

Trust And Technology In A Ubiquitous Modern Environment Theoretical And Methodological Perspectives Premier Reference Source

"This book brings together scholars with significantly different backgrounds who share interests in the interplay between trust and technology, presenting novel theoretical perspectives on the topics of trust and technology, as well as some empirical investigations into the trust-building, trust-repairing, and trust-destroying practices in the context of technology"--Provided by publisher.

This book provides an introduction, discussion, and formal-based modelling of trust theory and its applications in agent-based systems This book gives an accessible explanation of the importance of trust in human interaction and, in general, in autonomous cognitive agents including autonomous technologies. The authors explain the concepts of trust, and describe a principled, general theory of trust grounded on cognitive, cultural, institutional, technical, and normative solutions. This provides a strong base for the author's discussion of role of trust in agent-based systems supporting human-computer interaction and distributed and virtual organizations or markets (multi-agent systems). Key Features: Provides an accessible introduction to trust, and its importance and applications in agent-based systems Proposes a principled, general theory of trust grounding on cognitive, cultural, institutional, technical, and normative solutions. Offers a clear, intuitive approach, and systematic integration of relevant issues Explains the dynamics of trust, and the relationship between trust and security Offers operational definitions and models directly applicable both in technical and experimental domains Includes a critical examination of trust models in economics, philosophy, psychology, sociology, and AI This book will be a valuable reference for researchers and advanced students focused on information and communication technologies (computer science, artificial intelligence, organizational sciences, and knowledge management etc.), as well as Web-site and robotics designers, and for scholars working on human, social, and cultural aspects of technology. Professionals of ecommerce systems and peer-to-peer systems will also find this text of interest.

Due to the growth of internet and mobile applications, relationship marketing continues to evolve as technology offers more collaborative and social communication opportunities. Managing Customer Trust, Satisfaction, and Loyalty through Information Communication highlights technology's involvement with business processes in different sectors and industries while identifying marketing activities that are affected by its usage. This reference is a vital source for organizational managers, executives, and professionals, as well as academics and students interested in this constantly changing field.

If you can't trust those in charge, who can you trust?From government to business, banks to media, trust in institutions is at an all-time low. But this isn't the age of distrust--far from it. In this revolutionary book, world-renowned trust expert Rachel Botsman reveals that we are at the tipping point of one of the biggest social transformations in human history--with fundamental consequences for everyone. A new world order is emerging: we might have lost faith in institutions and leaders, but millions of people rent their homes to total strangers, exchange digital currencies, or find themselves trusting a bot. This is the age of "distributed trust," a paradigm shift driven by innovative technologies that are rewriting the rules of an all-too-human relationship. If we are to benefit from this radical shift, we must understand the mechanics of how trust is built, managed, lost, and repaired in the digital age. In the first book to explain this new world, Botsman provides a detailed map of this uncharted landscape--and explores what's next for humanity.

One of the most persistent concerns about the future is whether it will be dominated by the predictive algorithms of AI – and, if so, what this will mean for our behaviour, for our institutions and for what it means to be human. AI changes our experience of time and the future and challenges our identities, yet we are blinded by its efficiency and fail to understand how it affects us. At the heart of our trust in AI lies a paradox: we leverage AI to increase our control over the future and uncertainty, while at the same time the performativity of AI, the power it has to make us act in the ways it predicts, reduces our agency over the future. This happens when we forget that that we humans have created the digital technologies to which we attribute agency. These developments also challenge the narrative of progress, which played such a central role in modernity and is based on the hubris of total control. We are now moving into an era where this control is limited as AI monitors our actions, posing the threat of surveillance, but also offering the opportunity to reappropriate control and transform it into care. As we try to adjust to a world in which algorithms, robots and avatars play an ever-increasing role, we need to understand better the limitations of AI and how their predictions affect our agency, while at the same time having the courage to embrace the uncertainty of the future.

"This book explores current advances in digital and mobile computing technologies from the user perspective, evaluating trust models and autonomic trust management covering the recent history of trust in digital environments to prospective future developments"--Provided by publisher.

We have a trust problem. Due to the rapid proliferation of data and technology across society, a disconnect has formed between employees and customers; the organizations they service and those that service them. This is causing an erosion of trust. Given that trust is the single most important asset of any organization, that's a problem. However, there is good news on the horizon. Pioneering business leaders and organizations have begun leading a charge to restore trust. The Business of Trust explores how thought leaders are rebuilding trust and uncovers insights you can apply across employee and customer experiences. In this book you'll discover: The economics of trust and how it translates to the bottom line Why employees are your most important customers The three trust drivers that will have the most impact This book is for working professionals looking to better understand how trust shapes their organization. Building trust is a journey with no end. It will be bui

Written by prominent thought leaders in the global fintech space, The AI Book aggregates diverse expertise into a single, informative volume and explains what artificial intelligence really means and how it can be used across financial services today. Key industry developments are explained in detail, and critical insights from cutting-edge practitioners offer first-hand information and lessons learned. Coverage includes: · Understanding the AI Portfolio: from machine learning to chatbots, to natural language processing (NLP); a deep dive into the Machine

Intelligence Landscape; essentials on core technologies, rethinking enterprise, rethinking industries, rethinking humans; quantum computing and next-generation AI · AI experimentation and embedded usage, and the change in business model, value proposition, organisation, customer and co-worker experiences in today's Financial Services Industry · The future state of financial services and capital markets – what's next for the real-world implementation of AI Tech? · The innovating customer – users are not waiting for the financial services industry to work out how AI can re-shape their sector, profitability and competitiveness · Boardroom issues created and magnified by AI trends, including conduct, regulation & oversight in an algo-driven world, cybersecurity, diversity & inclusion, data privacy, the 'unbundled corporation' & the future of work, social responsibility, sustainability, and the new leadership imperatives · Ethical considerations of deploying AI solutions and why explainable AI is so important

Bloggers in India used social media and wikis to broadcast news and bring humanitarian aid to tsunami victims in South Asia. Terrorist groups like ISIS pour out messages and recruit new members on websites. The Internet is the new public square, bringing to politics a platform on which to create community at both the grassroots and bureaucratic level. Drawing on historical and contemporary case studies from more than ten countries, Irene S. Wu's *Forging Trust Communities* argues that the Internet, and the technologies that predate it, catalyze political change by creating new opportunities for cooperation. The Internet does not simply enable faster and easier communication, but makes it possible for people around the world to interact closely, reciprocate favors, and build trust. The information and ideas exchanged by members of these cooperative communities become key sources of political power akin to military might and economic strength. Wu illustrates the rich world history of citizens and leaders exercising political power through communications technology. People in nineteenth-century China, for example, used the telegraph and newspapers to mobilize against the emperor. In 1970, Taiwanese cable television gave voice to a political opposition demanding democracy. Both Qatar (in the 1990s) and Great Britain (in the 1930s) relied on public broadcasters to enhance their influence abroad. Additional case studies from Brazil, Egypt, the United States, Russia, India, the Philippines, and Tunisia reveal how various technologies function to create new political energy, enabling activists to challenge institutions while allowing governments to increase their power at home and abroad. *Forging Trust Communities* demonstrates that the way people receive and share information through network communities reveals as much about their political identity as their socioeconomic class, ethnicity, or religion. Scholars and students in political science, public administration, international studies, sociology, and the history of science and technology will find this to be an insightful and indispensable work.

This book encapsulates some work done in the DIRC project concerned with trust and responsibility in socio-technical systems. It brings together a range of disciplinary approaches - computer science, sociology and software engineering - to produce a socio-technical systems perspective on the issues surrounding trust in technology in complex settings. Computer systems can only bring about their purported benefits if functionality, users and usability are central to their design and deployment. Thus, technology can only be trusted in situ and in everyday use if these issues have been brought to bear on the process of technology design, implementation and use. The studies detailed in this book analyse the ways in which trust in technology is achieved and/or worked around in everyday situations in a range of settings - including hospitals, a steelworks, a public enquiry, the financial services sector and air traffic control. Whilst many of the authors here may already be known for their ethnographic work, this book moves on from accounts of 'field studies' to show how the DIRC project has utilised the data from these studies in an interdisciplinary fashion, involving computer scientists, software engineers and psychologists, as well as sociologists. Chapters draw on the empirical studies but are organised around analytical themes related to trust which are at the heart of the authors' socio-technical approach which shows the nuanced ways in which technology is used, ignored, refined and so on in everyday settings.

This book constitutes the refereed proceedings of the 10th IFIP WG 11.11 International Conference on Trust Management, IFIPTM 2016, held in Darmstadt, Germany, in July 2016. The 7 revised full papers and 7 short papers presented together with an invited paper were carefully reviewed and selected from 26 submissions. The papers cover a wide range of topics including trust architecture, trust modeling, trust metrics and computation, reputation and privacy, security and trust, sociotechnical aspects of trust, and attacks on trust and reputation systems.

This comprehensive guide serves to illuminate the rise and development of FinTech in Sweden, with the Internet as the key underlying driver. The multiple case studies examine topics such as: the adoption of online banking in Sweden; the identification and classification of different FinTech categories; process innovation developments within the traditional banking industry; and the Venture Capital (VC) landscape in Sweden, as shown through interviews with VC representatives, mainly from Sweden but also from the US and Germany, as well as offering insight into the companies that are currently operating in the FinTech arena in Sweden. The authors address questions such as: How will the regulatory landscape shape the future of FinTech companies? What are the factors that will likely drive the adoption of FinTech services in the future? What is the future role of banks in the context of FinTech and digitalization? What are the policies and government initiatives that aim to support the FinTech ecosystem in Sweden? Complex concepts and ideas are rendered in an easily digestible yet thought-provoking way. The book was initiated by the IIS (the Internet Foundation in Sweden), an independent organization promoting the positive development of the Internet in the country. It is also responsible for the Internet's Swedish top-level domain .se, including the registration of domain names, and the administration and technical maintenance of the national domain name registry. The book illustrates how Sweden acts (or does not act) as a competitive player in the global FinTech arena, and is a vital addition to students and practitioners in the field.

This book provides information on trust and risk to businesses that are developing electronic commerce systems and helps consumers understand the risks in using the Internet for purchases and show them how to protect themselves.

Brings together research on the introduction of domestic technologies into country houses and their estates.

An increasing reliance on the Internet and mobile communication has deprived us of our usual means of assessing another party's trustworthiness. This is increasingly forcing us to rely on control. Yet the notion of trust and trustworthiness is essential to the continued development of a technology-enabled society. *Trust, Complexity and Control* offers readers a single, consistent explanation of how the sociological concept of 'trust' can be applied to a broad spectrum of technology-related areas; convergent communication, automated agents, digital security, semantic web, artificial intelligence, e-commerce, e-government, privacy etc. It presents a model of confidence in which trust and control are driven and limited by complexity in one explanatory

framework and demonstrates how that framework can be applied to different research and application areas. Starting with the individual's assessment of trust, the book shows the reader how application of the framework can clarify misunderstandings and offer solutions to complex problems. The uniqueness of Trust, Complexity and Control is its interdisciplinary treatment of a variety of diverse areas using a single framework. Sections featured include: Trust and distrust in the digital world. The impact of convergent communication and networks on trust. Trust, economy and commerce. Trust-enhancing technologies. Trust, Complexity and Control is an invaluable source of reference for both researchers and practitioners within the Trust community. It will also be of benefit to students and lecturers in the fields of information technology, social sciences and computer engineering.

Trustworthiness technologies and systems for service-oriented environments are re-shaping the world of e-business. By building trust relationships and establishing trustworthiness and reputation ratings, service providers and organizations will improve customer service, business value and consumer confidence, and provide quality assessment and assurance for the customer in the networked economy. Trust and Reputation for Service-Oriented Environments is a complete tutorial on how to provide business intelligence for sellers, service providers, and manufacturers. In an accessible style, the authors show how the capture of consumer requirements and end-user opinions gives modern businesses the competitive advantage. Trust and Reputation for Service-Oriented Environments: Clarifies trust and security concepts, and defines trust, trust relationships, trustworthiness, reputation, reputation relationships, and trust and reputation models. Details trust and reputation ontologies and databases. Explores the dynamic nature of trust and reputation and how to manage them efficiently. Provides methodologies for trustworthiness measurement, reputation assessment and trustworthiness prediction. Evaluates current trust and reputation systems as employed by companies such as Yahoo, eBay, BizRate, Epinion and Amazon, etc. Gives ample illustrations and real world examples to help validate trust and reputation concepts and methodologies. Offers an accompanying website with lecture notes and PowerPoint slides. This text will give senior undergraduate and masters level students of IT, IS, computer science, computer engineering and business disciplines a full understanding of the concepts and issues involved in trust and reputation. Business providers, consumer watch-dogs and government organizations will find it an invaluable reference to establishing and maintaining trust in open, distributed, anonymous service-oriented network environments.

'This is a welcome book. The issues of public understanding of science open many questions. What does "understanding" mean? How does understanding translate into attitudes towards science and trust in scientists? What is the role of the mass media? The essays in this book shed light on such questions bringing insights from several disciplines. They help to define a meaningful research agenda for the future. - Professor Dorothy Nelkin, New York University

Culture and Trust in Technology-Driven Organizations provides insight into the important role that culture and trust can play in the success of high-technology organizations. This book reviews the literature and results of an empirical study that investigated the relationship between mechanistic and organic cultures and the level of trust in technology-based organizations. The book outlines the literature on organizational trust and culture and the role theorists believe they play in the success of a changing domestic and global business environment. It identifies ways of defining culture and trust as well as the survey instruments used to measure them. The book then examines the results of two studies that demonstrate the connection between organizational culture and trust. The two studies were conducted at separate times using data collected from several companies within a three-hour radius of each other. These companies are highly dependent upon the ability to identify, hire, and retain highly skilled knowledge workers. These workers are critical for the companies to successfully compete within the scope of their business and expand into their current and other markets. The book provides a practitioner's guide—based on the literature review and the results of the studies examined—that can be used to assess, diagnose, and improve employees' perception of their work culture and improve trust found in organizations. This guide provides management with actions and activities that should be considered when handling the day-to-day business of the organization. If followed, these activities can be instrumental in designing a culture that leads to success and ease of operation for the organization and its members.

The objective of this book is to report on contemporary trends in the defence research community on trust in teams, including inter- and intra-team trust, multi-agency trust and coalition trust. The book also considers trust in information and automation, taking a systems view of humans as agents in a multi-agent, socio-technical, community. The different types of trust are usually found to share many of the same emotive, behavioural, cognitive and social constructs, but differ in the degree of importance associated with each of them. Trust in Military Teams is written by defence scientists from the USA, Canada, Australia and the UK, under the auspices of The Transfer Cooperation Programme. It is representative of the latest thinking on trust in teams, and is written for defence researchers, postgraduate students, academics and practitioners in the human factors community.

Erhvervsledere inden for udvikling og anvendelse af digital teknologi giver deres bud på, hvordan vi sikrer, at fremtidens teknologi bliver et gode for samfundet snarere end en trussel. Forfatterne til bogen beskriver de seks værdier, der som et kompas skal guide virksomheder, når de udvikler og anvender teknologi: åbenhed, respekt, relevans, ansvarlighed og tillid. Desuden bidrager forfatterne med overvejelser om etiske aspekter af teknologi

"This book provides an overall view of trust for e-services including definitions, constructs, and relationships with other research topics such as security, privacy, reputation and risk. It offers contributions from real-life experience and practice on how to build a trust environment for e-government services"--Provided by publisher.

Business approaches in today's society have become technologically-driven and highly-applicable within various professional fields. These business practices have transcended traditional boundaries with the implementation of internet technology, making it challenging for professionals outside of the business world to understand these advancements. Interdisciplinary research on business technology is required to better comprehend its innovations. Interdisciplinary Approaches to Digital Transformation and Innovation provides emerging research exploring the complex interconnections of technological business practices within society. This book will explore the practical and theoretical aspects of e-business technology within the fields of engineering, health, and social sciences. Featuring coverage on a broad range of topics such as data monetization, mobile commerce, and digital marketing, this book is ideally designed for researchers, managers, students, engineers, computer scientists, economists, technology designers, information specialists, and administrators seeking current research on the application of e-business technologies within multiple fields.

For scholars interested in how social concepts such as trust impact on new technologies, this is undoubtedly a valuable contribution. Ian Grant, Telecommunications Policy . . . the editors have managed to provide a comprehensive overview of current conceptual and empirical research on trust-related issues from multiple perspectives. . . Trust and New Technologies is an enlightening collection of research papers on trust. The book should be of interest to scholars, practitioners and researchers focusing on the applications of new technologies in marketing and business management. Since trust also is a key concept in information behaviour studies, researchers interested in this field will also find this book a useful resource. Madely du Perez, Australian Library Journal This book is a timely collection of research papers on one of the most critical subjects on the internet. It explores a wide range of trust related issues from multiple perspectives, and by researchers from around Europe and America. The papers address the different roles that trust plays in consumer marketing in online environments, in mobile media, and in organizational relations. The issues highlighted are relevant to both academics and practitioners. Feng Li, University of Newcastle upon Tyne, UK Trust and New Technologies presents versatile new research that illustrates the different roles that trust plays in the marketing and management of new technologies. The authors provide a comprehensive and much needed overview of the current state of conceptual and empirical research in the topical area of trust and new technologies. Comprising of sixteen chapters, the book is divided thematically into three sections: consumer trust in online environments trust and mobile media new technologies and trust within and between organizations. This enlightening book will be of great interest to scholars, practitioners and research students focusing on the applications of new technologies in marketing and management. Trust researchers across business disciplines and the social sciences will also find this timely and unique book a constructive resource.

As the use of technology has considerably increased in B2B e-commerce, it becomes imperative to address the issues of trust that emerge in the context of technology. Trust and Technology in B2B E-Commerce: Practices and Strategies for Assurance focuses on various trust issues that emerge from deployment of various e-commerce technologies in interorganizational relationships. Some of these issues relate to security, privacy, authentication, non-repudiation, quality of Web interface, system performance, infrastructure, and environmental factors. This book contributes to the ongoing process of developing a framework for understanding the process of building trust in B2B e-commerce.

As global communities are attempting to transform into more efficient and technologically-advanced metropolises, artificial intelligence (AI) has taken a firm grasp on various professional fields. Technology used in these industries is transforming by introducing intelligent techniques including machine learning, cognitive computing, and computer vision. This has raised significant attention among researchers and practitioners on the specific impact that these smart technologies have and what challenges remain. Applications of Artificial Intelligence for Smart Technology is a pivotal reference source that provides vital research on the implementation of advanced technological techniques in professional industries through the use of AI. While highlighting topics such as pattern recognition, computational imaging, and machine learning, this publication explores challenges that various fields currently face when applying these technologies and examines the future uses of AI. This book is ideally designed for researchers, developers, managers, academicians, analysts, students, and practitioners seeking current research on the involvement of AI in professional practices.

Experts from disciplines that range from computer science to philosophy consider the challenges of building AI systems that humans can trust. Artificial intelligence-based algorithms now marshal an astonishing range of our daily activities, from driving a car ("turn left in 400 yards") to making a purchase ("products recommended for you"). How can we design AI technologies that humans can trust, especially in such areas of application as law enforcement and the recruitment and hiring process? In this volume, experts from a range of disciplines discuss the ethical and social implications of the proliferation of AI systems, considering bias, transparency, and other issues. The contributors, offering perspectives from computer science, engineering, law, and philosophy, first lay out the terms of the discussion, considering the "ethical debts" of AI systems, the evolution of the AI field, and the problems of trust and trustworthiness in the context of AI. They go on to discuss specific ethical issues and present case studies of such applications as medicine and robotics, inviting us to shift the focus from the perspective of a "human-centered AI" to that of an "AI-decentered humanity." Finally, they consider the future of AI, arguing that, as we move toward a hybrid society of cohabiting humans and machines, AI technologies can become humanity's allies.

The vision of ubiquitous computing and ambient intelligence describes a world of technology which is present anywhere, anytime in the form of smart, sensible devices that communicate with each other and provide personalized services. However, open interconnected systems are much more vulnerable to attacks and unauthorized data access. In the context of this threat, this book provides a comprehensive guide to security and privacy and trust in data management.

Learn to analyze and measure risk by exploring the nature of trust and its application to cybersecurity Trust in Computer Systems and the Cloud delivers an insightful and practical new take on what it means to trust in the context of computer and network security and the impact on the emerging field of Confidential Computing. Author Mike Bursell's experience, ranging from Chief Security Architect at Red Hat to CEO at a Confidential Computing start-up grounds the reader in fundamental concepts of trust and related ideas before discussing the more sophisticated applications of these concepts to various areas in computing. The book demonstrates in the importance of understanding and quantifying risk and draws on the social and computer sciences to explain hardware and software security, complex systems, and open source communities. It takes a detailed look at the impact of Confidential Computing on security, trust and risk and also describes the emerging concept of trust domains, which provide an alternative to standard layered security. Foundational definitions of trust from sociology and other social sciences, how they evolved, and what modern concepts of trust mean to computer professionals A comprehensive examination of the importance of systems, from open-source communities to HSMs, TPMs, and Confidential Computing with TEEs. A thorough exploration of trust domains, including explorations of communities of practice, the centralization of control and policies, and monitoring Perfect for security architects at the CISSP level or higher, Trust in Computer Systems and the Cloud is also an indispensable addition to the libraries of system architects, security system engineers, and master's students in software architecture and security.

In the digital era, information is the most valuable resource, and protecting one's assets is a constant struggle for both individuals and organizations. Analyzing Security, Trust, and Crime in the Digital World explores techniques and technologies used to secure data and prevent intrusion in virtual environments. Within these pages, computer scientists, programmers, engineers,

and practitioners will find meaningful research on intrusion detection and authentication techniques in order to further defend their own systems and protect the information therein.

If governed adequately, AI (artificial intelligence) has the potential to benefit humankind enormously. However, if mismanaged, it also has the potential to harm humanity catastrophically. The title of this book reflects the belief that access to the benefits of AI, awareness about the nature of the technology, governance of the technology and its development process with a focus on responsible development, should be transparent, open, understood by and accessible to all people regardless of their geographic, generational, economic, cultural and/or other social background. The book is the result of a discussion series organized by the Association of Pacific Rim Universities (APRU) which was financially supported by Google.

Focused on the latest mobile technologies, this book addresses specific features (such as IoT) and their adoptions that aim to enable excellence in business in Industry 4.0. Furthermore, this book explores how the adoption of these technologies is related to rising concerns about privacy and trusted communication issues that concern management and leaders of business organizations. *Managing IoT and Mobile Technologies with Innovation, Trust, and Sustainable Computing* not only targets IT experts and drills down on the technical issues but also provides readers from various groups with a well-linked concept about how the latest trends of mobile technologies are closely related to daily living and the workplace at managerial and even individual levels.

How the blockchain—a system built on foundations of mutual mistrust—can become trustworthy. The blockchain entered the world on January 3, 2009, introducing an innovative new trust architecture: an environment in which users trust a system—for example, a shared ledger of information—without necessarily trusting any of its components. The cryptocurrency Bitcoin is the most famous implementation of the blockchain, but hundreds of other companies have been founded and billions of dollars invested in similar applications since Bitcoin's launch. Some see the blockchain as offering more opportunities for criminal behavior than benefits to society. In this book, Kevin Werbach shows how a technology resting on foundations of mutual mistrust can become trustworthy. The blockchain, built on open software and decentralized foundations that allow anyone to participate, seems like a threat to any form of regulation. In fact, Werbach argues, law and the blockchain need each other. Blockchain systems that ignore law and governance are likely to fail, or to become outlaw technologies irrelevant to the mainstream economy. That, Werbach cautions, would be a tragic waste of potential. If, however, we recognize the blockchain as a kind of legal technology that shapes behavior in new ways, it can be harnessed to create tremendous business and social value.

Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives IGI Global

Most aspects of our private and social lives—our safety, the integrity of the financial system, the functioning of utilities and other services, and national security—now depend on computing. But how can we know that this computing is trustworthy? In *Mechanizing Proof*, Donald MacKenzie addresses this key issue by investigating the interrelations of computing, risk, and mathematical proof over the last half century from the perspectives of history and sociology. His discussion draws on the technical literature of computer science and artificial intelligence and on extensive interviews with participants. MacKenzie argues that our culture now contains two ideals of proof: proof as traditionally conducted by human mathematicians, and formal, mechanized proof. He describes the systems constructed by those committed to the latter ideal and the many questions those systems raise about the nature of proof. He looks at the primary social influence on the development of automated proof—the need to predict the behavior of the computer systems upon which human life and security depend—and explores the involvement of powerful organizations such as the National Security Agency. He concludes that in mechanizing proof, and in pursuing dependable computer systems, we do not obviate the need for trust in our collective human judgment.

This open access book brings together perspectives from multiple disciplines including psychology, law, IS, and computer science on data privacy and trust in the cloud. Cloud technology has fueled rapid, dramatic technological change, enabling a level of connectivity that has never been seen before in human history. However, this brave new world comes with problems. Several high-profile cases over the last few years have demonstrated cloud computing's uneasy relationship with data security and trust. This volume explores the numerous technological, process and regulatory solutions presented in academic literature as mechanisms for building trust in the cloud, including GDPR in Europe. The massive acceleration of digital adoption resulting from the COVID-19 pandemic is introducing new and significant security and privacy threats and concerns. Against this backdrop, this book provides a timely reference and organising framework for considering how we will assure privacy and build trust in such a hyper-connected digitally dependent world. This book presents a framework for assurance and accountability in the cloud and reviews the literature on trust, data privacy and protection, and ethics in cloud computing.

[Copyright: 02503ffad85da49d1d13e80c88174cc0](https://doi.org/10.4018/9781609608817)