Journal of Information Systems and Informatics

Vol. 5, No. 2, June 2023 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

DOI: 10.51519/journalisi.v5i2.478 Published By DRPM-UBD

Case Study Analysis of the Use of Cloud Computing for Assessing Big Data Risks

Fadi Fataftah[1], Bassey Isong[2]

[1]Department of Computer Science, North-West University, Vanderbijlpark, South Africa
[2] Department of Computer Science, North-West University, Mafikeng, South Africa
Email: [1]fadi.fataftah@gmail.com, [2] isong.bassey@ieee.org

Abstract

Risks associated with adopting big data and cloud computing and exposing sensitive information must be evaluated as usage of these technologies continues to rise rapidly within businesses. Also, the company needs to investigate the potential consequences of cyber security threats, considering the severity of those risks. There has been no comparative analysis of the risk assessment methods available to businesses in various nations. Thus, the researcher in this study asked forty people from four countries (Canada, Jordan, South Africa (SA), and the United Kingdom (UK)) questions on the risk assessment procedures at their respective organizations using semi-structured interviews. After compiling and analyzing the data, it became clear that Canada and the UK were the frontrunners in adopting big data and cloud computing. It also demonstrated that Jordan and SA are in the early phases of an evolving adoptive relationship. Recommendations are made to strengthen the organization's standing in light of the different risk assessment frameworks used in each country.

Keywords: Big Data, Cloud Computing, Risk Assessment, Canada, Jordan, South Africa, United Kingdom.

1. INTRODUCTION

Big data is a key entity for organizations of all sizes nowadays. There are limitless opportunities and intellectual capital associated with big data [1]. Cloud computing is the computing resource that makes big data accessible and can be used to share, archive, and destroy data of many sizes [2]. However, some inherent risks are associated with big data on the cloud if poorly handled. Security threats such as data breaches, confidentiality issues, and threats due to data availability can cause severe damage to companies and their system [3]. The deliberate misuse of data-driven technology by malevolent players and the risks of falling into corporate insecurity can threaten companies. Big data is the large, diversified data set from different locations such as websites, electronic check-ins, organizational databases,


This work is licensed under a Creative Commons Attribution 4.0 International License.

sensors, call logs, and many other similar sources. Cloud computing is the virtual network-based storage where all the information and necessary data can be stored in service providers' hardware. To safeguard these, risk assessment methods are available [4]. In this study, the researcher focused on four nations: Canada, Jordan, South Africa (SA), and the United Kingdom (UK). In particular, cloud services in Canada are safe, convenient, and reliable [5]. In the past, there was a huge complexity in the cost efficiency of big data, but slowly major Canadian professionals shifted to cloud services for their operational efficiency. Industrial integration with cloud services results from wide private cloud data centres' opportunities to serve large Canadian organizations [6]. Jordan has seen a digital transformation, but due to high costs and lack of training, there are issues in implementing the cloud for big data management in Jordan [7]. In Jordan, indigenous companies and local Small and medium-sized enterprises (SMEs) are encouraged to use cloud services, and there is a need for large-scale transferring of operations and services to the cloud [8]. In SA, cloud computing services need advancement in infrastructure and internet availability [9]. However, the information technology (IT), Telecommunications, and manufacturing industries in SA have limited access to their big data through cloud services. Still, common people's overall cloud absorption may be challenging [10]. Cloud solutions have been fully immersed in industrial and private utilities in the UK. To safeguard the big data, direct routing and network coding systems alter the conventional pathways and make the cloud services more secure [11].

Big data utilization has exploded in healthcare, urbanization, and management, attracting scholars. Big data refers to enormous datasets that typical database software cannot clean and handle. Big data's speed and diversity of information sets require novel operationalization methods to aid insight discovery, management, synthesis, and process efficiency [12]. People and companies gain new opportunities and benefits [13]. Volume, variety, and velocity define big data [12]. The volume dimension shows data from multiple sources. Big data involves zettabyte-scale numbers. Data processing and analysis methods are varied. With more linked digital devices and platforms, structured data has shifted to unstructured data, including photographs, videos, and text. Velocity refers to the speed at which Facebook and Twitter generate data. Increasing data volumes and frequency require faster data analysis. Other authors have highlighted the following issues while saving and analyzing huge data: [14]. Veracity represents the data's precision and reliability. Data quality is varied, influencing precision and processing. Big data's worth can be reduced if it is not exact and does not offer accurate insights. Large data's value is shown. Also, data analysis shows relevance. If data does not benefit firms and customers, it is almost worthless. The value of data processing is in the information and insights it provides. Volume, velocity,

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

diversity, and authenticity are processed before value. Big data leverage clouds computing services like Amazon or Microsoft to operate, simplifying decision-support systems [15]. The cloud is the storage chamber, and big data is the item stored in it [14].

Big data management is very crucial to the rising demand of enterprises. Cloud's advanced utility to consolidate, integrate, build and manage large datasets makes it a highly trusted and practised resource [16]. However, there are various risks associated with big data using the cloud. A privacy breach is a common risk that exposes data at an alarming rate [17]. Having owned by third parties, the privacy risks can cause disasters for enterprises and private users [18]. Cloud-based service providers offer numerous real-time applications using big data. Still, these servers and nodes with storage clusters can be vulnerable to privacy breaches due to data leaks, irrelevant guest entries, and mass victimization on the cloud [19]. Another risk in managing big data using the cloud is governance and compliance. Security issues concerning an interface and user access are high due to non-regulated and unorganized service conformity [20]. Further, data availability problems pose huge risks to the technical sub-system as a large amount of big data is unorganized and scattered [21]. There are various advanced methodologies in practice, such as erasure and network coding, but their integration with the system is lacking. New advanced coding and access control systems are designed to prevent these concerns, and there is a need for increased intervention to manage these big data [22] ethically.

The empirical evidence has been derived from showcasing the risks in big data management using the cloud. Van Der Schyff & Krauss [23] conducted a thematic analysis of twelve experts for a semi-structured interview on the security threats in cloud computing in South Africa. The researcher studied virtualization-related security issues with the help of consolidating the issues in a classified manner. The findings revealed that data privacy and protection concerns arise due to multitenancy, malicious insider presence, and shared application usage. Sodikin [24] researched sixty-nine participants through a questionnaire and conducted four interviews with respondents from two organizations exposed to the cloud and virtual working and interviewed them on security issues in cloud computing with the help of analysis revealed that lack of reliability, integrity, and availability are the major issues in cloud computing that make organizations less likely to implement them. However, it can be handled with the help of authentication, auditing, and authorization to safeguard users' big data. Hammouri & Abu-Shanab [9] studied the importance of cloud computing and the utility of cloud services in Jordan with

the help of a quantitative analysis of one hundred and forty-three participants. The findings revealed that cost reduction, service quality, and control enhancement urge users to take cloud services. In the same vein, Machuga [25] researched cloud computing usage in European countries through secondary research based on Eurostat's findings, which suggested that adopting cloud technology was highly effective in European nations. People are familiar with the technology, and the presence of strong infrastructure helped make cloud computing usage safe and secure. Similarly, Flora et al. [26] researched forty-four experts on cyber security crimes and probable reasons for attacks with the help of thematic analysis through the expert elicitation method. The interview findings revealed a need for creating an integrated sub-system wherein human intervention to preserve confidentiality, ensure a timely and reliable flow of data, regular compliance, and control over intrusion via confidentiality building a cyber-system can be created.

The above-reviewed studies detailed the significant contributions of cloud services, issues concerning big data, and ways to curb the issues at hand. However, most studies did not emphasize risk assessment methods commonly used to evaluate big data using the cloud globally in different nations. The present study intends to bridge the gap and analyse the capabilities of the risk assessment methods in use. The comparative study demonstrates the risks that can be encountered in less competent methods of risk assessments compared to the more competent and efficient methods practised in some countries. This research is based on the risk assessment methods in use. The current paper throws light on their economy's country-wise technology advancement and cloud-based development.

The main research question explored in this study is "What are the risks associated with big data based on cloud computing technologies in Canada, Jordan, South Africa, and the United Kingdom?" Since big data is ever-growing and increasingly vulnerable at the same time, threats and privacy concerns need to be addressed through effective risk assessments. This goes with analysing the source of risks and the potential damage they can cause. Further, addressing the risks and security issues and effectively eradicating or curbing them is important. Therefore, understanding the risk assessment processes in big data services in cloud computing technologies is instrumental in curbing cyber-attacks and other risks of big data. The study compares the risk assessment methods for big data in the cloud in the respective countries. The contribution of this paper is summarized as follows (1) Analyze the management of big data using the cloud. (2) Study the risks and vulnerabilities associated with cloud services. (3) Study and analyze the risk assessment methods most used in the chosen countries.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

2. METHODOLOGY

This study planned and implemented a comparative risk assessment method for safeguarding big data using the cloud. To fulfil the objectives, an interpretive research paradigm was implemented and inductive. Ontologically, this study interprets the relationship between domains as per participants' views, intending to analyze and understand the risk assessment methods of different nations.

2.1. Data Types

The researcher used mixed methods, wherein quantitative and qualitative data were collected and reviewed. Moreover, in this paper, primary data was used and collected via semi-structured interviews wherein the respondents were asked open-ended questions.

2.2. Quantitative vs Qualitative Research

Quantitative research investigates numerical data or data translated into numbers using statistical methodologies. Quantitative research is concerned with numerical data that has been converted into numbers. Statistics refers to the most often used approaches for analyzing numerical data. Statistical procedures deal with the organization, analysis, interpretation, and presentation of numerical data. Statistics is a large field of study with numerous applications, including information systems and data analysis [27]. On the other hand, qualitative research is based on unquantifiable processes and meanings. According to Maanen [28], qualitative label techniques in the social sciences have no definite meaning. Qualitative research refers to the process of collecting, decoding, translating, and comprehending the term's meaning rather than the frequency of naturally occurring events.

In the context of this study, the use of qualitative research allowed the researchers to delve further into the research issue through extensive interviews highlighting professionals' experiences, expertise, and concepts on risk assessment procedures in their specialized areas. The qualitative study aided in comprehending specialists' perspectives on big data and cloud computing difficulties. The explanatory data aided in the formation of patterns from concepts and insights. The interactive interviews and triangulation process assisted in validating the acquired data and providing well-founded reputable information from credible sources [29]. This study used a four-step process to answer the research question and to accomplish

the objectives through qualitative research. This study initially defined the field of research connected to big data risk assessment using cloud services and then gathered more information depending on the research topic. This process involved choosing the unit, topic, and analysis. The analysis employs various methodologies to handle risk challenges in big data and cloud computing environments. The company itself was used as a supplementary unit of study. The study then obtained primary data from participants who were professionals operating close to cloud platforms. This step gathered data on various risk assessment approaches in big data and cloud computing. Data was collected through interviews with respondents from the four targeted countries who work in cloud platform organizations or use cloud services, secondary information available on the firms' websites for analysis, and information from the Internet in general, as detailed in Table 1.

Table 1. Data collection framework by the researcher

Qualitative research		
Data was collected via interviews, the firm's websites, and information from the Internet.	The focus is on Canada, Jordan, South Africa, and the UK. There are between 3-4 firms per country; 2-3 interviewees per firm (the target is ten participants from each country).	Inductive analysis and finding patterns. Triangulation to add rigour.

Following the gathering of information, the evidence was reviewed. The study determined if the information gathered was useful. The information was analyzed and examined to eliminate contradictory and irrelevant data and find missing data. The study detected patterns after reviewing the evidence. This stage attempted to organize the data to uncover intriguing patterns related to the problem (i.e., risk factors in big data and cloud computing settings). Grounded theory is based on systematically collecting, analyzing, categorizing, and (iterative) validating data that can aid in defining intriguing phenomena. The study used data and researcher triangulation to increase the research's quality and rigour. The researcher evaluated several factors to guarantee that this research fits the specific ethical criterion. This included obtaining the necessary approvals to carry out the study, securing participation, maintaining data confidentiality at all stages, educating participants about the potential hazards of participating in this research, and adhering to the ethical research process.

2.3. Sampling and Data Collection Procedure

Sampling is an important part of research methodology since it helps get information from the right respondents. Sampling is the process of selecting the right population sample to conclude. Unbiased and error-free sampling is needed to draw meaningful conclusions from the study. The target population is used to determine the sample size. The participants in this research are IT professionals and specialists working in organizations that use big data in the cloud. The study's sample size is 40 experienced individuals representing four countries. To ensure that the respondents had a thorough understanding of the risks and issues within their organizations and the concerns that have impacted the security and confidentiality of their big data in the cloud, we limited our sample to experts with solid experience in cloud-based platforms and IT service-providing firms. In addition, experts in the field of information technology could discuss the most up-to-date national risk assessment techniques and the seriousness of risk assessment approaches implemented by individual companies in response to the growing prevalence of remote work. Canada, Jordan, SA, and the UK sent samples.

Interviews were done with between three and four companies in each country. To validate and generalize the respondents' responses, we set a goal of having ten people from each country participate. The results of this research have been useful in getting IT department managers and staffers more familiar with big data's role in the cloud. Candidates were chosen for their expertise in areas such as risk analysis, big data, and cloud-based service management. The four countries were chosen because of the high concentration of cloud service users among their businesses. Regarding big data and cloud computing, Canada and the UK may claim to be among the first countries to do so. Canada has an extensive adoption of big data and cloud computing. Perception of people knowing risk assessment (RA) methods can significantly contribute to the study. The UK was selected as it is a developed European nation where cloud solutions have immersed fully in industrial and private utilities. Jordan is a fast-digital transformation nation, but due to high costs and lack of training, there are issues in implementing the cloud for big data management. The perception of participants in Jordan on RA methods is imperative to be included to provide a holistic approach to the investigation. While South Africa is struggling to adapt RA methods in cloud computing services, it needs advancement in infrastructure and internet availability still; sales in the Middle East and Africa's big data analytics market are expected to reach $68 billion by 2025, per research by Frost & Sullivan [30].

2.4. Interview

The researcher used grounded theory to perform qualitative analysis for data analysis. In this case, interviews of the respondents were recorded and turned into text. The major themes were distributed as per the evidence gathered, and a comparative study was performed based on the analysis. For effective reliability and validity of the research, the errors were double-checked. The completeness, relevance, and timelessness of data were checked for utility. The interview of respondents from different nations was done based on the perception of big data risks in their nations. Herein, some sets of questions were prepared, and some were left to be asked as per the replies and content provided by the interviewees. The information was systematically analyzed to find a pattern and generalize the findings. Further, the triangulation method confirmed the validity of the inferences drawn with the help of participant observation, research from secondary sources, and data validation.

The interviews were transcribed in Atlas.ti software, which was used to codify the answers. Firstly, the word clouds were generated and used to identify the codes. The data was then coded, and Atlas.ti identified the themes relevant to the research questions answered. Only knowledgeable professionals having relevant exposure and experience in information technology and cloud-based platforms were included in the study. Some of the professionals from relevant departments are considered included for this study was IT operations and infrastructure, IT operations and access management, enterprise architecture and support, IT lead (helpdesk, system administrators, network operations and security, and infrastructure/network administrators), and IT information and security Operations. All relevant data for answering the research questions were preserved in four categories: occurrences primarily impacting security in cloud computing, significant data contexts; company information; and technology advancements to solve risk issues in cloud computing and big data environments. Large sheets of sketch paper and pencils are the tools for organizing the data. Drawings, diagrams, and figures are often used to categorize data. Colour coding is used to distinguish between different data types (i.e., types of risk, potential solutions, and best practices).

2.4.1 Grounded Theory

Grounded theory uncovers patterns. Galal-Edeen [31] says a grounded theory researcher must gather, classify, and validate (iteratively) data. Formalize the data to assist future data collection and analysis. The grounded theory approach provides the methodologies and strategies needed to achieve this goal [36].

Grounded theory is data-based, as the name suggests. The researcher kept the analysis close to the data and established a theoretical framework. The researcher maintained a comprehensive analysis close to the acquired data. In this study, the researcher compared responder observations. Theoretical sampling followed coding and data collecting. This helped the researcher grasp risk evaluations for huge data in cloud computing. The interviews utilized grounded theory and Internet resources. The application of grounded theory to big data and cloud risk evaluation is justified since it provides a set of processes for classifying and evaluating data that are compatible with the interpretative method. It keeps the analysis close to the facts and yields inductive findings about the investigated phenomenon. [32]. The grounded theory process is iterative, with frequent movement between concept and data and comparison across sources [33]. The researcher used the following steps proposed by Bernard [34] to carry out grounded theory:

1) Compiling all of the data from those categories and comparing them.
    a. Create transcripts of interviews and read a small sample of text.
    b. Look for potential analytic categories (that is, themes) that emerge.
2) Thinking about how categories are related to one another.
3) Building theoretical models based on the relationships between categories, regularly evaluating the models against facts, predominantly negative scenarios.
4) Using quotes from the interviews to illustrate the idea, provide the findings of the analysis (exemplars).

2.5. Ethical Consideration

Ethical considerations were not a major concern as this study addresses questions about risk assessment in big data and cloud computing scenarios. However, because this study included individuals from various backgrounds and experiences, the researcher took the following factors into account to ensure the effectiveness of this research:

1) Obtaining the necessary written or verbal approval to perform this research.
2) Ensuring that participation was fully voluntary. Participants are under no obligation to contribute information to this study and may withdraw at any moment if they believe it is unnecessary.
3) Maintaining data confidentiality at all times. This includes storing and maintaining data properly. It also requires removing the raw data once the research has been successfully conducted.
4) Because this study did not contain any sensitive material, the chances were minimal.

3. RESULTS AND DISCUSSION

This section presents the qualitative and quantitative analysis of the data gathered to compare big data risk assessment techniques based on cloud computing for Canada, Jordan, SA, and the UK. The qualitative data is analyzed using thematic analysis with Atlas.ti software and the quantitative data were analyzed using statistical representation. The results obtained are discussed in the subsections that follow:

3.1. Level of Knowledge

The knowledge of big data allows individuals to be more aware of methods of data utilization to identify patterns and trends **[**35**]**. The respondents were enquired about their knowledge level of big data. The minimum amount of data considered in the question was considered as much as that allowed to draw a strong conclusion. The same is presented in Figure 1.

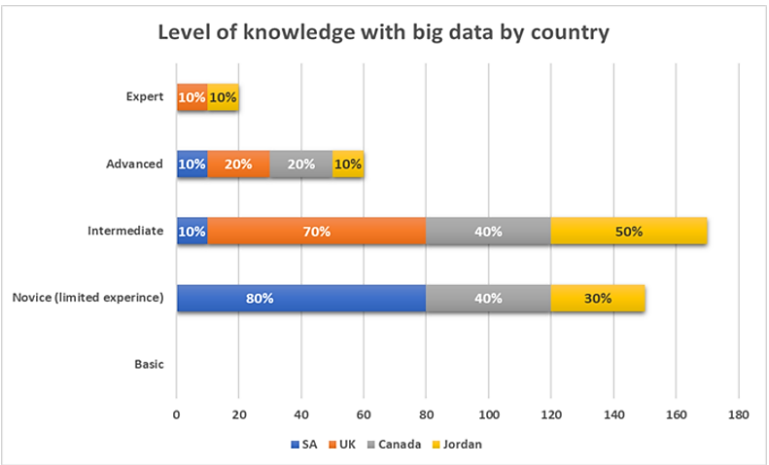

Figure 1. Level of knowledge of big data

Most respondents from all countries show intermediate or practical application knowledge of big data. In terms of the nation of the respondents, the maximum respondent or 80%, in SA have a novice level of knowledge,70% in the UK have intermediate-level knowledge, and 40% in Canada have intermediate, and novice levels of knowledge, respectively, and 50% in Jordan have attained the intermediate level. Only UK and Jordan have respondents with expert knowledge, and about 10% of the respondents are from each country. Similarly,

the respondent's knowledge of cloud computing was enquired to gauge the respondents' awareness of accurate and safe frameworks that provide access to different network sources [36]. The responses are compiled in the form frequency in Figure 2.

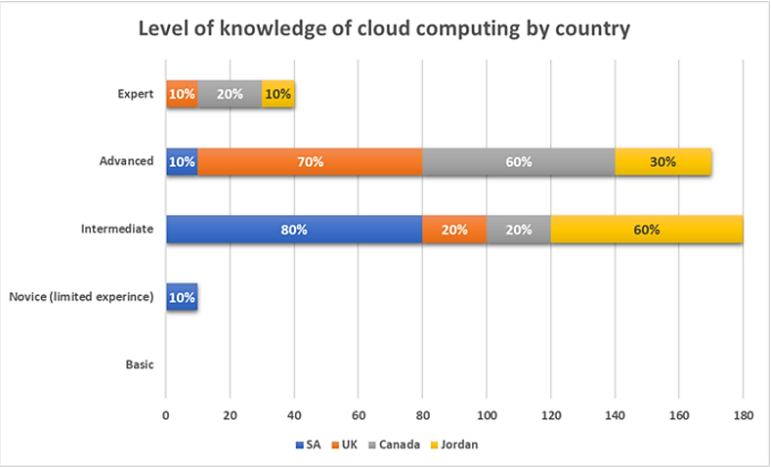

Figure 2. Level of knowledge of cloud computing

Most respondents from different nations were found to have either intermediate or advanced levels of knowledge. Based on the countries, SA has 80%, Jordan has 60% of respondents having intermediate knowledge, the UK has 70%, and Canada has 60% of respondents with an advanced understanding of cloud computing. Also, the quantitative analysis of respondents' answers revealed the knowledge of risk management in each country to find an organization's existing risk assessment methods and policies. The responses gathered are presented in Figure 3. Figure 3 reveals that 50% of respondents in SA had advanced knowledge of risk, 50% of respondents in the UK also had advanced knowledge, 60% of the respondents in Canada had expert-level knowledge, and in Jordan, 40% belonged to advanced and intermediate groups, respectively. Only SA has 20% of respondents in the limited experience domain and faces challenges in risk assessment.

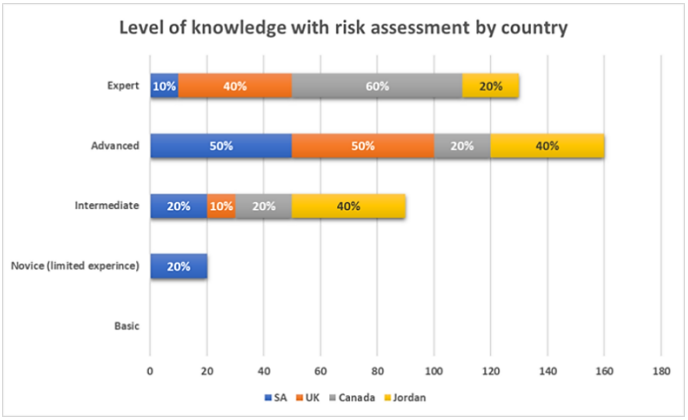

Figure 3. Level of knowledge with risk assessment

3.2 Implementation of Big Data and Cloud Services in the Organizations

To enquire about the implementation of big data and cloud services in the organizations across the four countries, respondents were asked whether or not big data is implemented in their organization; the responses gathered are presented in Figure 4.

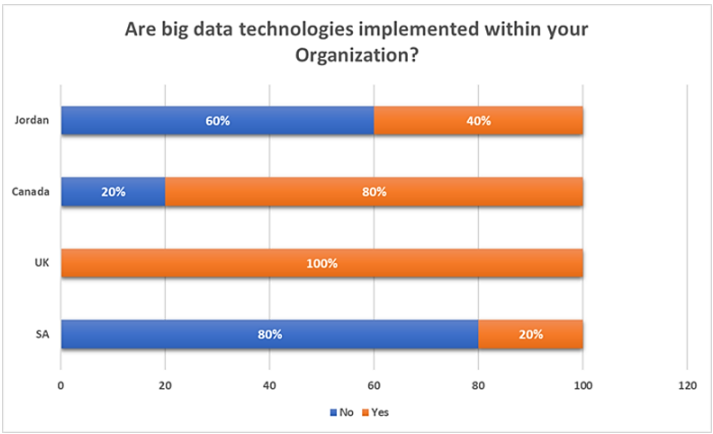

Figure 4. Implementation of big data technologies within organizations

Figure 5 reveals 100% implementation in the UK, 80% in Canada, 40% in Jordan, and only 20% in SA. The remaining respondents reveal that there was no adoption of big data. The respondents were further enquired about the level of cloud computing implemented in their organizations, and the responses are presented in the figure below. In SA, big data technology uses analytics to make smarter

decisions, enhance work efficiency through risk management models, create smarter policies and plans, and enable organizations to understand client needs. In Jordan, the government promotes big data technology to save time, and client base, gather customer insight, and cost savings, leading to focused retention of customers and more profits and sales. In Canada, big data application is implemented for convenience, reliability, and safety features. In the UK, the adoption of the technology is 100%.

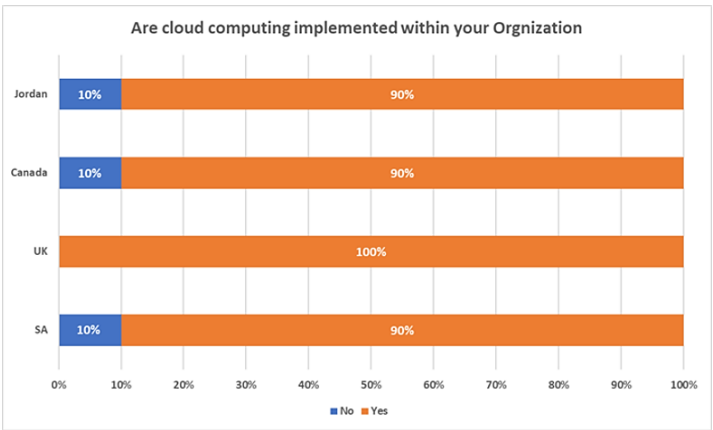

Figure 5. Implementation of cloud computing in organizations across all four countries

The responses reveal that cloud computing implementation is 90% in Canada, 100% in the UK, 90% in Jordan, and 90% in SA. The 10% of Canadians responding to the lack of implementation of cloud computing suggested they are in the adoption stage to prepare themselves for high customer demand and big data handling. In Jordan, the non-conformity, as suggested by the respondents, aroused due to the high cost of implementation, lack of qualified individuals, and analytical needs for comprehending the impacts of technology. In SA, the respondents working in nonconforming organizations suggested a lack of clarity of why the technology was not adopted as it could improve uptime and overall reliability.

3.3 Existing Risk Assessment Methods and Policies in the Organizations

To gauge the policies in place for risk assessments in the organizations in each country, the first policies adopted by the companies for termination or transfer of data to the cloud service were enquired about, and the responses are presented in the graph Figure 6.

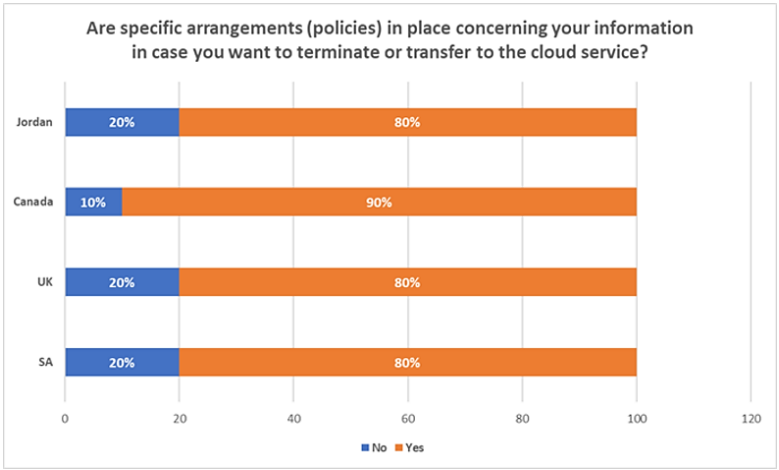

Figure 6. Are specific arrangements (policies) in place concerning your information in case you want to terminate or transfer to the cloud service?

Figure 6 shows that only Canada has 90% of respondents stated the presence of policies for termination or transfer of data to the cloud service, and the rest of the nation has 80% compliance in place. Those respondents showing non-presence of policy in Canada stated implementation based on the real-life scenario-based implementation of risk coverage. In SA, the respondents stated a lack of a clear Information Governance policy. In Jordan, the migration will be determined based on cost, and in UK policies, implementation has been delayed due to different factors, such as COVID-19. For having a clear risk management plan in place, the respondents reveal that in SA, there are Governance Risk and Compliance framework policies for management. The respondents in the UK suggested that part of organizational risk assessment is entwined with a business recovery plan, and it includes regular testing of data and network backup with recovery. In Jordan, the plan is not mature enough; however, the employees are trained. In Canada, there is a risk assessment plan and the case of a cyber-attack. To answer what was covered in the risk plans in organizations, the respondents in Canada identified the prominent themes of data in transit, security, encryption, leakage, and control systems. There was mitigation of data leakage and data protection practices in Canadian organizations. In organizations in the UK, the current risk plan covers training, data security and access, SSL, data authentication, data transmission, and end-user. There is high usage of secure channels for transmission and data backups, too, with TLS (Transport Layer Security) protection that supports end-user authentication and access control. In Jordanian companies, the risk plan covers data access, encryption, security, preventative measures, control systems, and handling of sensitive information. Further, in SA,

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

the themes included data in transit, data security, data encryption, and control systems. These themes are compiled and presented in the figure below.

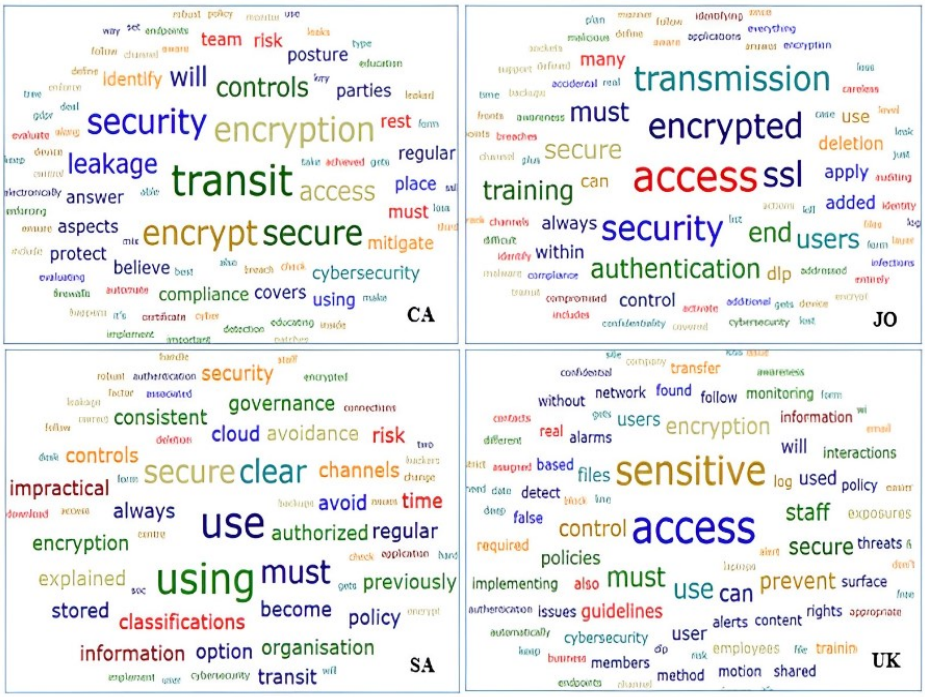

Figure 7. Themes covered in risk assessment plans in different countries

The risks related to data protection identified in various nations are presented in Figure 8. It shows the themes of the federal government's role, data protection, and the Personal Information Protection Act in Canada, such as the Personal Information Protection and Electronic Documents Act (PIPEDA). In Jordan, the risk of training, legal threats from clients, and a lack of authority to deal with the illegal use of data. In SA, the threats were related to the Protection of Personal Information Act introduced (POPIA) in July 2021 covered the themes of corruption, data loss, or disclosures that lead to legal issues. Further, in the UK, the risks were reported from individual rights, data access-related risks, regulation and rights-associated risks, lack of legal threats, and data protection around the Data Protection Act 2018.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

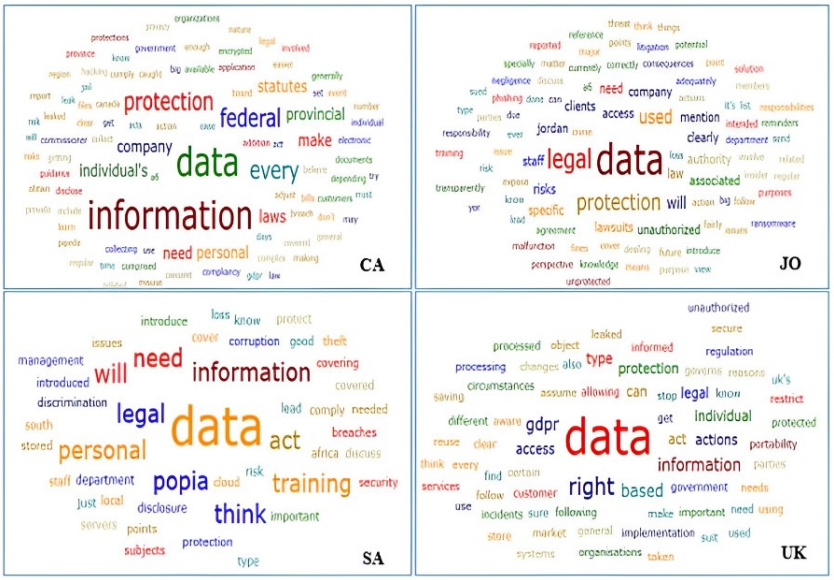

Figure 8. Risks related to data protection in various countries

3.4 Challenges and Shortcomings of the Risk Assessment Methods

The challenges and shortcomings of the risk assessment methods in Canada awareness and training related to identifying threats and cybersecurity. The problem also arises from not all parties taking cybersecurity seriously, leading to data breaches. In Jordan, staff training is a must, and data must be used adequately, fairly, transparently, and only for a specific purpose. In SA staff training to cover data-related risks, more was advised to overcome the shortcomings of the risk assessment methods. Lastly, in the UK, emphasis on awareness of acts governing incidences of security threat is less than acts as a challenge for implementing risk assessment. The challenge in the nation also arises from the type of data to be protected, as not all data is important and cannot be pursued with legal action.

3.5 Discussions

The study examines risk assessment methods in each country for managing big data using cloud services. The data analysis reveals that risk plans cover data encryption in Canada to prevent data loss and educate employees about cyber security. Concerning the same, Ali et al. [37] are suggestive of the implementation of the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) and Failure Mode and Effect Analysis (FMEA) to counter the problems of

database hack risks, broadcast data errors, cyber-attack, network interruptions, server failures, and virus effects. In the UK, the risk plan covers secure transmission channels, security and awareness training, data encryption in transit, Transport Layer Security, prevention of data leaks, and tracking suspicious activity. In addition, General Data Protection Regulation (GDPR) is responsible for transparency, fairness, data minimization, accuracy, accountability, and integrity, among other features [38]. In Jordan, data loss prevention practices, encryption, guidelines, and staff training to ensure cyber security are maintained. Creating management support, funding, technical expertise, alignment with the organization's objectives, and user security awareness is considered imperative [39]. Moreover, the conceptual framework for this study is shown in Fig.9. It provides a model representation of risk assessment and management of risk in big data using cloud services. The framework describes the relationship between big data usage under cloud computing and risk assessment methods. The risk assessment methods and the possible risks prevailing in the cloud-based virtual environment need strategic integration to improve services.

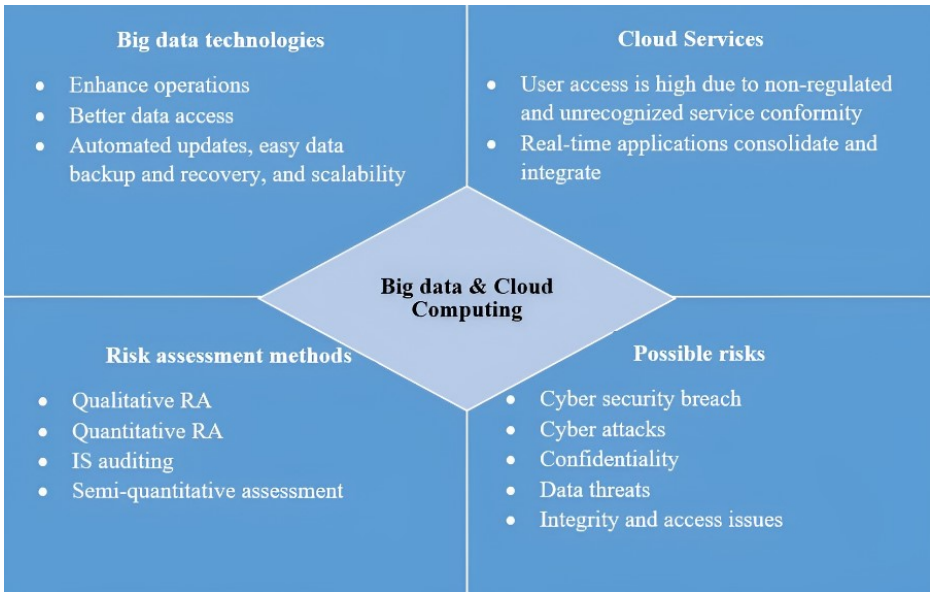

Figure 9. Conceptual framework

In SA, the risk assessment framework lacks a consistent information governance policy and is based on avoidance based on previous learning and training. The findings of Masilela and Nel [40] are similar and suggest adopting measures of

Information Security Policy, Email Archiving Solution, Data Linkage Prevention Solution, and Access Control Systems, among others.

3.6 Contribution to the knowledge

This study will help improve cloud service providers' risk assessment for cloud-integrated big data services. It examines the relationships between cloud computing, big data, and risk assessment. A greater grasp of these concepts is expected to improve academic debate and discussion on risk assessment in the cloud and big data contexts.

3.7 Study limitations

Finding interviewees was a challenge for this project. Jordan and South Africa were the hardest since the researcher had to contact too many people. The researcher used two alternative strategies. First, researchers created a Google Form with questionnaire questions and shared it on social media. The link was posted to a LinkedIn page, and network contacts shared it. The second contingency plan comprised the researcher contacting a US firm that helped share the questionnaires and target a specific population. Due to time constraints and numerous time zones, scheduling was very difficult. The pandemic made potential respondents unwilling to spend 30 minutes answering questionnaires. When the researcher could not interview confirmed responders, he suggested other possibilities, such as audio or video recordings. Due to the Covid-19 outbreak, face-to-face interviews were also impossible, and most potential responders refused to participate in video calls. Covid-19 has caused many to adjust their regular activities, including avoiding others, working from home, and virtually attending school. Again, the researcher gave responders options like voice or video recording or typing the answer.

3.8 Areas for future work

Big data and the issue of risk assessment are becoming crucial to organizations all over the world. This thesis adds to our understanding of big data and cloud computing risk assessment, primarily focusing on Canada, Jordan, SA, and the UK. This study acknowledges that new technology is now a requirement rather than a luxury. Some nations' risk assessment plans fail to incorporate the 4th IR. Big data's function and how to use it to your advantage in the competitive market have received little attention. To be completely realized, some of the cloud computing and big data concepts outlined in this thesis will need further development and extension. The researcher suggests the following areas for further research because she thinks they will add to the knowledge that will aid

organizations in better-identifying hazards while deploying big data and cloud computing technologies. First and foremost, the researcher contends that more study is necessary to properly understand how analytics and information management have evolved in cloud-based analytics. Another worrying finding of the study was how little cloud computing and big data were employed in less developed nations like Jordan and South Africa. Therefore, research on adaptation and mitigation techniques for dangers in big data and cloud computing is necessary. Thirdly, this study discovered that one of the major barriers to adopting cloud computing and big data is the concern of cyber security threats. Future research in developing tactics and solutions to address privacy and security problems is recommended in this regard by the study. Future research can focus on other areas as long as it strives to change the cloud system from just a data management platform to a scalable data analytics platform; thus, it is not restricted to the ones stated above.

4. CONCLUSION

The study reveals that UK organizations were leading in the different aspects of knowledge of big data, cloud computing, and risk assessment. However, implementing big data and the cloud completely in organizations is restrained by the pandemic. For Canada, the adoption of cloud strategies is on the rise; hence, organizations are also expanding their horizon on the systematic handling of risks. In Jordan, organizations are moving towards more big data and cloud computing adoption with the government's support. However, the sector faces problems of technological, legal, and organizational barriers. In SA, the adoption of big data is facilitated by acts such as POPIA. In the future, such legislation will allow organizations to advance in the information security domain. The recommendations for the study are as follows:

1) The government needs to explore cost-effective ways to enhance the use of big data. This will allow firms to gain in-depth industry knowledge and multidisciplinary expertise combining technological, Data & Analytical possibilities.
2) In Canada, adopting risk assessment and frameworks can be enhanced by adopting big data technologies and addressing the country's lack of knowledge or skill in implementing the technology.
3) In Jordan, the lack of training, legal threats from clients, and a lack of authority need to be addressed to adopt risk assessment processes better.
4) With legalizations in place, SA organizations must focus on encouraging the workforce to be data specialists and encourage the use of big data and cloud computing technologies.

REFERENCES

[1] K. Raja and S. M. Hanifa, "Bigdata Driven Cloud Security: A Survey.," *IOP Conference Series: Materials Science and Engineering.,* vol. 255, no. 1, Aug 2017.

[2] V. Rao and T. Rao, "Big Data and Its Applications," *International Journal of Advanced Research in Science, Communication and Technology,* vol. 2, no. 3, pp. 57-149, 15 Feb 2021.

[3] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," *nternational Journal of Computer Science and Information Technology & Security (IJCSITS),* vol. 1, no. 2, pp. 136-146, 2011.

[4] Y. Sivasubramanian, S. Z. Ahmed, and V. P. Mishra, "Risk assessment for cloud computing," *International Research Journal of Electronics and Computer Engineering,* vol. 4, p. 6, June 2017.

[5] P. R. Kumar, P.H. Raj, and P. Jelciana "Exploring data security issues and solutions in cloud computing," *Procedia Computer Science,,* vol. 125, pp. 691-697, 2018.

[6] M. H. Raza, A. F. Adenola , A. Nafarieh, and W. Robertson, "The slow adoption of cloud computing and IT workforce," *Procedia Computer Science,* vol. 52, pp. 1114-1119, 2015.

[7] C. K. Chen, and M. N. Almunawar, "Cloud Computing in Higher Education," *Impact of Economic Crisis on Education and the Next-Generation Workforce: IGI Global*, 2016, pp. 285-308.

[8] S. Y. Tabassam, I. Sattar, N. Manzoor, and S. Ashraf, "Cloud Service Providers: A Comparative Analysis of Cloud Storage Pricing," *International Journal of Computer Applications,* vol. 975, p. 8887, 2017.

[9] Q. Hammouri, and E. A. Abu-Shanab, "Major factors influencing the adoption of cloud computing in Jordan," *International Journal of Technology and Human Interaction (IJTHI),,* vol. 16, no. 4, pp. 55-69, 2020.

[10] M. Awad, and R. Khanna, "Efficient learning machines: theories, concepts, and applications for engineers and system designers," *Springer nature*, 2015.

[11] A. Sprintson, "Network coding and its applications in communication networks," in *Algorithms for Next Generation Networks*, Springer, 2010, pp. 343-372.

[12] E. Raguseo, "Big data technologies: An empirical investigation on their adoption, benefits and risks for companies," *International Journal of Information Management,* vol. 38, no. 1, pp. 187-195, 2018.

[13] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable*

Computing: Informatics and Systems, vol. 19, pp. 174-184, 2018.

[14] N. Zanoon, A. Al-Haj, and S. M. Khwaldeh, "Cloud computing and big data is there a relation between the two: a study," *International Journal of Applied Engineering Research,* vol. 12, no. 17, pp. 6970-6982, 2017.

[15] H. Y. a. X. C. S. Zhang, "Research on key technologies of cloud computing," *Physics Procedia,* vol. 33, pp. 1791-1797, 2012.

[16] S. Zhang, H. Yan, and X. Chen, "Recent applications of big data in finance," *Proceedings of the 2nd International Conference on Digital Tools & Uses Congress,* pp. 1-6, 2020.

[17] V. N. Inukollu, S. Arsi, and S. R. Ravuri, "Security issues associated with big data in cloud computing," *International Journal of Network Security & Its Applications (IJNSA),* vol. 6, no. 3, p. 45, 2014.

[18] B. M. Balachandran, S. Prasad, "Challenges and benefits of deploying big data analytics in the cloud for business intelligence," *Procedia Computer Science,* vol. 112, pp. 1112-1122, 2017.

[19] T. Alashoor, "Cloud computing: a review of security issues and solutions," *International Journal of Cloud Computing,* vol. 3, no. 3, pp. 228-244, 2014.

[20] N. Fotiou, A. Machas, G. C. Polyzos, and G. Xylomenos, "Access control as a service for the Cloud," *Journal of Internet Services and Applications,* vol. 6, pp. 1-15, 2015.

[21] H. Boinepelli, "Applications of big data," in *Big Data: A Primer*, Springer, 2015, pp. 161-179.

[22] A. L'heureux, K. Grolinger, H. F. Elyamany, and M. A. M. Capretz, "Machine learning with big data: Challenges and approaches," *Ieee Access,* vol. 5, pp. 7776-7797, 2017.

[23] K. V. D. Schyff, and K. E. M. Krauss, "Higher education cloud computing in South Africa: towards understanding trust and adoption issues," *South African Computer Journal,* vol. 55, no. 1, pp. 40-55, 2014.

[24] Sodikin, "Cloud computing," vol. 39, no. 1, pp. 1-15, Jan 2014.

[25] R. Machuga, "Factors determining the use of cloud computing in enterprise management in the EU (considering the type of economic activity)," *Problems and Perspectives in Management,* vol. 18, no. 3, p. 93, 2020.

[26] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation," *Risk Analysis,* vol. 42, no. 8, pp. 1643-1669, 2022.

[27] K. Williamson, G. Johanson, "Research methods: Information, systems, and contexts," *Chandos Publishing*, 2017.

[28] J. V. Maanen, "Reclaiming qualitative methods for organizational research:

A preface," *Administrative science quarterly,* vol. 24, no. 4, pp. 520-526, 1979.

[29] S. Yeasmin, and K. F. Rahman, "Triangulation research method as the tool of social science research," *BUP jounal ,* vol. 1, no. 1, pp. 154-163, 2012.

[30] G. Zissis, and P. Bertoldi, "Status of LED-lighting world market in 2017," *Ispra: European Commission*, 2018.

[31] G. H. Galal-Edeen, "Information systems requirements engineering: An interpretive approach," *The Egyptian Informatics Journal,* vol. 6, no. 2, pp. 154-174, 2005.

[32] R. W. Service, "Book Review: Corbin, J., & Strauss, A.(2008). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory . Thousand Oaks, CA: Sage," Organizational Research Methods, vol. 12, no. 3, pp. 614-617, 2009.," pp. 614-617, 2008.

[33] M. A. Abdel-Fattah, "Grounded theory and action research as pillars for interpretive information systems research: A comparative study," *Egyptian Informatics Journal,* vol. 16, no. 3, pp. 309-327, 2015.

[34] H. R. Bernard, "Social research methods: Qualitative and quantitative approaches," *Sage*, 2013.

[35] J. Wieczorkowski, and I. Pawełoszek, "Big data privacy concerns in the light of survey results," *IADIS International Journal on WWW/Internet, Available from: shorturl.at/kyIW3,* vol. 14, no. 1, pp. 70-85, 2016.

[36] H. Rezaei, B. Karimi, and S. J. Hosseini, "Effect of cloud computing systems in terms of service quality of knowledge management systems," *Lecture Notes on Software Engineering,* vol. 4, no. 1, p. 73, 2016.

[37] S. M. Ali, S. M. N. Hoq, A. B. M. M. Bari, G. Kabir, and S. K. Paul, "Evaluating factors contributing to the failure of information system in the banking industry," *Plos one,* vol. 17, no. 3, p. e0265674, 2022.

[38] S. Gutwirth, Y. Poullet, P. De Hert, and R. Leenes, "Computers, privacy and data protection: An element of choice," *Springer*, 2011.

[39] I. Obeidat, and A. Mughaid, "Implementing Factors of Information Security in Governmental Organizations of Jordan," *The Thirteenth International Conference on Digital Society and eGovernments,* 2019.

[40] L. Masilela, and D. Nel, "The role of data and information security governance in protecting public sector data and information assets in national government in South Africa," *Africa's Public Service Delivery and Performance Review,* vol. 9, no. 1, p. 385, 2021.