THE emerging paradigm of cloud computing provides a new way to address the constraints of limited energy, capabilities, and resources. Researchers and practitioners have embraced cloud computing as a new approach that has the potential for a profound impact in our daily life and world economy. However, security and privacy protection is a critical concern in the development and adoption of cloud computing. To avoid system fragility and defend against vulnerabilities exploration from cyber attacker, various cyber security techniques and tools have been developed for cloud systems. This special issue focuses on the challenging topic “Security and Privacy Protection on Clouds” and invites the state-of-the-art research results.

This special issue has collected 57 submissions and 15 of the submissions were eventually accepted to appear in this issue. Each accepted paper has been assessed by a careful review and evaluation process. The decisions consider both research quality and dimension balance such that we organize the papers into four dimensions, which are secure data sharing and storage in clouds, novel security cloud model/framework/architecture, new cryptography for cloud solutions, and cloud-oriented privacy protection and secure networks dimensions.

First, in the dimension of the secure data sharing and storage in clouds, four papers were accepted. Part 1: Ali et al., in their paper entitled DROPS: Division and Replication of Data in the Cloud for Optimal Performance and Security, propose an approach that collectively approaches the security and performance issues. They divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Part 2: Zhang et al., in their paper entitled Towards Privacy Preserving Publishing of Set-valued Data on Hybrid Cloud, study the issue of privacy-preserving set-valued data publishing. The study argues that existing data privacy-preserving techniques (such as encryption, suppression, generalization) are not applicable in many real scenes due to the large overhead for data query or high information loss. Part 3: Lee et al.’s paper entitled Model-based Thermal Anomaly Detection in Cloud Datacenters using Thermal Imaging develops a model-based thermal anomaly detection mechanism that compares expected (obtained using heat-generation and -extraction models) and observed thermal maps (obtained using thermal cameras) of datacenters. Part 4: Li et al. propose a lightweight data sharing scheme (LDSS) for mobile cloud computing in their paper, A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing.

Next, there are four papers being accepted in the dimension of novel security cloud model/framework/architecture. Part 5: Fowley at al. present a 3-pronged classification and comparison framework for broker platforms and applications in their paper, A Classification and Comparison Framework for Cloud Service Brokerage Architectures. The study investigates a range of specific broker development concerns like architecture, programming and quality. Part 6: Chen and his colleagues address the optimization of the computational efficiency and propose processor architecture that provides tightly-coupled datapaths that avoid information leakage during database access and query execution. The illustration of the architecture is described in their paper, CypherDB: A Novel Architecture for Outsourcing Secure Database Processing. Part 7: Islam and his team had a distinct focus and their paper entitled Assurance of Security and Privacy Requirements for Cloud Deployment Model introduces assurance as evidence for satisfying the security and privacy requirements in terms of completeness and reportable of security incident through audit. Part 8: Statistical Learning for Anomaly Detection in Cloud Server Systems: Sha et al., in their paper entitled A Multi-Order Markov Chain Framework, propose a feasible multi-order Markov chain based framework for anomaly detection. This approach adopts both the high-order Markov chain and multivariate time series to compose a scheme described in algorithms along with the training procedure in the form of statistical learning framework.

Moreover, three papers were involved in the dimension of new cryptography for cloud solutions. Part 9: Audit-Free Cloud Storage via Deniable Attribute-based Encryption (Chi et al.) presents a design for the new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Part 10: Luna et al. develop a decentralized probabilistic method for performance optimization of cloud services in their paper, Probabilistic Optimization of Resource Distribution and Encryption for Data Storage in the Cloud. Part 11: another encryption method has been proposed by Awad et al. in Chaotic Searchable Encryption for Mobile Cloud Storage. A secure searchable
Three-server swapping for access confidentiality in clouds. The authors new verification algorithms providing arbitrary secret sharing schemes with cheater detection capabilities, and prove their space efficiency with regard to other schemes appeared in the literature. Part 13: Zhang et al., in their paper "Architectural Protection of Application Privacy Against Software and Physical Attacks in Untrusted Cloud Environment." Part 14: Xu et al. have a different research interest and investigate how to cope with a strong threat model which is that the cloud vendors in the paper "Three-server swapping for access confidentiality," propose an approach to protect confidentiality of data and accesses to them when data are stored and managed by external providers. This approach is based on the use of distributed data allocation among three independent servers and on a dynamic re-allocation of data at every access.

We hope that the achievements gathered in this special issue will be of timely value to the community of cloud computing and readers of IEEE Transactions on Cloud Computing (TCC).

Meikang Qiu received the BE and ME degrees from Shanghai Jiao Tong University and the PhD degree in computer science from the University of Texas at Dallas. Currently, he is a faculty member with Columbia University. His research interests include cyber security, cloud computing, big data storage, hybrid memory, heterogeneous systems, embedded systems, operating systems, optimization, intelligent systems, sensor networks, etc. A lot of novel results have been produced and most of them have already been reported to research community through high-quality journal and conference papers. He has published 15 books, more than 400 peer-reviewed journal and conference papers (including more than 200 journal articles, more than 200 conference papers, more than 60 IEEE/ACM Transactions papers), and 3 patents. He has won the ACM Transactions on Design Automation of Electrical Systems (TODAES) 2011 Best Paper Award. His paper about cloud computing has been published in JPDC (the Journal of Parallel and Distributed Computing, Elsevier) and ranked #1 in Top Hottest 25 Papers of the Journal of Parallel and Distributed Computing 2012. He has won another 10+ Conference Best Paper Awards in recent years. Currently he is an associate editor of more than 10 international journals, including the IEEE Transactions on Computer and IEEE Transactions on Cloud Computing. He is the general chair/program chair of a dozen of IEEE/ACM international conferences, such as IEEE HPCC, IEEE CSCIong, IEEE BigDataSecurity. He has given more than 100 talks all over the world, including Oxford, Princeton, Stanford, and Yale University. He has won Navy Summer Faculty Award, in 2012 and Air Force Summer Faculty Award, in 2009. His research is supported by US government such as National Science Foundation, Air Force, Navy and companies such as GE, Nokia, TCL, and Caviun. He is the chair of IEEE Smart Computing Technical Committee. He is an IEEE senior member and ACM senior member.