Preface

Cloud computing has emerged as a new paradigm for on-demand delivery of computing resources to consumers as utilities. It offers unlimited computing resources to its users in a pay-as-you-go model with a higher level of quality of service such as availability and reliability in a substantially reduced infrastructure cost. With such an offering, it is not surprising that businesses are considering moving their IT infrastructure to cloud. However, it has been widely reported in the surveys of CTOs and CIOs that they have a number of reservations about adapting cloud computing for their businesses, and the security, privacy and trust of cloud systems is at the top of their list. The recent news reported in media about the leakage of customers' personal data have exacerbated their concerns even more. With the emergence of social media, such events are spreading faster than ever before and the impact of breach of privacy of their customers could be catastrophic to businesses. Businesses have serious concerns on moving their services and data to a cloud environment. These concerns need to be addressed to realize the vision of delivering IT services as utilities.

The vision of delivering unlimited computing resources, e.g., compute, network, and storage, as utilities, as promised by the cloud computing paradigm, has made some of the tasks—that were impossible to achieve a few years back for small and medium size businesses—possible. Businesses can run sophisticated data analytics tools without investing a big amount on IT infrastructure. This has been one of the driving forces behind the emergence of the new research area, called "Big Data". One of the key challenges in big data is transforming the raw data available to a business into business value and strategic advantage. Better management and analysis of data will become the next frontier of innovation, competition, and productivity, and cloud has a big role to play in this area. For example, according to a McKinsey Global Institute study, a retailer exploiting the full potential of big data could increases its operating margin by more than 60 %. Efficient and effective use of big data could save more than $300 billion for US government in the healthcare sector alone. Therefore, there is a need for effective and efficient management and analysis of big data. Cloud computing has emerged as a choice of technology platform for big data. However, the lack of security and privacy of data in the cloud has been a major hurdle for businesses to utilize the full potential of cloud to unlock the business intelligence residing in their data.

In order to take the full advantage of enormous amount of business data using cloud, the issues related to security, privacy, and trust of data services need a careful attention. The foremost concern for businesses is that they have to relinquish the full control of their data to the cloud service providers without knowing whether there are adequate measures in place to protect their data. They also need to be aware of legal implications to their data. As the cloud enable migration of data across different jurisdictions, which laws are applicable to the data becomes an important factor to be considered while moving data to the cloud. As pointed out by a cloud service provider in a recent conference, the cloud computing inadvertently provided a playground for lawyers. Therefore, it is important to address legal aspects of data protection in the cloud.

Cloud computing introduces challenges to traditional approaches to protecting data including authentication and authorization. There is a need to develop a new way of authenticating users for cloud data services and defining access control. The implications of cloud computing paradigm to identity management and user authentication need to be further analyzed. Related to identity management is the issue for intercloud data migration. Unless there is a way of achieving seamless transition of data migration from one cloud provider to another, just like changing utility providers today, the security, privacy, and trust issues will continue to have implication beyond a single cloud provider.

Cryptographic approaches have been used to protect data where the data is encrypted both in motion and at rest so that they are never revealed to anyone other than data owners themselves. In such an approach, the data is encrypted before storing to cloud storage services and is never decrypted, while residing in the cloud. The data is retrieved into the trusted local environment before decryption. But the cloud introduces new challenges due to the cost of moving and processing big data. This means we need to look at the mechanisms of processing encrypted data in the cloud without compromising confidentiality. This demands privacy preserving analysis of big unstructured data as well as privacy preserving queries over relational databases. The privacy preserving querying and analysis of data enables to process data in the encrypted forms. A number of researchers have looked at the new form of encryption techniques, called homomorphic encryption. Developing effective and efficient fully homomorphic encryption techniques still remains as a challenging problem. In the coming years, we expect to see a reasonable progress made in this direction.

In the past few years, outsourcing firms have been increasingly used by businesses to provide their services to customers in cost-effective ways. The core strategy is to outsource certain aspects of a business process to skilled, but cost-effective, external service providers. The cloud computing paradigm needs to support this business model to be adapted successfully by enterprises in practice. Outsourcing requires multiple organizations working together to achieve a goal. Competing organizations may use the same outsourcing firms to perform a certain process within their businesses (such as billing). The cloud platform should

support the sharing of data and processes across different organizations while preserving the privacy of both data and processes. Not all processes can be outsourced. Some of the processes are going to be performed within organizations to preserve the competitive advantages of enterprises. How to support the sharing of data in cloud across collaborating organizations in such a way that competitive advantage of businesses and privacy of the data can be preserved. Meeting these two conflicting requirements is a challenge in itself.

Recent reports on cloud data services have indicated that data owners would like to know what is happening with their data. Who have accessed it? When it was accessed? Where it is stored? When the movement of the data occurred? How often the data is backed up? How many copies of the data are kept? The metadata about the data becomes as important as the data itself and sometime the size of the metadata becomes larger than the original data. A cloud data service should be able to answer all these questions with a clear separation of duties. This means the data management and activity logging components should work independently so that the data owner can trust the integrity of logged data. The answers to these questions can be found in the data accountability. How to standardize the data accountability service and implement it is as an integral part of cloud data service is an interesting and challenging problem.

Cyber attacks have been on the rise in recent times. The effect of cyber attacks in cloud is severe. For example, the denial of service attacks on cloud data services may not only disrupt the services and keep the genuine customers out of enterprise services, but also increase the costs due to the underlying pay-as-you-go model. Cloud service providers should be able to provide a "credit card" like security measure to their customers and should be able to refund all costs incurred through cyber attacks. However, there is no way cloud service providers can vouch that a service request is genuine or the result of a cyber attack. Thus, the cloud service providers should not only be able to detect and prevent the cyber attacks on the services deployed on their clouds, but also should establish clear guidelines on how to resolve the disputes arising from such attacks. It is thus clear that some of the challenges related to cloud security, privacy, and trust go beyond the technological solutions. We need to look at the social and legal aspects of the cloud data services.

Another interesting debate around cyber attacks is whether the cloud data service is more attractive to cyber attacks than an individual enterprise data service. Some believe that cloud data services are more attractive for attackers as they know they can unlock a large number of valuable information if the attacks on cloud services are successful. They thus believe that the data become prone to more attacks when it is kept in the cloud. An alternative thought is that cloud service providers can probably have a large number of security experts working on preventing cyber attacks on enterprise data than any single enterprise could afford at any time. They believe that the cloud providers are better equipped to protect

enterprise data than enterprises themselves. The reality may lie in between these two opposite views. Time can only tell which view is right!

In recent times, we have seen an increasing number of cloud service providers that operate within a single jurisdiction or across multiple jurisdictions. The choice of providers is good for consumers, but the emergence of a large number of cloud service providers poses a number of challenges from the point of view of trust. How do you know which provider is best for you? Reputation based on past experience has been used as a mechanism of addressing the issue of trust. Although this approach has a foundation on economics, marketing, social, and behavior sciences, we believe that we need to look at the holistic solutions that take into account of the technological and social aspects of trust.

In the past few years, there have been an increasing number of efforts toward developing cloud standards by national and international standard bodies. Such efforts could go a long way to address some of the concerns about security, privacy, and trust in cloud systems. However, the success relies on the adaptation of such standards in practice.

In this book, we have outlined the problems in developing secure, private, and trusted cloud systems from different points of views. Researchers, students, and practitioners need to understand the complexity of developing such systems from the point of views of standards, technologies, tools, economics, and social and behavioral sciences. As the cloud computing is a new and evolving paradigm, the solutions are being researched and still emerging. Therefore, this book is intended to pose key research challenges and some emerging solutions along with future trends.

Overview and Scope of the Book

This book, entitled "Security, Privacy and Trust in Cloud Systems" presents cloud security fundamentals and related technologies to-date, with a comprehensive coverage of evolution, current landscape, and future roadmap. It provides a smooth organization with introductory, advanced, and specialist content, i.e., from basics of security, privacy, and trust in cloud systems, to advanced cryptographic techniques, case studies covering both social and technological aspects, and advanced platforms. The book builds on academic and industrial research and developments, and case studies that are being carried out at many different institutions around the world. In addition, the book identifies potential research directions and technologies that drive future innovations. We expect the book to serve as a valuable reference for larger audience such as systems architects, practitioners, product developers, researchers, and graduate level students.

Organization

This book will enable readers to understand the basics, identify the underlying technology, summarize their knowledge on concepts, ideas, principles, and various paradigms which span on Cloud security, privacy, and trust domains. The book is organized into three parts, namely, Part I: "Cloud Security"; Part II: "Cloud Privacy and Trust"; and Part III: "Case Studies: Cloud Security, Privacy, and Trust". Specifically, the topics of the book are the following:

- Cloud security fundamentals
- Secure information sharing and data protection in the cloud
- Cloud security architecture and protocol
- Autonomic security in cloud systems
- Cryptography and crypto-protocols for cloud systems
- QoS-based trust model and QoS monitoring mechanism
- Enterprise cloud security case study
- Open research issues in cloud security and future roadmap

Part I of the book focuses on the basic ideas, techniques, and current practices related to "Cloud Security". "Cloud Security: State of the Art", by Soares et al., presents a comprehensive analysis of the state of the art on cloud security issues. In addition to presenting the key concepts on cloud security, this chapter discusses the most prominent security issues tackled in literature, surveying vulnerabilities, gaps, threats, attacks, and risks in cloud environment. Thilakanathan et al., in "Secure Data Sharing in the Cloud", provide a review on methods of achieving secure and efficient data sharing in the cloud. The presented research outcome is particularly useful for secure sharing of real-world critical data from the business, government and/or medical domains. In "Adaptive Security Management in SaaS Applications", Almorsy et al. discuss on a security management framework to deliver autonomic security where the security level, enforced on the cloud platform and cloud services, automatically adapt to match the current security risks and threats. Addressing the limitations of using the virtualization technology in cloud systems, Caron et al. in "Smart Resource Allocation to Improve Cloud Security" present a resource allocation technique to improve cloud security. They introduce a way for users to express security requirements and demonstrate how a cloud service provider can address those requirements. Building on cryptographic mechanisms to guarantee security properties such as data confidentiality and integrity, "Mandatory Access Protection within Cloud Systems" by Bousquet et al. describes mandatory access protection in cloud systems.

Part II of this book highlights technologies to ensure "Cloud Privacy and Trust". Tormo et al. in "Identity Management in Cloud Systems" present, analyze, and compare current identity management standards, technologies, and solutions from the cloud perspective, taking into account their features and requirements. They provide a set of recommendations to be taken into consideration when

designing and deploying any identity-based service in a cloud environment. It is followed by a "Data Accountability in Cloud Systems" on data accountability, by Ko, reviewing definitions, existing techniques and standards in the area of data accountability in cloud systems. Based on MapReduce, "Privacy Preservation over Big Data in Cloud Systems" by Zhang et al. discusses on data privacy preservation and data quality in the cloud under given privacy requirements. This chapter demonstrates a prototype privacy-preserving framework to anonymize large-scale data sets in the cloud. In "Securing Outsourced Databases in the Cloud", Liu talks about privacy of database services in cloud systems. He presents an indexing scheme and an associated encryption scheme to encrypt databases and query encrypted databases in the cloud. This part of the book is ended with "Trust Model for Cloud Systems with Self Variance Evaluation", by Wang et al., presenting reputation-based trust models for cloud systems. They introduce a general trust model to get a more comprehensive and robust reputation evaluation.

Part III, the final part of the book, consists of a handful of representative "Case Studies on Cloud Security, Privacy, and Trust". In "Cryptographic Role-Based Access Control for Secure Cloud Data Storage Systems", Zhou et al. describe access control models and the use of cryptographic techniques for secure cloud data storage. In their case study, authors cover a scheme which integrates cryptographic techniques with role-based access control and show how the scheme can be used to secure data storage in the cloud. "Accountability-Based Compliance Control of Collaborative Business Processes in Cloud Systems" by Yao et al. presents a case study on accountability-based compliance control of collaborative business process in cloud systems. Authors base their case study on Amazon EC2 using a loan application business process. A case study on 'Reputation as a Service' is presented next. In this chapter, Itani et al. demonstrate a secure and accountable reputation system for ranking cloud service providers. In "Combating Cyber Attacks in Cloud Systems Using Machine Learning", Khorshed et al. present a machine-learning approach to combat cyber attacks in cloud systems. The final chapter of the book, by Kertesz and Varadi, cover the legal aspects of data protection in cloud systems. They examine use cases and assess them against evaluation criteria derived from the relevant cloud computing law for the data processing of end-user details and materials, including roles and responsibilities necessary for legal compliance.

Acknowledgments

The book came into light due to the direct and indirect involvement of many researchers, academics, and industry practitioners. We acknowledge and thank the contributing authors, research institutions, and companies whose papers, reports, articles, notes, Web sites, study materials have been referred to in this book. We offer our special appreciation to Springer and its publishing editor, Dr. Christoph Baumann, for helping us to bring this book out in a quick time.

Prior technical sources are acknowledged citing them at appropriate places in the book. In case of any errors, we would like to receive feedback so that it could be taken into consideration in the next edition.

We hope that this book will serve as a valuable text for students, especially at graduate level and a reference for researchers and practitioners working in the Cloud security, privacy, and trust domains.

Surya Nepal
Mukaddim Pathan

http://www.springer.com/978-3-642-38585-8

Security, Privacy and Trust in Cloud Systems
Nepal, S.; Pathan, M. (Eds.)
2014, XX, 459 p. 146 illus., 95 illus. in color., Hardcover
ISBN: 978-3-642-38585-8