Higher education cloud computing in South Africa: Towards understanding trust and adoption issues

Karl van der Schyff*, Kirstin E.M. Krauss†

*Department of Computer Science, Rhodes University, South Africa
†Department of Information Systems, Rhodes University, South Africa

ABSTRACT

This paper sets out to study the views of key stakeholders on the issue of cloud information security within institutions of Higher Education. A specific focus is on understanding trust and the adoption of cloud computing in context of the unique operational requirements of South African universities. Contributions are made on both a methodological and theoretical level. Methodologically, the study contributes by employing interpretivism and using a data-driven approach to thematic analysis in a topic area often studied quantitatively, thus affording researchers the opportunity to gain the necessary in-depth insight into how key stakeholders view cloud security and trust. A theoretical contribution is made in the form of a trust-centric conceptual framework that illustrates how the qualitative data relates to concepts innate to cloud computing trust and adoption. Both these contributions lend credence to the fact that there is a need to address cloud information security with a specific focus on the contextual elements that surround South African universities. The paper concludes with some considerations for implementing and investigating cloud computing services in Higher Education contexts in South Africa.

KEYWORDS: Cloud computing, higher education, thematic analysis, trust, information security

CATEGORIES: K.3.1

1 INTRODUCTION

Cloud Computing offers users and organizations convenient access to computing without having to understand the intricacies of exactly how processing is performed within the cloud [1]. The National Institute of Standards and Technology (NIST) defines cloud computing as:

> a model for enabling 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 cloud provider interaction. [2]

To utilize Cloud Computing requires users and organizations to trust cloud providers. This subsequently raises issues regarding the security and reliability of the "shared pool of computing resources" [1]. Chen and Sion [3] suggest that these security concerns are the main reasons why organizations are hesitant to adopt cloud computing.

The Data Security Council of India provides evidence to support this claim. In their 2010 survey, 95% of participating organizations agreed that data security and privacy are their greatest concerns when considering a move towards the cloud [4]. Moreover, confidentiality, legal, and contractual concerns are mentioned by Joint, Baker and Eccles [5]. Farrell [6] also states that even with all the information security benefits, cloud adoption is still impeded by perceived information security risks that may potentially face adopting organizations.

It is for these reasons that early adopters are mostly hosting less sensitive data with cloud providers [7] and in most cases opt for a hybrid cloud [4]. In an effort to increase the level of control subscribers have over their sensitive information resources in hybrid clouds, responsibilities are shared between the cloud provider and cloud subscriber. Even so, delegating some responsibilities to a cloud provider requires some form of trust on the part of the cloud subscriber. According to Tian, Lin, and Ni [8], the concept of trust remains one of the greatest cloud adoption stumbling blocks. Unlike in the past, where an implicit form of trust existed between a telecommunications provider and its customers [9], there are today more stakeholders to consider and it is no longer commonplace for telecommunication infrastructures to be owned by a single entity [9]. This complicates the concept of trust mainly because there are more aspects involved [9].

Adoption considerations for Higher Education Institutions are not much different. Universities have had to find creative ways to teach relevant subject material

Email: Karl van der Schyff k.vanderschyff@ru.ac.za, Kirstin E.M. Krauss k.krauss@ru.ac.za

in a cost-effective manner using modern technologies. One approach is to make use of cloud services such as Google Apps for Education[1] and Microsoft's Office 365[2]. Adopting these technologies enables universities to:

> achieve large-scale efficiencies without sacrificing performance. [10]

This also enables universities to reduce the complexity of their systems, affording them the opportunity to effectively deliver services to an increasingly mobile student population [11]; not to mention cost-saving benefits [12]. Although many universities make use of cloud computing, very little research in the interpretive paradigm has been conducted on the topic of trust and cloud adoption. This is amplified by the lack of research within the South African context. As such, this article explores the concept of trust within higher education clouds by analyzing in-depth interviews conducted with key stakeholders from a number of South African Universities. Because of a lack of literature in the topic area, a more inductive (or data-driven) approach is employed to explore cloud adoption concerns in high-education [13] (also see Section 4.2).

The paper is structured as follows. This section provides the reader with some background on the topic of cloud computing, briefly highlighting the lack of research within the South African Higher Education context. The following section provides the reader with a brief literature review and more detail about the study objectives. The methodological approach is then presented, followed by a discussion of a conceptual framework for understanding trust in Higher Education cloud adoption. The article concludes with a summary of findings, recommendations, limitations, and possible areas for future work.

2 BACKGROUND

Over and above the trust and information security challenges mentioned earlier, South African universities also have had to contend with poor telecommunications infrastructure [14] and expensive Internet access [15] in the past. To address these issues the then (in 2003) Department of Arts, Culture, Science and Technology started planning the South African National Research Network (SANReN). They received final government approval for its implementation in 2006, while actual implementation started from 2011 onwards. The main thrust behind SANReN was to enhance the environment in which research is conducted at South African universities, allowing them to participate globally [16]. The implementation of this project was entrusted to the Council for Scientific and Industrial Research's (CSIR) Meraka Institute, who have been assisted by the Tertiary Education and Research Network of South Africa (TENET) in the running of SANReN.

Not all South African universities serve the same purpose, though. In 2010, the Centre for Higher Education Transformation (CHET) issued a report [17] whereby South African universities were grouped into distinct clusters, based on their overall purpose. To accurately ascertain the purpose of each South African university, the following data sources were consulted:

- Higher Education Information Management System (HEMIS) data on staff and students,
- Data on research publications, and
- Financial statements of Higher Education Institutions.

Using the data from these sources, CHET put forward three colour-coded (red, green, and blue) clusters. Five South African universities were categorized as Research Intensive universities (red cluster). It was found that these universities produce the majority of South African postgraduates, have the majority of academics with PhDs, and have a high research output [18].

Universities within the green cluster are classified as comprehensive universities. These nine South African universities exhibited levels of performance which declined after merging with 'historically disadvantaged' tertiary institutions [18].

The remainder of South African universities categorizes in the blue cluster and has relatively low levels of performance in terms of postgraduate success, qualified staff, income, and research outputs. These universities, however, exhibit high levels of enrolment in science, technology, and engineering with a high student versus staff ratio [18]. Moreover, the CHET report [17] emphasizes that these universities provide 'occupation ready' education to a relatively poor student population.

Table 1 indicates each participating university's cluster assignment.

In view of the above, a study focused on such a diverse group of South African universities is needed, since their operational and security contexts will almost certainly differ. This information could then be used by key stakeholders to make informed decisions around the adoption of cloud computing and the information security concerns that could influence this process.

3 STUDY OBJECTIVES

Information security concerns remain a key issue in the adoption of cloud computing in South African universities. This is confirmed by Monfared [19] who states that concerns with regard to the confidentiality, integrity and availability of information have been the main driving force behind slow cloud adoption rates. Pardeep [20] narrows this down by stating that there is a need to understand why consumers (key university stakeholders specifically) do not fully trust cloud computing, both from a business and technological perspective [21].

With the expectation that universities utilize cutting edge technology, and especially since little research is available on the topic, it makes sense to explore (i.e. build authentic understanding of [13]) the views of key stakeholders with regard to cloud information security. To gain the necessary insight, the following research questions are put forward:

[1] `https://www.google.com/edu/higher-education/`
[2] `http://office.microsoft.com/en-za/academic/`

Table 1: Interview details per university

University pseudonym	**# of participants**	**Participant pseudonyms**	**Purpose according to CHET [17]**
A	5	A, B, C, D, E	Research intensive (red cluster)
B	5	F, G, H, J, Z	Comprehensive (green cluster)
C	2	L, M	Research intensive (red cluster)

What are the views of key stakeholders within South African universities with regard to the security of cloud-based information and how does it affect cloud adoption decisions?

This main research question is divided into two sub-questions:

1. What are the views of key stakeholders within South African universities on how cloud computing threats affect the security of cloud-based information?

   The purpose of this question is to understand the views of key stakeholders with regard to cloud-based threats and how key stakeholders evaluate whether or not to adopt the cloud.
2. What are the views of key stakeholders within South African universities with regard to security incidents within a higher education cloud?

   The purpose of this question is to understand how South African universities view security incident response, given the unique operational context of participating universities.

This study aims to gain a deeper understanding of the views of key stakeholders at South African universities with regard to the security of cloud-based data, while a specific emphasis is placed on contextual elements and the implications of SANReN.

4 METHODOLOGY

According to Klein and Myers [22], interpretive research enables a researcher to comprehend how humans think and act within their respective socio-organizational contexts. They argue that interpretivism has the capability of generating a profound comprehension of the phenomena produced in the context of an information system. Walsham further suggests that interpretive research methods are

> aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context. [23]

Interpretive research essentially targets context-specific meanings [24]. It is this focus on the views of key stakeholders as well as their contextual characteristics, situatedness, and the situatedness of knowledge holders (researchers and participants alike), that forms an innate contribution of this study.

The following philosophical foundations are put forward, as derived from Klein and Myers [22]:

Knowledge does not exist separate from the context in which it is used. This applies to the research participant as well as the researcher and thus requires the researchers to reflect on the context of participating universities.

The meaning attributed to a point of view of a participant might change over time and may also differ depending on the position of the research participant or researcher. Knowledge is thus intrinsically situated in context and informed by prior knowledge.

Participant experience and social factors influence the meaning they attribute to concepts explored, as well as views formed during the social engagement or the act of interviewing.

Multiple socially created realities thus exist, and should be explored.

Due to the qualitative nature of this study, a smaller number of participants were selected. This is supported by Patton, who states that

> qualitative inquiry typically focuses in-depth on relatively small samples, even single cases, selected purposefully. [25]

As such only twelve in-depth interviews were conducted with key stakeholders from three South African universities (see Table 1). As suggested by Simons [26], their identities are anonymized. This allowed participants to share more information and assisted the researchers in mitigating any responses that are sensitive or that possibly reveal inadequacies at the institutions.

Participants were sourced from senior IT management (e.g. IT Directors, Systems Managers, IT Managers, Operations Managers, and System Administrators) at the various universities. Although not strictly part of senior IT management, System Administrators were included due to the technical knowledge they possess and the fact they often serve as an interface between the technical team and senior IT management. The primary goal of sampling this way was to ensure that the researcher may elicit relevant and in-depth information integral to each institution's cloud adoption strategy. Potential interviewees were initially contacted by telephone. This afforded the researcher an opportunity to explain the purpose of the interviews and how they relate to the study as a whole. All the interviews were recorded and varied between 45 to 60 minutes each.

Before interviews were conducted, the interview guide was piloted to ensure accuracy and flow. The final interview guide comprised six questions (see Table 2). It is important to note that although these questions investigate a number of topics related to cloud information security, they did not explicitly address the concept of trust. The fact that the issue of trust in cloud adoption so strongly emerged from the

Table 2: Interview questions

Interview question	**Purpose of question**
How do you view the benefits that cloud computing offers your university, taking into consideration the additional threats and potential security incidents it could expose your university to?	This question aims to understand how university stakeholders view this issue and whether or not they agree that it can enhance the services they offer their students. It enquires into whether or not they deem a move towards the cloud as beneficial to their day-to-day running (administratively) of the university. In a survey conducted by Appirio [27], 28% of cloud adopters cite security as the biggest misconception with regard to cloud adoption, which may or may not be echoed by key stakeholders within higher education. Additionally authors such as Erenben [28] state that the use of the cloud could enhance security, thus forming part of the benefits of cloud computing.
Some individuals have described cloud computing as a security nightmare, so much so that it can't be handled in traditional ways. In your opinion, how does the openness of most university networks affect threat mitigation techniques and/or technologies within a university cloud infrastructure?	The purpose of this question is to find out if key stakeholders think threat mitigation can be applied in traditional ways, or whether the cloud indeed require special treatment with regard to threat mitigation and information security. In essence this question investigates the participant's views on the traditional way of dealing with threats that compromise information security and whether or not this is applicable to the cloud. For example, the Ponemon Institute found that IT practitioners don't believe that their organization is capable of securing data and applications within the cloud [29]. Responses to this question might confirm that universities also fall into this category.
In your university what role do you think cloud computing threats play with regard to cloud information security, specifically the confidentiality, integrity and availability of information?	The purpose of this question is to understand how the participant thinks about cloud computing threats and the relationship between these threats and information security. Do their views align with literature and to which extent? Also, do participants attach as much importance to threats, and the management thereof, as the participants of the study conducted by the Data Security Council of India [4]. Responses to this question might also uncover additional concerns over and above the others mentioned, fostering further conversation around this theme.
How does your university currently respond to security incidents?	The Cloud Security Alliance [30], the SANS Institute [31], as well as Grobauer and Schreck [32] mention that both the cloud provider and customer should be in agreement as to how security incidents in the cloud should be handled and who will be responsible for which aspect of the security incident response process. The purpose here is to ascertain whether or not key stakeholders do indeed share this point of view and to what extent. It also endeavours to uncover whether or not South African universities have security incident response plans in place. If they do, a comparison could be made with what is suggested by the authors in the literature mentioned above. From a higher education perspective there may be additional factors to consider.
How do you think the transparency of cloud provider operations would influence the cloud adoption process within your university?	The purpose of this question is to understand whether or not participants from institutions of higher education perceive cloud provider transparency as a good method for accelerating cloud adoption or not. This question is also aimed at probing their views on the adoption process, but it is equally applicable to security incident response as well as threats and threat mitigation. In essence this question sets out to investigate whether or not transparency in terms of threat mitigation, threats (realised or unrealised), breaches, and security incident responses are of concern to universities and how it ultimately affects the adoption process itself.
In your opinion, what are the major cloud adoption stumbling blocks in your institution?	Authors cite security as one of the top adoption stumbling blocks [4], [27], [29], [33]. This question aims to find out if the participant agrees with these findings and whether there other more prominent adoption stumbling blocks from a higher education perspective. Responses to this question might also afford the researchers the opportunity to obtain a deep understanding of all the concerns that affect adoption within South African universities.

interview data underpins its importance and subsequently emphasizes the relevance of this contribution. Each of these questions covered a particular theme and naturally became a point of departure for discussion.

4.1 Thematic analysis

Once transcribed, the interview data was analyzed using thematic analysis as outlined by Braun and Clarke [34]. Thematic analysis allowed the researchers to rigorously identify, analyze, and report on patterns or themes within qualitative data. To accurately identify thematic patterns, Braun and Clarke suggest a six-phased approach.

During the execution of Phase One, they suggest that the researcher become acquainted with the data collected. The first author, therefore, personally transcribed all of the interviews, making sure to read and re-read the transcripts during the process of analysis. This assisted in the process of generating meaning from the data. Although this process is usually taken as a mere requirement in order to perform follow-up analysis, the authors believe that the nature of the problem demanded more than just transcribing the actual words of the interviews.

Initial codes pertaining to 'interesting aspects' of the primary data were created during the execution of Phase Two. Guided by the themes addressed in the interview questions (Table 2), an initial coding framework was created [35] for the entire data corpus (Table 3 contains an example). The reader will note that Table 4 contains multiple data extracts associated with a single code. This is the result of grouping sets of data extracts associated with a specific code. Using the coding framework produced in Phase Two (Tables 3 and 4), the researchers were able to identify several candidate (preliminary or unrefined) themes (Table 5 gives examples), which together with an initial thematic map formed the deliverables of Phase Three. Due to the interpretive nature of this study only latent themes were identified.

It is important to note that Braun and Clarke [34] suggest that no candidate themes be eliminated during this phase, since themes which appear to be irrelevant may be merged with other themes during Phase Four. As such Phase Four was mostly concerned with the refinement of these candidate themes (Table 6). This process was characterized by either identifying new themes, merging themes, or eliminating themes altogether.

The end of Phase Four resulted in a final coding framework spanning the entire data corpus followed by a process of further refinement in Phase Five. This process of further refinement differed from Phase Four in the sense that the themes were now defined by providing a persistent narration (i.e., the findings) created from all of the collated data extracts within each theme (as contained in the coding framework in Table 6), thus illustrating interpretive rigor [36]. In addition to the narrative, a final thematic map (Figure 1) was constructed from the refined themes created during Phase Four and Five. It was during the final phase that the detailed analysis and interpretation of each theme within the framework of the final thematic map took place.

Although multiple themes are illustrated by the final thematic map, the following section only addresses the themes related to the concept of trust.

4.2 Process of analysis

Of all the themes identified during the process of thematic analysis, only those pertaining to cloud computing trust were subjected to further interpretation, resulting in the creation of a narrative centred around this main theme (see Figure 1 and Section 6). Although Braun and Clarke make a clear distinction between theory and data-driven analysis, the researchers found that the quality of analysis increased substantially when these two approaches were used in a complimentary fashion (see also Fereday and Muir-Cochrane [36] and Schutz [13], [37], [38]). In fact, Braun and Clarke specifically state that 'data are not coded in an epistemological vacuum' [34].

This became even more evident after transcribing and reading through the first few interviews. The researchers, however, employed a more data-driven approach during the initial phases of analysis.

In this study a data-driven approach implies that the researchers allowed the themes to emerge primarily from data, as opposed to using a theoretical framework upfront to seek out predetermined themes from data. During the initial phases of data collection, the researchers relied on subjective, situated knowledge (or contextual data) to inductively construct themes [39]. This adds to the paper's relevance, because 'induction promises to generate an authentic account of localized events' [39].

After the identification of relevant themes from the raw data, the researchers were able to relate some of this back to literature. Ketokivi and Mantere [40] equates such inductive research as a means to "amplify" existing knowledge, adding further relevance to the inductive nature of this study. Together these inductive-based contributions made it possible for the authors to contextualise the data, resulting in the extraction of themes absent from the literature as well as the interview questions.

This hermeneutic cycle [22], [41] was employed throughout all six phases of analysis, with a strong focus on the identification of latent as opposed to semantic themes. In addition to the methodology described earlier, details constituting the actual process of analysis are provided below.

As stated earlier, Phase One was seen as an important part of the analysis process, because it formed the foundation of all the analysis work and afforded the researchers the opportunity to become acquainted with the data. Transcribing all the interviews personally, aided in this familiarisation process. It is during this phase that the researchers made an initial list of relevant concepts that may form part of possible themes. This in turn assisted in the execution of Phase Two, since at least some initial analysis had been performed.

Table 3: Data extracts coded multiple times

Data extract	**Code**	**Transcript line ref.**
The major thing as far as our lot is concerned is connectivity and that's the thing we suffer from the most. Getting disconnected. And that's kind of foremost in our minds about if we're not connected then we can't work we'd rather have it here and when the connection does go down at least we can get on with what we are doing.	Concerned about connectivity to cloud Prefers data to be hosted locally	114–119
A lot of people see [the] cloud as something they don't use. I would not even just talk about the security threats etc—but take it from the most basic. Let's understand cloud computing then work through the security issues etc—I think there is a lot of hype. Unnecessary hype in terms of the security. I think we are [there] are so many other things we are making a mountain out of a mole hill.	Understanding cloud first then security Cloud security surrounded in hype	521–527
Yes and the reason being I want to know, because it firstly would be a test in terms of how they react to things. The fact that it didn't affect me would be a good sign. So it's part of understanding how they react in terms of when they're at risk. Secondly if there's consistent breach I would possibly want to change my service provider.	Cloud providers should disclose Insight into their incident response practices Constant breach prompts change	636–641

The execution of Phase Two required coding the entire data corpus, which resulted in a coding framework containing information beyond the core concepts of this paper. This process involved analysing each interview transcript bearing in mind the list that was created in Phase One. Initial coding was more data than theory driven so as to not miss any information that might be of interest later. This involved creating codes for specific data extracts. According to Phase Two, data extracts may be coded multiple times. This is illustrated with examples in Table 3, where column two contains multiple codes for the data extract in column one. The third column in Table 3 allowed for easy navigation of each participant's transcript.

Some of the codes could also be associated with more than one data extract, which is illustrated in Table 4. In Table 4 the first row contains an example of three data extracts that are associated with one code (in column two). During the execution of Phase Two the researchers were cautious not to interpret the data extracts, but to rather create a coding framework based on that which was actually said.

In Phase Three the researchers identified candidate themes and associated sub-themes from the coded data extracts. An extract of one such candidate theme (and sub-themes) is given in Table 5. The alphabetic character (in column three) is used to identify the participant where the code originated from and to aid further analysis. Using this form of data organization became especially useful during Phase Four where the candidate themes had to be refined and their associated data extracts collated. Care was taken not to eliminate any themes at this stage, but to rather form as many candidate themes as possible.

Phase Four consisted of a dual process whereby the candidate themes were refined on two levels. Firstly, the collated data extracts had to undergo scrutiny as to whether or not they tied into the candidate themes with which they were associated. Once complete, evaluating the themes across the entire data set took place. This ensured that the identified themes were valid in relation to the data set as a whole and that it captured the meanings as they were portrayed by the participants. This two-step process resulted in some themes being eliminated, renamed or merged with other candidate themes. An extract of one such theme, together with the data extracts collated under it, is illustrated in Table 6.

After reading the entire data corpus researchers used the output of Phase Four (refined themes) to construct the final thematic map (Figure 1). As suggested by Braun and Clarke [34] these themes were organized so that they do not overlap, which is illustrated by the fact that there is no association between the two main themes ("Trust in Cloud" and "Views as Subscribers").

As the primary output of Phase Five, it was the final thematic map (Figure 1) which enabled the researcher to interpret the data extracts associated with these themes. Phase Six concluded the process of analysis, resulting in the creation of a narrative based on the researcher's interpretations of the identified themes and the data extracts associated with them, the context within which these data extracts were embedded, and each university's unique operational and security context.

Table 4: Data extracts classified under the same code

Data extract	**Code**	**Transcript line ref.**
The availability of Internet bandwidth is of major concern. The only concern that has ever been raised is what happens when the Internet goes down, which astounds me. The availability of Internet bandwidth was a big thing. It has not fallen off the radar.	Availability concerns	37, 211–212, 858–859
combine your knowledge, combine your skills, combine your understanding, and then come with recommendation[s]. Whereas [an] individual institution, you might feel isolated, you might be scared even financially is it the right way to go? Why do you have to recreate, at each institution re-establish, redevelop, you know, why do you have to have your skill . . . you can't have one institution have the complete skill set to serve all the needs on campus. We know that's the truth. So what do we do? Rather combine those strengths.	Advantages in community cloud	171–175, 218–221

Table 5: Data extracts classified under the same code

Candidate theme	**Sub-themes**	**Code** [associated participants]
Knowledge of cloud security	Mitigation in the cloud Threats in the cloud Cloud security awareness	Knowledge of contract with cloud provider [E] First understanding the cloud then security [A] Knowledge of mitigation from experience [D]

Table 6: Refined theme with collated data extracts

Refined theme	**Data extracts** [associated participants]
Security by assumption	For instance it's reasonably easy to assume that [Provider A] takes security fairly seriously. [E] between [System B] and [University A] is a stipulation that they do two backups. So yes those backups are run and they are then . . . I think one is on campus and I think the other one is off campus. I'm not sure, but I trust them. [A] You have to be transparent, because people assume all sorts of amazing things of what's going on. So unless you're upfront of what you do and what you don't, particularly what you don't do. People assume their data is always backed up and you have to [be] upfront?[D] I wasn't part of that evaluation process; obviously security must have been. [L] I think fair use and abuse and those sort of things are highlighted or the understanding is that [Provider F] endeavours, because they [are] offering a service, they endeavour to do everything in their power you know to make sure that that's not being abused or open. [G]

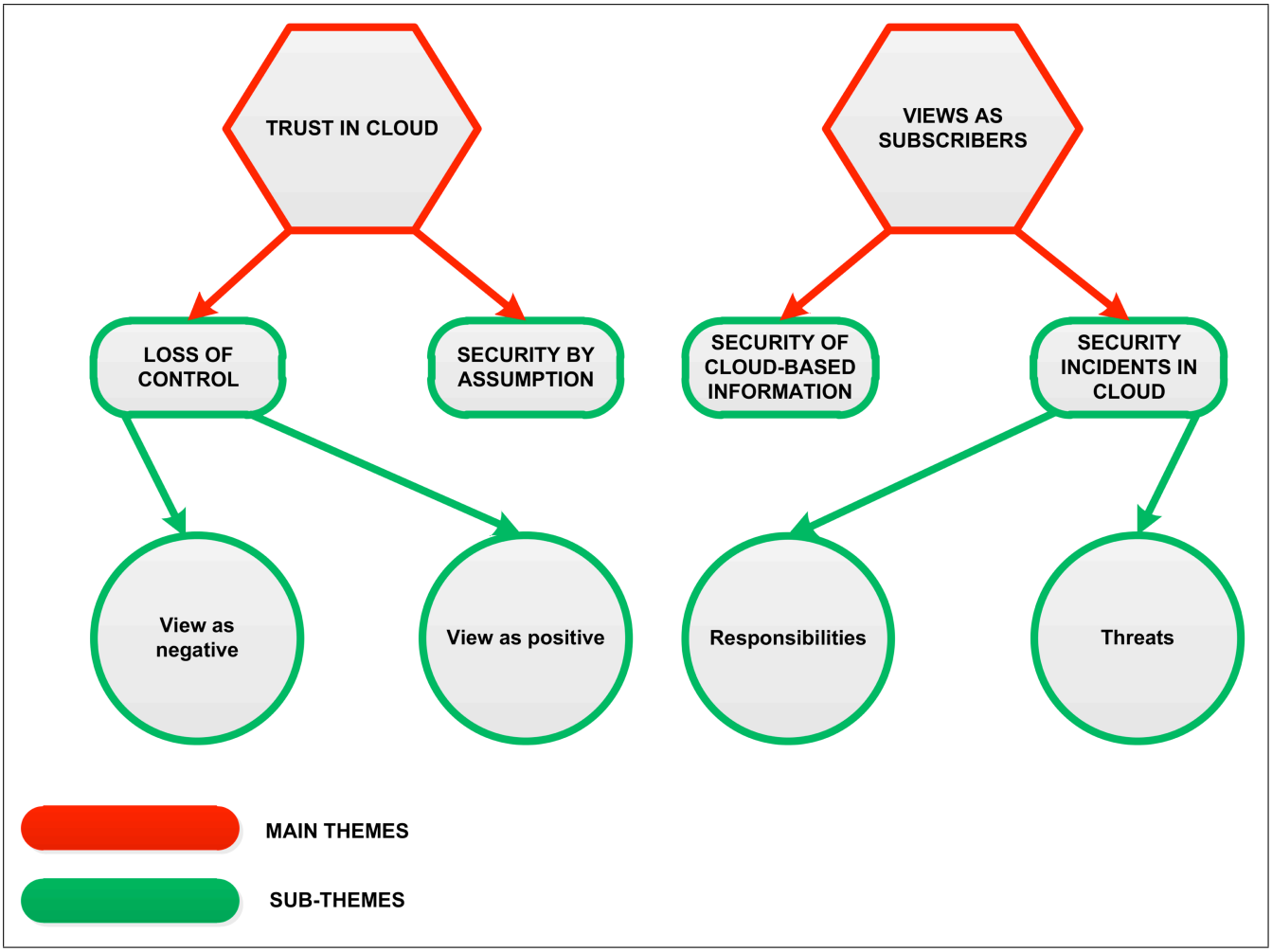

Figure 1: Final thematic map

5 CONTEXTUAL FINDINGS

As stated earlier, this study's primary focus is to conduct research within the context of South African universities. For this reason some contextual information about the universities, listed in Table 1, is required. This not only provides the reader with additional background information, but more importantly the contextual lens needed to interpret the identified themes.

5.1 University A

As one of the smaller research intensive universities in South Africa, participants from University A expressed mature thoughts on cloud security. Using the cloud for more than just one system, make their views even more compelling. During the interview process it became apparent that the university's mature views may not only be the result of meticulous planning, but also that they act as a cloud provider; not only to its own staff and students, but also to other universities in its region. Most of the participants involved in the process of adopting the cloud had very clear and well-defined ideas on what would be required to make their cloud implementations safe and secure, and cloud operations feasible.

With University A still evaluating some components of their public cloud solution, adoption has only partially been completed. From the interview data some of the reasons for this include:

- Immature information policy with regard to information hosted in the cloud,
- Lack of procedures regarding emergency access to institutional information in the cloud, and
- To a lesser degree, the lack of availability and resiliency of Internet connectivity.

This does not preclude some unique views on the security of cloud-based information, which the researchers could attribute to the differing backgrounds of each participant. From the interviews it was also clear that SANReN will have an effect on the future of cloud adoption within this university, but that it was too soon to know what exactly this effect will be. This is mostly due to the fact that they have only recently (in October 2012) attained a high speed connection to SANReN. The participants do not consider that the university's somewhat isolated location makes a substantial difference to cloud security or adoption.

5.2 University B

University B has one of the larger user populations and is spread across six geographically dispersed campuses.

They have been making use of public cloud computing for quite some time. This together with the fact that they employ a dedicated information security officer makes for some interesting views on cloud information security. Regardless of any security concerns that may have existed, they still decided to go ahead and adopt the cloud; albeit only for a subset of their user population. This seems to have been a financial decision, since the sheer cost of providing the same features as the cloud provider would have been too great, as stated by Participant G:

> Now obviously the benefits outweigh the security concerns at the time we went over, because the infrastructure cost to house the students [email] at that point in time I think really outweighed security concerns.

However, from the interview data it is clear that they do not intend to adopt the cloud wholesale, especially not for core university systems. There is therefore no positive relationship between their experience in using cloud services and their willingness to host core services in the cloud. From the data collected in this context, reasons for this include:

- Having prioritized the university's data in accordance with its relative importance. For example, University B did not deem the data currently hosted in the cloud to be mission-critical, hence their hosting it in the cloud. Their Enterprise Resource Planning (ERP) systems on the other hand are mission critical and therefore not hosted in the cloud.
- Mistrust of cloud providers. University B decided not to host mission-critical information in the cloud, which indicates their reluctance to trust the cloud provider,
- Issues relating to local versus international bandwidth. Even with the arrival of SANReN, University B still had some doubts about the stability and quality of the bandwidth they currently have access to, especially when experiencing connectivity issues related to cable faults,
- The importance of the geographic location of cloud-based data. This reason hinges on various legal concerns the participants have on the security of cloud-based information, and
- Experiential knowledge gained from using their current cloud computing solution.

It is also worth noting that although they are cloud subscribers to a system provided by University A, none of the participants viewed it as such. This may be that their definition of a cloud differs from the participants at University A. Unlike University A, University B is classified as a comprehensive university by CHET [17]. It has also been connected to SANReN for quite some time with many of the participants viewing a high speed Internet connection as a major cloud enabler [42], one without which they would probably not have adopted their current cloud solution.

5.3 University C

University C, a research intensive university, has a substantial number of staff and students spread across four campuses. The university also offers a wide range of graduate and postgraduate programs. Interview participants mentioned a wide variety of cloud adoption stumbling blocks. This seems to indicate that they have thoroughly assessed the cloud. According to them, adoption stumbling blocks include:

- Concerns surrounding continued access to institutional information hosted in the cloud,
- Uncertainty around the financial implications of using the cloud,
- Job security for IT staff,
- Quality of access to cloud-based information, and
- An IT department who believes that they should provide all the required services in-house.

Connectivity to SANReN is seen as a positive driving force towards cloud adoption. Participants also have a strong belief that South African universities should work together. Participants hinted that such collaborative work could include participating in a community cloud built specifically for South African universities. As far as the major proponents of cloud adoption are concerned, University C's participants had very diverse answers and therefore yield somewhat inconclusive findings.

6 THE NARRATIVE

In the previous section, the researchers highlighted some contextual differences between the participating universities. In the following sections a narrative is presented and a conceptual framework discussed as it pertains to the issue of trust in adopting cloud computing in higher education. Other aspects of the thematic map, not related to trust per se, will be scrutinized in future work by the authors.

6.1 Trust as a concept

During further analysis of the illustrated themes in Figure 1, several related concepts emerged. This prompted the creation of two conceptual frameworks, one for each of the main themes. Used in combination, these conceptual frameworks and the final thematic map guided the interpretation process.

The conceptual framework in Figure 2 was construed from the interpretations of the main theme, namely "Trust in Cloud". This will not only assist the reader in understanding how the concepts are related, but importantly, why they are related.

The inductive (data-driven) nature [34] of how this main theme was generated resulted in few references made to the literature during interpretation. Findings may therefore be scrutinised in follow-up research. However, as indicated earlier, despite the fact that the term "Trust" was not explicitly used in any of the interview questions, it still emerged as a central theme. This makes for an important consideration and cloud adoption factor.

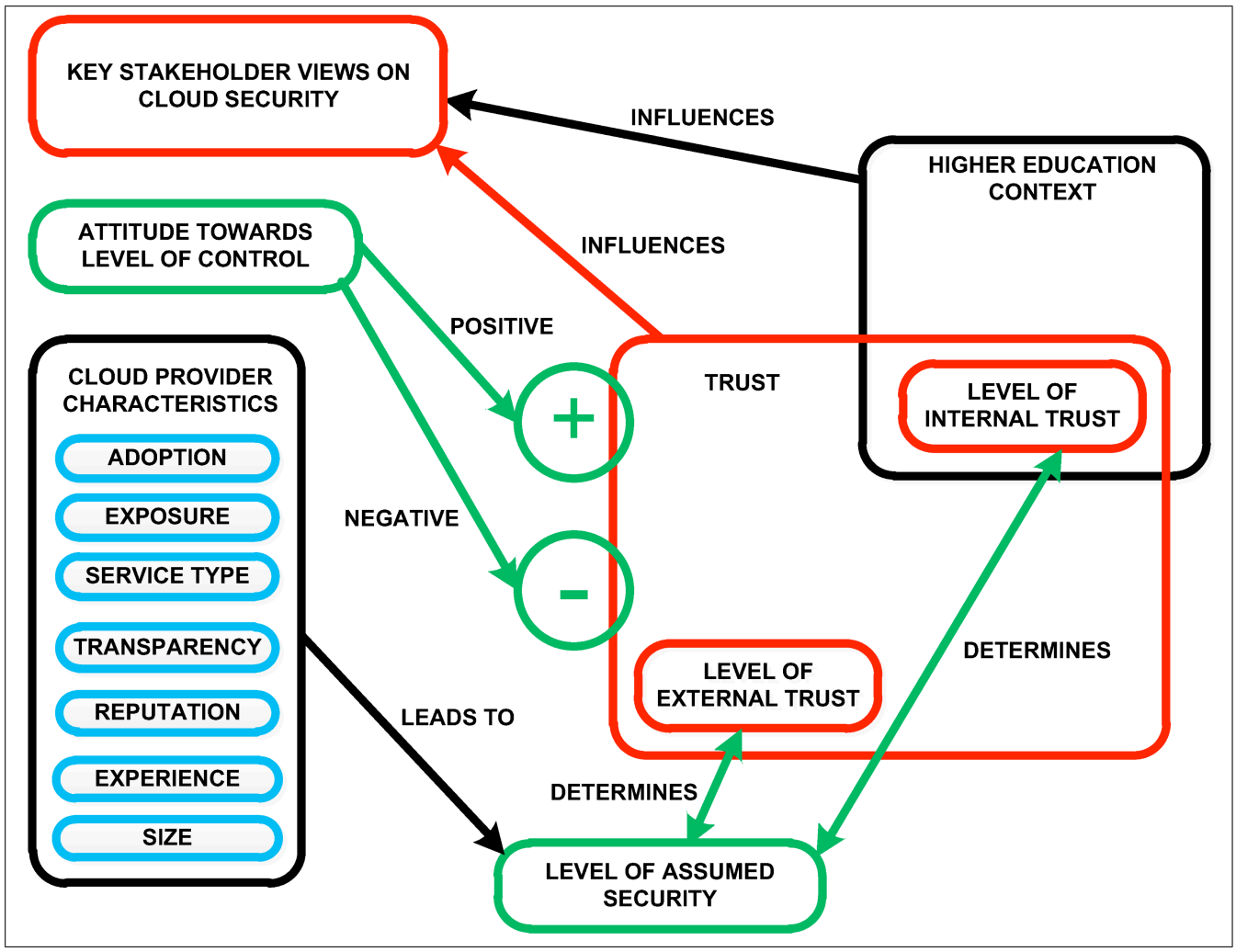

Figure 2: Final thematic map

6.2 Security by assumption

One of the more prominent sub-themes, 'Security by Assumption', emerged because many of the participants assumed that information security is a priority for cloud providers. Participants appeared to assume information security was considered during the evaluation of the cloud solutions, a process assumed to be internal to most organizations. The following statement by Participant L, from University C, demonstrates this:

> I wasn't part of that evaluation process; obviously security must have been.

There are three noteworthy aspects here. The first is the fact that a department who is considering migrating to the cloud should involve all senior members of staff, especially key stakeholders with a technical background in the decision process. From the statement above it seems that this is not the case with University C. Secondly it would seem that unfounded assumptions about security are also evident at the level of the evaluating committee, meaning that decisions are made in silos and not communicated adequately amongst parties with a vested interest in the adoption process. Thirdly, with University C being classified as a research intensive university, it sheds some light on assumptions that are made about the knowledge of postgraduates and academics with regard to cloud security. Currently it seems that the university does not investigate what their users know and do not know about cloud security.

Interpretation of these assumptions of participants leads to the following inferences:

- Insufficient internal communication takes place between the evaluators of the varying cloud solutions and the future users of the cloud solution,
- Participants implicitly trust the evaluating committees' judgment in this regard, and/or
- This university expects its postgraduates and academics to be aware of cloud security, so much so that the evaluation process does not adequately cover security of cloud-based information.

To participants from University A, the concept of 'Security by Assumption' took on a more pronounced form, with most of the participants discussing some aspect of this sub-theme. The researchers conclude that this could very well be because they have been successfully providing this service for such a long time (at least five years). This has instilled confidence in most of the key stakeholders. This in turn affects their levels of trust as a cloud subscriber. In essence the confidence and experience gained from providing cloud infrastructure

has positively influenced their views on the subject of cloud security and trust. In Figure 2 this sub-theme is illustrated by the concept 'Level of Assumed Security', where the relationships between it and internal as well as external trust is depicted. These relationships are bi-directional in nature mainly because the interview data indicated that the levels of trust also had an effect on the assumptions participants have with regard to cloud security.

With University B having used their cloud solution for quite some time (approximately 3 years), their focus is operational in nature and not necessarily on issues of security. This seems to stem from the fact that key stakeholders received official support from senior management and that this is the 'correct' cloud solution to pursue. In fact, more than one participant from University B confirmed that the major driving forces behind their cloud adoption strategy were directives from senior IT management.

Assumptions made about service providers reflect this operational-centric view of the cloud. Although no real auditing is provided by their service provider, the assumption is still there that the said provider takes information security seriously. This is confirmed in the following statement by Participant G:

> I think fair use and abuse and those sort of things are highlighted or the understanding is that [Provider F] endeavours, because they [are] offering a service, they endeavour to do everything in their power you know to make sure that that's not being abused or open.

The absence of issues directly related to cloud provider trust, and the fact that participants from University B have not experienced any known cloud related incidents, makes it apparent that the use of their cloud solution has had a positive effect on their views of cloud security. Another factor which could explain the positive attitude towards trust could be that they have a post dedicated to information security. The presence of this person could be interpreted as a form of internal trust.

For University A, this has been more pronounced. Their steering committee did not have any major information security concerns regarding cloud adoption. The following statement from Participant E captures the essence of this:

> the only concern that has ever been raised is what happens when the Internet goes down, which astounds me.

From this the researchers infer that there is not only a level of trust between the steering committee and the architects of the proposed cloud solution, but also a general lack of awareness regarding information security. This exhibits an even deeper level of trust on a wider scale. Not only are the subscribers or users of this system trusting the architects (internal key stakeholders in this instance), but in doing so there is an implicit trust relationship between the users and the cloud provider. From a user perspective Participant D had this to say:

> there's elements of trust and the idea of a pre-packaged solution like [System Y] ... it's a sort of thing that out there it's working and basically when was the last time I worried whether my private personal [System Z] stuff was backed up or not.

As such the concepts 'Internal Trust' and 'External Trust' are depicted as components of the core concept, namely 'Trust'. In the context of this study these components ('Internal Trust' and 'External Trust') encapsulate where the 'trusted' party resides from the perspective of either the key stakeholders or the participating universities. As such, the term 'Internal Trust' refers to trusted parties within the university itself. On the other hand the term 'External Trust' refers to trusted parties residing outside the participating university's operational context. The overlap between trust and the concept of 'Higher Education Context' is indicative of the varying contextual factors upon which internal trust is based.

The concept of trust does not only apply to general aspects of information security, but also to some very specific areas (see Figure 2). Many of the participants were able to articulate exactly where trust factors in into cloud information security. Participants in managerial positions mentioned aspects reflecting their operational context, which was not technology or vendor specific. Participants with a technical background made more references to the actual mechanics of information security, although not as in-depth as expected.

Other than internal trust the specific areas addressed by the concept of trust more often than not, involved factors external to the participating universities. These areas of external trust include:

Trusting cloud providers' Application Programming Interfaces (APIs). This was one of the few instances where a participant made reference to an area of concern mentioned in the literature. The literature specifically mentions that the existence of insecure APIs [43] should be seen as a threat. If on the one hand subscribers trust providers to supply them with secure APIs, it becomes plausible that subscribers inadvertently use this form of external trust as a means of threat mitigation, possibly without even thinking of it as such.

Physical access to the cloud provider's infrastructure. With regard to physical security, Participant C (from University A) stated that it is fair to assume that the same rules and regulations are in place at the provider as is on their site. The existence of any additional threats is accepted at face value and only experience will be able to confirm whether or not these assumptions were indeed incorrect.

Trusting cloud provider backups. Participant A specifically mentions that there is no certainty as to whether the cloud-based data is backed up. This does not deter this participant from assuming that it is being done and relates directly to what

is specified in the service level agreement between a university and their cloud provider/s.

So, over and above the external trust relationships between the cloud provider and subscriber, there are other more intricate trust relationships internal to University A. Interpretation of the interview data lead the researchers to infer that these trust relationships are based on assumptions when the following holds true of cloud providers:

1. The cloud provider has a good reputation;
2. The cloud provider is considered to be of substantial size;
3. Subscribers (key stakeholders) view them as experienced and mature;
4. They have acceptable levels of transparency;
5. Levels of exposure from the institutions' (as subscribers) perspective lends itself to such an assumption;
6. Their services are not free; and/or
7. Their services have already officially been adopted.

Some of these core criteria are depicted in Figure 2 under the concept "Cloud Provider Characteristics". From the interview data they seem to be the initial reasons why key stakeholders assume security, hence the relationship with "Level of Assumed Security" in Figure 2. The operational context of University B, as well as their choice in provider, corroborates the first five criteria on the aforementioned list. In their case the fifth criterion does not apply, since their cloud provider offers them their service free of charge.

As mentioned earlier, University B also has a post dedicated to information security. This would allow them to make informed decisions about some of these criteria, especially those criteria which require specific industry exposure. It is more likely that the incumbent of such a post would have regular contact with other information security professionals, allowing him or her to base their decisions on an even larger knowledge base. This can be seen as yet another form of internal trust, which may or may not be unfounded.

For University C, the list of criteria is less operational and more preparatory in nature, since they are evaluating the cloud at this stage. With some of the participants stating that they were supposed to have implemented their cloud solution already, the researchers infer that this could very well be related to the cost of Internet access. From this perspective University C is unique in the sense that Internet access or data is not supplied to students free of charge. So, it is plausible that the above criteria do not play such a large role as with the other two universities.

The operational context of University A is a mixture, in that they are evaluating and using the cloud, albeit for different systems. Their experience as a cloud provider also adds credence to the views of the participants from University A, since these views are based on external trust, internal trust, and being trusted by the other members of the community cloud. The participants from University A mentioned the concept of trust the most. The researchers believe this can be attributed to their mixed approach to cloud computing. This mixed approach is not only defined by their use of different clouds for different systems, or evaluating the cloud versus adopting the cloud, but also the use of free services as well as services charged for.

Another factor that distinguishes University A from the other universities is the sensitivity of the data that has been hosted by cloud providers. In this instance University A hosts most of their sensitive data with providers who charge for their services. This leads the researchers to infer that key stakeholders make more assumptions about the concept of trust and information security when they have to pay for a cloud service. This is depicted in Figure 2 as the term "Service Type", which forms part of the cloud provider characteristics that lead key stakeholders to assume security and accountability.

There is also an expectation that these cloud providers are more likely to be transparent, especially with regard to information security. In general it would seem that if a cloud provider satisfies a number of the aforementioned criteria, key stakeholders assume that their information is secure. Given enough time this develops into a sense of trust in the cloud provider.

A further factor is whether or not a cloud service has been officially adopted. Universities who have officially adopted the cloud tend to have a positive outlook on the security of their cloud-based information. This is especially true of University B who has officially adopted the cloud for some services. From the interview data of University B the researchers infer that, because their cloud solution and operational context satisfies some of the criteria listed above (specifically, criteria 2–5 and 7), their positive views on cloud adoption have allowed them to assume that their information is secure. This in turn leads to a sense of trust in their cloud provider.

All of the concepts that make up the sub-theme of trust have been illustrated in Figure 2. A number of cloud provider characteristics are also depicted, including how they relate to the idea of assumed security. Given enough time (i.e., allowing for post cloud adoption views), university stakeholders develop a sense of trust in the cloud provider, which influences their views on the security of cloud-based information. Context also influences key stakeholder views, hence the relationship between the concepts "Higher Education Context" and "Key Stakeholder Views on Cloud Security".

6.3 Loss of control

During the phases of analysis it became evident that participants viewed the loss of control over cloud infrastructure and services as either negative or positive. For this reason, control from the participant's perspective, has strong connotations to the concept of trust. This is illustrated in Figure 2 where the level of trust (internal or external) is either increased or decreased depending on whether or not the participant had a negative or positive view (attitude) of the levels of control they have in their respective clouds. Several data extracts

confirmed this. From these extracts three specific areas of control emerged.

The first is the level of control pertaining to cloud-based data. Participant A's views the loss of control over cloud-based data in a positive manner. According to this participant, they (University A) never lose control over their data. This is attributed to the fact that they have backups.

> between [System B] and [University A] is a stipulation that they do two backups, so yes those backups are run and they are then ... I think one is on campus and I think the other one is off campus. I'm not sure, but I trust them.

Literature makes specific mention of backups [43], [44], [45] as a means of protecting an organization from data loss or corruption. This is seen as a form of mitigation. It is further suggested that backups be controlled contractually, which is true for the example above. This translates to trust on an external and internal level. It is external in the sense that there is an assumption that the provider makes backups and therefore controls the security of backups. On the other hand, it is internal in the sense that the participant trusts other internal university key stakeholders who entered into the agreement. This form of internal trust would encapsulate whether or not these internal cloud evaluators performed with due diligence, and assuming also that there was an evaluation process. Thus, as long as there is an agreement in place through which this university can control its cloud-based data (e.g., backups), the levels of internal and external trust increases. This in turn leads to assumptions by the cloud subscriber with regards to the effects of loss of control. In this instance it pertains to the security of their cloud-based information.

A second area is about 'criteria' for cloud provider selection and assessing the impact of loss of control over cloud-based services. Participant M (University C) stated that control or the loss thereof is not a concern, since there are ways of judging the levels of security of cloud services. These include:

1. Choosing a provider that matches your requirements,
2. Assurances from providers as to the levels of service and security they offer, and
3. Choosing vendors who understand the industry.

However, with University C currently evaluating the cloud, it can be inferred that their level of experience with regard to the aforementioned criteria would be limited.

Although the second and third items above could result in an adequate assessment of control risks, cloud subscribers also rely on a level of cloud provider transparency. This in turn is interpreted as having a positive effect on trust.

The concept of internal trust within the context of information security takes on a different meaning for some participants at University C. Research output is seen as the most valuable information asset and yet it is believed to be unprotected, as stated here:

> that stuff [research] is the most unprotected of the lot.

Here an assumption is made about the insecurity of the cloud-based data. With some of the institutional data already in the cloud, these judgments become personal at the user level, since the products mentioned in the following statement are consumer based:

> you find that much of your research information is actually sitting out there synced to [System I] and [System K] and [System J]

In this example the choice of cloud provider is done at the user level and not at an institutional level. This in turn requires internal trust, i.e. the university trusts the judgments of its internal users (such as students and academics) in their use of cloud services.

The third area of control is also cloud provider based. From an operational perspective, participants from University B view the loss of control over their cloud (internet downtime in this case) as a negative issue, so much so that the cloud is not being considered for staff members. The fact that they have yet to encounter any serious issues with their current implementation makes this a noteworthy point of view, since the lack of incidents in itself should bolster their levels of cloud provider trust.

From several of the interviews conducted at University B it was clear that the physical location of data is also a concern. Cloud subscriber bandwidth was a major concern for participants with a technical background.

Participants within a managerial role view legal concerns as a key issue. Both cloud subscriber bandwidth and legal concerns are directly affected by the physical location of cloud-based data. Within the context of University B it is possible that it does become a concern with time (i.e., with experience). Thus, the fact that cloud providers have control over specific aspects of a cloud infrastructure should make participants view the loss of control as a negative. However, Participant G had the following to say in this regard:

> It's not that they don't trust you. It's something they control across the whole platform of services. They don't want you to damage this or break this component of [System H].

This statement may imply that Participant G views the loss of control as a means of protection, which cloud providers employ to protect them from cloud subscribers. Here the loss of control, as a function of trust, is seen as a positive. The fact that Participant G does not view this as a form of mistrust on the part of the provider, could be explained by this participant's strong technical background.

The concept of control is depicted on the new conceptual framework as an attitude that a key stakeholder has towards the amount of control they have over their cloud infrastructure. If they have a positive attitude they trust the provider more, whereas a negative attitude detracts from the amount of trust key stakeholders place in cloud providers. In most cases participants viewed the loss of control in such a way

that it resulted in a decrease in the level of trust in the cloud provider.

As a main theme, 'Cloud Provider Trust' is influenced, as demonstrated, by subscribers assuming some level of security based on their presuppositions and their attitude towards loss of control. This in turn affects the views that key stakeholders have on the issue of cloud security.

7 CONCLUSIONS

In the previous sections the researchers presented the views of key stakeholders at three South African universities (two research intensive universities and a comprehensive university) regarding cloud information security and the issue of trust as an adoption factor. Some contextual differences between the various universities and their participants were highlighted. Through interpretivist research and following a more data-driven approach (i.e., inductive reasoning) to thematic analysis, two prominent sub-themes associated with trust as an adoption factor, emerged from the data, namely, 'Security by Assumption' and 'Loss of Control'.

The paper demonstrates the importance of trust as a cloud computing adoption factor in Higher Education. Subsequently, a trust-centric conceptual framework is put forward for understanding and evaluating cloud computing adoption in Higher Education contexts. The authors have shown that the purpose of a university does not necessarily allow for any generalizations to be made; that trust in cloud security can be viewed as either internal or external to the university; that stakeholders often make judgements about whether cloud services can be trusted based on unfounded assumptions about cloud security and how cloud security is evaluated; and that there are differing (negative and/or positive) views associated with the loss of control of cloud-based data.

The inductive nature of the work has specific benefits in terms of relevance. It offers an authentic account of locally contextualized events [39] and a knowledge construction approach that can amplify existing knowledge on trust and adoption issues in higher-education. Although this study is limited to a small number of participating universities as well as being averse to specific cloud technologies and vendors, it still provides future researchers with a framework, concepts, and recommendations (next section) for further work. It is anticipated that further work would uncover even more detailed concepts which could either directly or indirectly affect cloud adoption.

Further limitations include that this study only focused on IT professionals within two types of South African universities and did not include any participants from academia. Views expressed in this study should therefore be seen in an operational light, with few considerations on the challenges faced by academic departments themselves. The context-sensitive nature of this study also limits the generalizability of its results to other situations.

8 RECOMMENDATIONS

Based on the findings, the authors put forward a number of considerations for implementing and investigating cloud computing services in Higher Education contexts, specifically in South Africa.

The first consideration is to adequately engage with the prospective users of the cloud solution as early as possible in the adoption planning process. Such engagements should include awareness campaigns with a specific focus on the security of cloud-based information. Surveys on what is currently being used (specifically consumer cloud services) should form part of this consideration. Evaluating any given cloud solution should include other non-technical university key stakeholders. This can take the form of regular meetings or the establishment of a forum where matters of urgency can be discussed. These discussions may feed into the formulation of information policies, guidelines, requirements (for academics and students), and strategy. Once adopted, such meetings may continue to monitor what has been implemented and make changes as required.

Cloud providers play an integral role in cloud adoption decisions. As such, South African universities should incorporate cloud providers into decision making processes. The intended purpose and the unique operational contexts of South African universities make it difficult to generalize in terms of cloud computing requirements. However, the establishment of a country-wide cloud consortium focused on higher education could go a long way towards fostering such forms of engagement.

South African universities should employ specialized staff to facilitate cloud adoption. For University B the presence of an information security officer enhanced the adoption and operation of their cloud infrastructure. In fact, from the information gathered, the researchers deem the presence of such a staff member as a requirement for cloud adoption. These members of staff should be tasked with the establishment of security incident response procedures, communication channels with relevant cloud providers, and regular information security awareness campaigns. They should also negotiate levels of cloud subscriber and provider transparency.

Once a decision has been made to adopt the cloud for certain services, the criticality of the cloud-based institutional information should be rated, because certain services and types of information may not be well suited to the cloud. In this study it was found that not all key stakeholders agree on the criticality of certain types of information. For example, some participants indicated that email could easily be located in the cloud, since not being able to access email for several hours is not a major concern. The same could not be said of financial systems or anything related to teaching, since these are deemed critical systems. Rating the criticality and suitability of information in this way should be regarded as a requirement for cloud adoption.

Performing a threat assessment is recommended. Many key stakeholders were not aware of specific threats to cloud infrastructure. This highlights the need to not only become familiar with these threats, but to also identify the likelihood of their occurrence. In the South African context, SANReN is seen as a cloud enabler and for this reason the impact of network outages needs to be explored. Measures need to be taken to address potential internal threats.

The researchers recommend that South African universities should collaborate and share knowledge on cloud adoption. Many participants explicitly stated that the competitiveness amongst South African universities is counterproductive and that many problems (not only limited to cloud adoption) can be addressed if South African universities work together. Some participants even hinted at the notion of establishing shared data centres, which could act as community clouds. This has the potential to save costs in the long term, not only on hardware and software, but also on salaries, since the same staff members could effectively service multiple universities. At least one of the participants felt that TENET should act as the pioneers of such a community cloud.

REFERENCES

[1] M. Okuhara, T. Shiozaki and T. Suzuki. "Security architecture for cloud computing". *Fujitsu Sci. Tech. J*, vol. 46, no. 4, pp. 397–402, 2010.

[2] W. Jansen and T. Grance. *Guidelines on security and privacy in public cloud computing*. Washington DC: National Institute of Standards and Technology, 2011. URL `http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf`.

[3] Y. Chen and R. Sion. "On securing untrusted clouds with cryptography". In *Proceedings of the 9th annual ACM workshop on privacy in the electronic society*, pp. 109–114. ACM, 2010.

[4] "Data protection challenges in cloud computing: An Indian perspective", 2010. URL `https://www.dsci.in/sites/default/files/Data%20Protection%20Challenges%20in%20Cloud%20Computing.pdf`. Last accessed 18 November 2014.

[5] A. Joint, E. Baker and E. Eccles. "Hey, you, get off of that cloud?" *Computer Law & Security Review*, vol. 25, no. 3, pp. 270–274, 2009.

[6] R. Farrell. "Securing the cloud: Governance, risk and compliance issues reign supreme". *Information Security Journal: A Global Perspective*, vol. 19, no. 6, pp. 310–319, 2010.

[7] I. Ion, N. Sachdeva, P. Kumaraguru and S. Čapkun. "Home is safer than the cloud!: privacy concerns for consumer cloud storage". In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, p. 13. ACM, 2011.

[8] L.-q. Tian, C. Lin and Y. Ni. "Evaluation of user behavior trust in cloud computing". In *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, vol. 7, pp. V7–567. IEEE, 2010.

[9] L. A. Martucci, A. Zuccato, B. Smeets, S. M. Habib, T. Johansson and N. Shahmehri. "Privacy, security and trust in cloud computing: The perspective of the telecommunication industry". In *Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2012 9th International Conference on*, pp. 627–632. IEEE, 2012.

[10] "Cloud 101: Developing a cloud computing strategy for higher education". White paper, 2012. URL `http://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/cloud-collaboration/cloud_101_higher_education_wp.pdf`. Last accessed 18 November 2014.

[11] T. S. Behrend, E. N. Wiebe, J. E. London and E. C. Johnson. "Cloud computing adoption in community colleges". *Behaviour and Information Technology*, vol. 30, no. 2, pp. 231–240, 2011.

[12] S. Tout, W. Sverdlik and G. Lawver. "Cloud computing and its security in higher education". *Proceedings of ISECON, v26 (Washington DC)*, vol. 2314, 2009.

[13] A. Schutz. *The phenomenology of the social world*. Illinois: Northwestern University Press, 1967.

[14] A. Gillwald. "Good intentions, poor outcomes: Telecommunications reform in South Africa". *Telecommunications Policy*, vol. 29, no. 7, pp. 469–491, 2005.

[15] Genesis Analytics (Pty) Ltd. "Telecommunications prices in South Africa: An international peer group comparison", April 2005. URL `http://www.tips.org.za/files/satpp-telecom_0.pdf`. Last accessed 18 November 2014.

[16] SANReN. "SANReN Overview", n.d. URL `http://www.sanren.ac.za/overview/`. Last accessed 18 November 2014.

[17] "Institutional clusters in higher education in South Africa", April 2010. URL `http://www.chet.org.za/resources/institutional-clusters-higher-education-south-africa`. Last accessed 18 November 2014.

[18] K. MacGregor. "South Africa: New university clusters emerge", May 2010. URL `http://www.universityworldnews.com/article.php?story=20100523104119724`. Last accessed 18 November 2014.

[19] A. T. Monfared and M. G. Jaatun. "Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments." In *CloudCom*, pp. 772–777. 2011.

[20] P. Kumar, V. K. Sehgal, D. S. Chauhan, P. Gupta and M. Diwakar. "Effective ways of secure, private and trusted cloud computing". *International Journal of Computer Science Issues*, vol. 8, no. 3, pp. 412–421, 2011.

[21] M. T. Khorshed, A. Ali and S. A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing". *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833–851, 2012.

[22] H. K. Klein and M. D. Myers. "A set of principles for conducting and evaluating interpretive field studies in information systems". *MIS quarterly*, pp. 67–93, 1999.

[23] G. Walsham. *Interpreting information systems in organisations*. New Jersey: Wiley, 1993.

[24] D. Yanow and P. Schwartz-Shea. *Interpretive research design: Concepts and processes*. New York: Routledge, 2012.

[25] M. Patton. *Qualitative evaluation and research methods*. New York: Sage Publications, 1990.

[26] H. Simons. *Case study research in practice*. New York: Sage Publications, 2009.

[27] Appirio. "State of the public cloud: The cloud adopters' perspective". White paper, 2010. URL `http://thecloud.appirio.com/rs/appirio/images/State_of_the_Public_Cloud_Results_FINAL-102910.pdf`. Last accessed 17 November 2014.

[28] C. Erenben. "Cloud computing: the Economic Imperative", 2009. URL `http://www.ecampusnews.com/top-news/cloud-computing-the-economic-imperative/`. Last accessed 18 November 2014.

[29] L. Ponemon. "Security of cloud computing users: A study of practitioners in the US and Europe", May 2010. URL `http://www.ca.com/~/media/Files/IndustryResearch/security-cloud-computing-users_235659.pdf/`. Last accessed 18 November 2014.

[30] "Security guidance for critical areas of focus in cloud computing, v3.0", 2011. URL `https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/`. Last accessed 18 November 2014.

[31] J. Reed. "Following incidents into the cloud", September 2010. URL `http://www.sans.org/reading-room/whitepapers/incident/incidents-cloud-33619`. Last accessed 18 November 2014.

[32] B. Grobauer and T. Schreck. "Towards incident handling in the cloud: challenges and approaches". In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 77–86. ACM, 2010.

[33] "Trial by fire", October 2009. URL `https://www.pwc.com/en_US/us/it-risk-security/assets/trial-by-fire.pdf`. Last accessed 18 November 2014.

[34] V. Braun and V. Clarke. "Using thematic analysis in psychology". *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[35] J. Attride-Stirling. "Thematic networks: An analytic tool for qualitative research". *Qualitative Research*, vol. 1, no. 3, pp. 385–405, 2001.

[36] J. Fereday and E. Muir-Cochrane. "Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development". *International journal of qualitative methods*, vol. 5, no. 1, pp. 80–92, 2008.

[37] A. Schutz. *Collected papers: The problem of social reality*. Massachusetts: Kluwer Academic Publications, 1982.

[38] A. Schutz. *Alfred Schutz on phenomenology and social relations*. Illinois: University of Chicago Press, 1999.

[39] U. Schultze. "A confessional account of an ethnography about knowledge work". *MIS quarterly*, pp. 3–41, 2000.

[40] M. Ketokivi and S. Mantere. "Two strategies for inductive reasoning in organizational research". *Academy of Management Review*, vol. 35, no. 2, pp. 315–333, 2010.

[41] M. Cole and D. Avison. "The potential of hermeneutics in information systems research". *European Journal of Information Systems*, vol. 16, no. 6, pp. 820–833, 2007.

[42] H. E. Schaffer, S. F. Averitt, M. I. Hoit, A. Peeler, E. D. Sills and M. A. Vouk. "NCSU's virtual computing lab: a cloud computing solution". *Computer*, vol. 42, no. 7, pp. 94–97, 2009.

[43] "Top threats to cloud computing, v1.0", 2010. URL `https://cloudsecurityalliance.org/research/top-threats/`. Last accessed 18 November 2014.

[44] R. Choubey, R. Dubey and J. Bhattacharjee. "A survey on cloud computing security: Challenges and threats". *International Journal on Computer Science and Engineering*, vol. 3, no. 3, pp. 1227–1231, 2011.

[45] S. Subashini and V. Kavitha. "A survey on security issues in service delivery models of cloud computing". *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.