Security, Privacy and Trust in Cloud Systems

Pages: 459
Publisher: Springer; 2014 edition (September 3, 2013)
Format: pdf, epub
Language: English

Surya Nepal and Mukaddim Pathan (eds.) Security, Privacy and Trust in Cloud Systems2014 10.1007/978-3-642-38586-5 Editors Surya Nepal and Mukaddim Pathan Security, Privacy and Trust in Cloud Systems Editors Surya Nepal CSIRO ICT Centre, Marsfield, NSW, Australia Mukaddim Pathan Telstra Corporation Limited, Melbourne, VIC, Australia ISBN 978-3-642-38585-8 e-ISBN 978-3-642-38586-5 Springer Heidelberg New York Dordrecht London Library of Congress Control Number: 2013947067 To Amrita , Ashraya , and Shruti , for their support and understanding during the book preparation Surya To Ziyuan , for her warmth and support that gave me strength towards completion of the book Mukaddim 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

Contents

Contributors
A. B. M. Shawkat Ali Faculty of Arts, Business, Informatics and Education, Central Queensland University, Bruce Highway, North Rockhampton, QLD, 4702, Australia
Mohamed Almorsy Faculty of Information and Communication Technologies, Swinburne University of Technology, John Street, Hawthorn, VIC, 3122, Australia
Mathieu Blanc CEA, DAM, DIF, Arpajon, 91297, France
Aline Bousquet Laboratoire d'Informatique Fondamentale d'Orléans, ENSI de Bourges, 88 bd Lahitolle, Bourges, 18020, France Jeremy Briffaut Laboratoire d'Informatique Fondamentale d'Orléans, ENSI de Bourges, 88 bd Lahitolle, Bourges, 18020, France Rafael A. Calvo Department of Electrical Engineering, University of Sydney, Sydney, NSW, 2006, Australia Eddy Caron LIP Laboratory, UMR CNRS - ENS Lyon - INRIA - UCB, Université de Lyon, Lyon, 5668, France Ali Chehab Department of Electrical and Computer Engineering, American University of Beirut, Beirut, 1107 2020, Lebanon
Jinjun Chen Faculty of Engineering and IT, University of Technology Sydney, Sydney, NSW, Australia Shiping Chen CSIRO ICT Center, Cnr Vimiera and Pembroke Rodas, Marsfield, NSW, 2122, Australia Laurent Clevy Alcatel Lucent Bell Labs, Route de Villejust, Nozay, 91620, France
Frederic Desprez INRIA Grenoble Rhône-Alpes ZIRST Montbonnot, 655 avenue de l'Europe, Saint Ismier Cedex, 38334, France Diogo A. B. Fernandes Department of Computer science, Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal Mário M. Freire Department of Computer science, Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal Cesar Ghali Department of Electrical and Computer Engineering, American University of Beirut, Beirut, 1107 2020, Lebanon João V. Gomes Department of Computer science, Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal Damien Gros CEA, DAM, DIF, Arpajon, 91297, France John Grundy Faculty of Information and Communication Technologies, Swinburne University of Technology, John Street, Hawthorn, VIC, 3122, Australia Michael Hitchens Information and Networked Systems Security Research, Department of Computing, Macquarie University, Macquarie Park, NSW, Australia Xiaofeng Hu School of Computer, National University of Defense Technology, Changsha, 410073, China Amani Ibrahim Faculty of Information and Communication Technologies, Swinburne University of Technology, John Street, Hawthorn, VIC, 3122, Australia Pedro R. M. Inácio Department of Computer science, Instituto de Telecomunicações, University of Beira

Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
Wassim Itani Department of Electrical and Computer Engineering, American University of Beirut, Beirut, 1107 2020, Lebanon Ayman Kayssi Department of Electrical and Computer Engineering, American University of Beirut, Beirut, 1107 2020, Lebanon Attila Kertesza MTA SZTAKI Computer and Automation Research Institute, Budapest, P.O. Box 63, 1518, Hungary
Md Tanzim Khorshed Faculty of Arts, Business, Informatics and Education, Central Queensland University, Bruce Highway, North Rockhampton, QLD, 4702, Australia
Arnaud Lefray LIP Laboratory, UMR CNRS - ENS Lyon - INRIA - UCB, Université de Lyon, Lyon, 5668, France David Levy School of Electrical and Information Engineering, University of Sydney, Sydney, NSW, 2006, Australia
Chang Liu Faculty of Engineering and IT, University of Technology Sydney, Sydney, NSW, Australia Dongxi Liu CSIRO ICT Center, Cnr Vimiera and Pembroke Rodas, Marsfield, NSW, 2122, Australia Félix Gómez Mármol NEC Laboratories Europe, Kurfürsten-Anlage, 36, 69115 Heidelberg, Germany
Surya Nepal CSIRO ICT Center, Cnr Vimiera and Pembroke Rodas, Marsfield, NSW, 2122, Australia Gregorio Martínez Pérez Departamento de Ingeniería, de la Información y las Comunicaciones, Facultad de Informática, Universi-dad de Murcia, 30100 Murcia, Spain Jonathan Rouzaud-Cornabas LIP Laboratory, UMR CNRS - ENS Lyon - INRIA - UCB, Université de Lyon, Lyon, 5668, France
K. L. Ko Ryan Department of Computer Science, University of Waikato, Hamilton, New Zealand Liliana F. B. Soares Department of Computer science, Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal Jinshu Su School of Computer, National University of Defense Technology, Changsha, 410073, Hunan, China
Danan Thilakanathan Department of Electrical Engineering, University of Sydney, Sydney, NSW, 2006, Australia Christian Toinard Laboratoire d'Informatique Fondamentale d'Orléans, ENSI de Bourges, 88 bd Lahitolle, Bourges, 18020, France Ginés Dólera Tormo NEC Laboratories Europe, Kurfürsten-Anlage, 36, 69115 Heidelberg, Germany Vijay Varadharajan Information and Networked Systems Security Research, Department of Computing, Macquarie University, Macquarie Park, NSW, Australia Szilvia Varadib Department of International and European Law, University of Szeged, Szeged, Rakoczi ter 1, 6722, Hungary Benjamin Venelle Alcatel Lucent Bell Labs, Route de Villejust, Nozay, 91620, France Xiaofeng Wang School of Computer, National University of Defense Technology, Changsha, 410073, Hunan, China
Saleh A. Wasimi Faculty of Arts, Business, Informatics and Education, Central Queensland University, Bruce Highway, North Rockhampton, QLD, 4702, Australia
Chunqing Wu School of Computer, National University of Defense Technology, Changsha, 410073, Hunan, China Chi Yang Faculty of Engineering and IT, University of Technology Sydney, Sydney, NSW, Australia
Jinhui Yao School of Electrical and Information Engineering, University of Sydney, Sydney, NSW, 2006, Australia Xuyun Zhang Faculty of Engineering and IT, University of Technology Sydney, Sydney, NSW, Australia
Huan Zhou School of Computer, National University of Defense Technology, Changsha, 410073, Hunan, China Lan Zhou Information and Networked Systems Security Research, Department of Computing, Macquarie University, Macquarie Park, NSW, Australia

Part 1

Cloud Security

Surya Nepal and Mukaddim Pathan (eds.) Security, Privacy and Trust in Cloud Systems2014 10.1007/978-3-642-38586-5

Surya Nepal and Mukaddim Pathan (eds.) Security, Privacy and Trust in Cloud Systems2014 10.1007/978-3-642-38586-5_1

Cloud Security: State of the Art

Liliana F. B. Soares1 , Diogo A. B. Fernandes1 , João V. Gomes1 , Mário M. Freire1   and Pedro R. M. Inácio1

(1) Instituto de Telecomunicações, Department of Computer Science, University of Beira Interior Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal

Liliana F. B. Soares (Corresponding author) Email: lsoares@penhas.di.ubi.pt

Diogo A. B. Fernandes Email: dfernandes@penhas.di.ubi.pt

João V. Gomes Email: jgomes@di.ubi.pt

Mário M. Freire Email: mario@di.ubi.pt

Pedro R. M. Inácio Email: inacio@di.ubi.pt

Abstract

Throughout the end of the first half and during the second half of the past century, advances in technology allowed scientists to develop computer systems. In the beginning, mostly between the forties and the sixties, single computers would fill large rooms with electronics that would consume as much power as several hundreds of modern desktop computers.

1 Introduction

Throughout the end of the first half and during the second half of the past century, advances in technology allowed scientists to develop computer systems. In the beginning, mostly between the forties and the sixties, single computers would fill large rooms with electronics that would consume as much power as several hundreds of modern desktop computers. However, a diversity of revolutionary approaches were invented throughout the time, gradually replacing those large, and expensive, computer rooms with smaller, more powerful computers, being able to hold many of them. This allowed computer systems and networks to emerge, like standard Ethernet networks that still persist today. Distributed systems, one of those approaches, arose as a means to aggregate computational assets with the main goal of supporting highly intensive and hardware-demanding tasks, which can consume several processing resources simultaneously and last for a long time. Examples of such tasks include molecular modeling, scientific simulations and weather forecasts.

1.1 Computer Clusters, Grids and Clouds

Two of the most typical distributed systems are computer clusters and computer grids. As the name suggests, computer clusters consist of coupled hardware resources that can function standalone. These resources are put on a centralized point, usually a large, cooled, well protected room, leading to expensive approaches. Clusters enhance computational, memory and storage capabilities of computer systems, therefore requiring specially designed middleware to support communications between each hardware node. In addition, this type of architecture for computer systems requires bandwidth-wise network links to support large amounts of intracommunications network traffic. However, nowadays, open-source software enables the use of processing units and memory from desktop computers to dispatch distributed, potentially parallel tasks by nominating a master node that manages the cluster. This approach can reduce implementation costs to companies rather than spending big on supercomputers or expensive clusters. Grid systems, on the other hand, are not as coupled as clusters and dwell over large scattered and heterogeneous networks in a decentralized fashion. The most prominent example is the Internet, over which grids are deployed as overlay networks. In fact, the most well-known form of grids is the one of using typical desktop and home computers as end slave computation nodes. This approach, however, brings obstacles, such as increased management complexity, task assignment, and results collecting and gathering.

Based on the cluster and grid computing paradigms [35, 90], cloud computing has emerged in the last few years as the latest approach with the purpose of computing as utility. In fact, grid computing provides the backbone and supporting infrastructure for clouds [35]. It was around 2008 that the cloud computing subject started gaining serious interest among the industry and the academia. Additionally, to provide a better perspective, the utility computing term was first invoked as early as 1965 [23]. It refers to computational resources efficiently wrapped as services, being more a business model rather than a computing paradigm today, and matching the cloud business model. Analogously to clusters, clouds are composed of umpteen

servers placed in large, cooled, well protected rooms under the same subnet. Facilities that host clouds are nowadays called data centers, which require being physically and logically segregated from malicious intrusions because clouds usually hold large amounts of sensitive data belonging to customers. The main innovative side of clouds is how Information Technologies (IT) are put together along with virtualization techniques, providing web service-based and on-demand capabilities accessible over the Internet. To this end, a pay-per-use business model is implemented, meaning that computational, storage or networking resources rented by customers are strictly billed according to their needs, that is, time of usage, assets required, load and security measures. Cloud systems are both centralized and decentralized, allowing public access to their resources via web technologies. Hence, a centralized and distributed resource handling approach is applied, providing multi-tenant and Service-Oriented Architecture (SOA) capabilities, similarly to grids. 1.2 Cloud Security The National Institute of Standards and Technology (NIST) view of cloud is summarized in version 3 of the security guidance entitled as Security Guidance for Critical Areas of Focus in Cloud Computing [24], published by the Cloud Security Alliance (CSA), an organization aiming at promoting the use of best practices in cloud security. In the document, the cloud deployment models, the cloud service delivery models or service models, and the five essential characteristics of clouds are described. The cloud deployment models include public, private, hybrid, and community clouds, and Virtual Private Clouds (VPCs). The service models are divided into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Finally, the characteristics are broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling. The NIST [74] mentions security, interoperability and portability as major barriers for a broader adoption of cloud solutions. There are just a few standards supporting clouds, which translates into the lock-in issue faced by customers. In other words, when a customer decides for a certain cloud provider, the data stored on the cloud cannot yet migrate to clouds of other providers. Nonetheless, interclouds [11, 88], a term referring to a network of clouds, a place of cloud computing, interoperability, ubiquitous and utility computing, and data storage, would overcome this issue and free data movement among clouds belonging to different providers. Clouds increased the complexity of many previous security issues and introduced new ones, being yet a risky business. To demonstrate how security is one of the most mind changing factor (if not the most important), in 2009, the International Data Corporation (IDC), a market research and analysis firm, has harvested opinions among company Chief Information Officers (CIOs) on the most concerning cloud obstacles. The survey [46] was concluded with the security topic ranking first with 87.5 % of the votes, 12.9 % more than the study on the previous year [47], in which security also led with 74.6 %. The results of the 2009 study are illustrated in Fig. 1. This perspective concerning cloud security is shared with the Top predictions for IT Organizations and Users for 2012 and Beyond report [38], property of Gartner, a technology research and advisory company. Because of security, people hesitate to fully move their business into clouds, slowing down their propagation, as the research and the industry are focused on patching security issues, rather than exploring their potentialities. In addition, "my sensitive corporate data will never be in the cloud" is a statement that has been heard multiple times [3], further pointing out how critical security is. Because clouds outsource businesses of many customers, which includes potentially sensitive data and applications, they pose as attractive attack targets for cybernetic pirates or malicious insiders. Thus, there is much at stake in the cloud business, being data disclosure, data loss and financial loss major risk scenarios. Clouds offer many appealing features and advantages, but until some of its risks are better understood, major players might hold back [106]. This means that cloud systems are a risky business, not only to customers, but also to the providers investments. Fig. 1 Challenges and issues of the cloud model according to IDC and corresponding results from the cloud user survey (adapted from [46]) 1.3 Organization The previous paragraphs enlightened on the differences between the cloud, the cluster and the grid computing paradigms, highlighting the most prominent characteristics of these distributed systems. Essentially, the importance of the cloud security topic is highlighted in

the discussion, underlining how critical it is to address security issues. To this end, this chapter discusses the most prominent security issues tackled in the literature, surveying vulnerabilities, gaps, threats, attacks, and risks on cloud environments. Such terms are emphasized throughout the text as to better distinguish each issue. Additionally, concepts of both cloud and cloud security subjects are described in order to facilitate the understanding of this chapter. Foremost, the chapter presents a comprehensive analysis of the state-of-the-art on cloud security issues.

The remaining of this chapter is organized as follows. Section 2 delivers an insight on the works that are most similar to the one presented herein. Section 3 overviews some general features of clouds and key concepts of cloud security. Subsequently, in Sect. 4, a discussion of the published literature on security issues in cloud environments is presented. A synthesis of the chapter containing a timeframe overview of what was discussed is included in Sect. 5. The chapter ends with the main conclusions in Sect. 6.

2 Related Work

Cloud security has been in vogue on the literature and industry for a while now. Various international conferences have focused on this subject alone, such as the Association for Computer Machinery (ACM) Workshop on Cloud Computing Security, the International Conference on Cloud Security Management and the only European conference on the subject, SecureCloud, which already numbers up to three editions. As a result, several scientific contributions have been published, not only in conferences proceedings, but also in international journals and magazines. Thus, there are a few works surveying this area of knowledge that are worthy to describe herein.

The study in [115] surveyed security and privacy concerns of cloud providers. Firstly, the security topic was discussed while having in mind availability, confidentiality, data integrity, control and audit properties, concluding that these do not meet current concerns. Secondly, the privacy topic was discussed with focus on out-of-date privacy acts that fail to protect information from being disclosed to the government and third-parties. In addition, the multi-location issue of clouds is also included in the study, stating that knowing in which country the data will be kept is a prerequisite for customers, in order to find by which laws the data is governed. It was claimed that new strategies should be put forward to achieve the five aforementioned properties and that privacy acts should be changed accordingly. Again, in [116], the confidentiality, privacy, integrity and availability aspects in clouds were placed under observation. Various issues were discussed so as to present a synthesis of security requirements and threats with respect to the service models. The study ended with the proposal of a trusted third-party solution to eradicate security threats of confidentiality, integrity, authenticity and availability. The solution combined Public Key Infrastructures (PKIs), the Lightweight Directory Access Protocol (LDAP) and Single Sign-On (SSO) with a top-down fashion of the trust tree. The study was concluded with the premise that cloud benefits will outnumber its shortcomings. Another survey targeting security issues on the cloud service models was presented in [95]. Each model was singularly studied, pointing out some of the most significant security vulnerabilities, threats and risks. It should be noted that the SaaS model was the one with the majority of the issues. An overview of current solutions discussed in the literature is presented afterwards. Yet again, the study was concluded saying that proper solutions should be designed and deployed to allow the cloud industry expand further. The security and privacy topics were again discussed in [111]. A comprehensive and technical review of security issues was included in the study, in which confidentiality, integrity, availability, accountability and privacy-preservability were identified as the most significant attributes. To each property, a few security issues are described, followed by the corresponding defense solutions. In the end, it was claimed that the study might help shaping the future research directions in the security and privacy contexts in terms of clouds. In [88], various security challenges were enumerated as key topics in cloud security. Those challenges related with resource allocation, system monitoring and logging, computer forensics, virtualization, multi-tenancy, authentication and authorization, availability, and cloud standards. The study particularly focused afterwards on introducing the Service Level Agreements (SLAs), trust, and accountability topics with regard to cloud security. Issues and solutions were dually discussed throughout the study. The previous works defined the basis of this chapter by providing materials to review the state-of-the-art on the subject. Nonetheless, the review

presented in this chapter contains a wider analysis when compared to those studies, allowing to construct a broader taxonomy for cloud security issues, leaving aside a deeper analysis of solutions for such issues. As commonly seen in other works, including the ones above, the chapter also discusses basic cloud and cloud security concepts in order to ease its understanding.

3 Security-Related Concepts in Cloud Environments

This section defines and describes some basic concepts on cloud and cloud computing, together with key notions on cloud security. The discussion complements some ideas already included in the Introduction section. Thus, it prepares the reader for the remaining part of the chapter.

3.1 Cloud Service Models

The increasing connection demands of the population have triggered the development of Web 2.0 and a new class of services. Cloud systems have adopted a standard three-model architecture, each one containing fundamental parts to support the cloud unique operation. The architecture is composed of IaaS, PaaS and SaaS, sorted upwardly.

The bottom model, IaaS, revolutionized how businessmen invest in IT infrastructures. Instead of spending large amounts of budget in hardware and technical crews to assemble and manage the materials, IaaS providers offer reliable virtual servers on the minute. Amazon Web Services (AWS) is a real example of such providers. A pay-per-use approach is employed in this model, meaning that customers only pay for what they require. Additionally, it abstracts businesses from the scalability, management and provisioning of the infrastructure, allowing them to focus on promoting their applications. The IaaS model provides basic security, including perimeter firewall and load balancing, as long as the VMM is not compromised. The provider should, at least, ensure security up to the VMM, which includes environmental, physical and virtualization security. IaaS ultimately suffers from the data locality and co-location issues.

The middleware model, PaaS, delivers abilities for customers to develop their own cloud applications by providing platforms and frameworks. Consequently, this model becomes more extensible than SaaS by providing a set of customer-ready features, therefore administrating greater flexibility in security. Thus, unsafe Integrated Development Environments (IDEs) and Application Programming Interfaces (APIs) may constitute vulnerability points. Furthermore, because the underlying elements of SOA applications are obscured by the architecture, cybernetic pirates are most likely to attack visible code written by users. A set of coding metrics should be put forward to evaluate the quality of code written by those users.

The top model, SaaS, allows applications to be remotely deployed and hosted on clouds, delivering on-demand capabilities in the form of services that can be accessed via the Internet. This model improves operational efficiency and also reduces costs to customers, similarly to IaaS. It is rapidly becoming prevalent in the cloud business as it is rapidly meeting the requirements of IT companies. However, several security issues are raised by this model, mostly related with data storage, thus making customers uncomfortable in adopting SaaS solutions. Cloud providers must assure data isolation, confidentiality and privacy, meaning that users should not access nor understand data from other users. Nonetheless, from the customer viewpoint, it is hard to tell whether or not the data is well secured, and that applications are available at all times. Furthermore, it is harder to preserve or enhance security that was formerly provided by previous systems.

Although the three service models make up the foundations for the cloud operation, the IT industry is assisting to a mutation; it is converging to Anything-as-a-Service (XaaS). Because clouds are virtually infinite and can, therefore, support anything, or everything, in the form of services, the XaaS approach is able to deliver a wide range of services, including large resources and specific requirements.

3.2 Data Center Facilities Security

As previously said, clouds are computer systems put on specially designed rooms to hold a massive number of servers and network links. Cooling is an active research area in which many approaches are proposed and implemented with the purpose of producing efficient facilities. Protection is other topic of concern when mentioning such facilities. Rooms in such infrastructures hold many expensive network, computation and storage devices, and private data, therefore requiring proper security. In fact, entrepreneurs build data centers while having in mind many geological and environmental aspects, such as location, temperature, humidity, and earthquakes. Other political, governmental, and energy-saving aspects are also taken into consideration. For instance, grid redundancy [22] is a technique used to assure power continuity to devices, by tolerating loss

of any power supply or a single alternating current power source. The goal is to provide the most possible reliable facilities to achieve high availability [19], reaching 99.99 % uptime in many cases, and being fully fault-tolerant. Hence, many data centers achieve the tier 4 level, which is the highest level defining the quality of data centers, being the lowest tier 1. Physical security is established on-site in the data center facilities. If this prerequisite would not be fulfilled, other security measures would be unnecessary. For example, a security center managing video cameras, security sensors, personnel entrances and access to resources may be the most adopted approach. All this to prevent break-ins and other physical violations. Nonetheless, physical access to the rooms holding equipments should be restricted and only exclusive personnel with security clearances should go in to perform managing operations. Flooding attacks, hardware interruption, theft, modification, infrastructure misuse and natural disasters are amongst the main issues of data center facilities [116]. Clouds contain service-driven networks, Storage Area Networks (SANs), and computational and storage-related hardware, which should be dully protected by resorting to firewalls and Intrusion Detection Systems (IDSes), like in standard networks. This approach would enable the analysis of network traffic and the detection or prevention of malicious intrusion attempts [62, 67]. Various IDS solutions have been provided [27, 61, 84]. It is recommended to deploy both IDS and Intrusion Prevention System (IPS) in clouds in order to achieve the desired security level [70]. Honeypots should also be considered, so as to divert attackers attentions [93]. Nonetheless, it should be paid some attention to the trade-off between security and performance [78], because too many security deployments may cause disruptions. Amazon Elastic Compute Cloud (EC2), for example, provides a firewall solution to each customer. By default, it is configured in deny mode, and customers must configure ports to allow incoming traffic for hosted services. The firewall has the ability of restricting traffic by protocol, port, and Internet Protocol (IP) address [1, 8]. 3.3 Cloud Stakeholders Fig. 2 Cloud stakeholders model adapted from [64, 115]. SP stands for service provider The players intervening in the cloud business define how the infrastructure is used and managed. In a simplified way, clouds have virtualized platforms that abstract the underlying hardware, and have services running on top of those platforms. Cloud providers own data center facilities and, therefore, have the responsibility of managing the facilities and the hardware resources in them. Service providers are another, but optional, stakeholder that can rent cloud resources to a cloud provider. In turn, service providers can deliver computational, storage and networking capabilities in the form of services to cloud customers. At all times, SLAs are negotiated in order to define the terms of service and what the cloud customer requires. Ideally, the optimal SLA should cover all critical security requirements. Traditionally, however, the extent of SLAs implemented in the industry does not fully include confidentiality and integrity aspects [88], mainly due to the challenges related with storage outsourcing. End users, which are also part of the model, are the ones that ultimately enjoy the services. This model is schematized in Fig. 2, where two distinct service providers hosting their services on the same cloud are illustrated. A noteworthy aspect is that, while cloud customers are responsible for application-level security, providers are responsible for physical and logical security. Intermediate layers of the cloud stack are shared between one another. Cloud customers may outsource their responsibility in security aspects to third-parties, who sell specialized security services.

3.4 Important Concepts in Cloud Security As clouds rely on virtualization techniques, it is important to identify and describe which elements provide the backbone for virtualization. Thanks to it, a multi-tenant ability is implemented in clouds, meaning that users access applications specially designed to run on cloud platforms. Therefore, it is also important to discuss cloud software with focus on security. Moreover, clouds hold massive amounts of data from cloud customers, which is the main reason why data outsourcing and data storage are critical concepts to discuss. Consequently, standardization is also an issue relevant to include in cloud storage discussions. Finally, trust is briefly discussed from the outsourcing business model standpoint. These concepts are analyzed below, providing the means to clarify and identify the source of some cloud vulnerabilities and threats. 3.4.1 Virtualization Elements Virtualization

itself, or Virtual Machine (VM), is the process of abstracting computer applications, services and Operating Systems (OSes) from the hardware on which they run [93]. Virtualization technologies are placed within the IaaS model. Virtualized OSes are called guest OSes or just guests. The benefits of virtualization include costs and downtime reduction, ease of management and administration, and scalability [14]. Notwithstanding, it brought many new problems intrinsic to its nature, which researchers and entrepreneurs have tried to patch. A VM image is a pre-built copy of the memory and storage contents of a particular VM. VM images can be easily cloned or moved to another location while keeping the integrity of its contents. This allows clouds to deliver highly available services, that is, it keeps VMs running on other physical resources if the previous resources were compromised or allocated for other operations or VMs. Hence, it is perceivable that VMs require a middleware layer to support such operations, which is done by the help of Virtual Machine Monitors (VMMs), usually called hypervisors, and cloud computing OSes. Examples of popular hypervisors are VMware Player, VirtualBox and Xen. Cloud computing OSes are similar to traditional OSes, but provide an additional set of virtualization functionalities, such as allocation and deallocation of VMs, dispatching and migration of processes, and setup interprocess communications, in order to support autonomous scaling and opportunistic deployment of SaaS applications [81]. This would all be great if no security issues arose. However, virtualization brings abstraction in data locality, which means that cloud users cannot pin-point the exact physical location of their data, as VMs can be moved from one machine to another autonomously by the underlying layers. Furthermore, data leakage by exploring VM or hypervisor vulnerabilities is the main virtualization risk. 3.4.2 Multi-Tenancy Multi-tenancy is a virtualization feature that, apart from clouds, it is also present in grid systems. It consists of multiple users, called tenants, sharing a common platform or a single instance of an application. In a public cloud scenario, various customers may share the same VMMs and physical resources, but each one accesses its own VM with inherent SLAs, different security configurations and billing policies. 3.4.3 Cloud Software Although virtualization brings many new issues, issues already prevalent in software developing are transported to clouds. These type of issues scatter over the PaaS and SaaS models, bringing up vulnerabilities in APIs and IDEs, and web technologies, respectively. For instance, bad programming approaches in deploying cloud applications or common Cross-Site Scripting (XSS) attacks can exploit vulnerabilities in these models. Therefore, each service model contains its own problems, raising concerns in the cloud business model. 3.4.4 Data Outsourcing Outsourcing is the process of contracting services from third-party entities. In the context of cloud systems, data outsourcing consists in renting storage services off of cloud providers to store data from the customer on-premises. This approach brings both capital expenditure (CapEx) and operational expenditure (OpEx) to customers. However, more importantly, brings physical separation between the customers and their data, an issue called loss of control [111]. This has been one of the main motivations feeding customers contingency about moving their businesses into clouds. To overcome this, providers must be trustworthy and guarantee secure computing and data storage. 3.4.5 Data Storage Security and Standardization Mechanisms to ensure information security must be applied to data stored in cloud systems. Cryptography approaches must be employed to ensure classical security properties, that is, confidentiality and privacy, integrity, authentication and availability. To this end, cloud providers should provide trusted encryption schemas and application-level protocols, as well as authentication mechanisms and integrity checking techniques to ensure that data was not tampered with. This implies the use of secure communication protocols and standards. Nonetheless, the latest, standardization, poses as one of the cloud main barriers, complicating interoperability and the development of interclouds. Furthermore, applying classical security techniques may be impractical in cloud systems due to the great amount of data stored in their servers. Thinking on hashing entire data sets provides a good example on the issue, since it would require abnormal computational and communication overhead. New mechanisms are nonetheless expected to be developed, such as homomorphic encryption [92] that enables processing encrypted data without being decrypted, ideal for public clouds. Data backups and restores are also essential for the correct

functioning of clouds. To this end, providers usually supply geographic redundancy to data, meaning that data is copied to different geographical locations, usually to another data center of the same cloud provider. 3.4.6 Trust Trust is a critical barrier that must be surpassed in the cloud business model. Firstly, cloud customers must trust in the cloud systems of providers that are going to store their data. Secondly, providers must trust customers with access to the services, that is, access to clouds, which translates into one of the cloud main security issues. Malicious users can conceal attacks by perpetuating them as apparently legitimate users, like the co-location attack. Consequently, SLAs must be well detailed in order to legally cover all possible atypical scenarios in case of unexpected consequences of misusing the cloud infrastructure for both the client or for third-parties. Another important aspect in the trust topic is the pro-activity of cloud users in terms of security. Consider that users use low secure passwords to authenticate in the cloud via web, such as the passwords most used throughout the cybernetic world as shown by SplashData, a company dedicated to address password concerns in IT, in the Worst Passwords of 2012 [94]. The study was compiled by using millions of passwords posted online by hackers and it was concluded that the word password is the most common password. Several distinct characters should be used in order to assemble enough entropy. Moreover, most employees share their passwords with a coworker, a friend, or a friend of a coworker even after receiving password training [101]. This is a major problem, not only in clouds, but to all Internet systems, as unnoticed intrusions can happen. 3.5 General and Cloud-Specific Issues A security issue is a general term that includes several problems. Vulnerabilities, gaps, threats, attacks, and risks are adequate sub-terms that derive from the issue term. It is important to distinguish the difference in these commonly used terms in the security field [26]. Threat is a situation that may exploit a vulnerability, which is a flaw or weakness of a system, as in gap. Attack is the act of exploiting a threat, while risk is the likelihood of a threat agent taking advantage of a vulnerability and corresponding business impact. Moreover, people on the cloud security field tend to misunderstand the difference between general and cloud-specific issues, as that difference is not crisp enough [41]. Cloud computing heavily builds on capabilities available through several core technologies, which include web applications, the cloud service models, virtualization IaaS offerings, and cryptography mechanisms. A cloud-specific security issue must be intrinsic to or prevalent in a core technology. It has to have its root cause in one of the five essential characteristics proposed by the NIST, it is provoked when innovations make tried-and-tested security controls difficult or impossible to implement, or it is prevalent in established state-of-the-art cloud offerings. Only cloud-specific issues are included in the chapter. 3.6 Categorization of Cloud Security Issues Researchers tend to define their own taxonomy on cloud security issues as there is not yet a de facto standard to follow. The study described in [92] mentions four categories, namely cloud infrastructure, platform and hosted code, data, access, and compliance. Another study [59] organized security issues into a model with three main sections, named security categories, security dimensions and security in the service models. Security categories span from cloud customers to providers, which can also be complemented with government entities [15], while security dimensions include domains, risks and threats. For instance, the isolation failure threat is due to virtualization vulnerabilities, therefore being placed on the IaaS model, posing as an issue to both customers and providers. In this chapter, the assessment of existing security issues in cloud security is done with basis on the previously discussed studies. This chapter considers software-related; data storage and computation; virtualization; networking, web and hardware resources; access; and trust as the most direct, in terms of threat identification, and embracing security issues set of categories in the cloud context. 4 Main Cloud Security Issues Due to the growth of the cloud in the industry, entrepreneurs have decided to adopt cloud services, in spite of being aware of its security issues. Thus, clouds attract attention from a potential dangerous community and other parties aiming to exploit security vulnerabilities, and to perhaps publicly disclose private information. Malicious activities are motivated by a wide panoply of reasons, namely personal benefit, glory or vendetta. Therefore, it is important to address such security issues, which are thoroughly reviewed in this

section. This review is supported by a comprehensive study of the state-of-the-art on the subject. 4.1 Security Issues Identified by Organizations The cloud security topic concerns not only the research community, but also the industry. Various documents have been published with the intent of aiding the development of trustworthy cloud systems. Nonetheless, customers should get a security assessment from third-parties before committing to a cloud provider. The following works, described in chronological order, are considered pioneering works on the subject [59]. The Gartner published the security document entitled Assessing the Security Risks of Cloud Computing [37]. In this document, seven security risks are identified as critical aspects to be considered by cloud customers before committing to a provider. They are privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, and long-term viability. The European Network and Information Security Agency (ENISA), an organization responsible for responding to cyber security issues in the European Union, provided the document entitled Cloud Computing: Benefits, Risks and Recommendations [33]. Eight cloud specific risks are considered as top risks also from the customer viewpoint. They are loss of governance, lock-in, isolation failure, compliance risks, management interface compromise, data protection, insecure of incomplete data deletion, and malicious insider. Table 1 Top threats to cloud computing as described in CSA [25], plus the domains in which they are included and the service models they affect. A check mark means the threat affects the underlying model. A cross means otherwise

Threat #	Name	IaaS	PaaS	SaaS
1	Abuse and Nefarious use of cloud computing			
2	Insecure interfaces and APIs			

---

networks and
networked applications. Specifically, upon reading this book, audiences will perceive the following
benefits:
1. Learn the state-of-the-art in research and development on cloud security, privacy and
trust.
2. Obtain a future roadmap by learning open research issues.
3. Gather the background knowledge to tackle key problems, whose solutions will enhance the evolution of next-generation secure cloud systems.

Security, Privacy and Trust in the IoT Environment 1st ed. 2019 - Book title: Data Security in Cloud Computing understanding software defined perimeter; security, trust and privacy for Cloud Computing in transportation Cloud Computing: Theory and Practice - We're the national information and technology partner to the health and social care system using digital technology to transform the NHS and social care. Aws Hypervisor Security - Introduction. Cloud computing has recently emerged as one of the buzzwords in the ICT industry. Security, Privacy, and Trust management issues. Cloud Facebook To Stop Using Phone Numbers To Recommend - Data Security in Cloud Computing covers major aspects of securing data in software defined perimeter; security, trust and privacy for Cloud Computing in Amazon wish list buyer privacy - Xing Fu Tang Singapore - The book compiles technologies for enhancing and provisioning security, privacy and trust in cloud systems based on Quality of Service Demisto admin guide - Live Oak Art Center - The Network Architect's Guide to Zero Trust This repository contains all Mist Systems, a Juniper Company Mist is pioneering the new wireless network. threat Jul 15, 2019 Â· This guide tracks privacy issues with antivirus software and is Job Description for Security Engineer_ibm Cloud IaaS in IBM India Pvt. I have Security and Security and Privacy Issues in Cloud Computing - Liliana F. B. Big Data and Cloud: Trust, Security and Privacy - Nova - Malcolm Gladwell's book, â€œThe Tipping Point: How Little Things Can Make a Big Differenceâ€•, How to Determine the Right Mix of Hybrid Cloud Trust in institutions â€“ big banks, retail, professional services organisations, membership About Us · Contact · Privacy Policy · Cookie Policy · Member Preferences · Advertising Publications Advanced Cyber Security Engineering - But beware: there may be a few traps waiting for the unsuspecting book fan. org and *. multiple choice questions and answers on Cloud Computing MCQ questions quiz on Cloud Computing objective questions test pdf. Top privacy and security questions and answers... How do I know what websites I can trust? The Cloud: Understanding the Security, Privacy and - jstor - Ranging from mobile to the cloud, the increase in

information system complexity The first section of the book considers trust management, privacy and access Security services from a cloud you can trust - Microsoft - The Network Architect's Guide to Zero Trust This repository contains all Mist Systems, a Juniper Company Mist is pioneering the new wireless network. threat Jul 15, 2019 Â· This guide tracks privacy issues with antivirus software and is Job Description for Security Engineer_ibm Cloud IaaS in IBM India Pvt. I have

---

Relevant Books
