2019

Cloud privacy and security issues beyond technology: championing the cause of accountability

Joshua K. Mwenya
University of Cape Town, mwnjos003@myuct.ac.za

Irwin Brown
University of Cape Town, AfrJIS.Editor@gmail.com

Cloud privacy and security issues beyond technology: championing the cause of accountability

Full Paper

Joshua K. Mwenya
Department of Information Systems
University of Cape Town
Cape Town, South Africa
Email: mwnjos003@myuct.ac.za

Irwin Brown
Department of Information Systems
University of Cape Town
Cape Town, South Africa
Email: irwin.brown@uct.ac.za

Abstract

Cloud computing provides IT service providers increased efficiency of resource utilization while enabling consumers to benefit from innovative advantages like access to up-to-date IT resources and low upfront investment. A significant hindrance to adoption of cloud computing is the lack of trust arising from worries over privacy and security when data resources of cloud service consumers are handled by third parties. A key factor in fostering cloud privacy and security is accountability, which increases trust by obligating an entity to be answerable for its actions. This paper uses a hermeneutic literature review to investigate (i) the prevailing methods and strategies of fostering privacy and security through accountability, (ii) the key actors in championing cloud accountability and (iii) the key barriers to cloud accountability. This literature review provides insight into current practices associated with championing cloud accountability and contributes to cloud service provider awareness of ways to improve cloud computing trustworthiness.

Keywords Accountability, Hermeneutic, Privacy, Security, Trust

1 INTRODUCTION

In recent years cloud computing has emerged as a key information technology (IT) service delivery paradigm and a major innovation driver that offers a new business model that suits both IT service consumers and IT service providers (Aguez et al. 2016). For IT service providers, cloud computing provides new opportunities, such as realization of economies of scale by increasing efficiency of resource utilization (Sunya and Schneider 2013). For IT service consumers, cloud computing is a technology that allows organizations to selectively adopt specific resources from a wide range of cloud-based services and to outsource their entire IT based businesses process so they can concentrate more on their core business (Diener et al. 2016; Khana and Al-Yasiri2016). However, evidence indicates that migration to the cloud paradigm is often hampered by concerns over security and privacy (Coppolino et al. 2017; Mazhar et al. 2015). A major impediment to cloud adoption is the lack of trust by potential customers, arising from the worry over privacy, security, and data protection when data resources are handled by third parties and accessed via networks (Adjei 2015; Habib et al. 2012; Ko et al.2011; Pearson 2011). Trust in a cloud service provider (CSP) is an important issue and the lack of this trust is considered one of the biggest concerns preventing cloud computing from quickly attaining its full technical, social, and economic potential (McLeod and Gormly 2017). For cloud computing to earn the full trust it deserves, cloud service consumers should be able to store their data in the cloud with the same confidence that they have when they deposit their money and other valuables in banks (Asadi et al. 2017). Trust is comprised of four main components: (i) Security - the mechanisms which make it difficult or uneconomical for an unauthorised person to access some information; (ii) Privacy - the protection against the exposure or leakage of personal or confidential data; (iii) Auditability - the relative ease of auditing a system or an environment; and (iv) Accountability - the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations (Al-Rashdi et al. 2015; Ko et al. 2011).

This paper takes the view that accountability is the main construct and key enabler of trust and that achievement of accountability in a cloud environment brings about the other three trust components (privacy, security and auditability) as by-products. The paper contributes to research and knowledge on cloud privacy and security by establishing a relationship between accountability and both privacy and security and then addressing privacy and security issues through accountability by investigating the prevailing accountability practices in cloud ecosystems, the key actors in championing cloud accountability, and the key barriers and challenges associated with championing and implementing cloud accountability. The rest of this paper is organized as follows: The next section highlights the concept of accountability and its dimensions that are relevant to trust (and, hence, to privacy and security) building and explains how the achievement of accountability brings about privacy, security and auditability. The section ends with identification of our research problem and research questions. The third section outlines the research methodology we adopted - a hermeneutic circle based literature review. The fourth section presents our research findings while the fifth section gives a brief discussion of the findings and provides suggestions for further research. The paper concludes with section six.

2 CONCEPT OF ACCOUNTABILITY

2.1 Accountability and its Attributes

Accountability is about defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly (Contractor and Patel 2017; Felici et al. 2013). Bovens (2007, p.450) defines accountability as "a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor may face consequences". In terms of its components, accountability is viewed and interpreted in terms of a set of key attributes and properties, including the following five key attributes identified by several researchers: transparency, responsibility, remediability, attributability and verifiability (Felici and Pearson 2014; Al-Rashdi et al. 2017; Jaatun et al. 2018). Viewing accountability in terms of the foregoing key attributes strengthens the view of accountability as a basis for satisfaction of obligations along the cloud service provision chain, which ensures that all partners are accountable and that there has been proper allocation of responsibilities along the service provision chain (Contractor and Patel 2017; Pearson *et al.* 2012). Implementing accountability by putting its core attributes into practice is identified as an effective method of addressing issues of privacy, security and trust (Pearson and Benameur 2010). Achievement of accountability is, thus, a practical and effective catalyst for bringing about cloud privacy, security and trust. Table 1 describes the five key accountability attributes that organisations put into practice to enforce accountability.

Accountability attribute	Description
Attributability	The possibility to trace a given action back to a specific entity.
Remediability	The property of a system, organization or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms.
Responsibility	The property of an organization or individual in relation to an object, process, or system of being assigned to take action to be in compliance with the norms.
Transparency	The property of an accountable system that is capable of giving account of, or providing visibility of how it conforms to its norms, governing rules and commitments.
Verifiability:	The extent to which it is possible to assess norm compliance.

Table 1. Key Accountability Attributes

2.2 How Accountability brings about Privacy, Security and Auditability

How accountability brings about privacy: According to ISO/IEC29100 guidelines, accountability requires a data controller to document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organization, provide suitable training, inform about privacy breaches, and give access to effective sanctions and procedures for compensations in case of privacy breaches (Berthold 2013). Furthermore, full accountability is derived from contracts and other transparency mechanisms that govern active interactions among cloud stakeholders, all with the primary objective of reducing the risk of disproportionate harm to the data subjects and permitting the amelioration of negative consequences for the data controllers in case of harms arising from failure to provide sufficient privacy protection (Pearson and Charlesworth 2009). This means that accountability imposes transparency and privacy liability on cloud data controllers and their partners in the service delivery chain, ensuring that achievement of accountability by cloud data controllers engenders privacy as a by-product.

How accountability brings about security: Cloud security is often compromised by the lack of or absence of several key attributes, notably confidentiality (ensuring that a customer's data and computation tasks performed on the data are kept confidential from both the cloud service providers and other customers), integrity (data integrity which ensures that a customer's data is honestly stored on cloud servers and computation integrity which ensures that data manipulation programs are executed without being distorted by malware, cloud providers, or other malicious users and that any incorrect computing is detected), and availability (ensuring that each expected service is available and the quality of service meets the agreed Service Level Agreement) (Xiao and Xiao 2013). Accountability provides constraints and control mechanisms for cloud data controllers and others in the service provision chain by encompassing the obligation for each one to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate processing and use of that information beyond mere legal requirements and to provide remediation in case of failure to ensure availability, confidentiality and integrity of the data (Pearson and Wainwright 2013). Thus, achieving accountability engenders cloud security as a by-product.

How accountability brings about auditability: Auditability is an enabler of accountability in that auditability ensures that events are recorded while accountability ensures that events deemed important are logged and not missed (Doiphod and Channe 2015; Ko 2013). Auditability helps ensure availability of evidence required by accountability in determining that both users and cloud service providers at all levels are in compliance with security and privacy policies. Auditability serves as a retrospective enabler of accountability as auditability furnishes evidence allowing an action to be reviewed against a pre-determined policy, enabling relevant parties to hold accountable the person or organization responsible for that action (Ko et al.2011). Thus achievement of accountability requires that auditability be attained as a by-product.

2.3 Research Problem and Questions

In practice, implementing accountability in clouds raises several compelling issues that should concern cloud privacy and security researchers. First, accountability has the power to increase cloud trust (Doiphod and Channe 2015), but its implementation can produce contrasting and unintended outcomes for different actors (Pearson and Benameur 2010). Second, accountability aspects such as regulation can stifle innovation and thwart the desired cloud trust increases if it is not introduced in an intelligent way (Pearson 2011). Third, because its implementation can yield a positive outcome for one cloud provider

while at the same time yielding negative outcomes for others, accountability has been identified as needing urgent attention (Ko et al. 2011). It is these three key concerns that pose a relevant problem and provide the motivation for this research study. Research on the aforementioned aspects of accountability in clouds enables us to understand emerging relationships among cloud actors and allows us to identify accountability based mechanisms and appropriate tools available to support privacy, security and trustworthiness in cloud ecosystems (Felici et al. 2013).

As regards our research focus, we agree with Al-Rashid et al. (2017) that research in the area of cloud security has been largely technical in nature, creating a need for more research focused on non-technical aspects. Thus, our paper focuses more on non-technical approaches to championing and implementing accountability through a combination of public law (legislation and regulation), private law (contracts and SLAs) and self-regulation (through standards and certification). Specifically, this study contributes to the body of knowledge on the role of accountability in fostering cloud privacy, security and trust by answering three related questions:

What are the prevailing non-technical approaches to championing the cause of accountability in cloud computing?

Who are the key actors in championing the cause of accountability in cloud computing?

What are the key barriers and challenges to championing the cause of accountability in cloud computing?

3 RESEARCH METHODOLOGY

This paper adopts a hermeneutic literature review approach, a literature review framework known to be well-suited for theory generation and knowledge building (Boell and Cecez-Kecmanovic 2014; Greenhalgh et al. 2018). The hermeneutic approach assumes that the meaning emerges through a dialogue between a text (a paper) and a reader, through an inherently interpretive process which enables the researchers to expand and deepen their understanding of relevant literature as they iteratively interpret a paper from their own pre-understanding of literature and then incrementally develop better understanding of the literature based on each interpreted paper (Boell and Cecez-Kecmanovic 2014; Baghizadeh et al. 2019). In this study, the literature searching started with Google Scholar, a popular and flexible scholarly search facility and the hermeneutic circle was implemented through an iterative process. The initial set of articles was obtained by querying Google Scholar for particular keywords and phrases appearing in the title of published articles as shown in the first column of Table 2.

Keyword search phrase	Number of Articles returned	Meeting inclusion criteria	Rejected as less relevant	Number included
allintitle: Accountability for cloud Privacy	9	5	1	4
allintitle: Accountability for cloud security	3	1	0	1
allintitle: Cloud computing accountability	44	9	1	8
allintitle: Cloud computing regulation	36	6	0	6
allintitle: Cloud computing trust	511	37	23	14
allintitle: Trust accountability cloud computing	9	3	2	1
allintitle: Accountability in cloud	162	11	6	5
allintitle: Cloud trust issues	34	6	3	3
allintitle: Cloud computing legal	178	7	3	4
Total	986	85	39	46

Table 2. Keyword Search phrases and Results relevant to research issues

The returned articles totalling 986 were initially reviewed both by title and abstract in order to filter out articles that were not relevant to the key concepts and to ensure investigating accountability in cloud computing mainly from a non-technical perspective, thereby ruling out articles that focused on purely technical aspects and solutions. The hermeneutic principles are accomplished through two interlinked cycles: 1) accessing and interpreting the literature (column 2 and 3 of Table 2), focusing on a systematic but flexible and iterative searching and 2) understanding and developing an argument (column 3 and 4 of Table 2), focusing on recognising emerging ideas and perspectives and rejecting less relevant sources through progressive focusing (Boell and Cecez-Kecmanovic, 2014). The final part of the review resulted in identification of three main themes that emerged from the findings regarding our research questions:

(i) articles that identify current approaches and practices adopted in championing the cause of accountability in cloud computing; (ii) articles that identify the key actors and stakeholders that champion the cause of accountability in cloud computing; and (iii) articles that identify key barriers and challenges to the implementation of accountability in cloud computing. Finally, based on the resulting knowledge generated from hermeneutic literature review, we addressed the argument development process by identifying emerging issues and providing suggestions for further research and direction.

4 RESEARCH FINDINGS

Our research findings are presented in the following three tables. To answer our first research question, we took a deep look into the literature for the prevailing non-technical approaches and methods that stakeholders adopt to help enhance one or more of the five key attributes or properties of accountability identified by Felici and Pearson (2014), Al-Rashdi et al. (2017) and Jaatun et al. (2018). We identified nine (9) prevailing non-technical approaches as shown in Table 3. It should be noted that even though Jaatun et al. (2018) found nine (9) core attributes, only five key attributes listed in Table 1 were found to be relevant for this study. Other attributes were not considered relevant. For example, effectiveness and appropriateness measure technical aspects while observability is an element of transparency.

Prevailing Accountability Practice	Accountability aspect enhanced	How the identified accountability property is enhanced or enacted	Literature Source (s)
Legislation	Responsibility	Legislation, such as the EU Data Protection Act, create obligations on service providers to engage in sound data governance and stewardship, providing a basis for responsibility.	Pearson et al. (2012); Ryan (2013)
Auditing by external agents/entities	Transparency, verifiability, attributability	Auditing allows an action by any cloud actor to be reviewed against a pre-determined policy and to shed light on compliance.	Ryoo et al. (2014)
Contractual assurances	Responsibility, remediability	Contractual assurances promote accountability by enabling parties to a cloud contract to both claim their rights and fulfil their obligations.	Ryan (2013); Seddona and Currie (2013)
Third-party Certification	Transparency, verifiability	Third-party certification enables cloud providers to implement accountability and give users and other data governance actors a way to check and monitor use of data in clouds.	Pearson et al. (2012)
Imposition of Penalties	Attributability, remediability	Failure to comply with regulation can lead to costly penalties: e.g. violation of HIPAA in the USA earns a maximum possible fine of $1.5 million.	Al-Rashdi et al. (2017); Hoover (2013)
Compliance Regulation	Verifiability, responsibility	With strict accountability in place, compliance regulators enforce the law on the 'first in the chain' of cloud providers in regard to the misdeeds of anybody in the chain.	Pearson and Charlesworth (2009); Takabi et al. (2010)
Service level agreements (SLA)	Transparency, verifiability, remediability	An accountable CSP is not only able to guarantee service availability via SLA, but must also provide documentation to show that their service is available when the customer needs evidence.	Mazhar et al. (2015); Pearson (2011)
Enforcement of industry standards	Responsibility, transparency	Standards such as ISO/IEC 27018 cloud standard primarily aim at fostering and verification of legal and/or contractual compliance and transparency.	de Hert et al. (2016); Löhe and Blind (2015)
Monitoring by special interest groups and market places.	Transparency, verifiability	Notably, the A4Cloud project helps promote accountability by holding CSPs accountable through an orchestrated set of preventive, detective and corrective mechanisms.	Habib et al. (2012); Pearson et al. (2012)

Table 3. Prevailing approaches to championing the cause of accountability

To answer our second question, we examined the literature to identify those actors that played a prominent and active role in championing the cause of accountability in cloud computing. We identified six (6) key actors as shown in Table 4 which indicates a combination of institutions of various types, ranging from national governments to special interest groups.

Name of actor	Type of actor	Championing activities	Source (s)
National governments (e.g. USA, German, UK, China, Spain, Russia)	Governmental bodies	Governments impose a variety of tailored data protection laws and penalties (e.g. the HIPAA Omnibus law in the United States, the German data protection Law, Golden Shield Project of China, and the Russian data storage localization law enacted in 2015).	Hoover (2013); Maughan (2016) Millard (2015); Rieger et al. (2013); Yaraghi and Gopal (2018)
Office for Civil Rights (OCR) in the USA	United States Governmental agencies	Enforces the Health Information Portability and Accountability Act (HIPAA), which protects the privacy of individually identifiable personal health information.	Klein (2011); Ryoo et al. (2014); Seddona and Currie (2013)
The European Union (EU)	Inter-governmental body	The EU develops regulations and standards which the 27 Member States must embed into their own national data privacy and security laws that apply whenever an individual or institution collects personal data related to an EU citizen.	Seddona and Currie (2013)
International Standards Organization (ISO)	Independent/ Professional bodies	Produces industry standards such as the ISO/IEC-27018, which address the lack of trust and transparency, by developing controls and recommendations for CSPs.	de Hert et al. (2016]
Cloud Security Alliance (CSA)- incorporated in the USA	Not-for-profit industry organization concerned with cloud security.	Promotes accountability via a toolkit used by key stakeholders to assess clouds against industry established best practices, standards and compliance requirements.	Habib et al. (2012)
The Cloud Accountability (A4Cloud) Project	A European based Cloud Accountability Initiative fully funded by EU	The primary focus of this Project is accountability under data protection laws for personal data processed in cloud service provision ecosystems: accountability obligations owed by CSPs to other cloud stakeholders.	Pearson *et al.* (2012)

Table 4. The key actors responsible for championing the cause of accountability

To answer our third question, we examine literature to identify the major challenges and barriers that may negatively impact on stakeholder efforts in championing the cause of accountability in cloud computing. We identified eight (8) significant barriers and challenges as shown in table 5.

Key sources of challenges to accountability	Nature or description of accountability barriers and/or challenges	Source (s)
Government surveillance or intervention	Government's surveillance or intervention, such as the USA Patriot Act (UPA) of 2001, may pose serious challenges to cloud accountability by obliging cloud suppliers and service providers, for reasons of national security or other reasons, to provide government agencies access to customer data without consent of the customers, thereby violating SLAs.	Aguez et al. (2016); Fernandes et al. (2014); Marston et al. (2011)
Self-regulatory and industry-targeted regulatory approaches	Self-regulatory mechanisms such as the Safe Harbour Agreement are viewed as inadequate and legitimately seen as a way of watering down existing strong privacy protections, notably those granted to EU citizens.	King and Raja (2012); Pearson *et al.* (2012); Yang and Borg (2012)

Key sources of challenges to accountability	Nature or description of accountability barriers and/or challenges	Source (s)
Lack of genuine Transparency and verifiability in CSP service level agreements (SLAs)	Most often, Service Level Agreements lack transparency as they are made using non-negotiable standard contracts which mainly deal with protecting the rights of the CSP, neglecting consumer needs. This leads to distrust of cloud stakeholders and diminishes accountability.	Fernandes et al. (2015); Khan (2016); Ryan (2013); Sfondrini et al. (2015)
Challenges due to cloud data location.	CSPs ensure efficient service availability by replicating data in multiple data centres. Thus, cloud based data is stored on the CSP's servers in undisclosed locations, which could be in the USA, Europe, or anywhere else. This key tenet of the cloud business model conflicts with various legal requirements, notably in EU and Russia.	AbuOliem (2013); Hon and Millard (2018); Takabi et al. (2010); Yaraghi and Gopal (2018)
Challenges to enforcement of ISO standards	Standards like the ISO/IEC 27018 act as non-legal forms of regulation by complementing legal regulations. However, the audit and certification of compliance with ISO/IEC 27018 is not driven by public authorities, but by private entities. This tends to leave open a choice for some CSPs to ignore key aspects like interoperability.	de Hert et al. (2016); Löhe and Blind (2015)
Securing the accountability of subcontractors and CSP employees not guaranteed	Although a contract may exist to forbid the CSP from disclosing the data to third parties, it may be difficult to implement because employees and subcontractors of the CSP may not be locked into the contract too, making it very hard to oblige them all to the terms and standards requested by the data owner.	Felici et al. (2013); Mazhar et al. (2015; Ryan (2013)
Conflicting legal structures of different countries.	Incompatible in legislative regimes of different countries pose serious challenges to accountability. For example, the USA PATRIOT Act is known to conflict with both the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada and EU Data Protection Directive.	Fernandes et al. (2014); Pearson and Charlesworth (2009)
Regulatory and Compliance challenges in highly regulated sectors	Highly regulated sectors like banking and healthcare face unique cloud accountability challenges. Many banking regulators require that financial data for banking customers stay in home country regulations require that banking data does not get intermixed with other data.	Bejju (2014); Maughan (2016); Ryoo et al. (2014); Young and Borg (2012)

Table 5. Key challenges to championing the cause of accountability

5 DISCUSSION AND IMPLICATIONS

This literature review provides several insights on aspects of cloud accountability: Firstly, the literature revealed five key attributes of accountability and current practices that cloud service providers need to be aware of if they are to be considered accountable CSPs who contribute to making cloud computing more trustworthy. Secondly, unlike some of the previous waves in computing, cloud computing raises significant challenges in identifying who are the responsible entities, in order to assign accountability obligations. Multiple actors are involved at various levels and, thus, cloud computing also demands a thoughtful and coordinated response from governmental agencies. Appropriate domestic laws can then be applied in order to ensure service providers protect sensitive data in certain sectors. Thirdly, some key actors in championing accountability are also seen as sources of challenges to accountability in clouds. For example the USA government is a leading champion of accountability through the introduction and enforcement of various relevant and progressive regulations and Acts such as Sarbanes-Oxley and HIPAA Omnibus laws. The US PATRIOT Act of 2001, on the other hand, passed and enforced by the USA government, is cited as an example of an Act that fails to adequately protect data privacy by forcing the disclosure of data to government entities without the consent of data owners. Acts of this type may pose challenges to cloud accountability. They may lead to CSP violations of existing terms of SLAs and subsequent breakup of the chain of trust created between cloud customers and cloud providers. Fourthly, the literature revealed that conflicts and inconsistencies among legislative regimes

of different countries pose serious challenges to accountability particularly for highly regulated sectors like banking and healthcare.

To complete our hermeneutic review, we address the argument development aspect of the hermeneutic review by identifying emerging issues and proposing a research agenda for future research directions with regard to some of the key accountability methods and associated challenges identified in this study. The proposed research agenda is shown in Table 6. For each research issue identified, a description of the research concern is presented and pertinent research questions suggested.

Research Issues	Description of Research Concerns	Suggested Research questions
Government surveillance and access to cloud data	To prevent and fight cyber related crimes, national governments have a justifiable need to access cloud based personal data for purposes such as adducing evidence. However, insights from this study indicate that government actions in this area have a potential to violate fundamental privacy rights of individuals and, in some cases, actions taken by one government may result in violation of another country's sovereignty. What about the effect of government cloud data access on CSP obligations? For example, under the EU General Data Protection Regulation (GDPR), it is no longer possible for CSP processors to excuse themselves as mere processors and escape the reach of data protection rules by passing blame to data controllers.	What laws exist, or should be formulated, to oblige a government or its agents to follow a lawful procedure when seeking to access cloud based personal data? What laws or regulations are there that oblige cloud service providers to notify their customers when a government or its agents access their cloud-based privacy data?
Regulation Challenges	Insights from this study indicate that regulation is a source of several issues of research interest. The cloud computing business model thrives on reducing the levels of control and visibility that cloud consumers have on their data as data is stored and manipulated away from visibility to data owners/subjects. On the other hand, a key objective of strong regulations such the EU directives is preservation of such control. Given that other key players like the US have less strict regulation in this aspect compared to the EU, the resulting regulatory inconsistencies and fragmentation among various jurisdictions pose accountability challenges for CSPs. The picture may get even more complex when regulatory and legal regimes in other jurisdictions are compared to those of the EU and the US.	What efforts are there toward achieving global regulatory harmonization to promote increased global consistency in accountability among countries and regional economic blocks? How do cloud regulatory frameworks in other countries compare with those in the EU and the US given that key cloud service providers such as Amazon and Microsoft now host data centres across the globe? How do global cloud service providers reconcile existing laws of one jurisdiction with contradictory legal requirements of another?
Standardization challenges	Lack of cloud service standardization compromises interoperability among cloud platforms, thereby reducing portability of cloud services. In turn, lack of portability promotes vendor lock-in which could be harmful to cloud consumers by preventing them from moving from one cloud provider to another when need arises to maximize business. Further, vendor lock-in can become a major problem in case of bankruptcy of the preferred cloud provider.	How do current standardization efforts and frameworks account for customer inputs and interests? How does lack of standardization of cloud based platforms and services influence vendor lock-in?
Supply chain and Insider Abuse Issues	Insights from this study indicate that insiders such as employees and subcontractors can abuse their position and compromise a CSP's contractual and accountability norms. For example, since the cloud business model thrives on spreading data over a number of different storage devices while consumer has reduced visibility regarding where their data is physically stored, it is not feasible for the consumer to verify secure deletion of their data when the data is deleted. This may create a loophole that insiders such as employees can maliciously exploit for data exfiltration from remnants of unsecured deletions.	What mechanisms enable a cloud consumer or regulatory agent to verify how a cloud service provider enforces compliance of insiders and subcontractors? What mechanisms ensure accountability in cases where two or more cloud providers are involved in providing a service to one consumer such as one customer using Microsoft 365 that is running on an Amazon ECS instance?

Table 6. Proposed research directions for cloud accountability

6 CONCLUSION

The aim of this paper is to contribute to a better understanding of accountability as a key non-technical mechanism for promoting privacy and security (and hence trust) in cloud computing and, by so doing, contribute to cloud service provider awareness of ways to improve cloud computing trustworthiness and cloud service adoption. This paper focuses more on non-technical approaches to implementation of accountability as research in areas of cloud security and privacy has been largely technical. This study has applied a hermeneutic literature review to provide new insights regarding the prevailing practices in championing accountability. It has identified the main actors actively involved in championing the cause of accountability and highlighted the key barriers and challenges to championing accountability in cloud computing. As a result of this analysis, a research agenda is proposed for future studies. One of the key limitations of the findings is that most of the literature addresses cloud computing issues in developed countries, notably the USA, Canada and the EU. The lack of literature from elsewhere offers opportunity to investigate the phenomenon in alternative contexts.

7 REFERENCES

AbuOliem, A. 2013. "Cloud computing regulation: An attempt to protect personal data transmission to cross-border cloud computing storage services," *International Journal of Computer and Communication Engineering*, (2:4), pp 521-525.

Adjei, J.K. 2015. "Explaining the role of trust in cloud computing services," *info.,* (17:1), pp 54-67.

Aguez, E.L.K., Hajji, N., and Barka, H. 2016. "The cloud computing: the impact of regulation on adoption," *International Journal of Computers*, (1), pp 22-32.

Al-Rashdi, Z., Dick, M., and Storey, I. 2015. "A conceptual framework for accountability in cloud computing service provision," i*n The Australasian Conference on Information Systems*, Adelaide, Australia.

Al-Rashdi, Z., Dick, M., and Storey, I. 2017. "Core elements in information security accountability in the cloud," In *Valli, C. (Ed.). 2017. The Proceedings of 15th Australian Information Security Management Conference,* pp 125-131 Perth, Australia.

Asadi, S., Nilashi, M., Husin, A.R.C., and Yadegaridehkordi, E. 2017. "Customers perspectives on adoption of cloud computing in banking sector," *Information Technology Management*, (18), pp 305-330.

Baghizadeh, Z., Cecez-Kecmanovic, D., and Schlagwein, D. 2019. "Review and critique of the information systems development project failure literature: An argument for exploring information systems development project distress," *Journal of Information Technology (00:0)*, pp 1–20. DOI: 10.1177/0268396219832010.

Bejju, A. 2014. "Cloud computing for banking and investment services," *Advances in Economics and Business Management*, (1:2), pp 34-40.

Berthold, S., Fischer-Hubner, S., Martucci, L., and Pulls, T. 2013. "Crime and punishment in the cloud - accountability, transparency, and privacy," in: *Pre-Proceedings of International Workshop on Trustworthiness, Accountability and Forensics in the Cloud in conjunction with the 7th IFIP WG 11.11 International Conference on Trust Management*.

Boell S.K., and Cecez-Kecmanovic D. 2014. "A hermeneutic approach for conducting literature reviews and literature searches. *Communications of the Association for Information Systems*, (34:12), pp 257-286.

Bovens, M. 2007. "Analysing and Assessing Accountability: A conceptual framework," *European Law Journal*, (13:4), pp 447-468.

Contractor, D., and Patel, D. 2017. "Accountability in Cloud Computing by Means of Chain of Trust," *International Journal of Network Security*, (19:2), pp 251-259.

Coppolino, L., D'Antonio, S., Mazzeo, G., and Romano, L. 2017. "Cloud security: Emerging threats and current solutions," *Computers and Electrical Engineering*. (59), pp 126-140.

de Hert, P., Papakonstantinou, V., and Kamara, I. 2016. "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection," *Computer Law & Security Review*, (32), pp 16-30.

Diener, M., Blessing, L., and Rappel, N. 2016. "Tackling the Cloud Adoption Dilemma - A User Centric Concept to Control Cloud Migration Processes by Using Machine Learning Technologies," *11th International Conference on Availability, Reliability and Security (ARES),* pp 776-785, Salzburg.

Felici M., Jaatun M.G., Kosta E., and Wainwright N. 2013. "Bringing Accountability to the Cloud: Addressing Emerging Threats and Legal Perspectives," in: *Felici M. (eds) Cyber Security and Privacy. CSP 2013. Communications in Computer and Information Science*, (182). Springer, Berlin, Heidelberg.

Felici, M., and Pearson, S. 2014. "Accountability, Risk, and Trust in Cloud Services: Towards an Accountability-Based Approach to Risk and Trust Governance," *2014 IEEE World Congress on Services*, pp 105-112, Anchorage. doi: 10.1109/SERVICES.2014.29

Fernandes, A.B., Soares, F.L., Gomes, J.V., Freire, M.M., and Inácio, R.P. 2014. "Security issues in cloud environments: a survey," *International Journal of Information Security*, (13), pp 113-170.

Greenhalgh, T., Thorne, S., and Malterud, K. 2018. "Time to challenge the spurious hierarchy of systematic over narrative reviews," *Eur JClin Invest*., (48:1). doi.org/10.1111/eci.12931.

Habib, S.M., Hauke, S., Ries. S., and Mühlhäuser, M. 2012. "Trust as a facilitator in cloud computing: a survey," *Journal of Cloud Computing: Advances, Systems and Applications*, (2012), pp 1-19.

Hon, W.K., and Millard, C. 2018. "Banking in the cloud: Part 3 – contractual issues," *Computer Law & Security*, (34), pp 595-614.

Hoover, J.N. 2013. "Compliance in the ether: Cloud computing, data security and business regulation," *Journal of Business & Technology Law,* (8:1), pp 255-273.

Jaatun, M.G., Tøndel, I.A., Moe, N.B., Cruzes, D.S., Bernsmed, K., and Haugset, B. 2018. "Accountability requirements in the cloud provider chain," *Symmetry*, (10:4), pp 124-144.

Khan, H.M., Chan, G., and Chua, F. 2016. "An adaptive monitoring framework for ensuring accountability and quality of services in cloud computing," *International Conference on Information Networking (ICOIN)*, pp. 249-253, Kota Kinabalu.

Khana, N., and Al-Yasiri, A. 2016. "Identifying cloud security threats to strengthen cloud computing adoption framework," *Procedia Computer Science*, (94), pp 485-490.

King, J.N., and Raja, V.T. 2012. "Protecting the privacy and security of sensitive customer data in the cloud," *Computer Law & Security Review*, (28), pp 308-319.

Klein, A.C. 2011. "Cloudy confidentiality: Clinical and legal implications of cloud computing in health care," *The Journal of the American Academy of Psychiatry and the Law*, (39:4), pp 571-578.

Ko R.K.L., Lee, B.S., and Pearson, S. 2011. "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," *Communications in Computer and Information Science*, (193). Springer, Berlin, Heidelberg.

Ko, R.K.L. 2013. "Data accountability in cloud systems," In *Security, Privacy and Trust in Cloud Systems, Springer-Verlag*, Berlin, Heidelberg.

Löhe, M.G., and Blind, K. 2015. "Regulation and standardization of data protection in cloud computing," *ITU Kaleidoscope: Trust in the Information Society*, pp 1-6, Barcelona.

Mazhar, A., Samee, U.K., and Athanasios, V.V. 2015. "Security in cloud computing: Opportunities and challenges," *Information Sciences*, (305), pp 357-383.

McLeod, J., and Gormly, B. 2017. "Using the cloud for records storage: issues of trust," *Arch Sci*., (17), pp 349–370.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., and Ghalsasi, A. 2011. "Cloud computing: The business perspective," *Decision Support Systems*, (51:1), pp 176-189.

Millard, C. 2015. "Forced Localization of Cloud Services: Is Privacy the Real Driver?" in *IEEE Cloud Computing,* (2:2), pp 10-14.

Maughan, A. 2016. "Cloud computing: A move toward harmonization, or continuation of a tiered service provision?" *Intellectual Property & Technology Law Journal*, (28:11), pp 9-12.

Pearson S., and Charlesworth A. 2009. "Accountability as a Way Forward for Privacy Protection in the Cloud," In: *Jaatun M.G., Zhao G., Rong C. (eds) Cloud Computing. CloudCom 2009. Lecture Notes in Computer Science*, (5931), Springer, Berlin, Heidelberg.

Pearson, S., and Benameur, A. 2010. "Privacy, security and trust issues arising from cloud computing," *IEEE Second International Conference on Cloud Computing Technology and Science*, pp 693-702, Indianapolis, IN.

Pearson, S. 2011. "Toward Accountability in the Cloud," *IEEE Internet Computing*, (15:4), pp 64-69.

Pearson, S., Catteddu, D., Südholt, M., Molva, R., Fischer-Hübner, S., Millard, C., Lotz, V., Jaatun, M.G., Leenes, R., Rong, C., and Lopez, J. 2012. "Accountability for cloud and other future Internet services," *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings,* Taipei, pp 629-632.

Pearson, S., and Wainwright, N. 2013. "An interdisciplinary approach to accountability for future internet service provision", *International Journal of Trust Management in Computing and Communications*, (1:1), pp 52-72.

Rieger, P., Gewald, H., and Schumacher, B. 2013. "Cloud-computing in banking: Influential factors, benefits and risks from a decision maker's perspective," *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, Illinois.

Ryan, D. M. 2013. "Cloud computing security: The scientific challenge, and a survey of solutions," *The Journal of Systems and Software*, (86), pp 2263-2268.

Ryoo, J., Rizvi, S., Aiken, W., and Kissell, J. 2014. "Cloud security auditing: Challenges and emerging approaches," in *IEEE Security & Privacy,* (12:6), pp 68-74.

Seddona, J.M., and Currie, W.L. 2013. "Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance," *Health Policy and Technology,* (2013:2), pp 229-241.

Sfondrini, N., Motta, G., and You, L. 2015. "Service level agreement (SLA) in public cloud environments: A survey on the current enterprises adoption," *5th International Conference on Information Science and Technology (ICIST)*, pp 181-185, Changsha, China.

Sunya, A., and Schneider, S. 2013. "Cloud services certification: how to address the lack of transparency, trust, and acceptance in cloud services," *Communications of the ACM*, (56:2), pp 33-36.

Takabi, H., Joshi, J.B., and Ahn, G. 2010. "Security and Privacy Challenges in Cloud Computing Environments," in *IEEE Security & Privacy*, (8), pp 24-31.

Yang, Y.T., and Borg, K. 2012. "Regulatory privacy protection for biomedical cloud computing," *Beijing Law Review*, (3), pp 145-151.

Yaraghi, N., and Gopal, R.D. 2018. "The role of HIPAA Omnibus rules in reducing the frequency of medical data breaches: Insights from an empirical study," *The Milbank Quarterly*, (96:1), pp 144-166.

Xiao, Z., and Xiao, Y. 2013. "Security and privacy in cloud computing," in *IEEE Communications Surveys & Tutorials*, (15:2), pp 843-859.