An Institutional Trust Perspective of Cloud Adoption Among SMEs in South Africa

Kenneth Ayong(✉) and Rennie Naidoo(✉)

University of Pretoria, Private Bag X20 Hatfield, Pretoria 0028, South Africa
ayongkenneth@gmail.com, rennie.naidoo@up.ac.za

Abstract. The purpose of this paper is to identify the major institutional trust mechanisms that facilitate the adoption of cloud services among South African SMEs. By drawing from Giddens' (1990) institutional trust theory and the existing IT trust literature, we developed a conceptual model to improve our understanding of the role of institutional trust between SMEs and cloud service providers. The model was also deployed as a sensitizing framework to deepen our understanding of how institutional trust factors influence SME cloud service adoption decisions. A qualitative field study based on 12 semi-structured interviews of SMEs and cloud service providers in South Africa suggests that the insights gleaned from concepts, such as *design faults* and *operator failure,* can be translated into useful policy guidelines for cloud service providers, state institutions and regulatory bodies that are working to improve the trustworthiness of the cloud ecosystem. Despite the belief held by experts that there is a need to strengthen institutional mechanisms in the cloud ecosystem, the relative advantage of cloud over alternative technology remains the primary motivational factor of SME adoption. The SMEs in this study were unaware of the risks involved in cloud adoption and are content to mimic the behavior of their peers when adopting cloud services. Other social actors in society will have to play a prominent role in evaluating and strengthening institutional trust in the cloud ecosystem.

Keywords: SME · Adoption · Cloud services · Institutional trust · Abstract systems · Relative advantage

1 Introduction

The South African Government considers SMEs to be a critical element for economic growth and a main source of employment [1]. In South Africa, SMEs make up about 56% of the private sector and contribute about 36% to the gross domestic product [2]. Information technology plays a crucial role in the survival and growth of SMEs. Cloud computing is a mechanism of delivering Information Technology (IT) services either as a software, platform or infrastructure through the internet. In this study, cloud computing is defined as information technology services delivered through the Internet to enable business processes. Like traditional utilities, these services are deployed as an on-demand and pay-as-you-use method, making it an attractive investment for an SME because it allows them to focus their efforts on their core business functions [3]

H. Venter et al. (Eds.): ISSA 2019, CCIS 1166, pp. 145–157, 2020.
https://doi.org/10.1007/978-3-030-43276-8_11

The slow rate of adoption among developing countries has been confirmed by the IDC (IDC, 2013) when compared to developed economies, such as Denmark (38%) and Finland (51%) [4, 5].

Despite cloud technologies providing benefits such as cost savings, flexibility, and, increased collaboration, it also has a number of challenges such as security concerns, data ownership concerns, lock-in, service availability, and the requirement for enforceable regulations [6]. The fact that many developing economies have weak institutional mechanisms to regulate the cloud service provisioning environment compared to developed economies provides an important explanation for this lagging adoption rate [7]. Examples of strong institutional instruments include the GDPR privacy regulation that protects European citizens' personal data anywhere in the cloud as well as the Patriot Act of the USA.

Though a substantial increase in scholarly research on the role of trust in inter-organisational transactions, such as cloud service transactions, has been recorded in recent years, these studies have been found to be highly disjointed [8]. Trust has appeared to be a dominant theme in understanding the relationships between organisations thus stressing the need to develop a deeper understanding of the nature of this construct [9]. Trust is emerging from various studies as a mechanism that organisations use to deal with uncertain relationships [10, 11].

Most trust literature has focused on the processes of trust building between individuals [12] and organisations as well as inter-organisations [13]. There has been a preference by researchers to focus on individual trust rather than structural trust [14]. This leaves a gap in understanding the role of institutional structures and mechanisms in these relationships, especially in instances where one party has more power than the other. For example, the cloud service provider generally has more power than the SME cloud user. Hence the study of institutional trust is important in these types of relationship.

This study focuses on the institutional mechanisms that facilitate trust between organisations, where one party has more knowledge and power than the other. The purpose of this article is to develop a conceptual framework that can improve our understanding of the role of institutional trust in cloud adoption among SMEs. This study explores the following research question: *What are the institutional trust factors that facilitate the adoption of cloud computing among South African SMEs?*

The rest of this paper is organised as follows. First, we provide a brief literature review of inter-organisational trust, cloud security risks and institutional trust theories as the foundation of the conceptual model. Then we present the conceptual model. The research methodology is described, then the data collection process and analysis results are reported. We then argue, using semi structured interviews, that trust in the cloud ecosystem mediates the path between privacy and security risks towards its adoption. We further discuss key findings, theoretical and practical implications. The study concludes with a few suggestions for future research work on institutional trust in cloud computing.

2 Conceptual Foundations

Trust is arguably one of the most important social phenomena in cloud computing. Many scholars maintain that trust is necessary for understanding new technology adoption decisions and economic exchanges [15]. Empirical literature suggests that trust has a favourable impact on consumer purchase intentions [16]. According to Gefen, [17] trust is a contributory factor in the adoption of Internet technologies. According to Morgan and Hunt [18], creating and maintaining trust in technology interface services, such as cloud computing, will attract new customers and maintain existing ones.

Bachmann, [19] explains that trust requires accepting dependency, reliability, and a relationship with another that can create an outcome that is otherwise not available. SME decision makers, due to their lack of technical knowledge and resources, assume that most privacy and security risks have been assured by the institutional mechanisms within the cloud ecosystem. Hence, in instances where these mechanisms are perceived to be weak, adoption rates will be slow compared to environments where they are strong.

Giddens' theory of structuration and modernity was chosen to develop theoretical insights about the role of institutional trust in cloud computing adoption among SMEs (See Table 1). We adopt Giddens' [20] insights on the crisis of trust in the contemporary society. In the process of the transformation from tradition to modernity, the trust issue has become increasingly significant both in day-to-day experiences and in theory. Giddens' account of trust recognises the transformation from traditional to modern systems. Modern systems are becoming increasingly complex for the end-user to understand, thus creating more uneasiness and anxiety. On the other hand, trust helps to create a sense of certainty about modern systems.

Table 1. A Giddens conception of institutional trust

Concept	Description	Example in cloud computing
Abstract capacity	Trust is based upon a vague and partial understanding of a system	The customer has confidence in the vendor's ability despite the remoteness of the vendor
Expert system	Technical systems that organise the social environments in which we live	Cloud-Based Expert System (CBES) model for decision making in various facets of modern society assisting cloud customers in areas such as health, transport, education, analytics, robotics and artificial intelligence
Structure	Structure refers to resources and guidelines for social practices and fulfilling the demands of users	The limited resources of SMEs to meet their business objectives requires them to adopt cloud computing due to the competitive global nature of business influencing their decisions

(*continued*)

Table 1. (*continued*)

Concept	Description	Example in cloud computing
Agency	This refers to human actors whom through their knowledge and capability of doing things use their cognitive skills [21]	Cloud computing service providers use their skills to facilitate business processes through technology on behalf of cloud users to achieve their business goals
Time-Space distanciation	This means that social actors can act without being physically present in the situation	Cloud users can establish a relationship with the cloud service provider and start transacting without a physical presence, even when the two parties are at different geographical locations
Ontological security	Identifying the validity of values incorporated in an institution and the assumption that this modern life makes satisfactory sense to a high number of people to motivate their ongoing active support for the institution and the compliance with its rules	The confidence that most cloud users have in the continuity of their existence and constant reliance on surrounding technological changing environments
Facework commitments	Personal trust is considered to facework commitment where there is mutual and an intimate personal relationship	When cloud service providers sell their products through presentations to gain trust and understand the specific needs of the users. Most cloud providers don't have a personal relationship with the users
Faceless commitments	Trust in expert system where ignorance and dependency drives trust	The more ignorant cloud users can depend on expert systems, such as a cloud technology that does not fail, the more they trust it. Just like users trust Google and the internet today
Design faults	The design of abstract systems may lead to malfunction and not meet the consumers' expectations, leading the consumer to deviate away from their projected benefits	Cloud technology is designed to be robust, secure and prevent human error but due to bad design the service is sometimes out of service, vulnerable to hackers, etc.
Operational failures	Abstract systems are operated upon by humans and humans can make mistakes or errors leading these systems to fail to meet the consumers' expected benefits. This is possible despite the quality of the design of such a system	Cloud technology, as a form of expert systems, is operated upon by the cloud service provider's technical resources who can make mistakes or errors leading to SMEs consuming these services to not achieve the expected benefits

Giddens' definition of trust considers the capacity of dealing with a lack of knowledge when he states that trust is "made based on a "leap into faith" which brackets ignorance or lack of information" [21]. Trust is inherently risky, and a trusting decision is a leap of faith [14]. There are two types of trust to be considered, traditional and institutional trust [22]. When organisations consider their experiences and the protection from institutions, trust is gained quicker [22]. According to Giddens [20], trusted expert systems adopted by social actors can be described as abstract systems. For example, the judicial, banking systems and air traffic control systems which have a combination of technical mechanisms, procedures, professional expertise and other structures enable them to function effectively and thus to be trusted.

Cloud technology is a combination of technical mechanisms (physical servers, applications, operating systems), procedures (service access procedures), and professional expertise (cloud brokers, cloud architects). SMEs adopt this technology with confidence in the absence of technical knowledge of how they function and no contact with its structures Using the air traffic control system as an analogy, the SME owner is similar to the traveler who is unaware of the air traffic control system (expert system). The traveler does not understand how this system functions but trusts that they will travel to their destination safely. Similarly, the SME owner focuses on the core needs of their business while relying on the cloud technology partner to perform as promised. Gollmann [23] supports this notion that users trust in complex technologies emerges through experience and not necessarily through understanding.

Social actors trust these abstract systems and act with confidence in the absence of personal technical knowledge of how these systems function and without contact with its structures but continue to use them without the detailed knowledge of how they work. Similarly cloud computing as a new technology, allows users to consume it through the internet without knowledge of how it works, hence it can be categorised as a modern abstract expert system

According to Giddens [20], abstract systems can prevent users from achieving their goals since they do not control these systems and cannot fully predict its future behaviour. The two factors, according to Giddens [20], that lead to the unpredictability or erratic character of abstract systems is *design fault* and *operation failure*. Following Giddens [20], an SME cloud user adopts an abstract system, such as cloud technology based on the following:

- *Faceless* commitments with the cloud vendor
- No *personal* trust relations with the cloud vendor
- Without the *physical co-presence* of cloud provider
- Confidence in the continuity of cloud services as a social practice

These risky features of abstract systems are sustained by high levels of trust, and more importantly institutional trust. The complexity of cloud technology requires its design to be embedded with robust mechanisms to prevent failures that will compromise the objectives of the user. If these embedded designs are not implemented into the technology as expected by the customer, there is a risk of design faults which creates various risks to the customer, such as security risks. We highlight a few security risks that arise because of failures in the design of this complex technology. Table 2 below highlights what the cloud service provider can do to prevent security vulnerabilities by better embedded designs.

Operational failures refer to the failure of abstract systems due to human error. This is possible despite the quality of the design of such a system. The better the design of these abstract systems the lower the possibility of operational failures. Cloud users do not have sufficient knowledge to assess the design quality of the cloud technology they seek to adopt, neither do they have contact with those operating on these systems.

Table 2. Security risks as a result of failure in design of cloud technology

Security risk	Vulnerability	Mitigation by CSP in technology design
Brute force attacks Dictionary attacks	Weak password policy Weak encryption or authentication	CSP implements password policy in the technology design that is consistent with industry standards such as 27001, CoBIT
Management interface compromise	Remote access System or OS vulnerabilities	CSP embed security designs to prevent penetration of systems
Data loss or Manipulation	Loss of physical control of the data and poor integrity or backup controls	Backup procedures defined, and how long data is kept
Cross - VM attack	Multi-tenancy	Media Access Control (MAC) spoofing, Address Resolution Protocol (ARP) should be protected
Denial of Service	Inadequate resource filtering Weak policies for resource capping	Controls are implemented to manage external and internal attacks, such as distributed denial of service

Cloud technology is a complex system which is operated and maintained by the provider on behalf of the customer. Though the customer has confidence that these operators are technical experts and professionals, they are just humans who can make mistakes and errors during the process. If the technology is not robustly designed, it is more prone to errors or if the operators are not well trained, they are prone to mistakes. We have listed in Table 3 below the risks that arise in instances of cloud providers'' operators making mistakes that create operational failures. The power imbalance between the cloud consumer and cloud service provider also add to the possible failures of these abstract systems. Wherever there is human intervention, Giddens claims that there will be unintended consequences beyond the control of the user, especially when there is an imbalance of power and technical knowledge of these systems. Governments have the monopoly power to make and enforce laws that regulate the cloud universe in the interest of all its consumers including SMEs. Giddens' defines trust as "confidence in the reliability of a person or system", regarding a given set of outcomes or events, where that confidence expresses a faith in the probity, or in the correctness of abstract principles "technical knowledge" [20, p. 33].

From this definition of trust by Giddens, we can extend this to the relationship between the SME cloud service adopter or prospective adopter's confidence in the cloud system with the belief that the relationship will yield the desired benefits and trusts the correctness of the abstract principles surrounding the cloud ecosystem. This trust in the abstract principles is also based on the belief that there are institutional

mechanisms in place protecting its interests. The conceptual model is based on this definition of trust and the role of institutional mechanisms in mitigating the risks surrounding the relationship between an SME cloud adoptor and the cloud provider.

Table 3. Security vulnerabilities of cloud technology

Security risk	Vulnerability	Mitigation by CSP in operating cloud technology
Service compromise	Hypervisor vulnerabilities Lack of resource isolation	CSP can isolate multitenant applications and data to mitigate cloud services from being compromised
Insider treat	Weak encryption or authentication Insiders on the provider side	Due diligence mechanisms in place for hiring employees with access to sensitive customer data and administrative rights
Physical threats due to theft or vandalism	Unreachable data storage location Weak physical security measures	Background checks done on cloud provider employees with physical access to cloud facilities done
Man-in-the-Middle data leakage	Communication encryption vulnerabilities Weak authentication mechanism	Customer VMs encrypted to prevent vulnerability
Cookie manipulation	Lack of hashes to protect the cookie	Cloud service provider to enforce code of ethics for employees
Fraudulent resource consumption	Exploitation of the Cloud Pricing Model	Cloud service provider to enforce code of ethics for employees on how long security logs are retained and who has access to such logs
Non-compliance poor Governance	Unclear roles and responsibilities and Lack of standard technologies and solutions	Employees must be certified and accredited with industry bodies

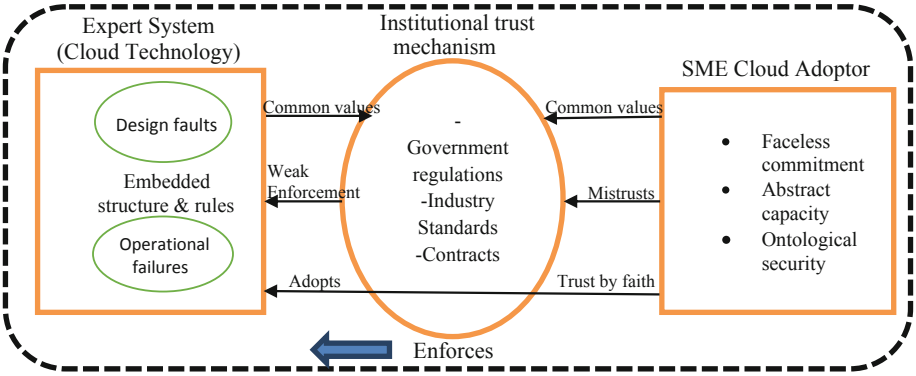

Fig. 1. An institutional-trust model of Cloud Adoption

The proposed research model and propositions are shown in Fig. 1. The characteristics of an SME cloud adopter as per Fig. 1 identifies faceless commitment towards the cloud service provider, since the SME does not have the technical knowledge to assess the design quality of the cloud technology and an ontological security for survival in the modern global economy for the SME. These characteristics of the SME within the South African economy slows adoption because the institutional trust mechanisms expected to be put in place by government and industry bodies are weak or unenforceable.

The cloud user will trust that a cloud service provider has the required expertise to embed the necessary structures and rules in place to prevent design faults, thereby ensuring reliable service [24]. Both the cloud service provider and the cloud user have common values which are the laws governing cloud technology provision, the industry standards and contracts signed between the parties. Though these values are known, the SME cloud user does not trust government institutions to enforce these values. Cloud consumers nevertheless trust this technology for its existence and the fact that its complexity expects the provider to have the required expertise to embed the necessary structures and rules within its design and operations to minimize or eliminate failures. Trust is required for SME ontological security and for the continuity of their existence, they therefore must rely on new technological changing environments [25]. Similarly, [26] suggest that inter-organisational trust is a fundamental factor in enabling and maintaining economic transactions between organisations.

Institutional trust factors such as government regulations, contracts and standards are important trust mechanisms in creating trust in impersonal or faceless economic environments where there is no sense common values [27, 28]. Guarantees and safety nets such as state laws, certifications and SLAs and other performance structures embody institutional trust and assure the trustor that the relationship can be trusted [29]. The common values and beliefs about the behaviour and goals of trusting parties increase the trust between them [18, 30]. The SME cloud user believes that the cloud service provider will work in their interest since they have a reputation to keep and as a legal business will respect the laws of the state. SMEs do not have the resources required to manage cloud service providers if there are service performance issues and hence put their trust in the institutions such as regulatory bodies and the judicial system to protect them [31].

McKnight and Chervany [15] define institution-trust as a key component of Internet transactions, such as cloud services transactions, and classify institutional trust into situational normality in situations where success is probable in normal situations and structural assurances where success is probable due to regulations, guarantees and legal contracts in place [15].

Other studies support this position, such as studies on ecommerce transactions by Gefen et al. [17] and on online auction by Pavlou and Gefen [32]. Credibility and benevolence can be built through various institutional structures between buyers and sellers in B2B transactions [33]. Applying these arguments to the SME cloud user and cloud service provider providing virtual technologies that enables trusted relationships requires built-in third party institutional trust mechanisms such as legislation, rules, escrow and certifications that improved the SMEs trusting belief in the relationship

[15, 17, 28]. Without these institutional safeguards, first time cloud users such as SMEs will be reluctant to adopt such technology.

Another perspective of institutional trust is concerned with routines and controlling mechanisms including external regulators in a business ecosystem such as cloud service [34]. Cook, Hardin and Levi [35, p. 196] suggest that "Societies are essentially moving away from trust relationships toward externally regulated behaviour". Government regulatory bodies fall short of their responsibility of enforcing regulatory and legislative mechanisms on expert systems such as cloud technology sometimes due to lack of technical knowledge. These lapses weaken the institutional trust embodied in these types of expert systems, making vulnerable users such as SMEs cautious in adopting these modern technologies, thereby reducing the adoption rate as compared to other developed economies.

According to Bachmann [19], this third-party guarantor performs a function that ensures trust between the trustor and the trustee that would otherwise not be possible because the institutional arrangements, such as legal regulations, certifications, professional code of conduct, corporate reputation, can reduce the risk that a trustee will behave untrustworthily. This allows a potential cloud service adopter such as an SME to make a leap of faith and invest trust in a relationship with a cloud service vendor. Institutions appear as formal institutional arrangements if they are based on explicit rules of behaviour. These practices are grounded on legal rules, practices of regulatory guidelines, certification bodies' principles, industry associations' standards, service level agreements and contracts creating an institutional arrangement leading to stable trusted relationships [21]. SMEs will generally have faith in the cloud service ecosystem if there are promises, contracts, regulations, and guarantees in place [15].

3 Method

The goal of this research is to more fully understand and describe the process by which SME adoption decisions about cloud services are motivated by institutional trust factors. This type of research relies on qualitative data. Adoption decisions are best understood by analysing informants' social constructions through language and shared meanings. Fieldwork based on semi-structured interviews lasting 30 to 60 min were used to collect the data. A set of 12 interviews was conducted as a primary data collection method. Interviews were recorded with the permission of the participants and transcribed for further analysis. These nine informants were categorised into three main groups. These were SMEs that had already adopted cloud computing services, SMEs that intended to adopt cloud computing services in the next three years and SMEs that did not intend to adopt cloud computing services soon. For better triangulation of findings, this data was supplemented with three interviews of SME cloud service providers. Thematic analysis was adopted as the qualitative data analysis strategy. The authors read the data sets multiple times and worked independently to generate a set of thematic categories. Finally, we selected exemplars to show the link between the data and the thematic analysis. The thematic findings show the four interrelated themes about institutional trust emerged from the data.

4 Findings

Mimicking the behavior of partners and competitors. Four SMEs stated that they fear going 'extinct' if they do not adopt cloud technology. Cloud computing is seen to be important due to their future competitiveness and hence has a significant influence on their adoption decision. An important influence in the adoption decision is the behavior of partners, such as suppliers and competitors in the industry. SMEs are more likely to trust cloud service if their partners and competitors have already adopted it.

Relative advantage mitigates the risk of poor institutional mechanisms. Some SMEs (T04, T06, T07, T08) were of the view that they have no choice but to trust the cloud providers, as the relative advantage outweighs the risk it has over traditional IT. Others indicated that security and privacy is a serious concern because they are responsible for their customers' data which is handed over to a third-party cloud service provider. However, five SMEs (T02, T04, T05, T07, and T08) say since large organisations are adopting this technology, they too feel that they can adopt it and benefit from the advantages promised. Some SMEs said "*Not really. It has always worked and is working for bigger companies why worry. Though I don't know much about cloud computing systems, but it seems to be working well for us* ". There is a perception of ownership that the service provider gives the customer. One cloud service provider (T09) says "*the fact that I am running the customer job doesn't mean I have access to them. I can perform backups but cannot log in and access your data except … the customer gives me access, I will be logged out*".

Lack of technical knowledge in SMEs creates reliance on the Cloud Provider expertise. The design faults in cloud technologies make them vulnerable to hackers. This can create mistrust and uncertainty among SMEs. The lack of technical knowledge by SMEs also creates reliance on the expertise of cloud service providers to ensure the service is secure, protected and available when required. Four of the SMEs (T05, T07, T09, and T10) disclosed that they do not have the technical ability, due to the technical nature of this type of technology, to verify if the promised security features have been implemented by the cloud service provider. The SMEs that adopted cloud services trust cloud service providers and the institutional mechanisms around various role players within the cloud ecosystem.

Assuming sufficiency of institutional trust mechanisms. Most of the uncertainty was about the enforcement of laws governing the cloud service providers. SMEs (T01, T02, T04, T06, and T08) were of the opinion that it is the responsibility of government to ensure that consumers of cloud services are protected against any abuse, though also concede that there exists some breaches in the past that proves that governments do not fully have control over what cloud services providers do. For example, an SME said "*Is ICASA not also controlling these service providers? I think this is part of communications*". Another SME said: "*If they were not regulated, they will not be providing such services in South Africa*". Most cloud service providers are self-regulated due to the global nature of their customer base and operations. Service provider T09 was of the opinion that "*Data sovereignty is often an issue for customers. That is where your data is stored is sovereign to that country. We stick to Microsoft ethical practices. We are regulated by Microsoft practices and rules. We are driven by the clients' specific regulations*" This is contrary to other institutional trust research (e.g. [19, 28, 32], which

proposes standardised rules and regulations that create certainty and structure. Some SMEs are not sure who is enforcing the rules or whose role it is to enforce these rules, one (T01) said "*I am not entirely sure exactly who is controlling these companies. What I know is that because they use Visa and Master card they are controlled by regulatory bodies as they have to settle using a local account*". Another SME is also very skeptical on the role of government agencies in enforcing regulations, "*I don't know exactly all the role players. I am sure government plays a part and maybe some international partners in regulating these providers, but I don't think they are doing a great job at it. If they were, we will not be hearing a lot of about breaches in big companies like Sony and even governments like USA government. Remember the guy who downloaded top secrets from the US government and exposed them. Imagine the US government with all the technology. I know there may be many players in the space of cloud computing, but I am not sure what roles they play in protecting us consumers*". The power of the cloud service provider in the relationship with the cloud user is real. Some SMEs (T02, T03, T05, T07, T08) are aware of the power of the cloud service provider with one saying that "*We depend on the cloud service provider to maintain our accounts and data. They back-up our data and we trust that our systems can be recovered in case it falls over"*. This is consistent with existing research that says, trust is not completely independent of inter-organisational relationships and other power relation structures due to complex interrelationships between cloud users and cloud service provider [36].

Adopters noted that they do not have the technical expertise to monitor the contracts and SLAs they sign with cloud providers, making them vulnerable to abuse and non-compliance. Strangely, the SMEs who adopted cloud services seem to think that government institutions and industry bodies have put mechanisms in place to govern cloud service providers and enforce these mechanisms to protect their interests.

5 Conclusion

The results of this study highlight how SMEs socially construct their perspectives of institutional trust in cloud services and explore how these constructions could be influencing SME cloud adoption decisions. Our study finds that in order to survive, some SMEs merely mimic the behavior of larger organizations, their partners and competitors when making the adoption decision. As predicted by the diffusion of innovation theory [37] the perception of the greater relative advantage of Cloud services also seems to mitigate the high risk of poor institutional mechanisms among SMEs. As predicted by Giddens [20], the lack of technical knowledge by some SMEs creates greater reliance on cloud provider expertise. Finally, we found that SMEs simply assume the sufficiency of institutional trust mechanisms in Cloud ecosystems. Since SMEs do not have the capacity to evaluate cloud service innovations effectively, other social actors in society will have to play a prominent role in evaluating and strengthening these institutional trust mechanisms. The empirical literature on the strength of institutional trust of cloud computing services and other new platforms in South Africa and other developing markets is sparse. Design faults and operator failure can be useful conceptual tools for the development of policy guidelines by global and regulatory bodies responsible for the cloud ecosystem. Improvements to the trustworthiness of the cloud ecosystem will safeguard the interests of SMEs that appear to

be naïve about the risks of cloud computing. Since SMEs lack the requisite technical knowledge and are often less powerful than CSPs, enforceable institutional mechanisms will be required to protect their interests.

We recommend that future research examine the strength of these institutional mechanisms in safeguarding the interest of SME cloud users in developing economies.

References

1. Berry, A., von Blottnitz, M., Cassim, R., Kesper, A., Rajaratnam, B., van Seventer, D.: The economics of SMMEs in South Africa. TIPS-Trade Ind. Policy (2002). http://www.tips.org.za/files/506.pdf. Accessed 22 Apr 2019
2. Fatoki, O., Smit, A.: Constraints to credit access by new SMEs in South Africa : a supply-side analysis. Afr. J. Bus. Manag. **5**(4), 1413–1425 (2011)
3. Alshamaila, Y., Papagiannidis, S., Li, F.: Cloud computing adoption by SMEs in the north east of England: a multi-perspective framework. J. Enterp. Inf. Manag. **26**(3), 250–275 (2013)
4. European-Commission, "ICT – Information and communication technologies, European," European Commission (2013)
5. Giannakouris, K., Smihily, M.: Cloud computing - statistics on the use by enterprises. Eurostat (2014). http://ec.europa.eu/eurostat/statisticsexplained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprise
6. Venkatraman, S., Wadhwa, B.: Cloud computing a research roadmap in coalescence with software engineering. Softw. Eng. Int. J. (SEIJ) **2**(2), 2 (2012)
7. Paik, S.: Supply management in SMEs: role of SME size. Int. J. Supply Chain Forum **12**(3), 10–21 (2011)
8. McEvily, B., Perrone, V., Zaheer, A.: Introduction to the special issue on trust in an organizational context. Organ. Sci. **14**(1), 1–4 (2003)
9. Zaheer, A., Harris, J.: Interorganizational Trust (2006)
10. Lumineau, F., Quélin, B.V.: An empirical investigation of interorganizational opportunism and contracting mechanisms. Strateg. Organ. **10**(1), 55–84 (2012)
11. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: a cross-discipline view of trust. Acad. Manag. Rev. **23**(3), 393–404 (1998)
12. Jap, S.D., Anderson, E.: Safeguarding interorganizational performance and continuity under ex post opportunism. Manag. Sci. **49**(12), 1684–1701 (2003)
13. Koza, M.P., Lewin, A.Y.: The co-evolution of strategic alliances. Organ. Sci. **9**(3), 255–264 (1998)
14. Lewis, J., Weigert, A.: Trust as a social reality. Soc. Forces **63**, 967–985 (1985)
15. McKnight, D., Chervany, N.: What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. Int. J. Electron. Commer. **6**(2), 35–53 (2002)
16. Jarvenpaa, S., Tractinsky, N.: Consumer trust in an internet store: a cross-cultural validation. J. Comput.-Mediated Commun. **5**(2), JCMC526 (1999)
17. Gefen, D., Karahanna, E., Straub, D.: Trust and TAM in online shopping: an integrated model. MIS Q. **27**(1), 51–90 (2003)
18. Morgan, R., Hunt, S.: The commitment-trust theory of relationship marketing. J. Mark. **58** (1), 20–38 (1994)
19. Bachmann, R.: Understanding institutional-based trust building processes in inter-organizational relationships. Organ. Stud. **32**(2), 281–301 (2011)
20. Giddens, A.: The Consequences of Modernity. Stanford University Press, Palo Alto (1990)

21. Giddens, A.: The Constitution of Society: Outline of the Theory of Structuration. Polity Press, Cambridge (1984)
22. Child, J., Möllering, G.: The development of contextual based trust in the Chinese context. Judge Institute of Management, University of Cambridge (2000)
23. Gollmann, D.: Why trust is bad for security. Electron. Notes Theor. Comput. Sci. **157**(3), 3–9 (2006)
24. Kumar, N.: The power of trust in manufacturer-retailer relationships. Harvard Bus. Rev. **74** (6), 92–106 (1996)
25. Ganesan, S.: Determinants of long-term orientation in buyer-seller relationships. J. Mark. **58** (1), 1–19 (1994)
26. Bachmann, R., van Witteloostuijn, A.: Analyzing inter-organizational relationships in the context of their national business systems: a conceptual framework for comparative research. Eur. Soc. **11**, 49–76 (2009)
27. Giddens, A.: Risk, Trust, Reflexivity, pp. 184–197. Polity Press, Cambridge (1994)
28. Zucker, L.: Production of trust: institutional sources of economic structure, 1840–1920. Res. Organ. Behav. **8**(1), 53–111 (1986)
29. Shapiro, S.: The social control of impersonal trust. Am. J. Sociol. **93**(3), 623–658 (1987)
30. Heide, J., John, G.: Alliances in industrial purchasing, the determinants of joint action in buyer-supplier relationships. J. Mark. Res. **37**(1), 24–36 (1990)
31. Reichheld, F.F., Schefter, P.: E-loyalty: your secret weapon on the web. Harvard Bus. Rev. **78**(4), 105–113 (2000)
32. Pavlou, P.A., Gefen, D.: Building effective online marketplaces with institution-based trust. Inf. Syst. Res. **15**(1), 37–59 (2004)
33. Pavlou, P.: Institutional trust in interorganizational exchange relationships: the role of electronic B2B marketplaces. J. Strateg. Inf. Syst. **11**(4), 105–143 (2002)
34. Sztompka, P.: Trust: A Sociological Theory. University Press, Cambridge (1999)
35. Cook, K., Schilke, O.: The role of public, relational and organizational trust in economic affairs. Corp. Reput. Rev. **13**, 98–109 (2010)
36. Mizrachi, N.D.I., Anspach, R.: Repertoires of trust: the practice of trust in a multinational organization amid political conflict. Am. Sociol. Rev. **72**, 143–165 (2007)
37. Rogers, E.M.: Diffusion of Innovations, 4th edn. Simon and Schuster, New York (1995)