South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Emerging South African smart cities: Data security and privacy risks and challenges

Authors:
Francois P. Cornelius[1]
Shandre K. Jansen van Rensburg[1]

Affiliations:
[1]Department of Criminology and Security Science, Faculty of Law, University of South Africa, Pretoria, South Africa

Corresponding author:
Shandre Jansen van Rensburg,
sissisk@unisa.ac.za

Dates:
Received: 26 Feb. 2024
Accepted: 24 June 2024
Published: 28 Aug. 2024

How to cite this article:
Cornelius, F.P. & Jansen van Rensburg, S.K., 2024, 'Emerging South African smart cities: Data security and privacy risks and challenges', *South African Journal of Information Management* 26(1), a1847. https://doi.org/10.4102/sajim.v26i1.1847

Copyright:
© 2024. The Authors. Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Read online:
Scan this QR code with your smart phone or mobile device to read online.

Background: Smart cities leverage advanced technologies such as the Internet of Things (IoT), fifth generation (5G) networks, and data analytics to enhance citizens' quality of life, focussing on creating efficient, functional, and eco-friendly urban environments. While these initiatives offer significant benefits, there are ongoing concerns about data security and privacy.

Objectives: This article investigates the data security and privacy risks and challenges in emerging South African smart cities. The objectives are to identify these risks, assess the effectiveness of current security measures, and contextualise these vulnerabilities within the South African and global contexts.

Method: A qualitative approach was adopted, involving virtual interviews with 20 Subject Matter Experts (SMEs) through purposive and snowball sampling. The raw data were thematically analysed, revealing significant themes.

Results: Emerging South African smart cities face several risks and challenges, including poor governance, a shortage of skills, a lack of awareness and training, insufficient funding, and a combination of these factors.

Conclusion: The research highlights the importance of safeguarding individuals' data and privacy in the context of smart cities, advocating the need for proactive measures to address these concerns.

Contribution: This article promotes interdisciplinary dialogue, leading to more comprehensive solutions. In addition, exploring data security and privacy in emerging smart cities aids in understanding the implications of information management practices. Although the article focuses on emerging South African smart cities, the challenges discussed have global relevance.

Keywords: cyberattacks; data breaches; data security and privacy risks; data security; emerging smart city; information security risks; information security; privacy; smart city.

Introduction

Smart cities are urban areas that leverage advanced technologies like the Internet of Things (IoT), 5th generation (5G) networks and data analytics to improve residents' quality of life. These technologies are combined to streamline city operations, enhance public services, support sustainability and address urban issues. The main aim of smart cities is to develop more efficient, functional and eco-friendly urban environments (Allam 2021; Cunha 2021; Mashau & Kroeze 2023; Vaidya et al. 2021). Despite its potential, scholars have expressed concerns about data security and privacy risks (Barlow & Levy-Bencheton 2019; Fabrègue & Bogoni 2023; Ismagilova et al. 2019; Trapenberg Frick et al. 2021). These risks, evident in smart cities worldwide, encompass service delivery interruptions, financial implications, decreased public trust, compromised data integrity, privacy breaches and legal repercussions, ultimately hindering innovation (Braun et al. 2018; Cui et al. 2018; Rao & Deebak 2023). Moreover, in the South African context, the relevance of smart cities is challenged in the face of significant socio-economic disparities (Balkaran 2019; Masiba 2023; Musakwa & Mokoena 2017). Nevertheless, South Africa is actively pursuing smart city initiatives, as evidenced by numerous ongoing projects and new developments (Bouwer 2022; BusinessTech 2022).

The coronavirus disease 2019 (COVID-19) pandemic intensified reliance on IoT for daily activities, emphasising the necessity of digital connectivity for transforming cities into smart cities (Kaspersky 2020; KPMG 2020). However, the escalating volume of data in smart cities raises

concerns about data security and privacy risks during collection, storage and analysis (Hassan et al. 2019; Ismagilova et al. 2019; Politou et al. 2022). As the digital landscape expands, cybersecurity risks, including cyberattacks, surge rapidly (Deloitte 2019, 2021; Neshenko et al. 2020; Silva, Khan & Han 2018). South Africa has witnessed a significant rise in risks because of increased country-wide cyberattacks (Mcanyana, Brindley & Seedat 2020). Further escalation in the scale and impact of data security and privacy risks were evident with the major TransUnion data breach in 2022, which compromised the personal information of 54 million consumers in South Africa (Moodley 2022).

International studies have explored data security and privacy risks in smart cities such as sustainability, vulnerabilities, risk management, prevention strategies, challenges and opportunities. In response to these challenges, continuous audits, assessments, regulatory reviews, standardised frameworks, advanced technologies and awareness and training programmes are implemented to mitigate these risks effectively (Farahat et al. 2021; Huda et al. 2024; Hussain 2024; Kitchin & Dodge 2020; Paes et al. 2023; Sookhak et al. 2018; Xia, Semirumi & Rezaei 2023). However, limited scientific studies have been conducted on data security and privacy risks linked to smart technology in emerging South African smart cities (Academy of Science of South Africa [ASSAf] 2019; Boyle 2020; Guya & Wilson 2020; Murray 2020). As a result, this article explores the data security and privacy risks faced by emerging smart cities in South Africa. This will be realised by identifying data security and privacy risks in emerging smart cities, evaluating the effectiveness of existing security measures and placing these vulnerabilities within the broader contexts of South Africa and the global landscape.

The article introduces and contextualises data security and privacy risks in emerging South African smart cities. It then outlines the research methodology used. It concludes by discussing the key findings on the risks and challenges associated with data security and privacy in these smart cities.

Contextualising data security and privacy risks in smart cities

Smart city infrastructure integrates advanced technologies like IoT, 5G networks, artificial intelligence (AI) and cloud storage (Akhuseyinoglu & Joshi 2020). This infrastructure encompasses physical components such as energy and transportation systems and digital technologies including AI, smart sensors and data analytics (Ahmad & Mehmood 2020; Ferreira 2021). Smart cities employ various technologies and strategies to collect (sensors and IoT devices, smart meters, video surveillance, mobile applications), store (cloud and edge computing) and process large volumes of data about residents, infrastructure and services (big data analytics, AI, data integration platforms) (Gracias et al. 2023). Neshenko et al. (2020) analysed 10 global smart cities to outline their architectural framework, defining five tiers: the physical world, enablers, data, applications and management layers.

The physical world tier of smart city architecture encompasses urban infrastructure, including office buildings, roads, buses and traffic lights (Neshenko et al. 2020). The enablers layer consists of hardware and communication technologies essential for collecting and transmitting data to subsequent architectural layers (Neshenko et al. 2020). However, Silva et al. (2018) caution that smart city infrastructure faces significant risks because of the proliferation of data generated by hardware such as smart grids, smart sensors, information and communication technologies (ICT) systems, AI and broadband networks. Le-Dang and Le-Ngoc (2018) warn that these risks may lead to system failures caused by cybercriminals executing data breaches and other forms of data manipulation. The data layer is a pivotal component of smart cities, serving as a central repository for vast amounts of structured, semi-structured and unstructured data collected from various sources (Ghandour, Elhoseny & Hassanien 2019; Neshenko et al. 2020). According to Arfat et al. (2020), these data hold significant value, and when coupled with AI and data analytics, play a crucial role in enhancing operational efficiency within smart cities. Neshenko et al. (2020) further explain that the data layer facilitates data exchange among stakeholders through open data platforms (ODPs). Moreover, the applications layer enables smart cities to offer diverse solutions to residents and visitors alike. For instance, the MyCiTi App in Cape Town allows users to plan journeys using the city's public transport system (MyCiTi 2021), demonstrating how data-driven transportation systems can address congestion, pollution, parking management and road safety (Neshenko et al. 2020). At the management tier, smart cities focus on service delivery, asset management and overall security (Neshenko et al. 2020). Aqib et al. (2020) emphasise that this tier also encompasses disaster and emergency management, addressing natural and man-made crises such as floods, hurricanes, earthquakes and terrorist attacks.

The threat landscape of smart cities includes exploratory threats, data manipulation, infrastructure sabotage and third-party vulnerabilities. 'Exploratory threats' are attacks that target critical resources and personal credentials. 'Data manipulation' are threats that compromise the confidentiality, integrity and availability of data within a network. 'Infrastructure sabotage' involves threats intending to disrupt or gain control over smart city infrastructure using malicious software such as ransomware or malware. 'Third-party vulnerabilities' refer to threats posed by malicious actors targeting third-party service providers crucial to smart city operations (Neshenko et al. 2020).

Privacy and security, along with the design, maintenance and implementation costs, are critical aspects of smart cities (Kasar & Kshirsagar 2021). Limited studies have addressed data security and privacy risks associated with smart cities

(Dhungana et al. 2015; Vitunskaite et al. 2019). Research indicates that privacy is easily compromised because of the high levels of interaction between people, devices and sensors, emphasising the need for enhanced data security and privacy mechanisms (Elmaghraby & Losavio 2014; Picon 2019). Furthermore, smart cities process large volumes of sensitive and private data daily within their IoT ecosystems, attracting cybercriminals seeking to exploit this data (Ahmed et al. 2021; Azmoodeh, Dehghantanha & Choo 2019; Magare, Dudhgaonkar & Kondekar 2021). This raises significant concerns about data security related to transmission, storage and server protection (Teing et al. 2019). Cornelius (2022) highlights concerns about cloud computing and storage, particularly the risk of data loss during communication between devices. According to Trapenberg Frick et al. (2021), smart cities depend on intricate ICT networks and numerous IoT-connected devices to provide essential services, making them vulnerable to malicious actors online. Al-Turjman, Zahmatkesh and Shahroze (2019) stress the need for smart cities to invest in robust methods to ensure data integrity during IoT device communications. Hassan et al. (2019) highlight the risks associated with classified organisational information stored by third-party providers, which could be hacked or corrupted. Cui et al. (2018) recommend implementing privacy protection, authentication, confidentiality and data availability measures using technologies like blockchain, cryptography, biometrics and machine learning to counter these threats.

Data analytics play a critical role in the decision-making processes of smart cities by tracking people and objects (Dhungana et al. 2015). However, the privacy of this data can be compromised if not properly secured (Politou et al. 2022; Vaidya et al. 2021). Privacy concerns in smart cities arise in areas such as employment, healthcare and home automation (Huang, Wang & Yang 2017). Cornelius (2022) warns that inadequate data security can lead to privacy breaches, identity theft and the selling of personal data or state secrets.

Local governments and emerging smart cities in South Africa handle and protect citizens' personal information, healthcare records, educational data and other confidential information (Masombuka, Grobler & Duvenage 2021; Research ICT Africa 2020). Additionally, private companies within smart cities collect large amounts of data on individuals for marketing purposes, posing privacy risks even from basic Internet searches (Lozada, Arias-Pérez & Perdomo-Charry 2019; Vaidya et al. 2021).

The security of data transmission, retention and storage is crucial for ensuring privacy (Al-Turjman et al. 2019; Vaidya et al. 2021). Hammi et al. (2017) emphasise that citizens will be reluctant to embrace IoT benefits if their privacy is threatened. IBM Security (2021) cautions that breaches in data security and privacy could lead to significant financial losses and undermine trust in smart city institutions and organisations. Thus, research on data security and privacy risks associated with emerging smart cities is warranted.

Research goal

The article examines data security and privacy risks and challenges in emerging South African smart cities. To achieve this aim, the article is guided by the following objectives: 1. To identify data security and privacy risks in emerging smart cities, 2. To assess the effectiveness of current security measures and 3. To contextualise these vulnerabilities within the context of the South African and global milieu. Thus, the article is premised on the following research question: What are the data security and privacy risks and related challenges in emerging South African smart cities?

Research methods and design

Design and procedures

A qualitative approach was employed to explore the main data security and privacy risks and challenges in emerging smart cities in South Africa. Utilising a qualitative methodology enhanced the depth of comprehension regarding the subject under investigation (Leavy 2023). The research investigation was exploratory as it ventured into a relatively novel issue with a limited understanding of the phenomenon in the South African context (Neuman 2020). This type of study produces descriptive and explanatory data that are not intended to be conclusive and requires a creative and open-minded approach (Hesse-Biber 2017). Therefore, a phenomenological research approach was employed to gain insights into perceptions, perspectives and experiences concerning data security and privacy within the context of emerging smart cities in South Africa (Schurink, Schurink & Fouché 2021). One-on-one interviews were conducted with 20 subject matter experts (SMEs) specialising in various domains associated with data security privacy risks in emerging South African smart cities. The research was informed and endorsed by the University of South Africa's (UNISA) Policy on Research Ethics (University of South Africa 2016:12), and ethical approval was subsequently obtained.

Sample

Purposeful sampling was utilised to obtain a comprehensive understanding of the phenomenon as perceived by the selected 20 SMEs (Flick 2018). Key stakeholders involved in smart city development encompass private and public sectors, technology providers, infrastructure developers, urban planners, architects, regulatory bodies, utility providers, financial institutions and investors. However, the article focussed on sourcing SMEs specialised in domains such as data security and privacy, cybersecurity, advisory and strategy, ICT, information technologies (IT), IoT security, information risk management and smart city technology. Thus, as detailed in Table 1, the findings are well-informed. Furthermore, purposive and snowball sampling were used to collect qualitative data from the research participants. Purposeful sampling enabled the researcher to select individuals based on specific criteria and intentions relevant to the phenomenon being investigated. This method ensures that the sample represents the diversity of perspectives and experiences related to the research topic (Fetters 2020).

TABLE 1: Demographic information of participants.

Participant	Age	Gender	Occupation	Level of education	Years of experience	Industry	Sector
1	53	Female	Director	- Doctor of Philosophy (PhD) Computer Security	- 27 total in data security and privacy	Cybersecurity	Private
2	36	Male	Head of IT	- Experience-based	- 12 total in IT and networks security management	Medical	Private
3	32	Male	Network security specialist	- Multiple IT qualifications - Expert-level network security	- 8 total in IT - 3 network security	IT	Private
4	49	Male	Senior cyber strategy and operations specialist	- PhD Informatics Cyber Counter-intelligence (CI) - Master in Commerce (MCom) Informatics - Multiple cybersecurity certifications (CISM, CISCO, CISSP)	- 27 total in information technology and cybersecurity	Cybersecurity	Public
5	39	Female	Information security and risk management manager	- Bachelor of Science (B.Sc.) Information Systems - B.Com Honours Information Systems (Computer forensics) ISC2 – cybersecurity certification	- 6 in digital forensic analysis/ Cybercrime investigator - 2 in Information security operations	Information security	Public
6	38	Male	Senior business intelligence analyst	- B.Sc. Economics - Certifications in data programming languages	- 11 total in data analysis - 3 in data analytics and analysis	IT	Private
7	34	Male	IT manager	- Cybersecurity certifications (cloud storage) - Expert-level network security	- 5 in IT management	Logistics	Private
8	47	Male	Government official	- PhD International Management - Master of Arts (MA) Security Studies - Published articles related to smart cities - Chief Information Officer (CIO)	- 22 total in designing and developing security solutions related to data security and privacy	Government	Public
9	52	Male	Cybersecurity consultant	- 83 industry certifications	- 34 total in IT - 19 cybersecurity	ICT	Private/Public
10	41	Male	Cybersecurity analyst	- Advanced Diploma in information management - Multiple cybersecurity certifications	- 19 total in software development - 9 cybersecurity	Cybersecurity	Public
11	49	Male	Information assurance engineer	- IT Diploma, - Multiple cybersecurity and data security certifications	- 29 total in IT and cybersecurity	Cybersecurity	Public
12	37	Male	Cyber investigator	- Multiple cybersecurity, data security and data privacy courses	- 14 total Cybersecurity - 5 years of data breach investigations	Cybersecurity	Public
13	35	Male	Cybersecurity consultant	- Cybersecurity courses (NQF 5)	- 14 total in technical fields - 8 cybersecurity	Cybersecurity	Public
14	41	Male	Information risk specialist	- Degree IT - Multiple data security certifications	- 18 total risk management - 7 cybersecurity	Banking	Private
15	31	Female	Technologist	- PhD in applied science: IoT security - EC Council certifications ethical hacking.	- 5 total in IoT security - 1 cybersecurity (ethical hacking)	IoT R&D	Public
16	43	Male	ICT security engineer	- Multiple certifications in network and data security	- 11 total ICT Security Engineering	ICT	Public
17	36	Female	Cloud solution architect	- Certifications in Microsoft Data and AI Cloud Solution Architect	- 12 total in IT and network security	IT	Private
18	40	Female	ICT customer relations	- National Diploma in IT: Software Development - Introduction Course to Cybersecurity	- 18 years' experience in ICT customer relations	IT	Public
19	45	Male	ICT security engineer	- Diploma in Computer Science	- 14 years in cybersecurity, incident detection and response and forensic analysis.	ICT	Public
20	42	Female	ICT customer relations	- Diploma in Information Technology	- 11 Working experience in ICT	ICT	Public

IT, information technology; AI, artificial intelligence; IoT, Internet of Things; ICT, information and communication technologies; R&D, research and development.

Snowball sampling was employed by asking initial research participants to suggest and nominate other potential participants who could make valuable contributions to the study. Snowball sampling was used by inviting initial research participants to recommend and nominate other potential participants who could provide valuable insights for the study (Babbie 2021). Both methods were utilised to gather data until reaching a point of data saturation. Participants were selected based on defined criteria to minimise sample bias, using diverse sources to identify potential participants and documenting the entire process. Personal biases were avoided by adhering strictly to these criteria rather than relying on subjective judgements, and ongoing reflection was employed throughout the sampling process. Additionally, triangulation was applied by combining purposive sampling with snowball sampling methods.

Data collection and analysis

The article incorporated both primary and secondary sources of information. Data were collected through virtual interviews on Microsoft Teams and Zoom platforms and interviews via email (Roulston & Choi 2018). The structured email interview questions mirrored those used in virtual, real-time interviews (Radigan & Mendez 2018). Research participants shared personal and public documents detailing data security and privacy risks they encountered in their professional experiences.

Thematic data analysis was conducted according to the conventional phases of analysis and interpretation outlined by Leavy (2023), during which themes emerged. The interview transcripts were thoroughly reviewed multiple times to gain a comprehensive understanding of the content.

Significant features were systematically coded across the entire dataset, focussing on recurring aspects related to data security and privacy risks. These codes were then reviewed and grouped into potential themes. Broader patterns and key themes capturing the essence of the data were identified. The themes were refined for accuracy and clearly defined, with appropriate labels reflecting the data they represent. Finally, the data were compiled into a manuscript, and the findings are presented in the next section.

To enhance the depth of understanding of the phenomenon under investigation, data triangulation was achieved by incorporating multiple sources of data (Hesse-Biber 2017).

Ethical considerations

The research study was approved by the UNISA 2022 Ethics Review Committee. The study was determined low-risk in compliance with the Unisa Policy on Research Ethics and Standard Operating Procedure on Research Ethics Risk Assessment (Ethical clearance number ST86-2022).

Findings and discussion

South Africa's emerging smart cities confront an increasingly complex threat landscape that endangers the data security and privacy of their citizens (Cornelius 2022; Mcanyana et al. 2020; Pieterse 2021). Given the ongoing development of smart cities in South Africa, incidents of data security and privacy breaches are highlighted to emphasise the associated severity of the issue. This issue is not isolated to South Africa; it reflects a global concern. In 2021 alone, data breaches reached a record high, with over 5.1 billion records compromised (Irwin 2022). Consequently, the findings on data security and privacy risks in South African smart cities are not only pertinent locally but also provide valuable insights for other developing nations worldwide.

Data security and privacy risks and challenges in emerging South African smart cities

Participants were tasked with identifying the data security and privacy risks and challenges facing emerging smart cities in South Africa. The identified risks and challenges include poor governance, a shortage of skills, a lack of awareness and training, insufficient funding and a combination of these factors.

Poor governance

Participants identified poor governance as a major risk to data security and privacy in emerging South African smart cities. Fabrègue and Bogoni (2023) emphasise the detrimental impact of inadequate governance on individual privacy and information security within smart cities, citing potential trade-offs between policy efficiency, business profitability, consumer convenience and personal privacy. The absence of accountability and disciplinary action has severely undermined good governance in local government, compromising the provision of basic services. Additionally, the financial instability of local governments, stemming from poor governance, has further hindered public service delivery (Thusi & Selepe 2023). The fiscal year 2021/2022 highlighted this issue, as only 38 out of 257 municipalities received clean audits, underscoring the widespread lack of consequence management and governance failures (Erasmus 2023). This illuminates scepticism about the potential for effective governance in emerging South African smart cities if basic services continue to go undelivered in many communities. Participants reported governance risks associated with non-compliance with data security and privacy legislation as a major concern. Participant 10 highlighted fears about the oversight of new technology implementation, emphasising that regulatory non-compliance poses serious risks. Despite South Africa's adoption of the National Cybersecurity Policy Framework (NCPF) in 2015, challenges persist in implementing the cybersecurity strategy at the national level (Malatji, Marnewick & Von Solms 2021).

Participants also pointed out governance risks linked to cybersecurity infrastructure, confidentiality concerns and third-party service providers. The absence of secure technology for data storage and transmission, potential misuse of data by third parties and insufficient contractual agreements with vendors pose substantial risks. Participant 6 stressed the need for well-drafted service-level agreements (SLAs) to mitigate security risks arising from interactions between governments, municipalities and the private sector in emerging South African smart cities. Pereira et al. (2018) and Ramparsad (2020) advocate for the adoption of 'smart' governance principles in smart cities to effectively address potential risks. Despite challenges faced by emerging South African cities, Ramparsad (2020) suggests that smart principles and initiatives leveraging urban data for enhanced governance should continue shaping their trajectory.

Participants 4 and 10 underscored the challenges associated with insufficient public-private partnerships (PPPs) in emerging South African smart cities. Strengthening PPPs is vital for smart city development, requiring effective collaboration among government agencies, the private sector and civil society organisations to address data security and privacy risks. Overcoming obstacles connected to diverse interests, priorities and varying awareness levels about cybersecurity risks is crucial. Public sector bureaucracy emerged as a significant challenge, hindering quick adaptation to dynamic cybersecurity needs. Administrative hurdles, influenced by political practices within South African municipalities, contribute to challenges such as politically influenced appointments and inadequately skilled personnel (Mncwabe 2020). Participant 6 stressed governance challenges in keeping up with rapid technological advances, relying on the private sector for due diligence on new systems. The general lack of data maturity in smart cities further hamper informed decision-making in smart governance.

Participants also highlighted key challenges linked to governance in emerging South African smart cities. Notably, concerns were raised about the absence of a dedicated national Cyber Security Incident Response Team (CSIRT) for the smart city IoT environment, as mandated by the NCPF (Malatji et al. 2021; State Security Agency [SSA] 2015; Sutherland 2017). Despite the establishment of the National Cybersecurity Advisory Council (NCAC) in 2013 to address organisational cybersecurity deficiencies, evidence suggests limited impact, leaving regulatory compliance, data governance and ethics concerns unaddressed. Monitoring mechanisms, often focussed on post-breach consequences rather than proactive evaluation, were identified as a weakness by Participant 8. Despite the establishment of the NCPF, South Africa lags in comprehensive cybersecurity legislation and engagement with businesses and citizens. Furthermore, Participants 15 and 16 called for appropriate consequences for the misuse of private information and highlighted challenges associated with load-shedding on data security and privacy. Load-shedding can lead to data continuity issues, especially for data centres relying on the national electricity grid, urging organisations to closely monitor schedules, particularly those using cloud storage (Seacom 2023; Thusi, Matyana & Jili 2023).

In addressing governance in emerging South African smart cities, Participant 6 emphasised the necessity of robust data protection and privacy policies. While the introduction of the *Protection of Personal Information (PoPI) Act* is a positive step, Participant 9 argued that effective implementation and enforcement of these policies are crucial for consistent data and privacy protection across smart city initiatives. Recent studies in Africa advocate for adopting an automated model for data protection compliance and enforcement using semantic web technologies and ontology. These systems streamline compliance checks effectively and identify instances of non-compliance with minimal effort (Tom et al. 2023).

Skills shortage

Professional development is considered crucial for ensuring a fair, efficient and sustainable shift towards smart cities. However, the available training to improve the skills of the smart cities' workforce is significantly restricted and frequently fails to meet the requirements of smart cities (Panagiotakopoulos et al. 2024). Participants raised concerns about the shortage of skilled professionals in the field of data security and privacy in South Africa. Participants 3 and 4 expressed their concerns about a general lack of knowledge and skills among employees, posing risks to citizens' data and privacy. Participant 5 accentuated the absence of specialised professionals at the municipal level as a significant risk for emerging South African smart cities. The scarcity of cybersecurity skills, including data privacy and protection expertise, is a prominent challenge not only in South Africa but also in the global market (Cornelius 2022). Despite high unemployment rates and numerous educational institutions, the skills shortage persists, attributed to insufficient national ICT planning and coordination (Malatji et al. 2021; Sutherland 2017).

Participant 8 warned that a skills shortage may hinder harnessing benefits from innovations like AI and machine learning in securing citizen data. Participant 11 cautioned against human errors because of skills shortages, risking data loss and operational disruptions without adequate backups or disaster recovery procedures. To mitigate these risks, the South African government can conduct a comprehensive risk assessment of data security and privacy practices (Malatji et al. 2021; Sutherland 2017). Such an assessment, leveraging industry standards, guidelines and best practices, would enhance cyber resilience in smart cities. However, scholarly research on data security and privacy within South African municipalities remains limited (Boyle 2020; Masombuka et al. 2021).

Participants illuminated the significant challenges linked to skill shortages in data security and privacy in emerging South African smart cities. Participant 6 expressed concern about the limited pool of cybersecurity expertise, emphasising the need for knowledgeable individuals to operate complex systems and anticipate threats. The lack of in-house skills contributes to cybersecurity ineffectiveness in South Africa. Addressing this gap requires interventions such as cybersecurity training, workforce diversification, pursuing certifications and educational enhancements organisations (Malatji et al. 2021; Mcanyana et al. 2020; Veerasamy, Mashiane & 2019).

Participant 8 noted the challenges associated with the lack of shared understanding among employees about risks in emerging South African smart cities but suggested that a combination of resources, risk-aware processes and appropriate technology could rectify this issue. Embracing technological advancements is crucial, including endpoint security, data encryption and secure wireless fidelity (Wi-Fi) networks (Cornelius 2022; Ismagilova et al. 2020; Politou et al. 2022). Participant 9 emphasised the need to build capacity and expertise. He further explained the challenges related to establishing a skilled workforce in cybersecurity, especially in developing countries facing a global shortage of professionals. Developing skills requires investment in training, education and professional development programmes. Participant 11 stressed the importance of skills for robust cybersecurity procedures, frequent security assessments and incident response plans to safeguard smart city infrastructure. Participant 15 highlighted the essential role of skills in establishing appropriate data protection infrastructure. Participant 16 noted the challenges related to the scarcity of skilled resources in managing data security and privacy, attributing it to factors like the absence of cybersecurity courses, limited funds for training, rapid technological advancements and an expanding threat landscape. These findings are corroborated by existing literature (Backhouse, Karuri-Sebina & Guya, 2020; Masombuka et al. 2021; Research ICT Africa 2020; Veerasamy et al. 2019).

Awareness and training

Participants highlighted the risks associated with awareness and training in data security and privacy for emerging smart cities in South Africa. Participants 2, 3, 8, 9 and 12 expressed concerns about limited citizen awareness. Participant 9 emphasised the need to raise awareness about cybersecurity risks, data privacy and individual rights, addressing the increasing vulnerability of individuals lacking digital literacy. Research ICT Africa (2020) suggested a comprehensive framework for proactive harm prevention, requiring extensive public awareness campaigns. Participant 4 expressed concern about a widespread lack of awareness in these cities, noting the potential for employees to become 'insider threats' because of a careless attitude towards cybersecurity. Participant 9 stressed the critical role of education and awareness programmes in mitigating risks linked to insider threats and social engineering attacks in South Africa. As an example, the Experian data theft incident in August 2020 exposed 24 million South Africans to cybercrimes like identity theft and social engineering (Hosken 2020). Ongoing risks of social engineering attacks were reported by IBM Security (2021), with potentially severe financial ramifications for smart cities and citizens. Earlier mentioned incidents, the 2022 TransUnion credit bureau data breach (Moodley 2022) and a 2023 claim of hacking the SANDF network systems (Daily Maverick 2023), further exemplify the vulnerability of sensitive data. As these incidents occur within the South African context, emerging smart cities will similarly be vulnerable to such attacks unless lessons are learned and proactive measures are implemented to prevent them.

The implementation of regular security awareness training in the workplace is considered essential for enhancing employees' awareness of threats and overcoming resistance to change (Ablon 2018; Fataar 2020; Ismagilova et al. 2020; Malatji et al. 2021). Participant 7 emphasised that such training could contribute significantly to addressing employees' resistance and educating them about potential risks and secure practices. Neglecting to secure personal devices, using them for work and lacking multi-factor authentication were identified as significant vulnerabilities, making data security and privacy awareness crucial for citizens in emerging smart cities in South Africa.

Participant 8 cautioned about inadequate understanding of data security and privacy risks among citizens, emphasising the importance of education to aid smart cities in safeguarding information integrity. Participant 12 highlighted challenges in educating end-users about cybersecurity risks, aligning with Mabaso's (2018) emphasis on the need for cybersecurity education in South Africa. Regular training and education are crucial for promoting a security-focussed cyberculture.

Participant 9 underscored the digital divide in South Africa, emphasising the importance of bridging this gap for effective cybersecurity measures. Initiatives like 'Smart Townships' and 'Smart Villages' aim to address digital inequality (Research ICT Africa 2020:84). Despite having the third-highest gross domestic product (GDP) (Varrella 2021) and the second-fastest Internet speeds in Africa (Larnyoh 2021), South African Internet users lack experience in cyberspace (Mcanyana et al. 2020; Research ICT Africa 2020). Citizens in emerging smart cities must possess data security and privacy awareness, and the smart city IT department must have the proper training and communication skills to inform and assist citizens effectively (Ismagilova et al. 2020; Malatji et al. 2021; Masombuka et al. 2021).

Participant 6 emphasised the importance of effective data collection management in emerging smart cities, highlighting the need for proper consent, transparency and citizen education. Managing data in smart cities involves addressing challenges in implementing data privacy regulations, deciding what to collect, implementing secure storage solutions, ensuring data quality and making informed decisions about its usage (Backhouse et al. 2020; Ismagilova et al. 2020).

Lack of funding

Participants emphasised the risks associated with inadequate funding to address data security and privacy risks. Participant 4 expressed concern about the lack of sustainable funding for implementing necessary measures, potentially leading to ineffective supervision of data security and privacy protection protocols. Participant 18 highlighted increased compliance costs with data security and privacy standards, aligning with Kandeh, Botha and Futcher (2018:8), who argue that compliance with the *PoPI Act* poses a financial burden to businesses and organisations in emerging South African smart cities. The ongoing issue of insufficient funding in smart cities within local government hampers effective cybersecurity supervision, making emerging South African smart cities susceptible to cyberattacks (Cornelius 2022; Masombuka et al. 2021; Norris et al. 2020). McKinsey and Company (2019) note organisations' reluctance to allocate resources for cybersecurity unless significant financial consequences are attached. Cornelius (2022) cautions that even with available investment, the shortage of skilled cybersecurity professionals limits efforts.

Participants highlighted insufficient funding as a major challenge for data security and privacy in emerging South African smart cities. Participant 4 expressed concerns about sustainable funding availability for securing data, emphasising its potential costliness. Participant 9 noted limited financial and technological resources for cybersecurity initiatives in developing countries like South Africa, raising concerns about budgetary constraints for training and retaining skilled professionals in small and medium-sized companies within their cities.

Persistent challenges stem from inadequate financial resources allocated to smart cities at the local government level, hindering effective oversight of cybersecurity measures (Cornelius 2022; Masombuka et al. 2021; Norris et al. 2020). The COVID-19 pandemic further strained financial resources

because of an upsurge in sophisticated cyberattacks (Nabe 2020). Participant 7 pointed out a lack of understanding among companies in emerging smart cities about the costs of cybersecurity systems, highlighting challenges in justifying expenses when decision-makers do not physically see the differences in devices. Outdated technology use by local governments, including emerging smart cities, is common because of funding limitations, leaving them vulnerable to cyberattacks (Masombuka et al. 2021; Pieterse 2021; Thompson 2019). Participant 18 emphasised the financial challenges associated with implementing and maintaining data security and privacy measures. Despite these challenges, South African organisations face record-breaking data breach costs, with an 8% increase over 3 years, reaching an average of R49.45 million in 2023 (IBM Security 2022, 2023).

Combination of risks

Effective data security and privacy rely on comprehensive security measures to mitigate potential risks (Cornelius 2022; Majid 2023; Malatji et al. 2021; Masombuka et al. 2021; Research ICT Africa 2020; Sharma & Arya 2023; Telo 2023; Verhulsdonck et al. 2023; Xia et al. 2023). However, participants emphasised that a combination of poor governance, skills shortage, lack of awareness and insufficient funding may result in inadequate data protection, exposing emerging South African smart cities to cyber threats and data breaches. Insufficient security measures, weak encryption, improper data storage and transmission procedures pose direct risks to data protection, as highlighted by Participant 11. Participant 6 echoed concerns, stating, 'Inadequate data protection is also a risk because they rely on robust data protection mechanisms to ensure that there is confidentiality, integrity and prudence in the system'. Participant 6 also argued that inadequate security measures may lead to the exposure of sensitive data.

Ransomware and phishing attacks were identified as specific threats linked to inadequate data protection measures, leading to data locking, malware installation or exposure of sensitive information, as noted by Participant 11. Phishing attacks were highlighted as a significant risk, with South Africa leading in cybersecurity threats on the continent in 2022 (Interpol 2022). The Federal Bureau of Investigation (FBI) reported that the majority of cybercrimes in 2021 involved phishing attacks (FBI 2021), and South Africa ranked third globally in the number of cybercrime victims, incurring an annual cost of R2.2 billion (Accenture 2020). Ransomware was emphasised by Participant 1 as a form of extortion following data breaches, aligning with the reported increase in extortion tactics by cybercriminals.

In terms of challenges, a combination of poor governance, skills shortage, lack of awareness and training and insufficient funding poses a significant challenge to achieving adequate data and privacy protection in emerging South African smart cities. Participants highlighted the collective neglect of these challenges, emphasising the major threat they pose to data security.

Participants 6 and 12 identified critical challenges with infrastructure vulnerabilities, stemming from ongoing underinvestment in securing ICT systems and cybersecurity initiatives within local government. Participant 6 attributed this vulnerability to the heavy reliance on interconnected infrastructure networks in smart cities, exposing sensitive data to cyber threats. The Mirai botnet attack in 2016 (Al-Turjman & Imran 2020) illustrated the potentially devastating impact of such attacks on smart cities dependent on IoT for operations (Patel & Doshi 2019; Vaidya et al. 2021).

Instances of sophisticated botnet-assisted cyberattacks in South Africa, including distributed denial of service (DDoS) attacks on the banking sector (Moyo 2019) and ransomware attacks on a city's power provider (Spadafora 2019), exemplify tangible risks faced by emerging smart cities. Participant 12 emphasised the challenge of safeguarding multiple sensors and IoT devices throughout smart cities, noting the lack of robust security measures and testing, creating opportunities for malicious exploitation and cybersecurity threats. Therefore, the combined data security and privacy risks can greatly compromise the advantages of smart cities, highlighting the critical need for strong security measures and continuous vigilant oversight.

Conclusion

Despite the benefits brought about by emerging smart cities, data security and privacy concerns persist. This study investigated these risks in emerging South African smarties. Several key challenges were identified, including poor governance, skill shortages, lack of awareness and training and insufficient funding. The findings emphasise the need for proactive measures to protect data and privacy in the emerging smart city landscape. This research promotes interdisciplinary dialogue for comprehensive solutions and provides globally relevant insights into the data security and privacy challenges of smart cities. The article's findings are limited by its sample size; however, the empirical insights offered by the research participants contribute to the literature on smart cities in developing countries. Future research prospects should explore how smart cities in other developing countries guard against data security and privacy risks.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

F.P.C. contributed towards the conceptualisation, methodology, data collection, formal analysis and writing of the original draft preparation. S.K.J.v.R. contributed towards the conceptualisation, methodology, writing, review & editing and supervision.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available from the corresponding author, S.K.J.v.R., upon reasonable request.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. The article does not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

References

Ablon, L., 2018, *Data thieves: The motivations for cyber threat actors and their use and monetization of stolen data*, RAND Corporation, 15 March, viewed 21 July 2023, from https://www.rand.org/pubs/testimonies/CT490.html.

Academy of Science of South Africa (ASSAf), 2019, 'The smart city initiatives in South Africa and paving a way to support cities to address frontier issues using new and emerging technologies', in *Proceedings report of the 3rd Innovation for Inclusive Development (IID) seminar*, 3 September, Pretoria, viewed 20 April 2022, from https://research.assaf.org.za/handle/20.500.11911/142.

Accenture, 2020, *Insight into the cyber threat landscape in South Africa*, 27 May, viewed 17 April 2022, from https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa.

Ahmad, N. & Mehmood, R., 2020, 'Enterprise systems for networked smart cities', in R. Mehmood, S.I. Katib & I. Chlamtac (eds.), *Smart infrastructure and applications: Foundations for smarter cities and ssocietie*, pp. 1–36, Springer, Cham.

Ahmed, S., Hossain, Md.F., Kaiser, S.M., Noor, M.B.T., Mahmud, M. & Chakraborty, C., 2021, 'Artificial intelligence and machine learning for ensuring security in smart cities', in C. Chakraborty, J.C.W. Lin & M. Alazab (eds.), *Data-driven mining learning and analytics for secured smart cities: Trends and advances*, pp. 23–47, Springer, Cham.

Akhuseyinoglu, N.B. & Joshi, J., 2020, 'Access control approaches for smart cities', in F. Al-Turjman & M. Imran (eds.), *IoT technologies in smart-cities: From sensors to big data, security and trust*, p. 1, Institution of Engineering and Technology, Stevenage.

Allam, Z., 2021, *The rise of autonomous smart cities: Technology, economic performance and climate resilience*, Palgrave, Macmillan, London.

Al-Turjman, F. & Imran, M., 2020, *IoT technologies in smart-cities: From sensors to big data, security and trust*, Institution of Engineering and Technology, Stevenage.

Al-Turjman, F., Zahmatkesh, H. & Shahroze, R., 2019, 'An overview of security and privacy in smart cities' IoT communications', *Transactions on Emerging Telecommunications Technologies* 31(8), 1–19. https://doi.org/10.1002/ett.3677

Aqib, M., Mehmood, R., Alzahrani, A. & Katib, I., 2020, 'A smart disaster management system for future cities using deep learning, GPUs, and in-memory computing', in R. Mehmood, S.I. Katib & I. Chlamtac (eds.), *Smart infrastructure and applications: Foundations for smarter cities and societies*, pp. 159–184, Springer, Cham.

Arfat, Y., Usman, S., Mehmood, R. & Katib, I., 2020, 'Big data for smart infrastructure design: Opportunities and challenges', in R. Mehmood, S.I. Katib & I. Chlamtac (eds.), *Smart infrastructure and applications: Foundations for smarter cities and societies*, pp. 491–513, Springer, Cham.

Azmoodeh, A., Dehghantanha, A. & Choo, K.K.R., 2019, 'Big data and Internet of Things security and forensics: Challenges and opportunities', in A. Dehghantanha & K.-K.R. Choo (eds.), *Handbook of big data and IoT security*, pp. 1–4, Springer, Cham.

Babbie, E.R., 2021, *The practice of social research*, 15th edn., Cengage Learning, Boston, MA.

Backhouse, J., Karuri-Sebina, G. & Guya, J., 2020, 'Discussion article on a South African approach to smart, sustainable cities and settlements', *South African Cities Network*, 8 May, viewed 13 November 2022, from https://inclusivecities.ukzn.ac.za/?mdocs-file=719.

Balkaran, S., 2019, 'Smart cities as misplaced priorities in South Africa: A complex balance of conflicting societal needs', *Journal of Management and Administration* 2019(2), 1–30.

Barlow, M. & Levy-Bencheton, C., 2019, *Smart cities, smart future: Showcasing tomorrow*, John Wiley & Sons, Hoboken, NJ.

Bouwer, J., 2022, 'SA is well positioned to accelerate the move to smart cities – Here's how', *BCX*, 19 December, viewed 30 September 2023, from https://techcentral.co.za/bcx-south-africa-smart-cities-bcxprom/218752/.

Boyle, L., 2020, 'Laying the foundations for open data in South African municipalities', in *South African Cities Network*: *Smart cities article series: Smart governance in South African cities*, pp. 16–22, viewed 27 October 2023, from https://www.sacities.net/wp-content/uploads/2020/10/Smart_Cities_Articles_Volume_1_Final-Draft.pdf.

Braun, T., Fung, B.C., Iqbal, F. & Shah, B., 2018, 'Security and privacy challenges in smart cities', *Sustainable Cities and Society* 39, 499–507. https://doi.org/10.1016/j.scs.2018.02.039

BusinessTech, 2022, *Government announced plans for 3 new 'cities' in South Africa – What you should know*, 21 February, viewed 10 April 2022, from https://businesstech.co.za/news/property/560744/government-announced-plans-for-3-new-cities-in-south-africa-what-you-should-know/.

Cornelius, F.P., 2022, *Cyber security risks in smart cities: A South African perspective*, MA dissertation, University of South Africa, Pretoria.

Cui, L., Xie, G., Qu, Y., Gao, L. & Yang, Y., 2018, 'Security and privacy in smart cities: Challenges and opportunities', *IEEE Access* 6, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

Cunha, D., 2021, 'Creating a smart ecosystem in Lisbon', in M.I.A. Ferreira (ed.), *How smart is your city?: Technological innovation, ethics and inclusiveness*, pp. 145–160, Springer, Cham.

Daily Maverick, 2023, 'SNATCHed – SANDF data leaked in cyberattack appears to be authentic, say cybersecurity analyst', *Daily Maverick*, 6 September, viewed 21 September 2023, from https://www.dailymaverick.co.za/article/2023-09-06-snatched-sandf-data-leaked-in-cyberattack-appears-to-be-authentic-say-cybersecurity-analysts/?nsl_bypass_cache=dbbc0f541dc83786201ef261d1b03728.

Deloitte, 2019, *Making smart cities cybersecure: Ways to address distinct risks in an increasingly connected urban future*, viewed 18 September 2022, from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Report_making_smart_cities_cyber_secure.pdf.

Deloitte, 2021, *The convergence of physical and digital infrastructure: Building secure and resilient smart cities and communities*, viewed 18 September 2022, from https://www2.deloitte.com/us/en/pages/risk/solutions/smart-city-cybersecurity.html/#1.

Dhungana, D., Engelbrecht, G., Parreira, J.X., Schuster, A. & Valerio, D., 2015, '*Aspern smart ICT: Data analytics and privacy challenges in a smart city*', paper presented at the IEEEWorld Forum on Internet of Things, WF-IoT, Milan, 14–16 December.

Elmaghraby, A.S. & Losavio, M.M., 2014, 'Cyber security challenges in smart cities: Safety, security and privacy', *Journal of Advanced Research* 5(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

Erasmus, D., 2023, 'Only 38 municipalities receive clean audits – AGSA', *Mail & Guardian*, viewed 14 June 2024, from https://mg.co.za/article/2023-05-31-only-38-municipalities-receive-clean-audits-auditor-general-sa/.

Fabrègue, B.F.G. & Bogoni, A., 2023, 'Privacy and security concerns in the smart city', *Smart Cities* 6(1), 586–613. https://doi.org/10.3390/smartcities6010027

Farahat, I.S., Tolba, A.S., Elhoseny, M. & Eladrosy, W., 2021, 'Data security and challenges in smart cities', in A.E. Hassanien, M. Elhoseny, S.H. Ahmed & A.K. Sigh (eds.), *Security in smart cities: Models, applications, and challenges*, pp. 117–142, Springer, Cham.

Fataar, R., 2020, 'Unpacking smart city development in Cape Town and Johannesburg', in *South African cities network: Smart cities article series: Smart governance in South African cities*, pp. 29–36, viewed 10 Aug 2022, from https://www.sacities.net/wp-content/uploads/2020/10/Smart_Cities_Articles_Volume_1_Final-Draft.pdf.

Federal Bureau of Investigation (FBI), 2021, *Internet crime report 2021*, viewed 10 Aug 2023, from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Ferreira, M.I.A., 2021, 'The right to the city: The right to live with dignity', in M.I.A. Ferreira (ed.), *How smart is your city?: Technological innovation, ethics and inclusiveness*, pp. 17–26, Springer, Cham.

Fetters, M.D., 2020, *The mixed methods research workbook: Activities for designing implementing and publishing projects*, Sage, Thousand Oaks, CA.

Flick, U. (ed.), 2018, *The SAGE handbook of qualitative data analysis*, Sage, Thousand Oaks, CA.

Ghandour, A.G., Elhoseny, M. & Hassanien, A.E., 2019, 'Blockchains for smart cities: A survey', in A.E. Hassanien, M. Elhoseny, S.H. Ahmed & A.K. Sigh (eds.), *Security in smart cities: Models, applications, and challenges*, pp. 193–210, Springer, Cham.

Gracias, J.S., Parnell, G.S., Specking, E., Pohl, E.A. & Buchanan, R., 2023, 'Smart cities – A structured literature review', *Smart Cities* 6(4), 1719–1743. https://doi.org/10.3390/smartcities6040080

Guya, J. & Wilson, J., 2020, 'The Durban EDGE open data platform: Redefining data use in eThekwini', in *South African cities network: Smart cities paper series: Smart governance in South African cities*, pp. 44–48, viewed 27 April 2022, from https://www.sacities.net/wp-content/uploads/2020/10/Smart_Cities_Papers_Volume_1_Final-Draft.pdf.

Hammi, B., Khatoun, R., Zeadally, S., Fayad, A. & Khoukhi, L., 2017, 'Internet of Things (IoT) technologies for smart cities', *IET Networks* 7(1), 1–14. https://doi.org/10.1049/iet-net.2017.0163

Hassan, M.K., El Desouky, A.I., Elghamrawy, S.M. & Sarhan, A.M., 2019, 'Big Data Challenges and opportunities in healthcare informatics and smart hospitals', in A.E. Hassanien, M. Elhoseny, S.H. Ahmed & A.K. Sigh (eds.), *Security in smart cities: Models, applications, and challenges*, pp. 1–26, Springer, Cham.

Hesse-Biber, S., 2017, *The practice of qualitative research*, 3rd edn., Sage, Thousand Oaks, CA.

Hosken, G., 2020, 'Data from huge Experian breach found on the internet', *TimesLIVE*, 13 September, viewed 30 April 2022, from https://www.timeslive.co.za/sunday-times/news/2020-09-13-data-from-huge-experian-breach-found-on-the-internet/.

Huang, Q., Wang, L. & Yang, Y., 2017, 'Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities', *Security and Communication Networks* 2017(1), 1–12. https://doi.org/10.1155/2017/6426495

Huda, N.U., Ahmed, I., Adnan, M., Ali, M. & Naeem, F., 2024, 'Experts and intelligent systems for smart homes' Transformation to Sustainable Smart Cities: A comprehensive review', *Expert Systems with Applications* 238, 122380. https://doi.org/10.1016/j.eswa.2023.122380

Hussain, I., 2024, 'Secure, sustainable smart cities and the Internet of Things: Perspectives, challenges, and future directions', *Sustainability* 16(4), 1390. https://doi.org/10.3390/su16041390

IBM Security, 2021, *How much does a data breach cost?*, viewed 23 September 2022, from https://www.ibm.com/za-en/security/data-breach.

IBM Security, 2022, *Cost of a data breach report 2022*, viewed 30 October 2022, from https://www.ibm.com/reports/data-breach.

IBM Security, 2023, *Cost of a data breach report 2023*, viewed 30 October 2023, from https://www.ibm.com/downloads/cas/E3G5JMBP.

Interpol, 2022, *African cyberthreat assessment report*, viewed 30 October 2023, from https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf.

Irwin, L., 2022, 'Data breaches and cyber attacks in 2021: 5.1 billion breached records', *IT Governance*, 20 January, viewed 11 November 2022, from https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2021-5-1-billion-breached-records#:~:text=The%20biggest%20data%20breaches%20of%202021&text=The%20incidents%20that%20resulted%20in,Facebook%20(533%20million).

Ismagilova, E., Hughes, L., Rana, N.P. & Dwivedi, Y., 2019, 'Role of smart cities in creating sustainable cities and communities: A systematic literature review', in A. Elbanna, Y.K. Dwivedi, D. Bunker & D. Wastell (eds.), *Smart working, living and organising*, Proceedings of the International Conference on Transfer and Diffusion of IT (TDIT), pp. 311–324, Springer, Portsmouth.

Ismagilova, E., Hughes, L., Rana, N.P. & Dwivedi, Y.K., 2020, 'Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework', *Information Systems Frontiers* 1(1), 1–22.

Kandeh, A.T., Botha, R.A. & Futcher, L.A., 2018, 'Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals', *South African Journal of Information Management* 20(1), 1–9, viewed 21 May 2022, from https://sajim.co.za/index.php/sajim/article/view/917/1315.

Kasar, S. & Kshirsagar, M., 2021, 'Open challenges in smart cities: Privacy and security', in S.C. Tamane, N. Dey & A.E. Hassanien (eds.), *Security and privacy applications for smart city development*, pp. 25–36, Springer, Cham.

Kaspersky, 2020, *Kaspersky security bulletin 2020: Statistic*, viewed 26 April 2022, from https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf.

Kitchin, R. & Dodge, M., 2020, 'The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention', in T. Inkienen, T. Yigitcanlar & M. Wilson (eds.), *Smart cities and innovative Urban technologies*, pp. 47–65, Routledge, London.

KPMG, 2020, *Smart city transformation in a post-COVID world: Reimaging the digital transformation of our cities on the road to recovery from COVID-19*, viewed 26 April 2022, from https://assets.kpmg/content/dam/kpmg/au/pdf/2020/smart-city-transformation-in-post-covid-world.pdf.

Larnyoh, M.T., 2021, 'Top 10 African countries with the fastest fixed broadband', *Business Insider Africa*, 27 July, viewed 23 July 2023, from https://africa.businessinsider.com/local/markets/top-10-african-countries-with-the-fastest-fixed-broadband/n4mrdkz.

Leavy, P., 2023, *Research design quantitative, qualitative, mixed-methods, arts-based, and community-based participatory research approaches*, 2nd edn., Guildford Press, New York, NY.

Le-Dang, Q. & Le-Ngoc, T., 2018, 'Internet of Things (IoT) infrastructures for smart cities', in M. Maheswaran & E. Badidi (eds.), *Handbook of smart cities software services and cyber infrastructure,* pp. 1–30, Springer, Cham.

Lozada, N., Arias-Pérez, J. & Perdomo-Charry, G., 2019, 'Big data analytics capability and co-innovation: An empirical study', *Heliyon* 5(10), 1–7.

Mabaso, N.J., 2018, *Assessing the cyber-security status of the metropolitan municipalities in South Africa*, Doctoral dissertation, University of KwaZulu-Natal, viewed 10 October 2022, from https://ukzn-dspace.ukzn.ac.za/handle/10413/18097.

Magare, S.S., Dudhgaonkar, A.A. & Kondekar, S.R., 2021, 'Security and privacy issues in smart city: Threats and their countermeasures', in S.C. Tamane, N. Dey & A.E. Hassanien (eds.), *Security and privacy applications for smart city development*, pp. 37–52, Springer, Cham.

Majid, A., 2023, 'Security and privacy concerns over IoT devices attacks in smart', *Journal of Computer and Communications* 11(1), 26–42.

Malatji, M., Marnewick, A.L. & Von Solms, S., 2021, 'Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa', *Sustainability* 13(1), 291. https://doi.org/10.3390/su13010291

Mashau, N.L. & Kroeze, J.H., 2023, 'Challenges that affect smart city implementation in small and rural municipalities', *South African Journal of Information Management* 25(1), a1703. https://doi.org/10.4102/sajim.v25i1.1703

Masiba, P.Z., 2023, *Are smart cities misplaced priorities for South Africa?*, 9 March, viewed 22 November 2023, from https://storymaps.arcgis.com/stories/e5cb1b5c6ece4a8a848102f21165454d.

Masombuka, M., Grobler, M. & Duvenage, P., 2021, 'Cybersecurity and local government: Imperative, challenges and priorities', Article presented to the 20th European Conference on Cyber Warfare and Security (ECCWS), Chester, 24–25 June.

Mcanyana, W., Brindley, C. & Seedat, Y., 2020, *Insight into the cyberthreat landscape in South Africa*, viewed 20 April 2023, from https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/pdf-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf#zoom=50.

McKinsey & Company, 2019, *Perspectives on transforming cybersecurity*, viewed 21 April 2022, from https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx.

Mncwabe, P.F.R., 2020, *The involvement of political parties in the politicization of the South African local government bureaucracy: The political-bureaucratic relations between municipal managers, politicians and political parties*, Masters dissertation, University of KwaZulu-Natal, Durban, viewed 30 August 2023, from https://researchspace.ukzn.ac.za/handle/10413/19287.

Moodley, N., 2022, 'TransUnion data breach leaves 54 million South Africans exposed', *Daily Maverick*, 19 March, viewed 21 March 2022, from https://www.dailymaverick.co.za/article/2022-03-19-transunion-union-data-breach-leaves-54-million-south-africans-exposed/.

Moyo, A., 2019, 'Bad day for SA's cyber security as banks suffer DDoS attacks', *ITWeb*, 25 October, viewed 30 April 2022, from https://www.itweb.co.za/content/LPp6V7r4OVzqDKQz.

Murray, M., 2020, *Cops and call records: Policing and metadata privacy in South Africa*, viewed 12 April 2022, from https://www.researchgate.net/publication/342078824_Cops_and_call_records_Policing_and_metadata_privacy_in_South_Africa.

Musakwa, W. & Mokoena, B.T., 2017, 'Smart cities in South Africa! A case of misplaced priorities?, paper presented at the 15th International Conference on Computers in Urban Planning and Urban Management, Adelaide, 11–14 July.

MyCiTi, 2021, *Download the official MyCiTi App*, viewed 27 April 2022, from https://www.myciti.org.za/en/discover-myciti/using-myciti-on-your-phone/.

Nabe, C., 2020, 'Impact of COVID-19 on cybersecurity', *Deloitte*, viewed 12 March 2022, from https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

Neshenko, N., Nader, C., Bou-Harb, E. & Furht, B., 2020, 'A survey of methods supporting cyber situational awareness in the context of smart cities', *Journal of Big Data* 7(92), 1–42. https://doi.org/10.1186/s40537-020-00363-0

Neuman, W.L., 2020, *Social research methods: Qualitative and Quantitative approaches*, 8th edn., Pearson Education, Boston, MA.

Norris, D.F., Mateczun, L., Joshi, A. & Finin, T., 2020, 'Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity', *Journal of Urban Affairs* 43(8), 1–28. https://doi.org/10.1080/07352166.2020.1727295

Paes, V.D.C., Pessoa, C.H.M., Pagliusi, R.P., Barbosa, C.E., Argôlo, M., de Lima, Y.O. et al., 2023, 'Analyzing the challenges for future smart and sustainable cities', *Sustainability* 15(10), 7996. https://doi.org/10.3390/su15107996

Panagiotakopoulos, T., Lazarinis, F., Stefani, A. & Kameas, A., 2024, 'A competency-based specialization course for smart city professionals', *Research & Practice in Technology Enhanced Learning* 19, 1–19. https://doi.org/10.58459/rptel.2024.19013

Patel, C. & Doshi, N., 2019, 'Security challenges in IoT CyberWorld', in A.E. Hassanien, M. Elhoseny, S.H. Ahmed & A.K. Sigh (eds.), *Security in smart cities: Models, applications, and challenges*, pp. 171–191, Springer, Cham.

Pereira, G., Parycek, P., Falco, E. & Kleinhans, R., 2018, 'Smart governance in the context of smart cities: A literature review', *Information Polity* 23(2), 143–162. https://doi.org/10.3233/IP-170067

Picon, A., 2019, 'Smart cities, privacy and the pulverisation/reconstruction of individuals', *European Data Protection Law Review* 5(2), 154–155. https://doi.org/10.21552/edpl/2019/2/4

Pieterse, H., 2021, 'The cyber threat landscape in South Africa: A 10-year review', *The African Journal of Information and Communication (AJIC*) 28(1), 1–21. https://doi.org/10.23962/10539/32213

Politou, E., Alepis, E., Virvou, M. & Patsakis, C., 2022, *Privacy and data protection challenges in the distributed era*, Springer, Cham.

Radigan, P. & Mendez, S.L., 2018, 'Historical research', in B.B. Frey (ed.), *The Sage encyclopedia of educational research, measurement, and evaluation*, pp. 782–785, Sage, Thousand Oaks, CA.

Ramparsad, S., 2020, 'Smart governance in South African Cities', in *South African cities network. Smart cities article series: Smart governance in South African cities*, pp. 9–15, viewed 17 July 2023, from https://www.sacities.net/wp-content/uploads/2020/10/Smart_Cities_Articles_Volume_1_Final-Draft.pdf.

Rao, P.M. & Deebak, B.D., 2023, 'Security and privacy issues in smart cities/industries: Technologies, applications, and challenges', *Journal of Ambient Intelligence and Humanized Computing* 14(8), 10517–10553. https://doi.org/10.1007/s12652-022-03707-1

Research ICT Africa, 2020, *Digital futures: South Africa's digital readiness for the 'Fourth Industrial Revolution'*, National Planning Commission, viewed 02 September 2023, from https://researchictafrica.net/wp/wp-content/uploads/2021/01/021220_Digital-Futures_SAs-Digital-Readiness-for-4IR_01.pdf.

Roulston, K. & Choi, M., 2018, 'Qualitative interviews' in U. Flick (ed.), *The SAGE handbook of qualitative data analysis*, pp. 232–249, Sage, Thousand Oaks, CA.

Schurink, W.J., Schurink E.M., & Fouché, C.B., 2021, 'Thematic inquiry in qualitative research', C.B. Fouché, H. Strydom & W.J.H. Roestenburgn (eds.), *Research at grass roots: For the social sciences and human service professions*, pp. 289–310, 5th edn., Van Schaik, Pretoria.

Seacom, 2023, *Load shedding impacts data and backups*, 10 March, viewed 02 September 2023, from https://seacom.co.za/business-insights/load-shedding-impacts-data-and-backups/.

Sharma, R. & Arya, R., 2023, 'Security threats and measures in the Internet of Things for smart city infrastructure: A state of art', *Transactions on Emerging Telecommunications Technologies* 34(11), 4571. https://doi.org/10.1002/ett.4571

Silva, B.N., Khan, M. & Han, K., 2018, 'Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities', *Sustainable Cities and Society* 38, 697–713. https://doi.org/10.1016/j.scs.2018.01.053

Sookhak, M., Tang, H., He, Y. & Yu, F.R., 2018, 'Security and privacy of smart cities: A survey, research issues and challenges', *IEEE Communications Surveys & Tutorials* 21(2), 1718–1743. https://doi.org/10.1109/COMST.2018.2867288

Spadafora, A., 2019, *Ransomware attack leaves Johannesburg without power*, 25 July, viewed 09 October 2022, from https://www.techradar.com/news/johannesburg-ransomware-attack-leaves-city-without-power.

State Security Agency (SSA), 2015, *The National Cybersecurity Policy Framework (NCPF)*, Government Gazette 609(3975), Government Printers, Pretoria, viewed 05 September 2022, from https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf.

Sutherland, E., 2017, 'Governance of cybersecurity: The Case of South Africa', *The African Journal of Information and Communication* 20(1), 83–112. https://doi.org/10.23962/10539/23574

Telo, J., 2023, 'Smart city security threats and countermeasures in the context of emerging technologies', *International Journal of Intelligent Automation and Computing* 6(1), 31–45.

Thompson, L.N., 2019, *Cybersecurity best practices for municipalities*, viewed 02 September 2022, from https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities.

Thusi, X. & Selepe, M.M., 2023, 'The impact of poor governance on public service delivery: A case study of the South African local government', *International Journal of Social Science Research and Review* 6(4), 688–697.

Thusi, X., Matyana, M. & Jili, N.N., 2023, 'Lack of political will: A barrier to public service delivery in South Africa and a high cost for citizens', *Journal of Studies in Social Sciences and Humanities (JSSSH)* 9(2), 137–147.

Teing, Y.Y., Homayoun, S., Dehghantanha, A., Choo, K.K.R., Parizi, R.M., Hammoudeh, M. et al., 2019, 'Private cloud storage forensics: Seafile as a case study', in A. Dehghantanha & K.K.R. Choo (eds.), *Handbook of big data and IoT security*, pp.73–128, Springer, Cham.

Tom, J., Adigwe, W., Anebo, N. & Bukola, O., 2023, 'Automated model for data protection regulation compliance monitoring and enforcement', *International Journal of Computing, Intelligence and Security Research* 2(1), 47–57.

Trapenberg Frick, K., Mendonca Abreu, G., Malkin, N., Pan, A. & Post, A.E., 2021, *The cybersecurity risks of smart city technologies what do the experts think?*, University of California Berkeley, CA, viewed 17 October 2022, from https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart_City_Cybersecurity.pdf.

University of South Africa (UNISA), 2016, *Policy on research ethics*, viewed 06 July 2022, from https://www.unisa.ac.za/static/corporate_web/Content/Apply%20for%20admission/MD/Documents/Policy%20on%20Research%20Ethics%20-%20rev%20appr%20-%20Council%20-%2015.09.2016.pdf.

Vaidya, G., Bindra, P., Kshirsagar, M. & Tamane, S.C., 2021, 'Privacy and security technologies for smart city development', in S.C. Tamane, N. Dey & A.E. Hassanien (eds.), *Security and privacy applications for smart city development*, pp. 3–24, Springer, Cham.

Varrella, S., 2021, 'GDP of African countries 2021, by country', *Statista*, 20 September, viewed 23 July 2023, from https://www.statista.com/statistics/1120999/gdp-of-african-countries-by-country/.

Veerasamy, N., Mashiane, C.T. & Pillay, K., 2019, 'Contextualising cybersecurity readiness in South Africa', in *Article presented to the 14th International Conference on Cyber Warfare and Security (ICCWS 2019)*, Stellenbosch, 28 February–01 March, viewed 17 October 2022, from https://researchspace.csir.co.za/dspace/bitstream/handle/10204/11247/RS%2022883_Contextualising%20cybersecurity%20readiness%20in%20South%20Africa.pdf?sequence=1&isAllowed=y.

Verhulsdonck, G., Weible, J.L., Helser, S. & Hajduk, N., 2023, 'Smart cities, playable cities, and cybersecurity: A systematic review', *International Journal of Human–Computer Interaction* 39(2), 378–390.

Vitunskaite, M., He, Y., Brandstetter, T. & Janicke, H., 2019, 'Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership', *Computers and Security* 83(1), 313–331. https://doi.org/10.1016/j.cose.2019.02.009

Xia, L., Semirumi, D.T. & Rezaei, R., 2023, 'A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy', *Sustainable Cities and Society* 98, 104771. https://doi.org/10.1016/j.scs.2023.104771