CHAPTER 1

Understanding Trust and Cloud Computing: An Integrated Framework for Assurance and Accountability in the Cloud

Theo Lynn, Lisa van der Werff, and Grace Fox

Abstract Trust is regularly cited as one the main barriers for increased adoption of cloud computing, however conceptualisations of trust in cloud computing literature can be simplistic. This chapter briefly introduces the trust literature including definitions and antecedents of trust. Following an overview of cloud computing, we discuss some of the cited barriers to trust in cloud computing, and proposed mechanisms for building trust in the cloud. We present a high-level framework for exploring assurance (trust building) and accountability (trust repair) in the cloud and call for a more integrated multi-stakeholder approach to trust research in this multi-faceted context.

T. Lynn (✉) • L. van der Werff • G. Fox
Irish Institute of Digital Business, DCU Business School,
Dublin, Ireland
e-mail: theo.lynn@dcu.ie; lisa.vanderwerff@dcu.ie; Grace.Fox@dcu.ie

T. Lynn et al. (eds.), *Data Privacy and Trust in Cloud Computing*,
Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-030-54660-1_1

Keywords Trust • Cloud computing • Trust building • Trust repair • Assurance • Accountability

1.1 Introduction

Trust. A word that, while commonly used, is a complex concept that means different things to different people in different contexts. Technology is no different. "We don't trust the cloud" is a common phrase used to describe consumer or industry reluctance to adopt cloud computing. You will find it, or wording to the same effect, in numerous scholarly studies, industry surveys, and media, new and old. No matter what part of the economy, society, or world that you are in, you can find a report or survey suggesting that significant proportions of the public, businesses of all sizes, and the public sector do not or should not trust the cloud. Similarly, there are a myriad of, often conflicting, proposals and 'solutions' for overcoming trust issues in cloud computing. These include greater regulation, increased certification, stronger security, anonymity, trust by design, privacy by design, and so on. Indeed the importance of establishing trust in the cloud has been highlighted time and time again both in industry and academic discourse, with trust heralded as a solution to ease any concerns related to privacy and security on the cloud.

The objective of this book is to make some progress in teasing out what trust means in the context of cloud computing through a variety of lenses—psychology, law, ethics, information systems, and computing. The remainder of this chapter briefly introduces the trust literature including definitions and antecedents of trust. Next, we provide an overview of cloud computing and some of the reported trust-related barriers to cloud adoption and proposed solutions. Finally, we present a high-level framework for exploring assurance and accountability in the cloud.

1.2 Trust

Trust is generally defined as a willingness to accept vulnerability based on positive expectations of another party (Rousseau et al. 1998). This definition has two critical elements—first, the psychological state of willingness to be vulnerable which represents a volitional choice or decision (van der Werff et al. 2019a). Second, there are positive expectations of another

party, which refers to the influence of proximal antecedents or drivers of trust. Thus far, the trust literature has focused predominantly on a relatively small subset of proximal trust antecedents known as trustworthiness (Baer and Colquitt 2018). Trustworthiness is an aggregate perception of the characteristics of another party along three sub-dimensions: ability, integrity, and benevolence (Mayer et al. 1995). These concepts have been applied within the context of technology and appear regularly in the information systems literature (see van der Werff et al. 2018 for a review). This section will provide an overview of several potential antecedents of trust in cloud computing organised into two broad categories: knowledge based antecedents, including trustworthiness, and heuristic antecedents.

1.2.1 Knowledge Based Antecedents

The two aspects of trustworthiness most commonly studied in the trust in technology literature are ability and integrity. Ability or competence refers to a perception that the other party possesses the skills and knowledge to complete the tasks expected. This aspect of trustworthiness is readily applicable to perceptions of technology in terms of its performance levels including accuracy, capability and functionality (McKnight et al. 2011; Söllner et al. 2016). That is, *can* this cloud service do what I need it to do well? Integrity generally refers to the perception that another party adheres to a set of principles that the trustor finds acceptable, acts honestly and fulfils their promises (Mayer et al. 1995; McKnight et al. 1998). In the technology environment, this concept has typically been translated as a perception of reliability and consistency in performance. For instance, *will* this cloud service do what I need it to do *every* time I use it? In this setting in particular, the conceptualisation of integrity is expanded to integrate aspects of predictability and the extent to which it is possible to anticipate the other party's behaviour accurately (van der Werff et al. 2018). Interestingly, as they are applied in the computer science literature (see Chap. 7), these aspects of trustworthy cloud computing are sometimes portrayed as an objective feature of the technology rather than a more subjective user's perception of the technology as the original trust theory intended. This difference has particularly important implications in situations where the decision maker is not a technology expert and so subjective perceptions of trustworthiness are likely to differ significantly from any objective reality.

The third aspect of trustworthiness, benevolence, has received less attention in the cloud computing literature. As a perception of the extent to which another party will act in your best interests, benevolence incorporates aspects of agency and motivation into calculations of trustworthiness. Does the other party *want* to act in my best interests? At the moment, cloud services are not likely to act with either agency or motivation and benevolence perceptions have been applied in this context as a perception of alignment between user needs and the technology's purpose, helpfulness and responsiveness (McKnight et al. 2011; Söllner et al. 2016). However, while we may have some way to go before cloud services are automated to the point of agency, for many users anthropomorphisation of technology is common and perceptions of its motives and intentions are likely to play a role in trust decisions (Shank and DeSanti 2018).

1.2.2 Heuristic Antecedents

The use of knowledge based cues for trust is sometimes described as trust based on "good reasons" or rational decision making (Lewis and Weigert 1985, p. 970). However, a growing body of theoretical work and empirical evidence suggests that trust processes can be influenced by less rational antecedents and by beliefs about other related entities. The idea that such factors impact trust has gained traction over the last decade particularly in relation to trust in new or unknown other parties (e.g. Baer et al. 2018; Kramer and Lewicki 2010; McKnight et al. 1998) and trust in technology (e.g. McKnight et al. 2011). This section will briefly discuss four antecedents that may have a heuristic influence on trust in cloud computing: situational normality, aesthetics, structural assurances, and relational context.

The concept of situational normality was originally introduced to the trust literature by McKnight et al. (1998) who proposed that feeling like a situation was normal, familiar or as expected could be a powerful heuristic in building trust in unknown other parties. Since then, empirical evidence has repeatedly demonstrated the utility of situational normality as an antecedent of trust in organisations (Baer et al. 2018), e-commerce (Gefen 2000), recommendation agents (Komiak and Benbasat 2006) and software using speech (Lee 2010). The concept of situational normality is also readily observable in the context of cloud computing where cloud storage solutions integrate with other software on a user's personal computer to make the transition from personal to cloud storage as normal and un-noteworthy as possible.

A second heuristic influence on trust is aesthetics. This cue for trust relies on the halo effect which began as a concept in the social psychology literature to describe how immediately observable positive attributes such as physical attractiveness influence perceptions of other attributes. It has since been applied to the trust literature and used to explain everything from the outcomes of elections (Todorov et al. 2005) and new employees trust in organisations (Baer et al. 2018) to trust in websites (Cyr et al. 2010) and mobile commerce (Li and Yeh 2010). Regardless of the referent, the general principle of aesthetics cues is that other parties who are seen as aesthetically appealing are also likely to be seen as trustworthy, particularly in the early stages of a relationship.

Structural assurance is a cue for trust that is based less on a perception of the trust referent itself but more on a perception of the environment within which an interaction takes place. Kramer and Lewicki (2010) refer to this type of trust as rule based trust influenced by a perception that some form of checking or restraint in the environment will prevent another party from acting in a way that is not trustworthy. Again this concept, has proved useful in understanding trust in technology and evidence suggests that the effectiveness of regulatory and assurance systems can influence consumer trust in technology (e.g. Gefen and Pavlou 2006).

The final cue that has received attention in the literature also relates to the wider context of the trust relationship. Recent theory suggests that the immediate relational context plays a significant role in creating trust motivation or a desire to trust another party on the basis of the social function of the relationship (van der Werff et al. 2019a). In essence, if a technological artefact fulfils an important role for us in terms of depending on it to do something necessary, enjoying interacting with it or seeing it as being in line with our identity and personal values, we are more likely to trust it. Many relationships take place in a wider context or chain of interrelated parties. A growing body of evidence suggests that information about parties at another level in that chain can be used as a cue for trust (De Cremer et al. 2018; Lipponen et al. 2020) and that trust in one party can be transferred to referents at another level (Stewart 2003). It is likely in the technology context that information regarding other parties in a chain and the trust this information engenders can lead to trust in other parties.

1.3 Cloud Computing

Despite its ubiquity, cloud computing, as we know it today, is a recent phenomenon. It is hard to relate to the idea that when a company known for selling books online, Amazon, launched Amazon Web Services in 2006, it would help create a public cloud computing market worth nearly US$200 billion by 2019 (IDC 2019). In its most widely referenced definition, NIST define cloud computing as:

> *…model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.* (Mell and Grance, p. 2)

For the most part, the cloud model defined by Mell and Grance and the subsequent cloud reference architecture introduced by Liu et al. (2011) continue to be the basis of cloud computing industry. However, it would be wrong to say that cloud computing has not evolved. In particular, the emergence of the Internet of Things and Big Data, has led to the introduction and increasing adoption of a new service model, Function-as-a-Service, and two new computing paradigms, fog computing and edge computing (Lynn et al. 2017; Iorga et al. 2018). While further discussion is beyond the scope of this chapter, it is useful to be aware of these concepts and technology paradigms when considering trust and privacy issues, not only in this chapter but throughout the book. It is also important to note that these are not the only developments in cloud computing but the most influential at the time of writing. Table 1.1 below provides a brief definition of these some of the key concepts in cloud computing.

The essential characteristics of cloud computing, provide a wide range of benefits to businesses including increased infrastructure reliability and scalability (up and down), improved cashflow through reduced capital expenditure (CapEx) and operational expenditure (OpEx), as well providing competitive capabilities through increased agility, faster time-to-market, and new revenue streams (Lynn 2018). The induced effect for consumers is better quality of service and quality of experience, at lower or no financial cost. In the last two decades, advances in the coverage, speed, and reliability of global telecommunications networks has made the large

Table 1.1 Definitions of key concepts in cloud computing

Concept	*Cloud essential characteristics*	*Source*
On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with each cloud service provider.	Mell and Grance (2011)
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.	
Resource pooling	The cloud service provider's computing resources (e.g. storage, processing power, network bandwidth) are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.	
Rapid elasticity	Capabilities can be elastically provisioned and released, to scale rapidly outward and inward commensurate with demand.	
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.	
Cloud service models		
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure and accessible by a client interface.	Mell and Grance (2011)
Platform as a Service (PaaS)	The capability provided to a consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using development technologies provided by the provider.	Mell and Grance (2011)
Infrastructure as a Service (IaaS)	The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources to deploy and run arbitrary software.	Mell and Grance (2011)
Function as a Service (FaaS)	The capability provided to the consumer to execute lightweight, single purpose stateless functions that can be executed on demand, typically through an API, without consuming any resources until the point of execution.	Glikson et al. (2017) and Lynn (2018)

(*continued*)

Table 1.1 (continued)

Concept	*Cloud essential characteristics*	*Source*
Cloud deployment models		
Private cloud	Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.	Mell and Grance (2011)
Community cloud	Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.	Mell and Grance (2011)
Public cloud	Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider or their designated datacentre provider.	Mell and Grance (2011)
Hybrid cloud	Cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.	Mell and Grance (2011)
Related computing paradigms		
Fog computing	Fog computing is a layered model for enabling ubiquitous access to a shared continuum of scalable computing resources. The model facilitates the deployment of distributed, latency-aware applications and services, and consists of fog nodes (physical or virtual), residing between smart end-devices and centralized (cloud) services.	Iorga et al. (2018)

(*continued*)

Table 1.1 (continued)

Concept	*Cloud essential characteristics*	*Source*
Edge computing	Edge computing is the network layer encompassing the end devices and their users, to provide, for example, local computing capability on a sensor, metering or some other devices that are network-accessible.	Iorga et al. (2018)
Dew computing	Dew computing is an on-premises computer software-hardware organization paradigm in the cloud computing environment where the on-premises computer provides functionality that is independent of cloud services and is also collaborative with cloud services.	Wang (2016)
Mist computing	Mist computing is an optional lightweight and rudimentary form of computing power that resides directly within the network fabric at the edge of that fabric, the fog layer closest to the smart end-devices, using microcomputers and microcontrollers to feed into fog computing nodes and potentially onward towards the cloud computing services.	Iorga et al. (2018)

scale outsourcing of information systems a reality. Consequently, more and more organisations are migrating from on-premise infrastructure to the cloud to focus on their core capabilities and to exploit potential IT efficiencies and business agility offered by the cloud (Kim 2009).

1.4 Trust Barriers to Cloud Adoption

Cloud computing is a form of outsourcing where organisations, and indeed albeit at a smaller scale, consumers, outsource some or all of their IT infrastructure (hardware, software, networks etc.) to one or more cloud service providers (CSP) on a metered basis. In return for fees, the CSP agrees to provide access to the cloud service at agreed service levels, typically contained in a Service Level Agreement (SLA).

Like all outsourcing, the decision to adopt cloud computing involves organisations assuming four main risks—relational, performance, compliance and regulatory, technological risks. Relational risk typically involves

poor cooperation and opportunistic behaviour (Das and Teng 1996). As a by-product of both the on-demand nature of cloud computing and dominance of a relatively small number of hyperscale CSPs, standard form contracts are commonplace. Only the largest customers or those customers a CSP considers strategic, for example governments, have room to negotiate terms, or to develop a personal relationship with these providers. In the absence of a personal relationship, cloud computing relies largely on rule- or calculus-based trust, represented by these agreements. As will be discussed later in Chap. 2, not only do cloud computing contracts typically favour the service provider but cloud customers can find themselves locked-in from a technical perspective and dependent on the CSP for business continuity with important implications for trust.

Historically, performance risk has been the primary concern with cloud computing as evidenced by the focus of industry and scholars on service levels and SLAs. Clearly, availability and access are critical if one outsources IT infrastructure to the cloud. This is often further complicated by uncertainty related to the functioning of the cloud services, transparency on how service levels are calculated and of the underlying cloud systems and associated system data, and exceptions included in cloud contracts. Again, given the disparity in dependence and impact in the vendor-customer relationship, the risk of failure is significantly higher on the part of the customer.

The third risk, compliance and regulatory risk is where a customer fails to adhere to regulatory standards due to the provider's errors (Anderson et al. 2014). Increasingly but not exclusively, the primary barriers to cloud adoption, by organisations and consumers alike, relate to data, and more specifically the location, integrity, portability, security and privacy of data (Lynn et al. 2014; Leimbach et al. 2014; Eurostat 2016). Cloud computing is a largely location-independent technology and is built on a chain of service provision which is largely opaque to the customer. Data may be stored, processed, and transported across borders, and/or come in to contact with a wide range of partners, without the knowledge of the customer. Furthermore, CSPs, no matter what size are not immune from security vulnerabilities. Each service model, deployment model, and architecture, and combination and configuration thereof has its own discrete set of security issues. For SaaS models alone, Subashini and Kavitha (2011) identify 14 security elements that need to be considered independently of the PaaS and IaaS infrastructure upon which these are situated. At and within each layer, different parties may be responsible and accountable for

the security of different elements. This is particularly pertinent in the context of data protection laws, such as the General Data Protection Regulation (GDPR), where misuse or mismanagement of data can result in significant fines and penalties, independent of the loss of reputation, and potential loss of corporate value associated with data and other security breaches (Goel and Shawky 2009).

Against this backdrop and in the absence of a personal relationship or knowledge, prospective customers and users of the cloud are faced with a relatively stark choice: To stay or go. The former involves assuming the risk laid out, relying on the contracts provided, and the competence, benevolence, and integrity of the CSP, while mitigating risks by other means, if possible or desirable. The alternative is to forego the benefits of the cloud altogether.

1.5 Existing Approaches to Overcoming Trust Barriers to Cloud Adoption

In addition to contracts, a variety of trust-building mechanisms have been proposed by policymakers, industry, and scholars. These include regulation, standardization, certification, communication, and technological innovation. For over a decade, the European Commission has sought to mitigate the impact of the risks outlined above through the activities leading to and from the 2012 European Cloud Strategy (European Commission 2012) and subsequent initiatives including the new European digital strategy, Shaping Europe's Digital Future (European Commission 2020). In addition to the GDPR, consumer protection regulations are in place to protect them from behaviour and contracts prejudicial to their consumer rights (see Chap. 2). Similarly, there have been numerous efforts to support standards not only for cloud system interoperability and data portability, but also for SLAs (see for example C-SIG-SLA 2014), however these are not mandatory. More recently, there has been a renewed focus on certification as a means of assurance.

Assurance involves expert practitioners evaluating an CSP against agreed criteria to improve the degree of confidence of intended users. In effect, this involves a cloud service provider redesigning their security and management processes to meet the requirements of a certification scheme, and then being audited by an independent third party to assess compliance periodically (Tecnalia 2016). This approach provides an opportunity for

rule-based trust to develop and, in situations where the providers of the certification are trusted, the potential for trust transfer to occur. In a report for the European Commission published in 2018, Tecnalia identified over 20 such schemes, the most popular being compliance with ISO 27001; others included CSA Star, PCI-DSS, ENISA-CCM and the SOC (ISAE-3402) (Tecnalia 2016). A major limitation of the certification approach is the timeliness and the depth of the audit. In-depth audits may only take place every three years with light-touch reviews annually. Similarly, given the complexity of cloud computing, the level of detail that a certification or an auditor can go to is limited.

Three common methods are used to communicate trust in CSPs—website design, feedback mechanisms, and third party endorsements (Lynn et al. 2016). There is a substantial body of literature on the direct and indirect impact of visual website appearance on trust including colour choice and design symmetry which represent powerful heuristic cues for trust. However, aesthetic preferences in website design tend to vary across demographic characteristics and thus may have limited practical utility for CSPs trying to communicate trust (Cyr et al. 2010; Tuch et al. 2010). Feedback mechanisms or reputation systems are an increasingly popular alternative mechanism for communicating trust. As cloud and API marketplaces have emerged, such as Salesforce AppExchange, Microsoft Azure Marketplace and RapidAPI, so too have market-driven feedback systems within these marketplaces. Ratings, reviews, and vendor ecosystem status all act as a signal to consumers that the vendor has an incentive to behave in an appropriate manner and that they have been informally certified by previous consumers (Pavlou and Gefen 2004). Again, these mechanisms are likely to impact trust by providing a level of structural assurance and cues regarding the rules governing trustworthy behaviour. Independently of the cloud sector, a plethora of general reputation and review systems, such as Feefo and Trust Pilot, have emerged in recent years that seek to provide prospective customers, both business-to-business (B2B) and business-to-consumer (B2C), with similar signals on an independent basis by aggregating ratings, surveys and reviews (Banerjee et al. 2020). Increasingly, these are integrated not only in to a vendor's website but into search engine ranking algorithms, providing additional incentives for vendors to behave. Notwithstanding their widespread and increasing use, feedback and reputation systems have been criticised for their vulnerability to false, manipulated or biased feedback (Sabater and Sierra 2005).

A third approach to communicating trust in CSPs involves the use of assurance seals or trustmarks that combine certification and communication to dispel consumer concerns about risk and communicate adherence with best practice, a code of conduct, or certification scheme using a third-party mark or symbol (Aiken and Boush 2006). Like certification, trustmark holders are typically subject to periodic third party verification. However, in addition to recognition and lack of information depth, trustmarks suffer from the same limitations as certification in general. They have been criticised for reliance on human intervention, limited scope, timeliness, lacking warranties, and subject to co-optation risk (Aiken et al. 2003).

Technological innovation to build trust in cloud computing largely revolves around designing clouds that meet the three pillars of trustworthy computing—security and privacy, reliability, and business integrity (Mundie et al. 2002). Chapter 7 discusses this topic in detail. It is important to note, however, that technical innovation in trustworthy computing overwhelmingly focuses on the first two pillars, security and privacy, and reliability. Research on the former focuses on the provision of effective attack resilient systems, typically using encryption techniques of increasing strength and complexity. Reliability research focuses on the design, monitoring, and measurement of highly reliable systems. Both domains are largely hidden from end-users. Business integrity is more nuanced and suffers from a lack of inter-disciplinary research. As such, it focuses largely on monitoring key service level metrics and ranking services based on this data. One of the main limitations of purely technological approaches, is that by and large, customers are human. Their decisions to trust are based on a vast array of conscious and subconscious signals that are often forgotten about in purely technological approaches and solutions.

In attempt to address this gap and marry the various approaches to mitigating trust issues in cloud computing, we have previously proposed an active dynamic online trust label (Lynn et al. 2014; Lynn et al. 2016; Emeakaroha et al. 2016; van der Werff et al. 2019b). Inspired by nutritional labels, these labels present consumers with corporate information, policies, and historic and near real-time service level metrics based on data from CSP monitoring systems (Emeakaroha et al. 2016). The system can allow for third party independent certification and could allow for corporate attestation using digital signatures. Based on an experimental study with 227 business decision makers, the proposed cloud trust label communicated trustworthiness effectively (van der Werff et al. 2019b). While these results are promising, such a system requires widespread support to be effective. Until then, it remains an academic exercise.

1.6 Assurance and Accountability Framework

In general, mechanisms to build trust in cloud computing fall in to two main categories—assurance and accountability. Standards, certification, and communication strategies seek to assure the consumers by providing cues of CSP competence, integrity, and benevolence, and to some extent consistency. Regulation and contractual mechanisms seek to hold CSPs accountable in the event of a trust violation. A key problem is that these initiatives are currently highly fragmented, with multiple initiatives by as many stakeholders, but no particular comprehensive, coordinated, and holistic framework of activity that provides direction for policy makers, users, cloud service providers, and indeed researchers.

Figure 1.1 below presents an integrated multi-stakeholder framework for assurance and accountability for cloud-based trust building. It extends the chain of accountability concept first proposed by Pearson and Wainwright (2013) to provide transparency and clarity on liability in the event of a data breach in the cloud. While Pearson and Wainwright (2013) envisaged a set of mechanisms for mitigating risk (preventative controls), monitoring and identifying risk and policy violations (detective controls), and providing redress (corrective controls), their approach is largely built on calculative trust-based model whereby accountability is both quantitative and absolute. The goal is to eliminate distrust or mitigate the negative impact of a trust violation. In effect, it is an *ab initio* pre-emptive trust repair approach.

In contrast, we propose, a more positive approach couched in theories of trust building and repair. The focus is on trust building mechanisms; trust repair mechanisms only initiate when a trust violation occurs. Based on our work in Lynn et al. (2014), we suggest that cloud consumers should have control of their data, how it is used, where it is used, and who should use it, and this should be auditable by all involved. They should have a say, if they want it, but as a default standard declarations should be weighed towards the best interests of the consumer, and neither prejudicial to consumer rights, nor contrary to government policy. As such, we propose that in addition to preventative controls, there are declarative controls where all parties can declare their policies and expectations irrespective of contracts or policies which seek to circumvent local laws and regulation. Furthermore, there are confirmative controls that report and alert stakeholders that these policies and expectations are being met. In this way, trust is not only being built on the basis on rules and transactions, but proactive mechanisms are in place so that knowledge-based

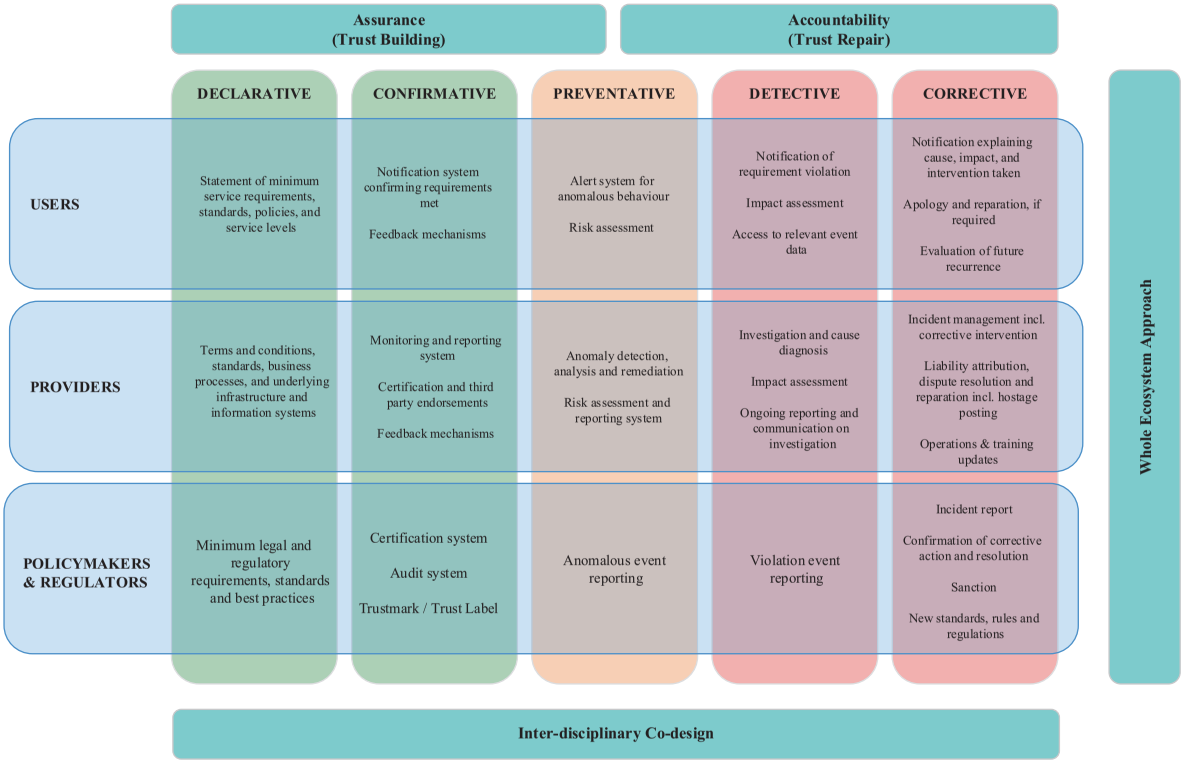

Fig. 1.1 An integrated multi-stakeholder framework for building and repairing trust in cloud computing based on assurance and accountability

trust is being built between all stakeholders. These two assurance based controls are necessities. Accountability mechanisms are contingent; they only come in to effect when a trust violation occurs. Furthermore, when initiated, these mechanisms are not mere objective features of the system but recognise the psychological impact of trust violation and largely follow accepted theory for repairing trust including immediate response, diagnosis, intervention performance, and evaluation (Gillespie and Dietz 2009). Specifically, the framework includes actions that are effective for repairing violations of different types of trust, whether competence-, benevolence- or integrity-based. The framework is technology-agnostic and in this way, can not only accommodate technological solutions to building and repairing trust, but new use cases and evolutions of cloud computing including the Internet of Things.

By recognising that policymakers and regulators, users and providers, have different priorities and perceptions of what trust means in the context of cloud computing, all stakeholders start on the basis of building trust rather than waiting for that trust to be violated. Ultimately, this should lead to greater understanding of the needs of different stakeholders, longer and deeper relationships, and innovation so that when a violation does occur, and it will, the relationship will be strong enough to survive.

1.7 Conclusions

This chapter introduces trust, cloud computing, and discusses some of the issues that present challenges to building trust in cloud computing, and wider and deeper adoption thereof. While there has been extensive work done to mitigate relational, performance, and compliance and regulatory risks, these initiatives are highly fragmented and lack cohesion. They are based on a conceptualisation of trust portrayed as an objective feature of cloud computing technology rather than either policymaker or user perceptions of trust. We suggest that all stakeholders in the cloud computing ecosystem need to come together and focus on how to build trust rather than focusing on what to do when there is a violation of trust, a reposition to assurance first, then accountability only when needed. To this end, we reiterate the need for an integrated multi-stakeholder approach to assurance and accountability, and related inter-disciplinary research to support the adoption of such approaches.

References

Aiken, D., Osland, G., Liu, B., & Mackoy, R. (2003). Developing Internet Consumer Trust: Exploring Trustmarks as Third-Party Signals. *Marketing Theory and Applications, 14*, 145–146.

Aiken, K. D., & Boush, D. M. (2006). Trustmarks, Objective-Source Ratings, and Implied Investments in Advertising: Investigating Online Trust and the Context-Specific Nature of Internet Signals. *Journal of the Academy of Marketing Science, 34*(3), 308–323.

Anderson, S. W., Christ, M. H., Dekker, H. C., & Sedatole, K. L. (2014). The Use of Management Controls to Mitigate Risk in Strategic Alliances: Field and Survey Evidence. *Journal of Management Accounting Research, 26*(1), 1–32.

Baer, M., & Colquitt, J. A. (2018). Moving Toward a More Comprehensive Consideration of the Antecedents of Trust. In R. H. Searle, A. M. Neinaber, & S. B. Sitkin (Eds.), *Routledge Companion to Trust* (pp. 163–182). Abingdon: Routledge.

Baer, M. D., Van Der Werff, L., Colquitt, J. A., Rodell, J. B., Zipay, K. P., & Buckley, F. (2018). Trusting the "Look and Feel": Situational Normality, Situational Aesthetics, and the Perceived Trustworthiness of Organizations. *Academy of Management Journal, 61*(5), 1718–1740.

Banerjee, A., Ries, J. M., & Wiertz, C. (2020). The Impact of Social Media Signals on Supplier Selection: Insights from Two Experiments. *International Journal of Operations & Production Management*. https://doi.org/10.1108/IJOPM-05-2019-0413.

C-SIG-SLA. (2014). Cloud Service Level Agreement Standardisation Guidelines. Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=6138

Cyr, D., Head, M., & Larios, H. (2010). Colour Appeal in Website Design Within and Across Cultures: A Multi-method Evaluation. *International Journal of Human-Computer Studies, 68*(1), 1–21.

Das, T. K., & Teng, B. S. (1996). Risk Types and Inter-firm Alliance Structures. *Journal of Management Studies, 33*(6), 827–843.

De Cremer, D., Van Dijke, M., Schminke, M., De Schutter, L., & Stouten, J. (2018). The Trickle-Down Effects of Perceived Trustworthiness on Subordinate Performance. *Journal of Applied Psychology, 103*(12), 1335.

Emeakaroha, V. C., Fatema, K., van der Werff, L., Healy, P., Lynn, T., & Morrison, J. P. (2016). A Trust Label System for Communicating Trust in Cloud Services. *IEEE Transactions on Services Computing, 10*(5), 689–700.

European Commission. (2012). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.* Unleashing the Potential of Cloud Computing in Europe. COM(2012) 529 Final.

European Commission. (2020). Shaping Europe's Digital Future. Retrieved from https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

Eurostat. (2016). Archive: Cloud Computing—Statistics on the Use by Enterprises—2016 Data. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Cloud_computing_-_statistics_on_the_use_by_enterprises_-_2016_data

Gefen, D. (2000). E-commerce: The Role of Familiarity and Trust. *Omega, 28*(6), 725–737.

Gefen, D., & Pavlou, P. (2006). The Moderating Role of Perceived Regulatory Effectiveness of Online Marketplaces on the Role of Trust and Risk on Transaction Intentions. *ICIS 2006 Proceedings*, 81.

Gillespie, N., & Dietz, G. (2009). Trust Repair After an Organization-Level Failure. *Academy of Management Review, 34*(1), 127–145.

Glikson, A., Nastic, S., & Dustdar, S. (2017, May). *Deviceless Edge Computing: Extending Serverless Computing to the Edge of the Network*. Proceedings of the 10th ACM International Systems and Storage Conference, pp. 1-1.

Goel, S., & Shawky, H. A. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management, 46*(7), 404–410.

IDC. (2019). *Worldwide Public Cloud Services Spending Guide*. Framingham, MA: IDC.

Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N. S., & Mahmoudi, C. (2018). *Fog Computing Conceptual Model*. (No. Special Publication (NIST SP)-500-325).

Kim, W. (2009). Cloud Computing: Today and Tomorrow. *Journal of Object Technology, 8*(1), 65–72.

Komiak, S. Y., & Benbasat, I. (2006). The Effects of Personalization and Familiarity on Trust and Adoption of Recommendation Agents. *MIS Quarterly*, 941–960.

Kramer, R. M., & Lewicki, R. J. (2010). Repairing and Enhancing Trust: Approaches to Reducing Organizational Trust Deficits. *Academy of Management Annals, 4*(1), 245–277.

Lee, E. J. (2010). The More Humanlike, the Better? How Speech Type and Users' Cognitive Style Affect Social Responses to Computers. *Computers in Human Behavior, 26*(4), 665–672.

Leimbach, T., Hallinan, D., Bachlechner, D., Weber, A., Jaglo, M., Hennen, L., Nielsen, R. O., Nentwich, M., Strauss, S., Lynn, T., & Hunt, G. (2014). *Potential and Impacts of Cloud Computing Services and Social Network Websites*. Publication of Science and Technology Options Assessment.

Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces, 63*(4), 967–985.

Li, Y. M., & Yeh, Y. S. (2010). Increasing Trust in Mobile Commerce Through Design Aesthetics. *Computers in Human Behavior, 26*(4), 673–684.

Lipponen, J., Kaltiainen, J., van der Werff, L., & Steffens, N. K. (2020). Merger-Specific Trust Cues in the Development of Trust in New Supervisors During an

Organizational Merger: A Naturally Occurring Quasi-Experiment. *The Leadership Quarterly, 31*(4), 101365.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture. *NIST Special Publication, 500*, 292.

Lynn, T. (2018). Addressing the Complexity of HPC in the Cloud: Emergence, Self-Organisation, Self-Management, and the Separation of Concerns. In *Heterogeneity, High Performance Computing, Self-Organization and the Cloud* (pp. 1–30). Cham: Palgrave Macmillan.

Lynn, T., Healy, P., McClatchey, R., Morrison, J., Pahl, C., & Lee, B. (2014). The Case for Cloud Service Trustmarks and Assurance-as-a-Service. preprint arXiv:1402.5770.

Lynn, T., Rosati, P., Lejeune, A., & Emeakaroha, V. (2017, December). *A Preliminary Review of Enterprise Serverless Cloud Computing (Function-as-a-Service) Platforms.* 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 162–169). IEEE.

Lynn, T., Van Der Werff, L., Hunt, G., & Healy, P. (2016). Development of a Cloud Trust Label: A Delphi Approach. *Journal of Computer Information Systems, 56*(3), 185–193.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review, 20*(3), 709–734.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a Specific Technology: An Investigation of Its Components and Measures. *ACM Transactions on Management Information Systems (TMIS), 2*(2), 12.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *Academy of Management Review, 23*(3), 473–490.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Draft). *NIST Special Publication, 800*, 145.

Mundie, C., de Vries, P., Haynes, P., & Corwine, M. (2002). Trustworthy Computing-Microsoft White Paper. Microsoft Corporation, October.

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-based Trust. *Information Systems Research, 15*(1), 37–59.

Pearson, S., & Wainwright, N. (2013). An Interdisciplinary Approach to Accountability for Future Internet Service Provision. *International Journal of Trust Management in Computing and Communications, 1*(1), 52–72.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review, 23*(3), 393–404.

Sabater, J., & Sierra, C. (2005). Review on Computational Trust and Reputation Models. *Artificial Intelligence Review, 24*(1), 33–60.

Shank, D. B., & DeSanti, A. (2018). Attributions of Morality and Mind to Artificial Intelligence after Real-World Moral Violations. *Computers in Human Behavior, 86*, 401–411.

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why Different Trust Relationships Matter for Information Systems Users. *European Journal of Information Systems, 25*(3), 274–287.

Stewart, K. J. (2003). Trust Transfer on the World Wide Web. *Organization Science, 14*(1), 5–17.

Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications, 34*(1), 1–11.

Tecnalia. (2016). Certification Schemes for Cloud Computing. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/3df22a89-1238-11e9-81b4-01aa75ed71a1/language-en

Todorov, A., Mandisodza, A. N., Goren, A., & Hall, C. C. (2005). Inferences of Competence from Faces Predict Election Outcomes. *Science, 308*(5728), 1623–1626.

Tuch, A. N., Bargas-Avila, J. A., & Opwis, K. (2010). Symmetry and Aesthetics in Website Design: It's a Man's Business. *Computers in Human Behavior, 26*(6), 1831–1837.

van der Werff, L., Legood, A., Buckley, F., Weibel, A., & de Cremer, D. (2019a). Trust Motivation: The Self-Regulatory Processes Underlying Trust Decisions. *Organizational Psychology Review, 9*(2-3), 99–123.

van der Werff, L., Fox, G., Masevic, I., Emeakaroha, V. C., Morrison, J. P., & Lynn, T. (2019b). Building Consumer Trust in the Cloud: An Experimental Analysis of the Cloud Trust Label Approach. *Journal of Cloud Computing, 8*(1), 6.

van der Werff, L., Real, C., & Lynn, T. (2018). Individual Trust and the Internet. In R. H. Searle, A. M. I. Nienaber, & S. B. Sitkin (Eds.), *The Routledge Companion to Trust* (pp. 391–407). Abingdon: Routledge.

Wang, Y. (2016). Definition and Categorization of Dew Computing. *Open Journal of Cloud Computing (OJCC), 3*(1), 1–7.