Preface

It is obvious that Information Technologies (IT) have had a major impact on all aspects of our lives. Information Technologies have made us more productive in our workplaces, brought us closer together, transformed our lives and ultimately, defined who we are as humans. We live in an age where information defines us. We are able to communicate more freely and effortlessly with one another, make more informed decisions, and have a higher standard of living, all, resulting from advances in Information Technologies (IT). The growth in Internet usage and e-commerce has offered businesses and governmental agencies the opportunity to collect and analyze information in ways never previously imagined. One result of the fast expansion of Information Technology in our daily lives is that it generates a large amount of data. The number of Americans who utilize the Internet for their daily business such as online purchasing, conducting online banking, and for entertainment value has increased in the past few years. Technological advances and the World-Wide-Web revolution have allowed for vast amounts of data, both internal and external sources, to be generated, collected, stored, processed, analyzed, distributed, and used at an ever-increasing rate by organizations and governmental agencies. According a survey by US Department of Commerce there is an astonishingly large growth in data, and this can be traced to the ever increasing number of Americans who are online on daily basis and are engaged in several activities, including engaging in online purchases and e-commerce, conducting banking online, learning, entertaining each other and being entertained by others, and above all, interacting socially. As a result, the size of a typical business database has grown a hundred-fold during the past five years. Data experts estimate that in 2008 the world generated 75 exabytes of data. While this amount of data is more than all the words ever spoken by human beings, it is far less than what was produced just a year later, in 2009. The rate of growth is just as staggering – the amount of data produced in 2008 was up 35% from previous years. The rate of growth in data has not slowed. International Data Corporation (IDC) estimates that the amount of data generated in 2009 was 1.2 million Petabytes. (A Petabyte is a million gigabytes.) Although this seems to be an astonishingly large amount of data, it is paled in compression to what IDC estimates to be the amount of data that will be generated in 2020. IDC estimates that the amount of data generated in 2020 will be 44 times as much as this year’s and will reach an incomprehensible amount of 35 Zettabytes (A Zettabyte is 1 trillion gigabytes).

Assuring the trustworthiness of this massive amount of data and the integrity of the technologies supporting it are formidable challenges facing organizations. Without security that guarantees the trustworthiness of the data and the integrity of the supporting technologies, the data cannot be used appropriately. This is chiefly due to realization that concerns over security of what is collected and the potential harm from personal privacy violations resulting from their unethical uses have also skyrocketed. This implies
that securing data and related technologies and ensuring the privacy of that information contained with it will be major areas of concern for researchers and practitioners alike.

With the emergence of the new paradigm in Information Technology, the role of information security and privacy will evolve. As a result, information security and privacy will be everyone’s business, not just IT’s. This change in the way companies view and approach information security and privacy will be driven primarily due to consumer demand. Consumers will demand more security for information about them and will insist on better ethical uses of that information. This demand will drive business profitability measures and will ultimately manifest itself as pressure on the government and other regulatory agencies to pass tougher and more intrusive legislation and regulations, resulting in greater pressure on the business organizations to comply and to demonstrate a commitment to information security and privacy. Therefore to be successful, organizations need to focus on information security not just as an IT issue, but rather as a business imperative. It is obvious that information security is a priority for the management, as it should be. Regardless of the source, the impact on organization can be severe ranging, from interruption in delivery of services and goods, loss of physical and other assets, loss of customer good will and confidence in the organization, to disclosure of sensitive data. Such sensitive data breaches can be very costly to the organization.

As we move forward, new security and privacy challenges will likely to emerge. It is essential that we are prepared for these challenges in order to take full advantage of the opportunities. This book is an attempt to help researchers and practitioners seeking answers to these complex problems. Optimizing Information Security and Advancing Privacy Assurance: New Technologies is a comprehensive collection of 16 chapters that explain the changing roles of Information Technology and its impact on security and privacy.

In chapter 1, “Provable Security for Outsourcing Database Operations,” written by Evdokimov, Fischmann, and Gunther, the authors present a new method to construct encryption schemes for exact selects and prove that the resolution schemes satisfy this notion.

In chapter 2, “A Host-Based Intrusion Detection System Using Architectural Features to Improve Sophisticated Denial-of-Service Attack Detections,” Tao, Yang, Peng, and Li identify hardware architecture features and integrate them into HIDS framework bases on a modern statistical Gradient Boosting Trees model.

In chapter 3, “A Keystroke Biometric System for Long-Text Input,” written by Tappert, Cha, Villiani, and Zack, describes the development and evaluation of a keystroke biometric system for long-text input.

Chapter 4, “A Six-View Perspective Framework for System Security: Issues, Risks, and Requirements,” by Yadav, proposes framework that presents a synergistic view of the system security in which the author presents an extensive list of heuristics/guidelines under each review, discussion security issues, risks and requirements.

In chapter 5, Sumeeth, Singh, and Miller examine the question of online privacy policies in their chapter “Are Online Privacy Policies Readable?” This examination is undertaken by collecting privacy policies from the most popular sites on the Internet and analyzing their readability.

In chapter 6, “Protecting User Privacy Better with Query l-Diversity,” Liu and Hua examine major privacy concerns in location-based services. Most user privacy techniques are based on cloaking, which achieves location k-anonymity. The key is to reduce location resolution by ensuring that each cloaking area reported to a service provider contains at least k mobile users.

Chapter 7, “Globalization and Data Privacy: An Exploratory Study,” by Totterdale, provides a summary of major data privacy laws in the U.S., Europe, and India, and their implication for businesses.
Additionally, in this chapter, relationships between age, residence (country), attitudes, and awareness of business rules and data privacy laws are explored for 331 business professionals located in the U.S and India.

Next, “Security Issues for Cloud Computing” by Hamlen, Kantarcioglu, Khan, and Thuraisingham, discusses security issues for cloud computing, presents a layered framework for secure clouds, and then focuses on two of the layers, i.e., the storage layer and the data layer. In particular, the authors discuss a scheme for secure third party publications of documents in a cloud.

Chapter 9, “Global Information Security Factors,” by White and Long, explores the global nature of information security from the perspectives of corporate professionals. Through an empirical study with corporate professionals, who have first-hand information security knowledge, the authors confirm that the proposed knowledge topics are relevant toward a comprehensive understanding of information security issues. Analyzing the empirical data, the authors found two global security factors: business protection of data and government/social issues.

In chapter 10, “The Integrated Privacy Model: Building a Privacy Model in the Business Processes of the Enterprise,” Majdalawieh discusses the challenges that faced in the “DigNet” age in terms of privacy and proposes a framework for privacy protection. This framework is integral in ensuring that personal data protection is part of business processes of any systems that are involved in collecting, disseminating, and accessing an individual’s data.

In chapter 11, “Policy Enforcement System for Inter-Organizational Data Sharing,” Awad, Khan, and Thuraisingham describe a Data Sharing Miner and Analyzer (DASMA) system that simulates data sharing among N organizations. Each organization has its own enforced policy. The N organizations share their data based on trusted third party. The system collects the released data from each organization, processes it, mines it, and analyzes the results.

In chapter 12, “Goals and Practices in Maintaining Information Systems Security,” by Erlich and Zviran, the authors discuss the goals of information systems security and the techniques to achieve them. Specifically, the chapter focuses on access control and the various authentication approaches, as well as intrusion detection and prevention systems.

In chapter 13, “Factors Influencing College Students’ Use of Computer Security,” by Pendegraft, Rounds, and Stone, the authors present and develop theoretically sound model linking student and system security characteristics to students’ security behaviors.

In chapter 14, “A Game Theoretic Approach to Optimize Identity Exposure in Pervasive Computing Environments,” by Zhu, Carpenter, Zhu, and Mutka, the authors propose the Hierarchical Identity model, which enables the expression of one’s identity information ranging from precise detail to vague identity information. The authors model privacy exposure as an extensive game. By finding subgame perfect equilibria in the game, the approach achieves optimal exposure. It finds the most general identity information that a user should expose and which the service provider would accept. The authors’ experiments show that their models can reduce unnecessary identity exposure effectively.

In chapter 15, “Hiding Message in Map along Pre-Hamiltonian Path,” by Muttoo and Kumar, the authors present an algorithm to embed information in a map along Hamiltonian path. A file based data structure in which a graph is treated as a composition of three components, node, segment, and intermediate points that constitute a segment, is used to store a graph.

In chapter 16, “Probabilistic Inference Channel Detection and Restriction Applied to Patients’ Privacy Assurance,” by Alhaqabani and Fidge, the authors present definitions and algorithms for detecting inference channels in a probabilistic knowledge base and maximising an attacker’s uncertainty by restricting
selected inference channels to comply with data confidentiality and privacy requirements. As an illustration, a healthcare scenario is used to show how inference control can be performed on probabilistic relations to address patients’ privacy concerns over Electronic Medical Records.

Hamid R. Nemati
The University of North Carolina at Greensboro, USA