Introduction

IT and business services have grown exponentially in size, diversity, and complexity over the past few years. With the advent of electronic data processing, business enterprises are using electronic methods to store and retrieve data, which has resulted in rapid increases in the size of data within business enterprises. The storage of data is a matter of concern for most of the business enterprises due to the high cost of managing and maintaining the high-end servers and storage facilities. Cloud environment is the most cost-effective solution that a business enterprise can use for storage and retrieval of data with less effort. However, security and authentication of the user in the cloud environment are the major concerns that need to be resolved. Improving the security of the cloud environment in general and cloud storage in particular has become absolutely essential. In an effort to address the array of security and authentication issues in the cloud environment, the use of biometric parameter-based security mechanisms are exponentially increasing.

This book starts with basic concepts of Bigdata computing strategies and takes readers through the cloud computing security issues and architecture, biometric authentication, NoSQL database, cloud database security issues and challenges, efficient KDC scheme to support dynamic scalability on multiple storage servers, threats of sensor cloud infrastructure in wireless sensor network, flow of Bigdata using bacterial forging, ECG biometrics, load balancing, and live migration of virtual machines.

This book has highlighted the usefulness of cloud storage for a business enterprise keeping in mind the futuristic scope of data size. The issues related to security and the possible solutions for ensuring the security of data has also been discussed in detail to give an understanding of the domain.

The salient feature of the book also includes discussion about the various biometric authentication systems, algorithms, and case studies for the benefit of practitioners, researchers, and students. The language of the book is simple, easy to understand, well organized, and illustrated in a simple manner. In addition, the book contains enough in-depth content to improve the understandability of different tools and techniques in the security domain.

I would unhesitantly recommend this book for IT security and bioinformatics professionals as well as those entering in the field of biometric parameter-based security, specifically for Cloud computing. I also recommend it to curriculum planners and instructors for use in classrooms.

Abdul Wahid
Maulana Azad National Urdu University, India