South African small and medium-sized enterprises' reluctance to adopt and use cloud-based business intelligence systems: A literature review

Moses Moyo
School of Computing
University of South Africa (UNISA)
Pretoria, South Africa
Mosesm50@gmail.com

Marianne Loock
School of Computing
University of South Africa (UNISA)
Pretoria, South Africa
Loockm@unisa.ac.za

Abstract— **The research work in this paper focused on cloud security challenges that prevented South African small and medium-sized enterprises from adopting and using various cloud-based business intelligence systems. The study conducted a literature review on 39 publications which were meticulously extracted from various electronic databases. Only 7 publications (5 journal articles, 1 conference proceeding, and 1 report) focused on security as a challenge to adoption of cloud-based services and BI systems by small and medium-sized enterprises. The results of the literature review indicated that security threats and vulnerabilities in various cloud deployments and services, and mistrust of cloud service providers by small and medium-sized enterprises were the main security challenges to adoption of cloud-based BIs by small and medium-sized enterprises in South Africa. The study also established that standard tools used by large business enterprises were unavailable or inapplicable to small and medium-sized enterprises which intended to adopt and utilise cloud-based BI systems.**

Keywords- cloud-based business intelligence, adopt

I. INTRODUCTION

The availability of cheap and easy-to-use cloud-based business intelligence (BI) systems has led to a major drive in stimulating the adoption and use of BI systems by small and medium-sized enterprises (SMEs), particularly in developing countries, but with little success [1]. In South Africa, SMEs remain marginalised as they struggle to access accurate and up-to-date information needed for correct decision-making in highly competitive and information-technology-driven market environments [2]. Hence, SMEs continue relying on manual systems and intuitive decision-making processes [3]. Studies show some discrepancies between SMEs and large business enterprises (LBEs) in terms of organisational set-ups [1]; information needs [4]; amount of data to process and few alternative cloud-based BI systems on offer for SMEs, because BI vendors or suppliers target mainly LBEs [5]. Few studies conducted in South Africa focus on security challenges to cloud-based BI systems' adoption by SMEs. For example, [2] examine several factors influencing adoption and use of BI by SMEs in South Africa, although silent on the influence of cyber security as one of the major challenges.

The research work addressed the question: *What were the security challenges to adoption and utilisation of cloud-based BI systems by SMEs in South Africa?*

The significant contribution of the study was highlighting the security challenges that SMEs in South Africa were facing in their quest to adopt and utilise cloud-based BI systems. The study also sought to contribute to the scholarly debate on cloud security as a major determinant factor that SMEs used to decide whether to adopt cloud-based services or not.

The research work in this paper reviewed literature on security in cloud-computing technologies, and how they affected the adoption and utilisation of cloud-based BI systems by SMEs in South Africa. The paper is organised into Section I: Introduction; Section II: Review of related literature; Section III: Methodology; Section IV: Results; Section V: Discussions; Section VI: Cloud security initiatives to overcome security challenges by SMES; and Section VII: Conclusion.

II. REVIEW OF RELATED LITERATURE

These days, cheap and easy-to-use cloud-based BI systems provide SMEs with an opportunity of accessing and processing data stored in various electronic sources distributed over the Internet, to business information and knowledge needed for decision-making [6]. This requires SMEs to migrate most of their data and transactions to the vulnerable cloud environments [7]. Research shows that cyber-criminals' activities can render information security in cloud-based resources almost unachievable [5]. This challenge requires SMEs to put in place secure strategies to access such cloud-based resources without exposing their information systems (IS) to the inherent cyber security threats [8]. Literature from a number of studies shows that information security breaches committed over the cloud-based technologies remain a major concern for adoption and utilisation of cloud-based BI systems and therefore SMEs adopt a wait-and-see attitude [9].

While it is acknowledged that SMEs are the cornerstones of many economies the world over, technologically, they remain peripheral users [9]. South African SMEs fail to compete with established LBEs in the market because they lack technological capabilities to do so [10]. Although cloud-based BI systems are a potential remedy, they have many security vulnerabilities that SMEs have to deal with, therefore the need for security

initiatives to assist them. Several studies on cloud-based BI systems indicate that SMEs need easy-to-use and lightweight BI technologies that are capable of providing online data analysis and graphical output [1]. Some cloud-based BI systems best suited for SMEs' needs are now available and also easily be accessed over the Internet [11].

A. Cloud-based BI Systems

Cloud-based BI systems depend on cloud-computing technologies to provide access to large volumes of data and computing resources that make use of a variety of interfaces accessed over the Internet [12]. Generally, cloud-based BI systems are deployable in private, community, public, or hybrid clouds, which have unique security bearing on enterprise data that SMEs have to deal with [10]. Ideally, public and community cloud services are the most viable for SMEs [13]. Public clouds provide the most viable BI solutions for SMEs because they are mainly offered free of charge or at a nominal annual fee [14]. Unfortunately, by adopting public clouds, SMEs would be classified as untrustworthy users and this would further leave them more exposed to cyber security threats [12].

Cloud-based technology offers three types of services, namely, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [7]. Of the three services, the IaaS and SaaS are more suitable for SMEs, which aim to economise by investing less in information technology (IT). With IaaS, SMEs can benefit on hardware infrastructure such as servers and storage devices which are delivered as services accessible over the Internet while being hosted by the cloud service provider (CSP). This reduces or eliminates the amount of hardware that SMEs need to purchase and install. SaaS also delivers a range of software, including BI systems over the Internet, as a service that SMEs can easily access and utilise [15]. Public cloud-based services are accessible anywhere gratis or at a relatively affordable price compared with traditional BI systems; and this makes them suitable for SMEs experiencing budget constraints for IT [15]. Despite many opportunities afforded by cloud-based BI systems, major challenges to adoption of cloud services reside in the perception that they are inherently insecure, and likely to expose an organisation's IS to unacceptable security threats, especially cyber-criminals [12].

III. METHODOLOGY

A. Identification of publications

This literature review was based on security challenges to adoption of cloud-based technologies, including BI systems and related services, particularly by SMEs in South Africa. Search terms and phrases used included:

- Security factors affecting adoption of cloud-based BI systems by SMEs in South Africa;
- security challenges to adoption of business intelligence by SMEs in South Africa;
- Security challenges to adoption of cloud-based business intelligence by SMEs in South Africa

Publications were obtained from electronic databases such as ScienceDirect, IEEE, and ACM, with dates ranging from 2009 to 2016. Some relevant articles were also extracted from the open web using Google Scholar. Results of publications' searches that yielded relevant keywords were listed and the most appropriate literature sources selected.

B. Inclusion and exclusion criteria

The process of excluding and including literature sources enabled the selection of publications that met the requirements in terms of literature suitability, focus, and dates of publication as recommended by [16]. Publications with dates before 2009, having multiple references, references with missing abstracts, or not specifically related to cloud-computing security or security in BI in SMEs, were excluded.

IV. RESULTS

A total of 110 publications were extracted from various databases. This report is on publications which met the date range of 2009 to 2016 and dealt with security in cloud computing, adoption of cloud computing in SMEs. Of the 110, only 66 articles were within the publication-date range, as shown on Table I.

TABLE I. DISTRIBUTION OF PUBLICATIONS BY YEAR OF PUBLICATION

Year	Number	%
2009	2	3,0
2010	11	16,7
2011	16	24,2
2012	6	9,1
2013	9	13,6
2014	14	21,2
2015	7	10,6
2016	1	1,5
Total	**66**	**100**

The results show an even distribution of articles published between 2009 and 2016 at the initial literature review. Fig 1 shows the distribution of articles with their types.

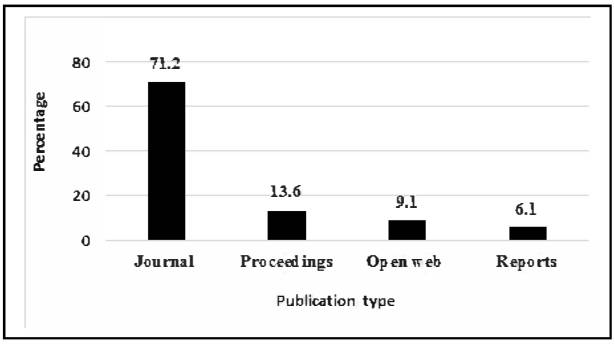

Figure 1: Distribution of types of article

Initially, 71.1% (47) of the articles used were journal publications, 13.6% (9) conference proceedings, 9.1% (6) open web, and 6.1% (4) various reports related to the topic under discussion. After excluding articles which did not deal with

security issues in cloud-based BI systems, publications were categorised according to the region or country of focus (Table II).

TABLE II. DISTRIBUTION OF PUBLICATIONS ACCORDING TO REGION

Region or country	Publications	%
General	42	63.6
South Africa	14	21.2
Africa	7	10.6
Europe	2	3.0
Asia	1	1.5
Total	66	100

Most of the publications, 42 (63.6%) were not specific to any country; 14 (21.2%) specifically covered South Africa; 7 (10.6%) Africa in general, including South Africa; 2(3.0%) were based on European SMEs; and 1 (1.5%) on Asian SMEs. The publications were further categorised according to focus on security in cloud-based services, technologies, or BI systems. Thirty-nine (39) publications were then selected. This exercise followed Von Broembsen and Wood (2005)'s [17] guidelines on how to select publications for literature review. The results are shown on Table III.

TABLE III. BREAKDOWN OF PUBLICATIONS BY REGION AND TYPE

Region	Journals	Open Web	Proceedings	Reports	Total
General	16	6	2	1	25
South Africa	5	0	1	1	7
Europe	1	1	1	0	3
Africa	2	0	0	0	2
Asia	0	0	2	0	2
Total	**24**	**7**	**6**	**2**	**39**

Of the 39 publications reviewed, 24 were journal articles, 7 open-web articles, 6 conference-proceedings articles, and 2 reports. There were only 5 journal publications, 1 conference-proceedings article, and 1 report that dealt with security in cloud BI systems in the South African SME context.

Some publications were also specific about the type of BI deployment most suitable for adoption by SMEs. Table IV shows the results.

TABLE IV. MOST APPROPRIATE CLOUD BI SYSTEMS FOR ADOPTION BY SMES

Type of cloud	Publications	%
Private	5	12.8
Public	18	46.2
Community	8	20.5
Hybrid	5	12.8
Not specific to cloud	3	7.7
Total	39	100

The results show that 36 (92.3%) of the publications were specific about which cloud deployment was most suitable for SMEs. Of the 39 publications reviewed, 5 (12.8%) recommended private clouds, 18 (46.2%) public clouds, 8 (20.5%) community clouds, 5 (12.8%) hybrid clouds, and 3 (7.7%) were not specific about cloud type. Further processing of publications based on security concerns in the cloud raised was done. Results are depicted in Table V.

TABLE V. SECURITY ISSUES RAISED BY PUBLICATIONS

Security issues	Number	%
General security concerns	30	76,9
Data breaches	25	64,1
Loss of data ownership	21	53,8
Data loss and leakage risks	20	51,3
Lack of privacy	18	46,2
Loss of data control	16	41,0
Disruption of data availability	15	38,5
Lack of tools to migrate data	10	25,6

Results show that 30 (76.9%) of the publications dealt with general security concerns; 25 (64.1%) on data breaches; 21 (53.8%) loss of data ownership; 20 (51.3%) data loss and leakage risks; 18 (46.2%) lack of privacy; 16 (38.5%) loss of data control; 15 (38.5%) disruption of data availability; and 10 (25.6%) related to data-migration issues.

Publications were also analysed in terms of perceived security threats in cloud environments. Results are displayed on Table VI.

TABLE VI. PERCEIVED SECURITY THREATS IN CLOUD ENVIRONMENTS

Security threats	Publications	%
Data theft by competitors	29	74.4
Unauthorised access to data	27	69.2
Unexpected closure by cloud provider	26	66.7
Malicious cloud insiders	23	59.0
Poorly secured BI interfaces /browsers	18	46.2
Denial of service attacks	15	38.5
Financial loss owing to data theft	15	38.5
Accounts' hijacking	12	30.8

Results show that top of the list was data theft by competitors 29 (74.4%), and this is high in public and community deployments; unauthorised access to data 27 (69.2%), high in public and community deployment; also, unexpected closure by cloud provided 26 (66.7%), which was high for all cloud types.

V. DISCUSSIONS

Literature reviewed in this research paper categorised security challenges into either cloud security issues or cloud security threats.

A. Cloud security issues

SMEs intending to adopt and utilise cloud-based BI systems have to deal with a number of cloud security issues.

Prevalent cloud security issues discussed in the reviewed literature were data breaches, loss of data ownership, data loss and leakage risks, lack of privacy, loss of data control, disruption of data availability, and lack of tools to migrate data and data privacy [15]. Cloud security issues were found to be associated with particular cloud deployments and services. In public clouds, SMEs as clients would lose both ownership and data control to CSP [12]. In view of these cloud security issues, it is always difficult for SMEs to determine whether the CSP would provide sufficient data protection in the cloud [3]. Unlike on-premises data centres in which an organisation has full control of its data resources, cloud-based resources present uncertainty to enterprises, particularly those that use public and community deployment [10]. Many SMEs that have adopted IT systems and those intending to do so believe that major cloud-based systems are less secure than on-premises' applications [8] and [12].

B. *Cloud security threats and vulnerabilities*

Threats identified in this review included data theft by competitors, unauthorised access to data, unexpected shutdown by CSPs, malicious cloud insiders, poorly secured BI interfaces/browsers, and denial of service attacks, financial loss due to data theft, and accounts' hijacking [3] and [8].

Security vulnerabilities in cloud-based BI systems depend on the deployment approach implemented [15]. Public clouds are the least secure and most vulnerable owing to easy access by many users with different intentions; they therefore experience more severe impact of data security breaches [13]. As it is, SMEs are unlikely to adopt a technology that they mistrust in terms of its security features.

C. *Virtualisation vulnerabilities*

Cloud-computing services, IaaS, and PaaS utilise virtualisation and physical machines shared and rented among several users [18]. Virtualised computing environments are weak and susceptible to cyber-attacks, which make data security difficult for SMEs [12]. Security vulnerabilities are comparatively high in public and shared clouds as their security perimeters may easily be broken from within, resulting in security breaches [18]. This security challenge is sufficient enough to deter those SMEs who would want to adopt and utilise clouds on economic grounds.

D. *Lack of physical ownership of data*

Cloud-based services prevent users from physically possessing their own data storage, and compel the enterprises to heavily depend on the CSPs [14]. In this context, an enterprise loses both control and security of its data [8]. These security issues deter SMEs from adopting and using cloud-based BI systems.

E. *Lack of tools of data migration from cloud to cloud*

Another key security weakness of cloud-based BIs highlighted by many authors was the challenge of data migration from one CSP to another [8]. CSPs hardly provide appropriate tools, techniques, or standard data formats, services or interfaces that might guarantee data security and service portability for SMEs [19]. According to [19], client enterprises utilising cloud-based services find it difficult to switch from one CSP to the other, to migrate data and services to or from on-premises to cloud. This situation is referred to as a vendor lock-in problem, in which a customer depends on a single cloud provider technology implementation, finding it difficult to change to another vendor without incurring large costs, legal problems, and even technical incompatibilities ([20]. In the event that a CSP shuts down owing to bankruptcy, client enterprises, especially SMEs, suffer massive business failure, possibly resulting in failure to transfer their data and services to other CSPs [1].

F. *Lack of appropriate tools to evaluate security vulnerabilities in BI systems*

When adopting cloud-based BI systems, an enterprise migrates its information and data processing from on-premise data centre(s) to the cloud-making data security the most important factor to consider [15]. The challenge is that most of the conventional standard processes for managing security risk used by LBEs to make important decisions cannot easily be applied to cloud computing, security details of cloud services are not typically being available to SMEs [13]. Lack of such crucial information usually translates to a lack of trust by SMEs that are unable to determine the level of security vulnerabilities in cloud–based BI services compared to on-premises' systems.

VI. CLOUD SECURITY INITIATIVES TO OVERCOME SECURITY CHALLENGES BY SMES

Currently, the viable security initiatives that SMEs may benefit from while using the cloud-based BI systems are basically technical initiatives offered by the CSPs. Depending on the Service Lease Agreements, where they exist, CSPs may provide security features for the client SMEs, such as filtering, patch management, hardening of virtual machine instances, and hypervisors, human resources, their management and vetting, hardware and software redundancy, and strong authentication and efficient role-based access control [19]. Although, in principle, this may seem to improve security, SMEs' perceptions and expectations of security levels may differ from the actual security CSPs are capable of offering. The fact that CSPs also depend on other security companies for security services may compromise the whole exercise, should CSPs decide to make a profit by reducing their costs, opting for low-quality security features.

VII. CONCLUSION AND FURTHER RESEARCH

This study explored a number of cloud security challenges and threats to adoption of BI systems by SMEs in South Africa. With the availability of cheap and easy-to-use cloud-based BI systems, new challenges also emerge, namely cyber-security threats and cloud security vulnerabilities that client organisation would have to deal with. The current trend in cloud-based BI systems is modelled along LBEs rather than SMEs, and hence most of the tools available present serious security challenges to SMEs. Currently, the major cloud security challenge for SMEs in South Africa is vendor lock-in, which makes it practically impossible for SMEs to migrate

their data and information to other CSPs. SMEs are threatened by loss of data ownership, theft of their data by competitors whom they would share the cloud with and cyber criminals who have also migrated to the cloud. Another challenge pertains to lack of security framework suitable for SMEs to assess security vulnerabilities in cloud-based BI systems they intend to adopt and utilise.

Further research is needed on security frameworks that are easy to use by none technical SMEs who intend to adopt and utilise cloud-based services.

REFERENCES

[1] W. Boonsiritomachai, M. McGrath, and S. Burgess, "A research framework for the adoption of Business Intelligence by Small and Medium-sised enterprises," in *27th Annual SEAANZ Proceedings for Small Enterprise Association of Australia and New Zealand Conference 16-18 July 2014*, 2014, pp. 16–28.

[2] L. Dawson and J. P. Van Belle, "Critical success factors for business intelligence in the South African financial services sector," *South African J. Inf. Manag.*, vol. 15, no. 1, pp. 545–557, 2013.

[3] A. A. Soofi, M. I. Khan, and F. Amin, "A Review on Data Security in Cloud Computing. International," *J. Comput. Appl.*, vol. 94, no. 12, pp. 12–20, 2014.

[4] F. Fedouaki, C. Okar, and E. S. Alami, "A maturity model for Business Intelligence System Project in Small and Medium-sized Enterprises: an empirical investigation," *Int. J. Comput. Sci. Issues (IJCSI)*, vol. 10, no. 6, pp. 234–250, 2013.

[5] M. Ghazanfari, M. Jafari, and S. Rouhani, "A tool to evaluate the business intelligence of enterprise systems," *Sci. Iran.*, vol. 18, no. 6, pp. 1579–1590, 2011.

[6] M. Dyczkowski, J. Korczak, and D. Helena, "Multi-criteria evaluation of bi systems. The case study of inkom dashboard," *nformatyka Ekon. Bus. Informatics*, vol. 3, no. 33, pp. 46–60, 2014.

[7] T. Vatuiu, M. Udrica, and N. Tarca, "Cloud Computing Technology - Optimal Solution for Efficient Use of Business Intelligence and Enterprise Resource Planning Applications.," *J. Knowl. Manag. Econ. Inf. Technol.*, vol. 2013, no. 1, pp. 395–406, 2013.

[8] M. Antoo, Z. Cadersaib, and B. Gobin, "PEST Framework for Analysing Cloud Computing Adoption by Mauritian SMEs," *Lect. Notes Softw. Eng.*, vol. 3, no. 2, pp. 107–112, 2015.

[9] M. Marefati and S. Hashemi, "Business Intelligence System in Banking Industry Case Study of Samam Bank of Iran. Software Engine," *ering Res. Manag. Appl. 2012 Stud. Comput. Intell.*, vol. 430, no. 2012, pp. 153–158, 2012.

[10] O. I. Adam and A. Musah, "Small and Medium Enterprises (SMEs) in the Cloud in Developing Countries: A Synthesis of the Literature and Future Research Directions," *J. Manag. Sustain.*, vol. 5, no. 1, p. 115:139, 2015.

[11] R. S. Tehrani and F. Shirazi, "Factors Influencing the Adoption of Cloud Computing by Small and Medium Size Enterprises (SMEs)," *Hum. Interface Manag. Information. Inf. Knowl. Appl. Serv. Lect. Notes Comput. Sci.*, vol. 8522, no. 2014, pp. 631–642, 2014.

[12] T. G. K. Vasista, "Strategic Business Challenges in Cloud Systems," *Int. J. Cloud Comput. Serv. Archit.*, vol. 5, no. 4, pp. 1–3, 2015.

[13] I. Potoczny-Jones, "Cloud Security Risk Agreements for Small Businesses, Galois, Inc.," 2011. [Online]. Available: https://www.galois.com/downloads/public/Cloud-Security-Risk-Agreements-for-Small-Businesses.pdf.

[14] O. Grabova, J. Darmont, J. H. Chauchat, and I. Zolota, "Business Intelligence for Small and Middle-Sised Entreprise," *Spec. Interes. Gr. Manag. Data Rec.*, vol. 39, no. 2, pp. 231–245, 2010.

[15] B. A. Sangar and A. N. Iahad, "Critical Factors That Affect The Success Of Business Intelligence Systems (BIS) Implementation In An Organization," *Int. J. Sci. Technol. Res.*, vol. 2, no. 2, pp. 25–35, 2013.

[16] J. Vom-Brocke, A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, and A. Cleven, "Reconstructing the giant: On the importance of rigour in documenting the literature search process," in *17th European Conference on Information Systems (ECIS 2009)*, 2009, pp. 2206–2217.

[17] M. Von Broembsen and H. E. Wood, "Global Entrepreneurship Monitor, South African Report," 2005. [Online]. Available: http://www.gbs.nct.ac.za/gbswebb/userfiles/gemsouthafrica2000pdf. [Accessed: 15-Mar-2016].

[18] S. Ristov, M. Gusev, and M. Kostoska, "Cloud Computing Security in Business Information Systems," *Int. J. Netw. Secur. Inf. Technol. Appl.*, vol. 4, no. 2, pp. 131–140, 2012.

[19] Europian Networks and Information Security Agent ENISA, "Cloud Computing Benefits, risks and recommendations for information security," 2010. [Online]. Available: https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport. [Accessed: 15-Mar-2016].

[20] J. Opara-Martins, R. Sahandi, and T. Tian, "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 5, no. 2016, 2016.