

Preface

Recently, and due to the large diversity of the hackers and attacks, information security algorithms and application have become a crucial need for protecting almost all information transaction applications. Cyber security is an important branch of information security that is applied in computers and networks. This volume covers the cyber security branch, and aims to ensemble the up-to-date advances in various topics in cyber security, and reports how organizations can gain competitive advantages by applying the different security techniques in the real-world scenarios. The volume will provide reviews of the cutting-edge technologies, algorithms, applications, and insights for cyber security-based systems. In particular, the book will be a valuable companion and comprehensive reference for both postgraduate and senior undergraduate students who are taking a course in cyber security. The volume will be organized in self-contained chapters to provide greatest reading flexibility.

This edited volume comprises 22 chapters, including an overview chapter, which provides an up-to-date and state-of-the art research on Cyber Security and Cloud Services.

The book is divided into four main parts:

- **Part-I:** Bio-inspiring System in Cyber Security
- **Part-II:** Mobile Ad Hoc Networks and Key Managements
- **Part-III:** Biometrics Technology and Applications
- **Part-IV:** Cloud Security and Data Services

Part I entitled *Bio-inspiring System in Cyber Security* contains five chapters that deal with several techniques of bio-inspiring in application to watermarking.

In Chap. 1, *A Bio-inspired Comprehensive Distributed Correlation Approach for Intrusion Detection Alerts and Events in Complex Computer Networks*, Ayman M. Bahaa-Eldin presents a Distributed Agent Correlation Model (DACM) providing a scalable alert correlation for large-scale networks. The proposed model utilizes multiple distributed agents to provide an integrated correlation solution. The model can be extended by creating new correlation agents, and can be tailored to a protected network by selecting what agents to use and configuring each individual agent's parameters. DACM correlates alerts from IDSs with other information source such as INFOSEC tools and system and application log files.

The results show that DACM enhances both the accuracy and completeness of intrusion detection by reducing both false positive and false negative alerts; it also enhances the early detection new threats.

Chapter 2, *Bio-inspired Evolutionary Sensory System for Cyber-Physical System Security*, by Mohamed Azab and Mohamed Eltoweissy discusses the current challenges to Cyber-Physical Systems security, survey relevant solutions, and present a novel system, CyPhyMASC, towards realizing pervasive Monitoring, Analysis, Sharing, and Control (MASC) for enhanced CPS security. CyPhyMASC is a bio-inspired intrinsically resilient, situation-aware system utilized by Security Service Providers (SSPs) to provision MASC services to the Target-of-Security system (ToSs) comprising numerous heterogeneous CPS components.

In Chap. 3, *An Optimized Approach for Medical Image Watermarking*, Mona M. Soliman et al. present an authentication scheme which enhances the security, confidentiality, and integrity of medical images transmitted through the Internet by invoking particle swarm optimization with its modifications including particle swarm optimization, quantum particle swarm optimization, weighted quantum particle swarm optimization techniques in adaptive quantization index modulation, and singular value decomposition in conjunction with discrete wavelet transform (DWT) and discrete cosine transform (DCT). The experimental results show that the proposed approach yields a watermark which is invisible to human eyes, robust against a wide variety of common attacks, and reliable enough for tracing colluders.

In Chap. 4, *Bio-inspiring Techniques in Watermarking Medical Images: A Review* authored by Mona et al. is reviewed and employed different bio-inspiring and computational intelligence techniques such as restricted Boltzmann machine, deep belief network, rough sets, swarm intelligence, artificial immune systems, and support vector machines to tackle various problems in watermark embedding and extraction procedure of medical image watermarking.

In Chap. 5, *Efficient Image Authentication and Tamper Localization Algorithm Using Active Watermarking*, Sajjad et al. propose an image authentication system with accurate tamper localization ability. In the proposed algorithm a 16-bit watermark key has been created from each block of pixels in a host image; various types of tampering attacks were performed in order to evaluate the proposed tamper detection method. The proposed tamper localization algorithm is evaluated by calculating False positive (FP) and False Negative (FN), and the results are compared to several current image authentication techniques, and the comparison results clearly proved the high level of our tamper detection rate.

Part II entitled *Mobile Ad Hoc Networks and Key Managements* contains six chapters that describe several cyber security techniques including trusted Ant Colony Multi Agent-Based Routing Algorithm for Mobile Ad Hoc Networks, Cybercrime Investigation Challenges: Middle East and North Africa, Multilayer Artificial Immune System for Network Security, and Key Pre-distribution Techniques for WSN Security Services.

In Chap. 6, *TARA: Trusted Ant Colony Multi Agent Based Routing Algorithm for Mobile Ad-Hoc Networks*, Ayman M. Bahaa-Eldin presents a model for using

Multi Intelligent Agents and Swarm Intelligence for trusted routing in mobile ad hoc networks (MANETs) is presented. The new algorithm called TARA is proved more efficient in different ways than the existing protocols. TARA uses a methodology to establish an objective trust value for each node based on self-monitoring. The protocol is tuned to minimize the number of messages to be exchanged and trust value propagation is eliminated. Ant Colony Optimization is used to find the optimal route resulting in a better performance and lower latency. The advantages and complexity of TARA are examined and it is compared with other protocols. Simulation results show that TARA works better than standard and trusted routing protocols in the presence of malicious nodes.

In Chap. 7, *An Overview of Self-Protection and Self-Healing in Wireless Sensor Networks*, Tarek Gaber and Aboul Ella Hassanien review the autonomic computing paradigm which is the key concept of self-protection and self-healing. It then describes the need of these features for WSN application. It also gives an overview of the self-protection and self-healing of WSNs. It finally highlights a number of open issues about the self-protection and self-healing in the WSN environment.

Chapter 8, *Cybercrime Investigation Challenges: Middle East and North Africa* by Mohamed Sarraf et al. focuses mainly on highlighting the main challenges of Middle East and North Africa's countries in cybercrime investigation system by considering the recent developments in the continents Internet infrastructure and the need for information security laws in these particular countries. In addition, it focuses on the Internet infrastructure development, particularly to show how they might become vulnerable to cybercrime attacks.

In Chap. 9, *Multilayer Machine Learning-Based Intrusion Detection System*, Amira Sayed A. Aziz and Aboul Ella Hassanien present a basic model of a multi-layer system, along with the basics of artificial immune systems and network intrusion detection. An actual experiment is included, which involved a layer for data preprocessing and feature selection using Principal Component Analysis, a layer for detectors generation and anomaly detection using Genetic Algorithm with Negative Selection Approach. Finally, a layer for detected anomalies classification using decision tree classifiers is presented. The principal interest of this chapter is to benchmark the performance of the proposed multi-layer IDS system by using NSL-KDD benchmark data set used by IDS researchers.

In Chap. 10, *An Improved Key Management Scheme with High Security in Wireless Sensor Networks*, Satish kumar et al. present solutions to the security issue in relay network which were developed with validation and privacy in mind using the Incorporated Network Topological control and Key management scheme.

Chapter 11, *Key Pre-distribution Techniques for WSN Security Services* by Mohamed Mostafa M. Fouad and Aboul Ella Hassanien, gives an overview of the desired security services required for the WSNs, their threats model, and finally the details of different pairwise key distribution security techniques for distribution WSNs.

Biometrics Technology and Applications is the **Third Part** of this volume. It contains five chapters discussing some biometrics approaches.

Chapter 12, *Fusion of Multiple Biometric Traits: Fingerprint, Palmprint and Iris* by Manasa et al., explores multiple biometric fusion using two architectures: Parallel architecture and Hierarchical-cascade architecture. Multi-biometric recognition systems designed with hierarchical architecture not only are robust, fast, and highly secure but also mitigate problems.

Chapter 13, *Biometric Recognition Systems Using Multispectral Imaging* by Abdallah Meraoumia et al., describes the design and development of a multimodal biometric personal identification system based on features extracted from multispectral palmprint. The experimental results, obtained on a database of 400 users, show very high identification accuracy. They also demonstrate that combining different spectral bands does significantly reduce the accuracy of the system.

Chapter 14, *Electrocardiogram (ECG): A New Burgeoning Utility for Biometric Recognition* by Manal et al., is a comprehensive survey on the employment of ECG in biometric systems. An overview of the ECG, its benefits and challenges, followed by a series of case studies are presented. Based on the survey, ECG-based biometric systems can be fiducial or non-fiducial according to the utilized features.

Chapter 15, *Image Pre-processing Techniques for Enhancing the Performance of Real-Time Face Recognition System Using PCA*, by Behzad Nazarbakhsh and Azizah Abd Manaf proposed a recognition framework for human face recognition. The comprehensive proposed frameworks, include different processes, techniques, and algorithms that are used for human face authentication.

Chapter 16, *Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues* by Reham Amin et al., reviews the current mobile authentication mechanisms: traditional and biometric, and their most commonly used techniques in the mobile authentication environment. In addition, the pro and cons of these techniques are highlighted. Moreover, a comparison among these techniques is conducted. The chapter also discusses the other techniques that could be much suitable for the current environment in mobile applications. Furthermore, it discusses a number of open issues of mobile authentication which needs further research in the future to improve the adoption of biometric authentication in the smart phones environment.

The **Final Part** of the book deals with *Cloud Security and Data Services*. It contains six chapters, which discusses Cloud Services Discovery and Selection, dynamic Self-Organizing Maps, and Hybrid Learning approach as well as Cloud Customers Self-Monitoring and Availability-Monitoring.

Chapter 17, *Cloud Services Discovery and Selection: Survey and New Semantic-Based System* by Yasmine Afify, presents a comprehensive survey on cloud services discovery and selection work. The survey highlights the need for a complete Cloud Services Discovery and Selection 25 system that assists SaaS users in finding the service that meets their functional and non-functional requirements efficiently. In response to this finding, a semantic-based SaaS cloud service publication, discovery, and selection system is proposed, which facilitates the process of mapping the user specified service request to real cloud offerings.

Chapter 18, *Data and Application Security in Cloud* by Nirnay Ghosh et al., reviews the recent works reported specifically in the area of *data and application security* relevant to cloud computing. Some works which use biologically inspired phenomenon to manage load balancing in cloud environment have also been studied. It provides an insight into the present state-of-the-art cloud security problems, proposed solutions, and identifies future research directions as well as scopes in various security issues.

Chapter 19, *Security Issues on Cloud Data Services* by Nour Zawawi et al., examines recent research related to data security and addresses possible solutions. Research in employing uncommon security schemes into Cloud environments has received increasing interest in the literature, although these schemes are neither mature nor rigid yet. This work aspires to promote the use of security protocols due to their ability to reduce security risks that affect users of data Cloud services.

Chapter 20, *A Reputation Trust Management System for Ad-Hoc Mobile Clouds* by Ahmed Hammam and Samah Senbel, proposes a reputation trust management system (TMC) for mobile ad hoc clouds. TMC system considers availability, neighbors evaluation, and response quality and task completeness in calculating the trust value for a node. The trust management system is built over Planet Cloud which introduced the term of ubiquitous computing. Eigen Trust algorithm is used to calculate the reputation trust value for nodes. Finally, performance tests were executed to prove the efficiency of the proposed TMC in terms of execution time, and detecting node behavior.

Chapter 21, *Secured and Networked Emergency Notification Without GPS Enabled Devices* by Qurban A. Memon, reviews various well-known systems in Location-Based Service Applications, followed by existing location detection methods and technologies. The privacy issues are also highlighted. The comparative study is done to highlight the strengths and weaknesses of various location detection approaches. Furthermore, various position equation methods are derived to estimate position location accuracy. In order to address privacy, a location detection system is developed for a limited geographical area as a case study. The simplicity and security of data transfer are also addressed by encryption using special-purpose microcontrollers. The standardization efforts for location identification are also summarized. Finally, the implemented system boosts privacy by (a) no data transfer except during emergencies and (b) encrypting data during transfer. Such a deployed system facilitates the safety management departments to address personal safety and security of the user in an operational area.

Chapter 22, *Towards Cloud Customers Self-Monitoring and Availability-Monitoring* by Sameh Hussein and Nashwa Abdelbaki, provides advices and guidelines for Cloud layers which can be under Cloud Customer control, to allow Cloud Customer contributes in Cloud infrastructure monitoring and controlling. In addition, they produce their developed monitoring tool to allow Cloud Customer contributes in service monitoring. It is for Cloud Customers to self-monitor the Availability as a metric of the outsourced IT service.

Finally, we are very much grateful to the authors of this volume and to the reviewers for their great effort by reviewing and providing useful feedback to the authors. The editors would like to express thanks to Dr. Thomas Ditzinger (Springer Engineering In house Editor) and the editorial assistant at Springer Verlag, Heidelberg, for the editorial assistance and excellent collaboration to produce this important scientific work. We hope that the reader will share our joy and will find the volume useful.

Egypt, April 2014
Korea, Republic of (South Korea)
Poland
Egypt

Aboul Ella Hassanien
Tai-hoon Kim
Janusz Kacprzyk
Ali Ismail Awad

Bio-inspiring Cyber Security and Cloud Services: Trends
and Innovations

Hassanien, A.E.; Kim, T.-H.; Kacprzyk, J.; Awad, A.I. (Eds.)
2014, XXII, 585 p. 235 illus., 17 illus. in color., Hardcover
ISBN: 978-3-662-43615-8