Multimedia Tools and Applications (2024) 83:6975–6999
https://doi.org/10.1007/s11042-023-15632-2

Future dynamic multimedia content access via aerial computing system

Ayodele Periola[1] · Akintunde Alonge[2] · Kingsley Ogudo[2]

Received: 10 November 2021 / Revised: 18 June 2022 / Accepted: 22 April 2023 /
Published online: 5 June 2023

Abstract
Multimedia content access sovereignty arises due to the intention of producers to enable subscribers from pre–defined regions access multimedia content. This limits the number of locations (with subscribers) that can access producer content. Therefore, the ability to access multimedia content across previously unconsidered locations is limited. The presented research addresses this challenge and focuses on multimedia content sharing among subscribers in arid and hyper–arid regions. The use of stratosphere based data centres (SBDCs) is proposed. The paper also presents multi–tier network architecture for network traffic management. This ensures that network traffic congestion does not limit access to multimedia content by subscribers across multiple regions. The use of SBDCs increases the number of locations that engage in the sharing of multimedia content. Evaluation shows that the proposed solution increases the number of data sharing locations by (75.8 – 88.2) % on average.

Keywords Multimedia content · Computing networks · Non-terrestrial systems · Data sovereignty · Content sharing

1 Introduction

Information storage and processing are important tasks being executed in computing platforms. However, data should only be shared with selected subscribers and entities. This concern is addressed via the design of suitable data retention laws and policies requiring siting data centres in favourable and unfavourable locations. Favourable locations such as Europe

✉ Ayodele Periola
periolaa@cput.ac.za; periola@hotmail.com

Akintunde Alonge
aalonge@uj.ac.za

Kingsley Ogudo
kingsleyo@uj.ac.za

[1] Electrical, Electronic and Computer Engineering, Cape Peninsula University of Technology, Cape Town, South Africa

[2] Electrical and Electronic Engineering Technology, University of Johannesburg, Johannesburg, South Africa

and North America are cold climate zones that enable low cost data centre cooling. The need to conform with data retention policies also necessitates siting data centres in unfavourable locations with unfriendly operation. Examples of such zones are arid regions such as Western Sahara, Egypt, Algeria and Libya. West African countries such as Chad, Mali, and Niger lie in this category. These regions have a combined population of 179.2 million.

Nevertheless, it is important to place data centres in arid zones due to the large subscriber population desiring low latency content access. It is also challenging and costly to realize cooling for terrestrial data centres sited in arid and hyper–arid regions due to high temperature and low water supply. However, data centres in arid and hyper–arid regions can be placed in the stratosphere where they benefit from free stratospheric cooling. Stratospheric cooling effect has been observed in [18, 20, 39]. In addition, the suitability of stratosphere based data centres (SBDCs) is recognized in [24–26]. However, the consideration in [24–26] is not focused on realizing data sovereignty aboard data centres in arid regions.

The deployment of cloud computing systems in arid regions plays an important role in launching multimedia applications. In [27], the discussion presents a novel mechanism enabling content access without considering content provider identity. The mechanism considers a cord shaver that is transiting to content access in the digital video broadcasting-internet (DVB-I). It does not consider the role of the cloud computing platform in enabling provider identity independent multimedia content access. The incorporation of cloud computing platforms is important in enabling access to content in the DVB–I context across geographical regions. In this case, the content developed for a given location can be viewed at another location when there is a viewing demand. In this case, the cloud computing platform (CCP) hosts the content for a given duration. The design of a CCP to meet this performance expectation has not been considered in previous and existing work.

The design of CCP to support rationed multimedia content access across different locations is the goal of the proposed research. The proposed CCP enables content access between regions that do not support cross–border data exchange. The content being accessed in this case are those desirable by subscribers in one region but initially designed for subscribers in another region. The proposed network architecture being presented in this paper overcomes the challenge for subscribers in arid and hyper–arid regions where the use of terrestrial data centres is challenging. This is because of the cooling challenges arising from high environmental temperature. The high temperature makes free air and water cooling challenging.

The problem being considered is that of realizing cloud computing systems (supporting data sovereignty) in arid and hyper–arid regions. This perspective considers how the need to deploy CCPs and data related services influences the design of future CCP networks. The presented research has two motives.

The first motive is improving multimedia content access to meet future subscriber demand. In the existing case, programmes are designed to be accessible at select locations for the concerned subscribers. However, these content are desirable for access by subscribers in other locations. The concerned locations are prevented from sharing multimedia content and related data. This form of data sovereignty is used to control multi–media content access. Cross–border content sharing is deemed feasible to improve the capability of the content access providers to meet subscriber demands.

The second motive is designing the cross–border while considering desertification as a dynamic event. The discussion considers the occurrence of desertification as a dynamic event such that areas that were previously non–desert regions are becoming desert regions. In addition, the paper considers the implementation of data sovereignty in a cloud computing system as being quantifiable. A cloud computing system is deemed as being characterised by the number of locations capable of engaging in cross–border data exchange and

the duration of a cross–border data exchange. In this case, the cross–border data exchange occurs in the context of accessing multimedia content across different geographical zones.

The paper focuses on the design of data exchange between regions that are unintended to communicate with each other. However, subscribers in these regions desire to access content initially developed with the aim of regional exclusivity. Therefore, the paper's focus is in the context of ensuring data sovereignty with support for data access in regions without an initial data sharing policy. The paper's contributions are:

1. The design of a new approach to ensure data sovereignty in mobile SBDCs being used in arid and hyper–arid regions. SBDCs should be capable of changing locations to mitigate against aerial threats. This concern is addressed in [24] without recourse to ensuring compliance to data retention policy or considering their role in future multimedia content access. This new approach considers that data retention should have dynamic locations. Hence, a data centre can have multiple locations in the proposed data retention policy. This differs from the existing consideration where terrestrial data centres have a fixed location. The proposed dynamic retention approach is two– dimensional. This is because it considers the number of locations and duration for which a data transfer session be executed. The existing approach considers a finite number of locations hosting data centres with which data transfer can be executed while conforming to the data retention policy.
2. The design of SBDC based network architecture is also presented. The network architecture being proposed incorporates intelligent capabilities in implementing data sharing across different locations. These locations host dynamic data sovereignty policies. The network architecture ensures that SBDCs are able to execute cross–border data exchange. This is done with the aim of executing data exchange within the framework of the proposed cognitive and dynamic data retention approach. The network architecture is designed with the goal of supporting multi–location data sharing while conforming to the dynamic data retention policy.
3. In addition, dynamic data retention incorporates the traffic management to avoid network congestion. The occurrence of network congestion results in a case where data exchange does not occur within the specified duration. This challenge is addressed via spot traffic offloading by incorporating spot terrestrial edge nodes (STENs) and spot aerial edge nodes (SAENs). The multi–tier network alleviates congestion in the proposed network by offloading SBDC traffic. In this case, SBDCs are supported by two entities i.e. spot terrestrial edge node (STENs) and spot aerial edge node (SAENs). STENs and SAENs enable communication between SBDCs in the realization of data sharing in the manner proposed. The use of STENs and SAENs is necessary when SBDCs have limited capability to handle cross–border exchange related traffic. The resulting traffic is offloaded to the SAEN or STEN or both. STENs are realized via ground based edge nodes. SAENs are realized via aerial entities such as unmanned aerial vehicles (UAVs).
4. The benefit of using the proposed mechanism is also investigated. This is done by formulating a performance model for the proposed dynamic data retention approach. The formulated performance metrics are the: (1) Number of locations (hosting data centres) and (2) Data exchange duration (between data centres). These metrics are formulated for the case of the existing approach (with static data retention policies; and using terrestrial data centres) and the proposed approach (with dynamic data retention policies; and now incorporating SBDCs). The use of the proposed approach considers two cases. The first case is one in which only SBDCs interacting with each other incorporate dynamic data retention policies. The second case is one in which the context concerns terrestrial based

data centres and SBDCs. This arises when the data exchange occurs between terrestrial and aerial locations.

The organization is as follows: Section 2 discusses the existing work. The challenge being addressed is described in Section 3 The proposed solution is presented in Section 4. Section 5 describes the proposed solution. The performance model is formulated in Section 6. Section 7 analyses the performance benefits. The presented research is concluded in Section 8.

2 Background and related work

The discussion here focuses on the paradigms of data sovereignty, associated network architecture and future multimedia content access. It is divided into three aspects. The first focuses on discussing existing paradigms on data sovereignty. The second discusses network architecture and management from the perspective of existing work. The third examines existing work perspectives on the multimedia access.

2.1 First aspect – existing paradigms on data sovereignty

Esposito et al [9] examines the realization of data sovereignty in smart cities to ensure the control of access in smart city sensors. The proposed approach utilizes data sovereignty as being capable of providing input enabling the realization of secured systems in smart cities. This is done to prevent crypt-analysis by malicious entities. The solution utilizes the concept of data sovereignty in the design of a cyber-security solution. In this case, the security is challenging because sensor location information is known to system installers who are not the cloud service provider entity.

Hummel et al [13] examine the different notions that define data sovereignty and explore the spectrum of concerns to be considered in defining data sovereignty. In addition, the roles of notion, agents, context, and values in formulating a definition for data sovereignty are identified. The use cases of data sovereignty in governmental institutions, non–governmental organizations and the health industry are also recognized. However, this does not consider the description of information infrastructure architecture.

Tang et al [37] recognizes the notion of data sovereigns and a data force with a view to realizing data sharing. This is necessary to actualize the full economic potential of data products in different areas. The perspective in [37] is that data is a resource by governments. The challenge of resource allocation i.e. data allocation is considered from a political perspective while designing relationships between data sovereigns (data centre service providers and operators) and applications. The relationships are executed to ensure the realization of data capitalization via the execution of data driven applications.

Jarke in [16] and Jarke et al [15] identify the important role of data sharing in application development. This is done in [15] with a focus on designing industrial data driven eco-systems and applications for domain specific meta-models. In the meta-models, data generated and stored by different entities are used by other orchestrating entities. The relation between the data producers, owners and orchestration is defined in the international data space approach. The international data space (IDS) presents architecture for designing data driven applications. Though, the role of the cloud computing platform is recognized; the implementation of an underlying cloud network does not receive further consideration.

Peterson et al [28] address the need to develop new algorithms and solutions for ensuring the integrity (security) of cloud based data. It is recognized that data should exist at a granularity enabling storage within a country's borders. The discussion in [28] identifies the notions of routing as a technical concern. The consideration of technical concerns arising from the implementation of a data sovereignty protocol receives consideration in [28]. Additional consideration focuses on binding data and network locations. However, network architecture for addressing compliance to data sovereignty policies is not considered.

The research in [9, 15, 16, 28, 37] shows that there are considerations on realizing underlying networks and data driven application frameworks for enabling data sovereignty. More focus is on the data driven application framework with less attention on the underlying computing platform network.

Gelhaar et al [11] aim to define a metric for characterising data ecosystems that arise from cross–industry data fusion processes. In this case, data sovereignty is modelled as a meta–dimension enabling the data resource control. The meta–dimension has three non inter-dependent components i.e. economic, technical and governance concerns. Inter–dependence is considered but within the context of intra– relations between actors within the governance meta–dimension and not relations towards defining a cloud network.

The impact of implementing data sovereignty protocols on the structure of the internet has not received attention in the identified and considered literature. The IDS considers some technical aspects of data sovereignty [15] but does not address its implementation and its influence on the internet architecture. This is addressed in [6] where it is recognized that the existing internet architecture is un-fragmented. The discussion in [6] notes that the national focus on realizing data sovereignty leads to a fragmented internet. However, the implication on application development has not been considered.

Pohle et al [29] identify the different views and perspectives on data sovereignty. Two views have been presented. The first and second view opines that internet challenges the notion of state sovereignty and that corporate entities influence the society via the online world, respectively. This is due to the internet's role in global advertising. However, the implementation of data sovereignty limits the open internet and requires communications between sovereign data silos. However, realizing the required communications is a challenge requiring attention. The notion of digital sovereignty is examined in [8] considering the transition from the state to the individual. However, the focus in [8] does not consider the effects of data sovereignty compliance on the internet architecture and cloud platforms.

The consideration of data sovereignty implicitly assumes the use of terrestrial data centres. However, water cooled terrestrial data centres are not suitable in arid locations. In this case, the use of aerial data centres such as SBDCs (benefitting from stratospheric cooling) is preferred. However, the realization of data sovereignty for aerial cooled data centre systems requires further research consideration.

2.2 Second aspect – existing paradigms on data sovereignty

Jing et al [17] propose an algorithm that achieves reliable scheduling while meeting subscriber's quality of service. The algorithm is deployed in a system incorporating virtualization technology. The virtualization being considered is inherent within a terrestrial cloud computing system. The quality of service (QoS) metric and parameters can be influenced by different parameters. However, the considered parameters are those influencing load balancing, and fault tolerance. These metrics i.e. deadline, scheduling and reliability are related to computing task execution. The proposed

solution is done using the discrete particle swarm optimization. However, the discussion in [17] has not considered improving the QoS from the perspective of the cloud computing platform node as a network. Instead, it focuses on improving the QoS of the cloud computing platform as an algorithm execution entity.

Maenhaut et al [19] discuss cloud resource management and identify different management objectives in cloud computing platforms and systems. Examples of recognized objectives are minimization of power consumption, operational costs, lower instance utilization costs and green computing realization. In addition, the discussion recognizes bursts in cloud computing resource demand. The discussion in [19] presents a survey of different approaches used for resource management in cloud computing systems. This is discussed from the perspective of executing low cost computing. In addition, network related bandwidth and latency are recognized. Furthermore, the role of the network resources in a hybrid/edge/fog cloud environment. However, the challenge of realizing objective focused QoS in the cloud bursting case has not been considered. This should be done with relation to network traffic management and congestion prevention.

The discussion in [7, 14] also recognizes the need to improve network performance and QoS within the context of virtualized platforms aboard terrestrial data centres.

Ferdousi et al [10] address the challenge of ensuring that disasters do not lead to loss of cloud functionality. The occurrence of a large scale disaster affects certain parts of the cloud and network infrastructure. Therefore, it gives rise to unexpected, unscheduled and unplanned internet fragments. The proposed capability recovery approach utilizes a progressive approach to realizing an operational network. This is done while considering the role of the data centre and the supporting network. The discussion in [10] focuses on restoring the network architecture and computing capability of the data centre and underlying network infrastructure. However, additional work is required to examine how network related algorithms are restored alongside a restored data centre with its underlying network.

Sharma et al [35] proposes the cog–chain paradigm intended for use in a network comprising aerial and terrestrial entities. The presented research is set in a network with multiple aerial and terrestrial nodes. The goal of the research is to realize resource management and caching in the aerial–terrestrial integrated network. The integrated network enables the realization of a sub–cloud network system. The discussion in [35] considers the realization of a logical context. Each context is a network realized via a unique combination of terrestrial, aerial and satellite (backbone) networks. This is done while realizing QoS friendly routing. The focus is on realizing security, alongside energy efficiency in the network. It is recognized that security related paradigms and algorithms should have a low network overhead.

In regard to the use of terrestrial data centres with virtual machines, research has extensively focused on improving resource usage to realize enhanced scheduling [2–4, 12, 34, 36]. These algorithms and solutions are expected to be functional within the larger context of implementing data retention policies.

The management of resources is also done with focus on networking resources [7, 10, 14, 35]. A low level granularity multi–tiered system with focus on the container abstraction to access the virtual machine abstraction model is also presented in [4].

However, additional consideration to design resource management solutions for CCPs in special cases such as those in [19, 36] is required. Special cases resulting in previously unconsidered contexts can also arise. This is because of the innovation in cloud computing systems especially in the aspect of data retention. The use of heuristics is also proposed in [12]. The consideration of heuristics considers a finite number of contexts and feasible scenarios that were not considered in defining and specifying heuristics arise. This can arise

when new paradigms such as data sovereignty [9, 11, 13, 15, 16, 37] have their policies implemented in containerized or virtual machine controlled cloud computing platforms. The challenge of the inadequacy of heuristics arises in cases where network algorithm results in internet fragmentation. The occurrence of internet fragmentation has been recognized to occur in research as seen in [5].

2.3 Third aspect – existing work: multi – media content and the cloud

Reznik et al [31] identify the advantages of using the cloud for multimedia broadcast applications. These benefits include low hardware cost, simple management and easy upgrade execution. The discussion in [31] presents a cloud friendly implementation of the digital broadcast system that comprises a convergence between traditional and cloud based online multimedia. Though the discussion recognizes the role of the cloud in future broadcasting, it does not present any mechanism showing how the incorporation of the cloud enables the realization of novel methods for multimedia content access.

The role of smart television in application testing is considered in [1]. This is done within the context of smart television apps that are developed using software kits. The Samsung Tizen Software development kit is presented and described. The focus of [1] is the development of user enabling applications for the smart television. The discussion in [23] presents existing enterprise perspective on the role of the cloud in future smart television technology. A screen casting service is recognized to benefit from advances in cloud computing and enables the integration of multiple online video streaming providers. In this case, the end user or subscriber pays for a finite number of online video service providers. In addition, an implicit control on content access is inherent. However, the provision of alternative feedback with the aim of improving value addition though feasible has not been considered.

Noam in [22] examines the context and capabilities of fourth generation television. The increasing transition of the television to the internet is recognized alongside the importance of the cloud. This is done in the context of maximizing producer creativity, realization of standardization options and ease of use by subscribers. However, the discussion does not discuss mechanisms enabling content access modes in migrating from old media to new media.

Ruiz et al [32] evaluate the role of cloud platforms in managing devices within the internet of things (IoTs) framework. In IoTs, smart televisions are nodes with internet connectivity. The focus of the presented research is on using the cloud platform as an integration point for other technologies However, the context of bi–directional communications for the smart television has not been considered.

Murschetz et al [21] note the change in television viewing habits by subscribers. This disruption arises due to technological change and incorporation gives rise to the connected television concept with subscriber interaction. This also results in a convergence between the internet and broadcast domain. In the connected television, big data arises from subscriber digital trail due to channel changes. The resulting data is used for audience analytics, engagement, and innovation. The possible future and potential roles of this integration has been recognized. However, a future cloud–broadcast integration has not been presented. Popescul [30] identify that the smart television can host sensors suitable for gathering data. However, the perspective in [30] focuses on the security concerns associated with smart television in its role as a data acquisition node.

Udoakpan et al [38] recognize the increasing preference of over the top television packages. The service offerings from different over the top television providers are described. The discussion focuses on understanding the factors influencing the selection of over the top television instead of conventional pay television. In addition, the factors that influence the selection of a given over the top television provider for different demographic profiles has not been considered.

The discussion in this section shows that there is an increasing transition to video on demand [1, 21, 33, 38]. In addition, the role of the smart television in data gathering is recognized [30, 32]. Advances in cloud computing networks also influence multimedia access [22, 23, 31]. The influence of demography on digital video on demand is considered in [38]. However, multimedia sovereignty has not been considered and is implicit as providers produce content for subscribers in different geographical regions. In addition, content designed for residents in a given location should be selectively accessible to residents in another location to meet viewing demand. However, addressing this requires further research.

The parameters that are used in this paper are presented in Table 1. The acronyms being used in this paper are presented in Table 2.

3 Problem description

This section presents the research problems that consider multimedia content sovereignty and enhanced content access. The discussion is divided into two aspects. The first presents the multimedia content sovereignty challenge. The second focuses on the challenge associated with enabling multimedia content access in an arid and hyper–arid region being subjected to dynamic desertification.

3.1 First challenge: multi – media content sovereignty and future access demand

The case under consideration is one in which multimedia content access providers that provide content to subscribers over different regions. Let z be the set of multimedia content access providers such that:

$$z = \left\{z_1, z_2, \ldots, z_E\right\} \tag{1}$$

The content from the e^{th} multimedia content access provider, $z_e, z_e \epsilon z$ is given as:

$$z_e = \left\{z_e^1, z_e^2, z_e^3, \ldots, z_e^D\right\} \tag{2}$$

where.$z_e^d, z_e^d \epsilon z_e$ is the d^{th} content associated with the e^{th} multimedia content access provider, z_e.

Let α be the set of sovereign states such that:

$$\alpha = \left\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_I\right\} \tag{3}$$

The content access indicator is given as $\left(z_e^d, \alpha_p, t_y\right) \epsilon \{0,1\}, t_y, t_y \epsilon t, t = \left\{t_1, \ldots, t_Y\right\}$. The content $\ddagger_{\mathrm{e}}^{\mathrm{d}}$ can be accessed at the location $\alpha_p, \alpha_p \epsilon \alpha$ at the epoch t_y if $I\left(z_e^d, \alpha_p, t_y\right) = 1$. The access to the content is not feasible at the epoch t_y due to content sovereignty if $I\left(z_e^d, \alpha_p, t_y\right) = 0$. In addition, let $I_{de}\left(z_e^d, \alpha_p, t_y\right) \epsilon \{0,1\}$ denote the content access demand

Table 1 List of parameters

S/N	Parameter	Meaning
1	z	The set of multimedia content access providers
2	$z_e, z_e \epsilon\ z$	The e^{th} multimedia content access provider
3	$z_e^d, z_e^d\ \epsilon\ z_e$	The d^{th} content associated with the e^{th} multimedia content access provider
4	α	The set of sovereign states
5	t_y, t_J	The y^{th} epoch and the J^{th} epoch, respectively
6	$I\left(z_e^d, \alpha_p, t_y\right)\epsilon\{0,1\}$	The content access indicator
7	$I_{de}\left(z_e^d, \alpha_p, t_y\right)$	The content access demand indicator
8	$\alpha_c, \alpha_c \epsilon \alpha, c\epsilon\{p,r\},$	The p^{th} sovereign region and the r^{th} sovereign region
9	$z_e^\ell, z_e^\ell \epsilon z_e$	The $\updownarrow^{th}$ content associated with the e^{th} multimedia content access provider
10	$I_A\left(\alpha_p\right)$	The arid location indicator of the p^{th} sovereign region α_p
11	$I_C\left(\alpha_p, \alpha_q, t_y\right)$	The cross–border platform data exchange indicator between data centres in the p^{th} sovereign location, α_p and the q^{th} sovereign location α_q
12	$I_A\left(\alpha_p, t_y\right)$	The arid location indicator of the p^{th} sovereign region α_p represented as a dynamic variable
13	$\varsigma_1\left(\alpha_p\right)$	The allowable duration for the p^{th} sovereign region α_p
14	$\varsigma_2\left(\alpha_p\right)$	Tuple of multimedia content described accessible from the p^{th} sovereign region α_p
15	θ_1, θ_2	The number of locations capable of supporting cross–border data (multimedia content) exchange in existing approach and proposed approach, respectively
16	γ	Set of SBDCs
17	$\gamma_m, \gamma_m \epsilon \gamma$	The m^{th} SBDC
18	$I_C\left(\gamma_m, \alpha_q, t_y\right)$	The communication status indicator between the m^{th} SBDC, γ_m and the q^{th} sovereign region α_q with a data centre at the y^{th} epoch

Table 2 List of acronyms

S/N	Acronym	Meaning	S/N	Acronym	Meaning
1	CE	Computing Entity	9	MSP	Micro–Sovereignty Policy
2	CSE	Convergence Server Entity	10	QoS	Quality of Service
3	DCSE	Dynamic Content Sovereignty Entity	11	SAEN	Spot Aerial Edge Node
4	DTAE	Data Type Analysis Entity	12	SBDC	Stratosphere based data centre
5	DVB–I	Digital Video Broadcasting – Internet	13	SLDE	SBDC Link Detector Entity
6	GA	Governmental Authority	14	STEN	Spot Terrestrial Edge Node
7	IoTs	Internet of Things	15	TME	Traffic Monitoring Entity
8	MAE	Multi–Access Entity			
9	MSP	Micro–Sovereignty Policy			
10	QoS	Quality of Service			
11	SAEN	Spot Aerial Edge Node			

indicator. The access to the content is desired and not desired at the location α_p at the epoch t_y if $I_{de}\left(z_e^d, \alpha_p, t_y\right) = 1$ and $I_{de}\left(z_e^d, \alpha_p, t_y\right) = 0$, respectively. An access challenge arises in the scenarios:

$$I_{de}\left(z_e^d, \alpha_q, t_y\right) = 1, I\left(z_e^d, \alpha_q, t_y\right) = 0, I\left(z_e^d, \alpha_r, t_y\right) = 1, \alpha_q \epsilon\ \alpha, \alpha_r \epsilon\ \alpha \tag{4}$$

$$I_{de}\left(z_e^\ell, \alpha_q, t_y\right) = 1, I\left(z_e^\ell, \alpha_q, t_y\right) = 0, I\left(z_e^\ell, \alpha_u, t_y\right) = 1, z_e^\ell, z_e^\ell \epsilon\ z_e \alpha_q \epsilon\ \alpha, \alpha_u \epsilon\ \alpha \tag{5}$$

The challenges in (4) and (5) arise because of the localization of the multimedia content in z_e^d and z_e^ℓ to the r^{th} sovereign state$\alpha_r, \alpha_r \epsilon \alpha$. In the case presented in (4), subscribers at the location α_q desire access to the multimedia content z_e^d at the epoch t_y. However, the desired multimedia content z_e^d is designed to be only accessible to subscribers in the r^{th} sovereign state α_r. The scenario in (5) describes the case in which access to the multimedia content z_e^ℓ is desired by subscribers in the location α_q. However, the multimedia content z_e^ℓ is only accessible to subscribers in the location α_u at the concerned epoch t_y. The concerned multimedia content is hosted aboard cloud computing platforms. The subscribers at the location α_q require access to the content initially intended for sole access to subscribers at the locations α_r andα_u. Multimedia content sovereignty is considered to arise from the localization of access for the content z_e^d and z_e^ℓ to the locations α_r and α_u respectively. A solution that addresses this challenge will enable flexible multimedia content access in a manner that overcomes this challenge arising from the multimedia content sovereignty.

3.2 Second challenge: multimedia content access in arid and hyper–arid regions

The considered scenario comprises the p^{th} sovereign location, $\alpha_p, \alpha_p \epsilon \alpha$ hosts multiple data centres. In addition, let $I_A\left(\alpha_p\right) \epsilon \{0, 1\}$ denote the arid location indicator of α_p. The data centre(s) in α_p is located and not located in an arid region when $I_A\left(\alpha_p\right) = 1$ and $I_A\left(\alpha_p\right) = 0$, respectively. Water cooled and air cooled data centres can be hosted in the p^{th} sovereign location when $I_A\left(\alpha_p\right) = 0$. In addition, the cross–border platform data exchange indicator between data centres in the p^{th} sovereign location, α_p and the q^{th} sovereign location,

$\alpha_q, \alpha_q \epsilon \alpha$ at the epoch $t_y, t_y \epsilon t, t = \{t_1, \ldots, t_Y\}$ is given$I_C(\alpha_p, \alpha_q, t_y) \epsilon \{0, 1\}$. The data centre in the p^{th} and q^{th} sovereign locations can and cannot engage in cross–border data exchange when $I_C(\alpha_p, \alpha_q, t_y) = 1$ and $I_C(\alpha_p, \alpha_q, t_y) = 0$, respectively. Data exchange between internet fragments between α_p and α_q in the between epochs t_y and $t_J, t_J \epsilon t$ is feasible when:

$$\{I_C(\alpha_p, \alpha_q, t_y), \ldots, I_C(\alpha_p, \alpha_q, t_J)\} = \{1, \ldots, 1\} \tag{6}$$

$$I_A(\alpha_p) = 0, I_A(\alpha_q) = 0 \tag{7}$$

The discussion in this section considers the notion of a regional internet. A regional internet arises as a sovereign state enforces its own data retention and sovereignty policies. The regional internet becomes a fragment of the internet after sovereignty policies are applied. Therefore, each sovereign state can be regarded as an internet fragment in the description of the problem i.e. challenges being addressed.

The exchange of data between the internet fragments in regions α_p and α_q for a duration spanning the epochs t_y and t_J can also be infeasible. This arises in two cases. Both cases consider that the epochs lying between t_y and t_J are $t_{y+1}, t_{y+1} \epsilon t; t_{y+2}, t_{y+2} \epsilon t; t_{y+3}, t_{y+3} \epsilon t$ and $t_{y+j}, t_{y+j} \epsilon t, y + j < Y; J > y + j$. The scenario in the first case can be given as:

$$\{I_C(\alpha_p, \alpha_q, t_y), I_C(\alpha_p, \alpha_q, t_{y+1}), I_C(\alpha_p, \alpha_q, t_{y+2}), I_C(\alpha_p, \alpha_q, t_{y+3}) \ldots, I_C(\alpha_p, \alpha_q, t_{y+j})\} = \{0, 0, 0, 0, 0\} \tag{8}$$

$$I_A(\alpha_p) = 0, I_A(\alpha_q) = 0 \tag{9}$$

The second case is given as:

$$\{I_C(\alpha_p, \alpha_q, t_y), I_C(\alpha_p, \alpha_q, t_{y+1}), I_C(\alpha_p, \alpha_q, t_{y+2}), I_C(\alpha_p, \alpha_q, t_{y+3}) \ldots, I_C(\alpha_p, \alpha_q, t_{y+j})\} = \{1, 1, 1, 1, 1\} \tag{10}$$

$$I_A(\alpha_p) = 1, I_A(\alpha_q) = 0 \tag{11}$$

$$I_A(\alpha_p) = 0, I_A(\alpha_q) = 1 \tag{12}$$

The validity of the conditions in (7) and (8) signify a case where cross–border data exchange occurs between the regions α_p and α_q over the duration spanning the epochs t_y and t_{y+j} is executed. The validity of the conditions in (9) and (10) signify that the cross–border data exchange cannot be successfully executed. This is because of the absence of data exchange agreements between the sovereign regions α_p and α_q even when these regions aren't arid. In addition, the conditions in (11) and (12) when valid indicate the existence of cross–border data exchange agreement between α_p and α_q. In this case; the sovereign region α_q is incapable of hosting water–cooled or air–cooled data centres. Hence, computing platform service providers do not deploy terrestrial data centres in the q^{th} sovereign region α_q.

The epochs considered in the scenario in the relations: (7) and (8), (9) and (10), (11) and (12); and (11) and (13) don't consider the occurrence of desertification as a dynamic event. However, the process of desertification can make a previously suitable region infeasible for hosting data centres. The event of desertification is deemed to occur due to the influence of climate change. In incorporating the event of desertification, the indicator variable $I_A(\alpha_p) \epsilon \{0, 1\}$ is dynamic and presented as $I_A(\alpha_p, t_y) \epsilon \{0, 1\}$. The p^{th} sovereign location α_p is deemed an arid region and not an arid region at the epoch t_y when $I_A(\alpha_p, t_y) = 1$ and

$I_A(\alpha_p, t_y) = 0$, respectively. The internet fragments in the p^{th} sovereign region α_p and q^{th} sovereign region α_q with existing cross–border data exchange agreement cannot share data when:

$$\{I_A(\alpha_f, t_y), I_A(\alpha_f, t_{y+1}), I_A(\alpha_f, t_{y+2}), I_A(\alpha_f, t_{y+3}), I_A(\alpha_f, t_{y+j}), I_A(\alpha_f, t_J)\} = \{0, 0, 1, 1, 1\}, f \epsilon \{p, q\} \tag{13}$$

The relations in (14) describe the case where desertification process occurs for 3 epochs. The scenario in (14) assumes that the existing policies allow a cross–border data exchange between the p^{th} sovereign region α_p and q^{th} sovereign region α_q. In this case, the progressive occurrence of desertification leads to the case where environmental conditions make the operation of terrestrial data centres (water–cooled or air–cooled) is infeasible. Therefore, a solution to address this challenge is required.

The validity of the conditions in (7) and (8), (9) and (10), (11) and (12); and (11) and (13) present a challenge that requires a novel solution. In this case, this is due to the absence of cross–border data exchange agreements. Therefore, two challenges have been identified. These challenges require the design of a novel network architecture. The first challenge is one requiring the execution of cross–border data exchange when there are no supporting cross–border data exchange agreements as seen in (7) and (8), (9) and (10); and (11) and (12). The second challenge arises due to the occurrence of increasing desertification in sovereign regions hosting data centres. In this case, the severity of desertification increases. The research presents a novel architecture that aims to address the challenges.

4 Proposed solution –multimedia sharing without content sovereignty limitation

The network architecture that addresses the challenges in (4) – (5) is presented in this section. In this case, it is important that computing platforms and servers hosting multimedia content can interact with each other. This interaction enables the multimedia content designated and initially intended for a given region to be viewed by subscribers in another region. In each region, the multimedia content is hosted aboard a convergence server in a cloud computing entity. The convergence server aggregates multimedia content from different service providers. Examples of service providers in this case are pay television service providers, online video streaming platforms and hybrid content streaming service providers.

The information on the multimedia content is stored alongside the multimedia content aboard servers that comprise the CSE. Each region is associated with a CSE i.e. distributed server networks that aggregate multimedia content from content producers. The sharing information for the content on a CSE is defined and stored on the DCSE. The DCSE hosts servers that allow content providers to specify new locations whose subscribers can access their content. The stored and shared content is hosted aboard the CSE that acts as the main server. The DCSE hosts sharing information for contents stored in the CSE and functions as a secondary server. The multi-media sharing entity receives network requests for multimedia content access from other regions. It determines if the DCSE allows the sharing of the requested content. The shared content is hosted aboard the MAE for a given duration. This is because media viewing laws do not initially support the sharing of the concerned multimedia content from the CSE. Relation between the CSE, DCSE and MAE is shown in Fig. 1. In Fig. 1, the CSE has own network access entity that communicates with the

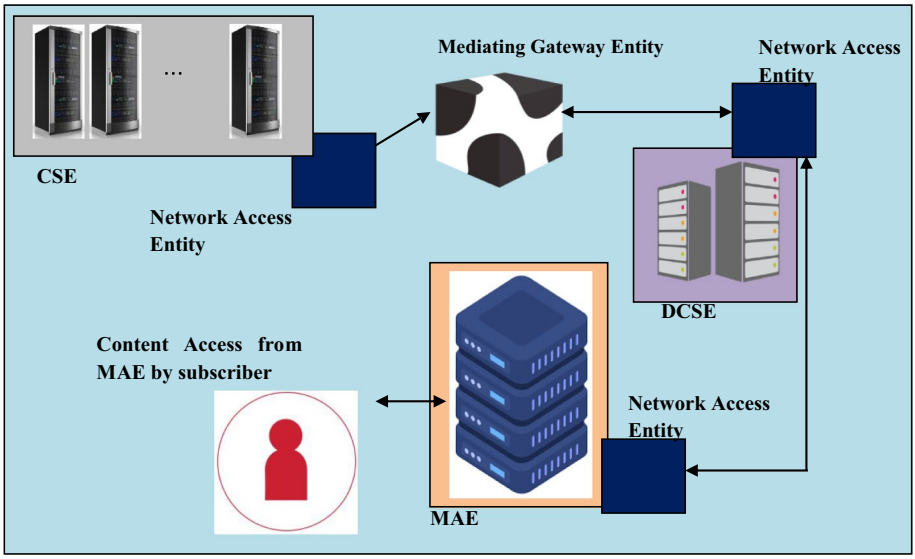

Fig. 1 Relations between entities in the proposed dynamic multimedia content access mechanism

DCSE's network access entity through the mediating gateway entity. The mediating gateway entity enables the sharing logic to be used in determining if the CSE contents can be shared. In addition, the DCSE also forwards multimedia content that can be shared to the network access entity. The CSE has larger data storage and processing capability than the DCSE. The mediating gateway entity enables the relations between CSE and DCSE. It also allows the upload of information to the CSE and DCSE. The data being uploaded to the CSE is multimedia content that can be streamed or downloaded by subscribers. In the case of the DCSE, new updates to multimedia content sharing policy are uploaded. These updates include adding new locations to participate in content sharing and removal of locations from supporting multimedia sharing.

Furthermore, the information on allowed multimedia content access duration is an important parameter that is considered in the multimedia content sharing policy. The multimedia content access duration determines the period for which the multimedia content is held aboard the MAE. The content access duration is determined for each multimedia file held aboard the CSE and for which the DCSE supports sharing. The content access duration is determined by the producer of the multimedia content. This information is defined for multimedia content prior to upload via the mediating gateway entity.

The multimedia content is assigned a content ID by the mediating gateway and uploaded to the CSE. The information on the allowable content sharing duration is uploaded to the DCSE. The two uploads being considered are executed by the media gateway entity. Multimedia content uploads are assigned and identified by the content ID. The content ID is used to identify the concerned multimedia content aboard the CSE. The content ID is also used to identify the allowable sharing duration of the concerned multimedia content aboard the DCSE. The information on the content sharing duration is used to determine the existence of the content intended for subscriber access in the MAE. Multimedia content is removed from the MAE after the expiration of the content allowable sharing duration. In the event that the content allowable sharing duration is changed, the new duration determines the

length of time that the content remains in the MAE. In Fig. 1, the subscriber accesses the content from the MAE via either streaming or download. This access is realized via a network with internet access capability. A content remains in the MAE only for the length of time defined in the content allowable sharing duration.

5 Proposed solution – network sovereignty involving aerial computing entities

The solution described and presented in Fig. 1 focuses on describing and presenting the communications and computing aspects related to the proposed solution. This does not consider how the proposed solution is integrated and realized using data centre systems. The data centres being used are aerial computing platforms i.e. SBDC intended for use in arid and hyper–arid regions that are subject to dynamic desertification. In the proposed system, each region is considered to host a portion of the internet i.e. an internet fragment. Each region hosts an internet fragment.

The challenge being addressed is one of ensuring communications enabling the exchange of multimedia content between internet fragments. The presented research aims to enable access of multimedia content by subscribers across different sovereign regions thereby necessitating a cross–border data exchange. The cross–border exchange enables the realization of multimedia content sharing between internet fragments. The discussion here is divided into two aspects.

The first aspect addresses the challenge associated with enabling cross–border data (multimedia content) exchange in the absence of supporting data exchange agreements. The second aspect focuses on addressing the challenges associated with realizing multimedia content exchange due to increasing desertification. Both aspects utilize aerial computing platforms i.e. SBDCs. This is because of their mobility and low water footprint. The use of SBDCs enables the realization of selective data sharing amongst internet fragments. In this case, internet fragments are portions of the internet that are under the control of different sovereign regions each with own data sovereignty and retention policies. In this case, the data sovereignty policies are specified by the concerned nations. A second aspect of the policies is specified by the content producers and providers. This is done to determine multimedia content that can be shared by the CSE to the MAE via the DCSE. The content sharing is accompanied by the allowable duration specified in the DCSE. The CSEs and DCSEs are realized using the proposed SBDC. The functionality of the CSE and DCSE can be integrated aboard servers that are located in a single SBDC. In our consideration, each SBDC hosts the entities that execute the functionalities of the CSE, DCSE and MAE. This implies that the SBDC hosts the network access entities enabling the upload of multimedia content and update of multimedia content sharing policies to the CSE and DCSE, respectively. In addition, the SBDC hosts the MAE alongside network access entities enabling the temporal storage of shared multimedia content. The consideration in other aspects is set in the context that an SBDC hosts servers that execute the functionalities of the CSE, DCSE and MAE. Prior to using SBDCs, these internet fragments enabling subscribers in arid regions are unable to engage in cross–border data (multimedia content) exchange.

Relation between internet fragments after SBDC incorporation is shown in Fig. 2. Prior to the incorporation of SBDC, the internet fragments are incapable of engaging in data communications. The case in Fig. 2 is one in which SBDCs enable selective data (multimedia content) sharing between the sovereign regions SR 1, 2, 3, 4, 5 and 6. In Fig. 2,

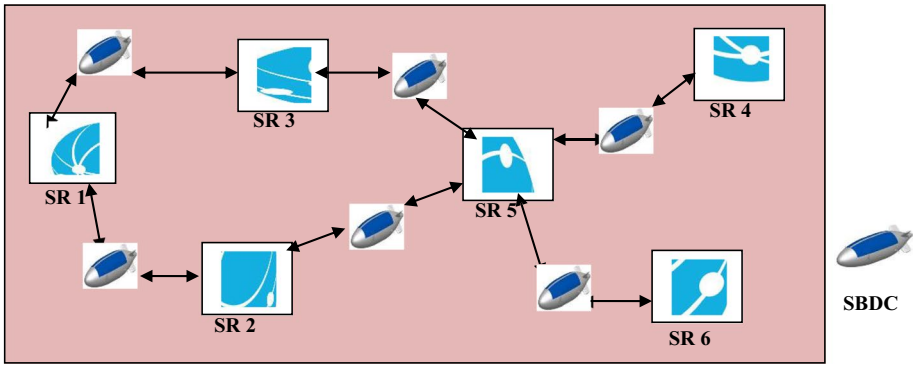

Fig. 2 Network scenarios showing communications via SBDC between the sovereign regions

communications between internet fragments in SR 1, 2, 3, 4, 5 and 6 is enabled by SBDCs. The six SBDCs are used to realize communications between SRs 1 and 2, SRs 1 and 3, SRs 2 and 5, SRs 3 and 5, SRs 4 and 5; and SRs 5 and 6.

5.1 First aspect: mobility and micro–sovereignty data sharing policies

The first aspect proposes a dynamic solution enabling multimedia content sharing in the absence of cross–border data sharing agreements. The sharing is realized by aggregating sharing status and allowable duration on the multimedia content in the MSP. The MSP is proposed to enable the sharing of multimedia content. The data sovereignty policy approach that is found in existing literature establishes relations between sovereign locations on data sharing for a long period.

However, the consideration of a shorter duration for the sovereignty relationship for multimedia content as seen in the MAE is also feasible. This is combined with a data–selective approach for ensuring that sensitive data remain within the borders of the sovereign nation. The MSP is presented from the perspective of data sovereignty policy disaggregation with relation to the sharing of multimedia content. A data sovereignty policy prevents data sharing at all epochs (for a significantly long duration). The long duration is the sum of all the duration associated with multiple MSPs. In addition, all locations being considered in data sovereignty policies are the aggregate of locations in multiple MSPs. Hence, an MSP can support data sharing between some locations in a given context while preventing data sharing between other locations.

The MSP is held aboard the DCSE and is processed by a cognitive agent aboard the SBDC's DCSE. In addition to the multimedia content storage duration, the MSP defines the allowable transmission duration. In this case, the allowable transmission duration exceeds the typical communication latency. The specification of this relation is necessary because of the influence of the wireless channel. In the case where there is a long latency, the access of the concerned multimedia content latency by the subscribers is more prone to errors and corruption from the wireless channel. These factors indicate that the concerned multi–media content may not be properly received by recipient SBDC (with MAE). This makes future useful access challenging to subscribers.

The process of accessing and using the MSP (aboard the MAE) is preceded by making a decision on the target location of the desired SBDC hosting the desired multimedia

content. This process has four stages. The first stage involves determining the location of the recipient SBDC requiring access to the multimedia content being held aboard a server in another sovereign region.

The second stage involves the transmission of the concerned multimedia content from the destination SBDC CSE server. This is completed after determining that the requested data can be shared by accessing information by the content producer defined in the MSP and held in the DCSE. The functionality of determining the sharing status of the concerned multimedia information is executed by the data type analysis entity (DTAE). The third stage is the execution of data transfer between the server and the SBDC. The fourth stage involves data transfer between the SBDC and the requesting data centre.

The first, second, third and fourth stages are executed for a significant number of multimedia content streaming and download requests between different sovereign locations. This is deemed feasible due to the increasing proliferation of streaming and viewing of multimedia content. In the event that the requesting subscriber (associated with a given SBDC) is significantly distant from the destination SBDC, a satellite link is used to realize the intended communications. In this case, the SLDE located at the requesting SBDC determines destination SBDC accessibility. The inability of the requesting SBDC to detect the destination SBDC necessitates using the satellite link.

Prior to being uploaded to the SBDC, a sovereign authority (governmental authority) determines multimedia content that can be shared (with significant consideration of provider preferences) and associated duration. This is done to determine the content to be transmitted to the SBDC from a network entity. The network entity is not a terrestrial based computing platform due to the challenges of cooling.

The allowable duration for the p^{th} sovereign region α_p is denoted $\varsigma_1(\alpha_p)$. In addition, the tuple of multimedia content described accessible from the p^{th} sovereign region α_p is denoted $\varsigma_2(\alpha_p)$. The governmental authority sends information on $\varsigma_1(\alpha_p)$ and $\varsigma_2(\alpha_p)$ to the computing entity. In this case, the computing entity plays the role of refining data to be later uploaded to the SBDC. The relation between the internet and the sovereign region's governmental entity is in Fig. 3. In Fig. 3, the governmental authority entities i.e. GA 1 and GA 2 interact with the computing entities (CEs) i.e. CE 1, CE 2 and CE 3. GA 1 and GA 2 send information on $\varsigma_1(\alpha_p)$ and $\varsigma_2(\alpha_p)$ to CE 1, 2 and 3. Each of the entities CE 1, 2 and 3 host the data in $\varsigma_1(\alpha_p)$ and $\varsigma_2(\alpha_p)$ for different sovereign regions. The entities GA 1 and GA 2 determine the values of $\varsigma_1(\alpha_p)$ and $\varsigma(\alpha_p)$ in line with data sovereignty policies for different sovereign regions and governmental authorities. This is done in conformance with sovereign policies on data sharing.

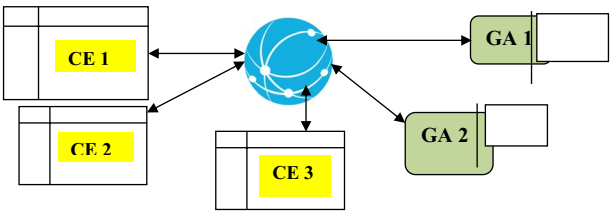

Fig. 3 Scenario showing communications between computing entities and governmental authorities

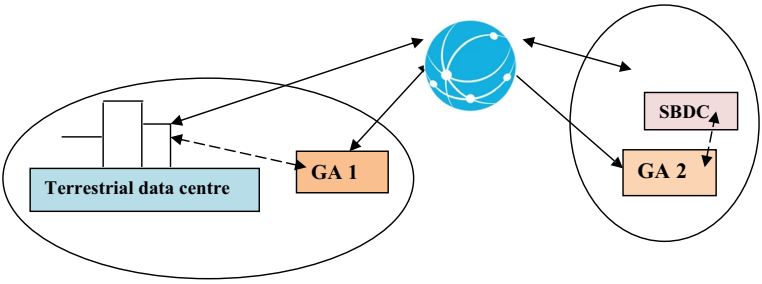

Fig. 4 Communications between governmental authorities, terrestrial data centres and SBDC

5.2 Second aspect—data exchange considering desertification

The progressive occurrence of desertification leads to increasing footprint of land becoming unsuitable for hosting terrestrial data centres. In this case, the functionality of the CEs is now realized by SBDCs. The SBDCs are launched in regions that are deemed unsuitable for hosting terrestrial data centres. The SBDCs engage in communications with terrestrial data centres in non–arid regions. A scenario showing the case of an SBDC involved in cross–border data exchange with a terrestrial data centres is presented in Fig. 4. The scenarios presented in Fig. 4 shows relations between governmental authorities GA 1, and GA 2. The scenario in Fig. 4 concerns GA 1 and GA 2. In Fig. 4, GA 1 and GA 2 sends the MSP to the terrestrial data centre and SBDC, respectively. GA 1 and GA 2 transmit their data via the internet. Another feasible case is one where direct communications between governmental authorities and CEs (terrestrial data centres and SBDCs) occur. In this case, GA 1 and GA 2 can directly communicate with the terrestrial data centre and SBDC, respectively.

5.3 Dynamic data sharing – traffic offloading and management

An important challenge that should be addressed is that of ensuring that the occurrence of network congestion does not prevent cross–border multimedia content exchange between two sovereign regions. The occurrence of congestion aboard an SBDC can prevent the execution of multimedia content exchange between two locations. This arises when there is a significant amount of traffic arising due to several MSPs.

In this case, each SBDC is associated with support network nodes. There are two types of network support nodes. These are the STENs and SAENs. The SAEN and STEN are used to ensure the execution of cross–border multimedia content exchange via offloaded traffic. The offloaded traffic arises from extra workload that can't be handled by the SBDC. Each SBDC is associated with an SAEN and STEN. In addition, SBDCs can communicate with own SAEN and STEN via a wireless link. The communications enable the realization and execution of traffic offloading. The SAEN or STEN being used for traffic offloading communicates with the neighbouring SAEN or STEN via the internet. Low latency and high speed communications in the context involving SAEN, STEN and SBDC is realized via high bandwidth. The use of STEN is not associated with cooling and a high water footprint. This is because STEN has lower capacity than terrestrial computing platforms.

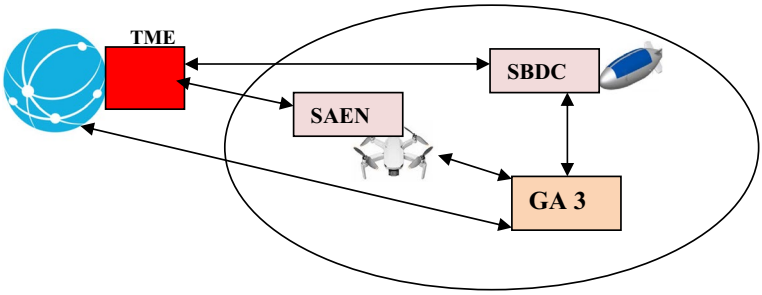

Fig. 5 Role of SAEN and TME in traffic offloading to prevent SBDC traffic congestion

SAENs and STENs can receive data being previously transmitted to a congested SBDC. In executing this action, the SAEN or STEN communicates with the concerned GA. The traffic offloading is executed by the mediating TME. The TME receives information on the traffic capability and current traffic level of traffic being processed by the SBDC. In the event that the pre–defined SBDC traffic threshold is exceeded, TME sends MSP related traffic to the SAEN. The role of the SAEN in traffic offloading from the SBDC for GA 3 is shown in Fig. 5.

The scenario in Fig. 6 presents the multi–tiered traffic offloading system comprising the aerial tier, terrestrial tier, decision tier and the data centre tier. The aerial tier and terrestrial tier host the SAENs and STENs, respectively. The decision tier hosts the TME. The TME hosts the sub–monitoring entities that determine the occurrence of traffic congestion aboard the SBDC, SAEN and STEN in a given context. This is done using information on the traffic capability and current traffic of the SBDC, SAEN and STEN.

In addition, the scenario in Fig. 6 shows the role of the TME (decision making tier) in interacting with the SBDC (data centre tier), aerial tier (SAEN) and terrestrial tier (STEN). In the presented scenario, the aerial tier entities i.e. SAEN is used to host offloaded traffic before the SBDC. The terrestrial tier (STEN) is used to execute the transfer of offloaded traffic when the capacity of the SBDC and SAEN are overwhelmed. This results in the occurrence of congestion of the SBDC and SAENs. The overwhelming traffic is offloaded to the STEN in this case.

The flowchart showing the execution of the proposed algorithm enabling content sharing is in Fig. 7. The flowchart in Fig. 7 shows content access considering the role of the SBDC's CSE, DCSE, DTAE, MAE and MSP. The flowchart in Fig. 8 shows the role

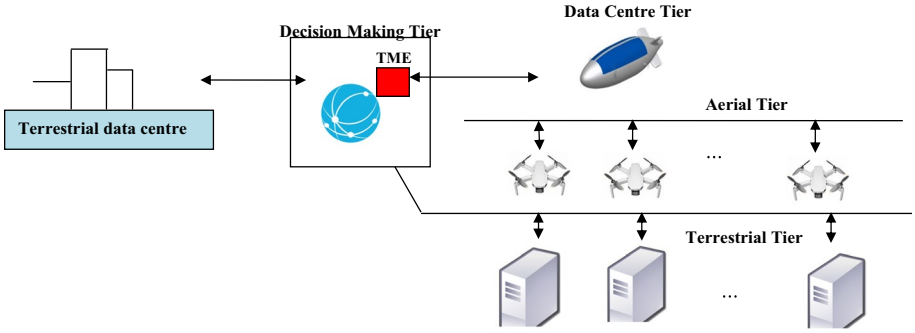

Fig. 6 Role of SAEN and TME in traffic offloading to prevent SBDC traffic congestion

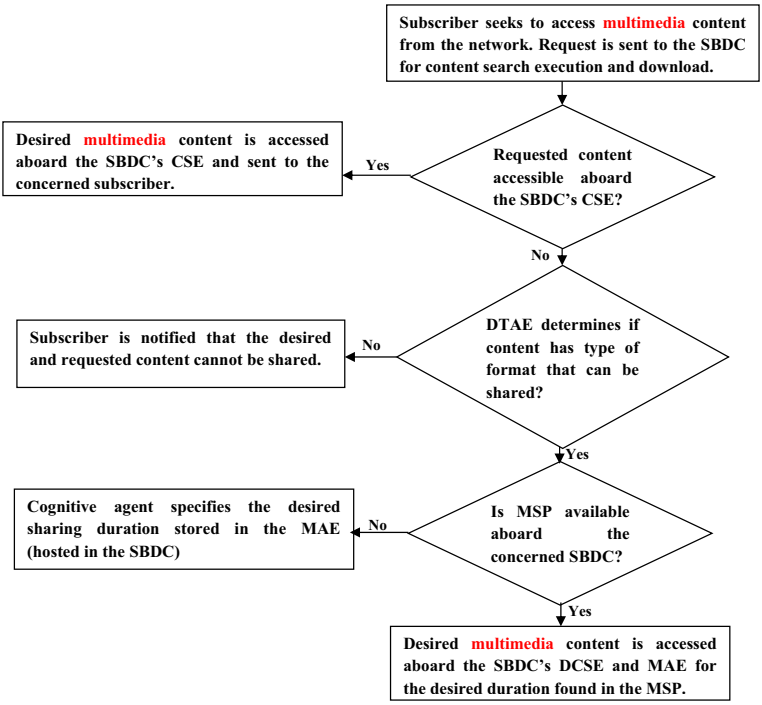

Fig. 7 Flowchart showing role of proposed mechanism and tasks executed in accessing multimedia content

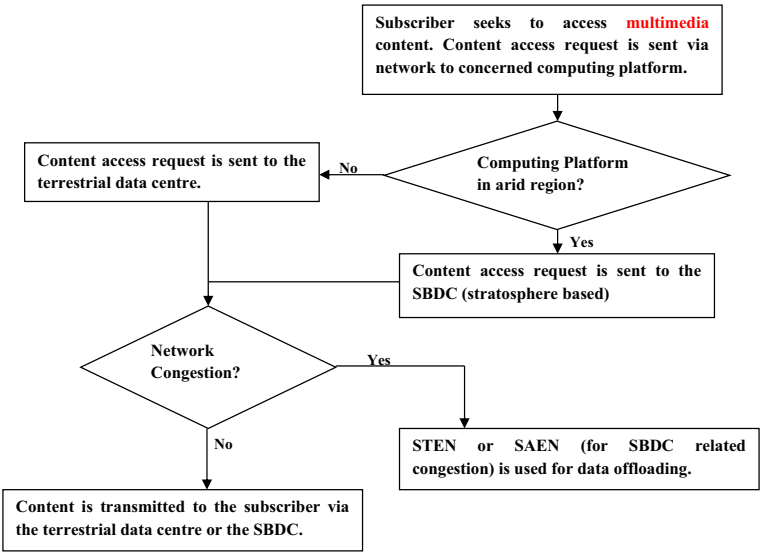

Fig. 8 Flowchart showing execution of proposed mechanism considering occurrence of congestion and requesting subscriber location

of the SBDC considering the occurrence of desertification. In this case, data centres in arid and non–arid regions are being considered.

6 Performance formulation

The section formulates this performance model for the case of the existing and proposed approach. The formulated metric is the number of locations engaged in cross–border data exchange. This describes the number of locations from which subscribers can access multimedia content that was initially intended for sole access to subscribers at a given location. The metrics is formulated considering cases prior to and after using the proposed mechanism. In the existing approach, terrestrial data centres in selected locations are able to engage in cross–border data exchange i.e. share hosted multimedia content with subscribers in pre–defined locations. The number of locations capable of supporting cross–border data (multimedia content) exchange in existing approach is denoted θ_1 and given as:

$$\theta_1 = \sum_{q=1}^{I} \sum_{p=2}^{I-1} \sum_{y=1}^{Y} \left(|\alpha| - \left| I_C(\alpha_p, \alpha_q, t_y) = 0 \right| \right), p > q \tag{14}$$

The existing approach is one in which terrestrial data centres enable accessing multimedia content across multiple regions by subscribers. In this case, data sovereignty and content sovereignty influences content that is accessible by subscribers at a given location. Subscribers at arid regions (where hosting data centres are challenging) are unable to access multimedia content at low latency. This is the existing case for multimedia content via online streaming platforms such as YouTube. In the case of YouTube, the sovereignty is relevant because some contents cannot be accessed from locations but at other locations. In the case of the existing mechanism (solution), the number of content access locations is influenced by the number of sovereign states and the number of locations where policies enable cross–border data exchange.

In the proposed mechanism, the number of locations that support cross-border data exchange is increased via the introduction of micro-sovereign policies (MSPs). In this case, the number of locations supporting data exchange increases. The increased in the number of locations arises from the incorporation of SBDCs. The number of locations capable of supporting cross–border data (multimedia content) exchange is denoted θ_2 and given as:

$$\theta_2 = \sum_{q=1}^{I} \sum_{p=2}^{I-1} \sum_{y=1}^{Y} \left(|\alpha| - \left| I_C(\alpha_p, \alpha_q, t_y) = 0 \right| \right) + \sum_{m=1}^{M} \sum_{q=1}^{I} \sum_{y=1}^{Y} \left(\left| I_C(\gamma_m, \alpha_q, t_y) = 1 \right| \right), m \neq q, p > q \tag{15}$$

$\gamma_m \epsilon \gamma, \gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_M\}$ is the m^{th} SBDC and γ is the set of SBDCs.

$I_C(\gamma_m, \alpha_q, t_y) \epsilon \{0, 1\}$ is the communication status indicator between the m^{th} SBDC, γ_m and the q^{th} sovereign region α_q with a data centre at the y^{th} epoch, t_y. The m^{th} SBDC, γ_m and the terrestrial data centre the q^{th} sovereign region α_q communicate and do not communicate at the epoch t_y when $I_C(\gamma_m, \alpha_q, t_y) = 1$ and $I_C(\gamma_m, \alpha_q, t_y) = 0$, respectively.

In (20), the second term describes the number of cross–border data exchanges arising from the incorporation of SBDCs and the MSP. The second term is an increment on the number of locations for the formulation that is presented in (19).

7 Performance evaluation

The performance evaluation is done with the aim of investigating the benefits of using the proposed mechanism using parameters in Table 3. In the simulation conducted using the parameters in Table 3, a sovereign region are covered by one SBDC. The SBDCs across each region communicates with each other in the execution of a data sharing epoch. The network configuration is one in which SBDCs communicate with each other in a line of sight network system. In the network, SBDC are able to communicate with each other where a line of sight exists. Furthermore, an SBDC can communicate with another SBDC using an intermediate SBDC as the connecting node. This is done when non line of sight occurs and limits inter – SBDC communications. Inter–SBDC communications occurs when the data sovereignty policy allows the concerned SBDCs to communicate with each other. In the simulation, some SBDCs are communicates with other SBDCs while others are not able to communicate with other SBDCs.

The performance simulation is done with the aim of investigating how the number of locations supporting content sharing varies for different number of sovereign regions and sharing epochs. In the existing approach, SBDCs are not used and arid regions are not considered. However, the simulation in the case of the proposed approach considers the use of SBDCs, and content access in arid regions.

The evaluation investigates the number of locations that supports cross–border data exchange for different number of sovereign regions and epochs. This refers to the number of new locations that can now access the multimedia content that was previously accessible from only one location. The case for one, two and three sovereign regions as obtained for the existing scheme is presented in Fig. 9a. The case of the number of locations for four, five and six sovereign regions in the existing scheme is presented in Fig. 9b. The existing approach is one where governmental authorities change the policies on data sharing and sovereignty. The consideration of more sovereign regions increases the number of locations. Analysis shows increasing the number of sovereign regions by 50% (from 1 to 2 sovereign regions), 66.7% (from 2 to 3 sovereign regions), 75% (3 to 4 sovereign regions), 80% (from 1 to 5 sovereign regions) and 83.3% (from 1 to 6 sovereign regions) enhances number of dynamic data sharing locations by an average of 41%, 63.1%, 70.7%, 74.4% and 78.2%, respectively. This implies that there is an increase in the number of new regions where new subscribers can access multimedia content. The resulting increase lies in the range (41–78.2) %.

Table 3 Performance evaluation and simulation parameters

S/N	Parameter	Values
1	Sovereign Regions (total number considered in the simulation)	15
2	Transmit Epochs (total number considered in the simulation)	56
3	Number of Data Sharing Support Epochs Across All regions	1559
4	Number of Data Sharing Prevent Epochs Across All regions	1577
5	Proportion of Data Sharing Support Epochs	49.71%
6	Proportion of Data Sharing Prevent Epochs	50.29%
7	Number of Sovereign Regions for SBDC	15

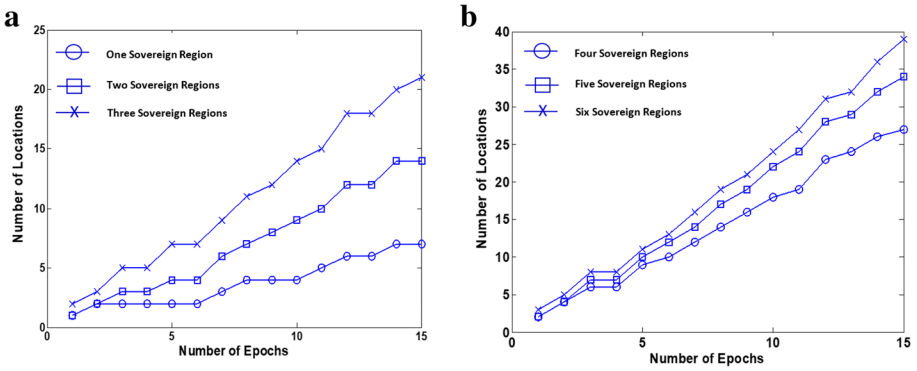

Fig.9 **a** Number of data sharing locations given one, two and three sovereign regions in the case of the existing scheme. **b** Number of data sharing locations given four, five and six sovereign regions with the use of existing scheme

In a similar manner, an increase in the number of sovereign regions by 33.3% (2 to 3 sovereign regions), 50% (2 to 4 sovereign regions),and 60% (2 to 5 sovereign regions) increases the number of data sharing locations by an average of 36.7%, 50.3% and 57.5%, respectively. In addition, an increase in the number of sovereign regions by 20% (from 4 to 5 sovereign regions), 40% (from 3 to 5 sovereign regions) and 25% (from 3 to 4 sovereign regions), enhances the number of data–sharing locations by an average of 14.4%, 32.3% and 21.2%, respectively. Therefore, the number of regions that can now access multimedia content from a previously infeasible region improves by an average of (14.4 – 32.3) %.

The results shows that transiting from a high number of sovereign regions to a case involving more sovereign regions results in a smaller mean increase in the number of locations that can share multimedia data. For example, an increase from 5 to 6 sovereign regions (an increase of 16.7%) results in the number of locations enabling the sharing of multimedia content by an average of 12.7%.

The effect of using the proposed mechanism in the number of data sharing locations is also investigated. The performance model is also evaluated using obtained results for the case of one and two sovereign regions are in Figs. 10a and 10b, respectively. This is done for two regions i.e. region 1 (considered in Fig. 10a) and region 2 (used alongside for the results presented in Fig. 10b). In the case of region 1, increasing the number of SBDCs by 33.3% (4 to 6 SBDCs), 50% (2 to 4 SBDCs) and 66.7% (2 to 6 SBDCs) increases the number of data sharing locations by an average of 12.1%, 8.3% and 22.4%, respectively. In a similar manner, increasing the number of SBDCs in the case of region 2 by 33.3%, 50% and 66.7% enhances the number of data sharing locations by 12.1%, 8.3% and 22.4%, respectively. This implies that increasing the network size to host more multimedia content and content producers increases the number of locations whose subscribers can access previously inaccessible content.

In this case, the performance model is also evaluated. This is done for two different regions that are considered in the performance evaluation. These regions are region 1 (considered in Fig. 10a) and region 2 (used alongside for the results presented in Fig. 10b). In the case of region 1, increasing the number of SBDCs by 33.3% (4 to 6 SBDCs), 50% (2 to 4 SBDCs) and 66.7% (2 to 6 SBDCs) increases the number of data sharing locations by an average of 12.1%, 8.3% and 22.4%, respectively. For the case of region 2, increasing the

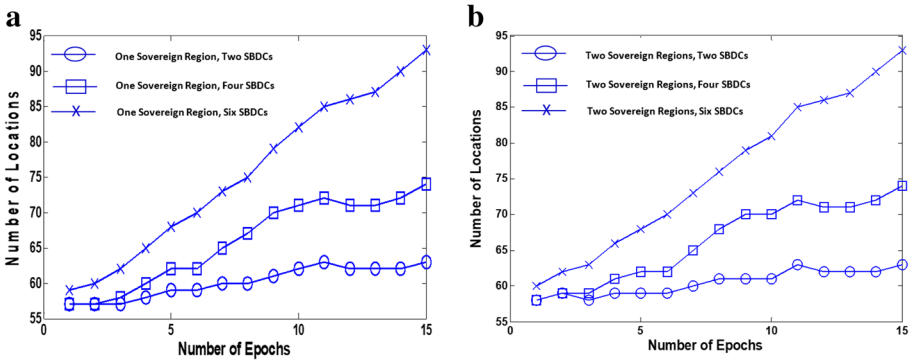

Fig.10 **a** Number of location engaging in data sharing given a sovereign region with the proposed scheme. **b** Number of location engaging in data sharing given two sovereign regions with the proposed scheme

number of SBDCs by 33.3%, 50% and 66.7% improves the number of data sharing locations by 12.1%, 8.3% and 22.4%, respectively.

Performance evaluation is also done for cases with and without the use of proposed mechanism. The use of 2, 4 and 6 SBDCs in region 1 instead of existing mechanism increases the number of data sharing locations by an average of 88.1%, 79.1% and 75.8%, respectively. In region 2, the use of 2 SBDCs, 4 SBDCs and 6 SBDCs instead of existing mechanism increases the mean number of data sharing locations by 88.2%, 79.1% and 75.9%, respectively. Therefore, the proposed mechanism instead increases the number of data sharing locations by (75.8–88.2) % on average.

Therefore, the performance evaluation procedure shows that the proposed mechanism increases the multimedia content sharing capable locations. This implies that subscribers in an increased number of locations can access previously inaccessible content due to the incorporation of the MSP (with dynamic multimedia content sharing policies) in the proposed mechanism and accompanying network architecture.

8 Conclusion

The research presented proposes a solution to enable flexible and dynamic data sharing for contexts involving data sovereignty. The focus of the paper is on the context of multimedia content sovereignty. The paper addresses the challenges on the limited access to multimedia content arising from the initial localization of content to a given region. The research being presented in the paper recognizes that there is an increasing demand for multimedia content in regions where an access was not initially intended. The enhanced access to multimedia content arises from the increasing subscriber demand across multiple regions. The research challenge is addressed for the case of subscribers in arid and hyper–arid regions when using it is infeasible to use terrestrial cloud computing platforms. The presented research proposes the use stratosphere based data centres (SBDCs) for the dynamic sharing of multimedia content. The use of SBDCs enhances the number of locations from which multimedia content can be accessed. Analysis shows that the number of locations capable of engaging in data sharing is increased by (75.8–88.2) % on average when the proposed mechanism is used.

Funding Open access funding provided by Cape Peninsula University of Technology.

Data availability All Concerned Data can be found in the Manuscript.

Declarations

Conflicts of interests The authors declare that there are no competing interests.

References

1. Ahmad BS and Bures M. (2018). Testing of Smart TV Applications : Key Ingredients, Challenges and Proposed Solutions', In K. Arai, R. Bhatia, S. Kapoor (eds), Proceedings of the Future Technologies, Conference (FTC) 2018, FTC 2018, Advances in Intelligent Systems and Computing, Vol. 880, Springer, Cham, pp 241–256.
2. Ala'Anzy M, Othman M (2019) Load balancing and server consolidation in cloud computing environments: a meta- study. IEEE Access 7:141868–141887. https://doi.org/10.1109/ACCESS.2019.2944420
3. Ali AT, Khayyambashi MR, Farsani HK (2020) OASM: An overload – aware workload scheduling method for cloud computing based on bio–geographical optimization. Int J Network Manage 30(4):1–17
4. Baresi L and Quattochi G. (2020). COCOS: a scalable architecture for containerized heterogeneous systems. IEEE Int Conf Software Architecture, 16–20 Salvador, Brazil, pp 103 – 113.
5. Bhardwaj K, Gavriloska A, Kolesnikor V, Saunders M., Yoon H, Bondre M, Babu M and Walsch J. (2019). Addressing the fragmentation problem in distributed and decentralized edge computing: a vision', IEEE Int Conf Cloud Eng (IC2E), 24–27 , Prague, Czech Republic, pp. 156 – 167.
6. Celeste E and Fabbrini F. (2021). Competing jurisdiction: data privacy across the borders', In data privacy and trust in cloud computing, (eds), T.Lynn, J.G.Mooney, L.V.D.Werff and G.Fox, pp 43 – 58
7. Choi J (2019) Virtual machine placement algorithm for energy saving and reliability of servers in cloud data centres. J Netw Syst Manage 27:149–165
8. Couture S, Toupin S (2019) What does the notion of sovereignty mean when referring to the digital? New Media Soc 21(19):2305–2322
9. Esposito C, Castiglione A, Frattini F, Cinque M, Yang Y, Choo KKR (2019) On data sovereignty in cloud – based computation offloading for smart cities applications. IEEE Internet Things J 6(3):4521–4535
10. Ferdousi S, Tornatore M, Dikbiyik F, Martel CU, Xu S, Hirrota Y, Awaji Y, Mukherjee B (2020) Joint Progressive network and datacenter recovery after large-scale disasters. IEEE Trans Netw Serv Manage 17(3):1501–1514
11. Gelhaar J, Grob T, and Otto B. (2021) A taxonomy for data ecosystems', proceedings of the 54TH Hawaii International Conference on System Sciences, pp. 6113 – 6122.
12. Geronimo G, Uriarte R, Westphall C (2019) Order@Cloud: An agnostic meta–heuristic for VM provisioning, adaptation, and organization. Int J Network Manage 29(6):1–20
13. Hummel P, Braun M, Tretter M, Dabrock P (2021) Data sovereignty: a review. Big Data Soc 8(1):1–17
14. Jacquenet C (2021) Optimized, automated and protective: an operator's view on future networks. IEEE Trans Netw Serv Manage 18(2):1350–1359
15. Jarke M. (2020). Data sovereignty and the internet of production', In S.Dustdar, E.Yu, C.Salinesi, D.Rieu, V.Pant, (Eds), advanced information systems engineering CAISE 2020. Lecture Notes in Computer Science, Vol. 12127, pp 549–558.
16. Jarke M, Otto B, Ram S (2019) 'Data sovereignty and data space ecosystems', business and information. Syst Eng 61:549–550

17. Jing W, Zhao C, Miao Q, Song H, Chen G (2021) QoS – DPSO QoS aware task scheduling for cloud computing system. J Netw Syst Manage 29(5):1–29
18. Kodera K, Eguchi N, Ueyama R, Kuroda Y, Kobayashi C, Funatsu BM, Chad C (2019) Implication of tropical lower stratospheric cooling in recent trends in tropical circulation and deep convective activity. Atmos Chem Phy 19:2655–2669
19 Maenhaut PJ, Volckaert B, Ongenae V, De Turck F (2020) Resource management in a containerized cloud: status and challenges. J Netw Syst Manag 28(2):197–246
20 Manabe S (2019) Role of greenhouse gas in climate change. Tellus A: Dyn. Meteorol Oceanogr 71(1):1620078
21. Murschetz PC, and Prandner D. (2018). Datafying' broadcasting: exploring the role of big data and its implications for computing in a big data–driven TV ecosystem', (eds) D.Khajeheian, M.Friedrichsen and W. modinger in competitiveness in emerging markets, pp. 55 – 71.
22. Noam E (2014) Cloud TV: toward the next generation of network policy debates. Telecomm Policy 38(8–9):684–692
23. Otrum, 'Cloud management and control of smart TVs, mobile devices, and casting solutions', Otrum_Interactive_2020_web.pdf, https://otrum.com/wp-content/uploads/2020/02/otrum_interactive_2020_web.pdf
24. Periola AA (2020) Aerial computing – security from missile threats and enhancing PUE. Aerospace Systems 3:327–342
25 Periola AA (2020) Novel tier reclassification for non - terrestrial data centre systems. Proc Niger Acad Sci 13(1):79–97
26. Periola AA, Alonge AA, and Ogudo KA. (2022). Intelligent scheduling for stratospheric cloud platforms', IEEE icABCD, 6– 7, Durban, South Africa, pp 1 – 7.
27. Periola AA, Osanaiye OA (2021) Low cost intent driven future multimedia content access system and network. Multimedia Syst. https://doi.org/10.1007/s00530-021-00789-3
28. Peterson ZNJ, Gondree M and Beverly R. (2011). A position paper on data sovereignty: The importance of geolocating data in the cloud', Proceedings of the 3RD USENIX Conference on Hot Topics in Cloud Computing, pp 9 – 13.
29 Pohle J, Thiel T (2020) Digital sovereignty. Internet Policy Rev 9(4):1–19
30. Popescul D. (2018). Smart TVs: What do they know (and Tell) about us? ', International academic conference on social sciences, prague, Vol. 10, IACSS 2018 – IACLPM 2018 Joint
31. Reznik Y, Cenzano J, Zhang B (2021) Transitioning broadcast to cloud. Appl Sci 11(503):1–23
32. Ruiz MC, Olivares T, Lopez J (2017) Evaluation of cloud platforms for managing IoT devices. Int Conf Inform Intell Syst App Larnaca Cyprus 27–30:1–6. https://doi.org/10.1109/IISA.2017.8316364
33. Schauerte R, Feiereiser S, Malter AJ (2021) What does it take to survive in a digital world, Resource–based theory and strategic change in the TV industry. J Cult Econ 45:263–293
34 Sebrechts M, Seghbroeck GV, Wauters T, Volkaert B, De Turck F (2018) Orchestrator conversation: distributed management of cloud applications. Int J Netw Manage 28(6):1–19
35. Sharma V, You I, Seo JT, Guizani M (2019) Secure and reliable resource allocation and caching in aerial– terrestrial cloud networks. EEE Access 7:13867–13881
36. Taherkordi A, Zahid F, Verginadis Y, Horn G (2018) Future cloud systems design: challenges and research directions. IEEE Access 6:74120–74150
37. Tang C, Plasek JM, Zhu Y and Huang Y. (2020). Data sovereigns for the world economy. Humanit Soc Sci Comm, 7, Article Number 184.
38. Udoakpan N, and Tengeh R.K. (2020). The impact of over – the – top television services on pay – television subscription services in South Africa. J. Open Innov Technol Market and Complexity, 6, 139, (4):1–28.
39. Yang Y, Ren C, Cai M (2016) Towards a physical understanding of stratospheric cooling under global warming through a process–based decomposition method. Clim Dyn 47:3767–3782