Management
- Cloud and Fog engineering
- Business
- Security Vulnerabilities and threats
WHAT THIS BOOK COVERS

In this book, we will present the current state of online banking security research advancements on design, and applications. So that we will summarize each advanced research, its influence in the science of online banking security measures and data protections as follows:

Chapter 1: Online Banking and Finance

In recent years, online banking has become an alternative channel for most traditional entities. The increase in the number of users and rapid expansion has resulted in a successful strategy among financial institutions. This chapter discusses the use of technology in the finance industry and the various factors associated with it, as well as introducing the reader to the basic characteristics of online financial services. We review the current literature identifying the relevant research questions for our purpose.

Chapter 2: Internet Banking Usage Level of Bankers: A Research on Sampling of Turkey

Banks provide service not only through branches in the countries but also offer banking services to customers over the internet. However, customers concern using internet banking because of the various troubles and adversities that may occur on the web and because of their habits. The using of internet banking is still not reached the desired level due to various reasons such as security, troubles on web and habits of customers. In this research, bankers using rate of internet banking and bankers approach on internet banking are determined. According to the survey results in Turkey, almost all of the bankers use internet banking but using of mobile applications does not appear to fully spread. Even though the using of internet banking is very common among the bankers, some of the participants said that they encountered some problems while using internet banking. Solutions of systemic deficiencies, password security problems and other security problems will increase the using of internet banking.

Chapter 3: Internet Banking and Financial Customer Preferences in Turkey

The first online banking service was introduced in Turkey by İş Bank in 1998. However, the number of internet users has been increasing rapidly in Turkey, the number of online banking users did not increase with a similar pace. Although banks
are taking measures for the security of online banking transactions, many financial consumers are still concerned about the security of these transactions therefore preferring not to use online banking. This study reveals the development of internet banking in Turkey and consumer percentages. Previous research on the factors affecting the usage of e-banking are also addressed in this study. It was found that the majority of these studies focus on the correlation between the security concerns which result in avoiding using internet banking.

**Chapter 4: Expectation and Perception of Internet Banking Service Quality of Select Indian Private and Public Sector Banks: Comparative Case Study**

This research paper mainly deals with expectation and perception of service quality of select Indian Banks i.e. SBI and HDFC on the customer satisfaction. The research survey was based on IS-QUAL dimensions a diagnostic model developed in 2014, which measures service quality and internet service quality in terms of customer expectations and perceptions of banking services. This present research tends to evaluate the overall idea of expected and perceived services of the two banks. This study is a cross-sectional survey that employed the use of pre-structured questionnaire to collect primary data from a sample of 120 respondents through personal contact, field survey and email. Collected data have been analyzed through SPSS 21 software by different statistical tools like Reliability test for judgment of internal consistency of collected data and paired t-test.

**Chapter 5: Towards Fully De-Materialized Check Management**

Banks worldwide are putting a big effort into de-materializing their processes, in order to streamline the processes and thus reducing overall costs. In this chapter, the authors describe how the de-materialization can be a big opportunity for banks, describing the European context. Furthermore, the de-materialization of check handling is taken as example, proposing a review of existing technologies and describing the advantages that a real framework can give to the users and to the bank systems.

**Chapter 6: Emerging Challenges, Security Issues, and Technologies in Online Banking Systems**

Online banking security is a critical issue over request-response model. But the traditional protection mechanisms are not sufficient to secure the online banking systems that hold information about clients, and banks. The infrastructure of networks, routers, domain name servers, and switches that glue these online banking
systems together could be fail, and as a result, online banking systems will no longer be able to communicate accurately or reliably. A number of critical questions arise, such as what exactly the infrastructure is, what threats it must be secured against, and how protection can be provided on a cost-effective basis. But underlying all these questions is how to define secure online banking systems. In this chapter, emerging challenges, security issues and technologies in Online Banking Systems will be analyzed and discussed systematically.

Chapter 7: The Influences of Privacy, Security, and Legal Concerns on Online Banking Adoption: A Conceptual Framework

Business globalization and the rising new technology enforced traditional banking to head towards online banking services, which facilitates customers to obtain access to their accounts from their business sites and personal computers to online banking services. The objective of this chapter is to construct a framework of adoption of online banking and represent the major influences of privacy, security, and legal concerns on online banking adoption. Furthermore, the chapter reveals the main challenges in the development of online banking system. The adoption of online banking can decrease the operating expenses and offer good and rapid services to their customers. The framework factors have been classified as facilitators and barriers of adoption of online banking. Performance expectancy, effort expectancy and social influence have been classified as facilitators whereas security concerns, privacy concerns and legal concerns have been classified as barriers. The results revealed various significant suggestions for online banking service providers, designers and developers.

Chapter 8: Analysis of Data Validation Techniques for Online Banking Services

The insufficient preparation for the information and communication technologies revolution led to few offering online transaction platforms, information security features, and credit facilities. One of the security concerns is a lack of data validation. Data that is not validated or not properly validated is the main issue for serious security vulnerabilities affecting online banking applications. In this chapter, the influences of security issues on world banks will be discussed. A number of data validation methods will be also reviewed to date to provide a systematic summary to banking environment. Based on the advantages and disadvantages of each method, the IT developer will decide which is best suited to develop the systematic online banking application. From this analysis, a global view of the current and future
tendencies of data validation will be obtained and therefore provision of possible recommendations for solving the security and privacy issues for the online banking services.

Chapter 9: Anytime Anywhere Any-Amount Anybody to Anybody Real-Time Payment (5A-RTP) with High Level Banking Security

This chapter introduces about a Proposal to any bank of any country for fast but secured transfer of money anytime anywhere any-amount by anybody to anybody on the spot with confirmation from the payee on the spot. This breaking scheme is entitled as “5A-RTP scheme” where ‘5A’ stands for Anytime Anywhere Any-amount Anybody to Anybody and ‘RTP’ stands for Real-Time Payment. There is no paperwork at all. It is highly secured, fast and 100% technology-based. It is completely secured, realization of payment happens immediately very fast, without any man-hour or manpower of the bank. It is claimed that 5A-RTP scheme, if incorporated in all the banks in any country, will give the country a huge momentum of customers’ satisfaction, huge momentum in country’s growth and economic progress. The revolutionary breakthrough in 5A-RTP scheme is that it dominates all of the existing banking instruments. The 5A-RTP scheme may even slowly cause a natural death of the existing instruments.

Chapter 10: An Algorithm for Securing Hybrid Cloud Outsourced Data in the Banking Sector

The Cloud has become a significant topic in the banking computing; however, the trend has established a new range of security issues that need to be addressed. In Cloud, the banking data and associated software are not under their control. In addition, with the growing demands for Cloud networks communication, it becomes increasingly important to secure the data flow path. The existing research related to security mechanisms only focuses on securing the flow of information in the communication banking networks. There is a lack of work on improving the performance of networks to meet quality of service (QoS) constrains for various services. The security mechanisms work by encryption and decryption of the information, but do not consider the optimized use of the network resources. In this chapter the authors propose a Secure Data Transmission Mechanism (SDTM) with Preemption Algorithm that combines between security and quality of service for the banking sector. Their developed SDTM enhanced with Malicious Packets Detection System (MPDS) which is a set of technologies and solutions.
Chapter 11: Prevention, Detection, and Recovery
of CSRF Attack in Online Banking System

Online banking system has created an enormous impact on IT, Individuals, and networking worlds. Online banking systems and its exclusive architecture have numerous features and advantages over traditional banking system. However, these new uniqueness create new vulnerabilities and attacks on an online banking system. Cross-site scripting request forgery or XSS attack is among the top vulnerabilities, according to recent studies. This exposure occurs, when a user uses the input from an online banking application without properly looking into them which allows an attacker to execute malicious scripts into the application. Current approaches use to mitigate this problem, especially on effective detection of XSS vulnerabilities in the application or prevention of real-time XSS attacks. To address this problem, the survey of different vulnerability attacks on online banking system performed and also presents a concept for the prevention, detection, removal and recovery of XSS vulnerabilities to secure the banking application.

Chapter 12: Ransomware: A Rising Threat
of New Age Digital Extortion

Compared to the last five to six years, the massive scale by which innocent users are being subjected to a new age threat in form of digital extortion has never been seen before. With the rise of Internet, use of personal computers and devices has mushroomed to immense scale, with cyber criminals subjecting innocent users to extortion using malware. The primary victim to be hit the most has been online banking, impacting the security and reputation of banking and financial transactions along with social interactions. Online security revolves around three critical aspects – starting with the use of digital data and files, next with the use of computer systems and finally the internet as an unsecure medium. This is where Ransomware has become one of the most malicious forms of malware for digital extortion threats to home and corporate user alike.

Chapter 13: Insider Threat in Banking Systems
Complete Recognition Capability

Insider threat poses huge loss to organizations since malicious insiders have enough knowledge to attack high sensitive information. Moreover, preventing and detecting insider attacks is a hard job because malicious insiders follow legal paths to launch attacks. This threat leads all kinds of attacks in banking systems in the amount of loss it causes. Insider threat in banking systems poses huge harm to banks due to
the importance and attractiveness of assets that banks have. This chapter discusses insider threat problem in banking sector, and introduces important surveys and case studies that show the severeness of this threat in this sector. Moreover, the chapter demonstrates some policies, technologies and tools that may prevent and detect insider threat in banking systems.

**Chapter 14: Achieving Security to Overcome Attacks and Vulnerabilities in Mobile Banking Security**

Mobile Banking is a means of connectivity between bank and its customers. It would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their mobile banking application. Mobile Banking is a provision and availability of both banking and financial services with the help of mobile telecommunication devices as an Application. It would be expected that the mobile application itself check the upgrades and updates and download necessary patches. Mobile banking has brought the advantage to have an alternate to debit and credit card usage. Mobile banking has the below three inter-related concepts: Mobile accounting, Mobile brokerage, Mobile financial information services. Mobile banking services are Account information provision, Monetary Transaction, Investment facilitation, Support and Content services. The threats involved in Mobile Banking are categorized as, Threats against end user and end user device, Threats against communication network, Threats against remote banking service.

**Chapter 15: Credit Card Fraud: Behind the Scenes**

In 2004, Dan DeFilippi was arrested for numerous counts of credit card fraud. This chapter will include a full length interview transcript between Katina Michael and Dan DeFilippi. The transcript will cover areas to do with: (1) how Dan became involved with credit card fraud, (2) the techniques used by fraudsters to evade detection; (3) the socio-ethical impacts of the fraud; (4) how he was detained by the FBI; and (5) how he reformed by becoming a key informant and evading jail. The interview is 12,000 words in length, and has numerous sections. It contains numerous illustrations and primary documentation of the offences of credit card fraud, and victim statements.