Abstract—Worldwide employment of mobile devices in various critical domains, particularly healthcare, disaster recovery, and education has revolutionized data generation rate. However, rapidly rising data volume intensifies data storage and battery limitations of mobile devices. Mobile Cloud Computing (MCC) as the state-of-the-art mobile computing aims to augment mobile storage by leveraging infinite cloud resources to provide unlimited storage capabilities with energy-dissipation prevention. Researchers have already surveyed varied MCC aspects and its challenges, but successful futuristic Mobile Storage Augmentation (MSA) approaches demand deep insight into the current storage augmentation solutions that highlights critical challenges, which are lacking. This paper thoroughly investigates the main MSA issues in three domains of mobile computing, cloud computing, and MCC to present a taxonomy. Also, it examines several credible MSA approaches and mechanisms in MCC, classifies characteristics of cloud-based storage resources, and presents open issues that direct future research.

Index Terms—Mobile Cloud Computing, Cloud Computing, Big Data, Mobile Data, Mobile Data Storage, Taxonomy

I. INTRODUCTION

MOBILE data volume has been increased drastically in recent years. Analysys Mason’s report [1] forecasts 6.3 times growth of mobile data volume traffic amid 2013 and 2018. One reason, among the bevy of inducements is the exploitation of mobile devices in various critical domains of healthcare [2], disaster recovery [3], and education [4]. The voluminous and rapidly generated data in various modalities, which is known as big data [5], demands high capacity, flexible, and reliable storage infrastructure.

However, mobile devices are characterized by storage constraints, limited processing, and a short span battery. Storage limitation and energy consumption are critical factors for resource constrained non-stationary computing devices, especially smartphones. High performance and energy-efficient data storage ensures the battery life’s augmentation. Despite advancements for augmenting a mobile device’s storage including employment of flash and Secure Digital (SD) cards, current rich mobile applications [6] demand higher storage capacity. Reducing the effects of mobile devices’ deficiencies and unreliable wireless connections in comparison with wired networks, are the ultimate goal in the plethora of efforts [7], [8] and research to realize end-users’ demand.

The emergence of the cloud as a rich resource with unlimited computing and storage capacities can be considered as a good solution to mobile devices’ resource constraints. The use of a wireless medium, the offloaded data, the dependency on a specific vendor, and data replication are among several challenges in this domain. Comprehensive studies [9]–[11] have reviewed and tried to address challenges in this area. However, the latest endeavor is to deploy cloud resources to augment computing [12] and storage [13] capabilities for a multitude of mobile devices which leads to the state-of-the-art MCC.

The MCC paradigm combines cloud computing, mobile computing, and networking [14] to enhance the performance and capacity of mobile devices. It is characterized by inherited mobility and rich services from mobile and cloud computing where a resource poverty (storage, computation, and battery) can impede the vision of time-, location-, and system type-free ubiquitous computing [15].

In the previous works [14]–[19], the MCC domain have been comprehensively investigated from various perspectives. In [19], authors presented an extensive survey of heterogeneity in the MCC domain, presented an MCC definition, identified major MCC challenges, devised its taxonomy, and highlighted several crucial open issues that help to identify future research directions. Cloud-based augmentation [16] surveys the recent mobile augmentation efforts that employ cloud computing infrastructures to enhance computing capabilities of resource-constraint mobile devices, especially smartphones. To the extent of our knowledge, investigation of storage augmentation issues in the MCC domain is a nascent literature and requires comprehensive study and analysis.

In this paper, we comprehensively analyze MSA issues in the context of mobile computing, cloud computing, and MCC where each domain’s issues are investigated. Based on the investigated issues, we classify MSA issues into three classes of mobile device, cloud-based and converged issues. Based on a review of prominent MSA approaches in MCC, we classify cloud-based storage characteristics in a taxonomy that encompasses architecture, capacity, tiering, mobility, location, and back-end connectivity. The paper highlights several open issues in MCC for MSA to pave the way for future efforts. Mobile devices and smartphones are used interchangeably in this paper. Table I provides a list of acronyms used throughout the paper.
Among real challenges that affect data availability in mobile computing devices, limited wireless throughput, and a small user interface are critical factors for resource constrained non-stationary battery. Hence, storage limitation and energy consumption by storage constraints, limited processing, and a short span of their intrinsic capabilities. Mobile devices are characterized by large elastic storage on mobile devices which is beyond mobile devices—named mobile data. Therefore, data availability on mobile phones (i.e., video, music, images, and any location related information) [21]. However, such rapid data generation by mobile devices—named mobile data—demands extremely high performance energy-efficient storage to alleviate storage shortcomings by leveraging lightweight methods.

The review of storage augmentation approaches in mobile devices, cloud resources, and MCC has led us to devise a taxonomy of issues as depicted in Figure 1. The taxonomy encompasses three main classes of mobile device, cloud-based, and converged issues, which are described in more details as follows.

### A. Mobile Device Issues

In the work [16], a taxonomy of augmentation motivation has been presented based on the intrinsic deficiencies of mobile devices. Storage augmentation approaches mainly facing issues pertaining to intrinsic and non-intrinsic deficiencies of mobile devices. Hence, the same taxonomy can be applied for the classification of storage augmentation issues. The processing power of mobile devices, energy resources, local storage, visualization capabilities, data safety, security, and privacy are the vital issues that pose challenges and encumber efficient and effective mobile data storage.

Mobile devices are characterized by limited processing power, which implies restricted cache equipment. Restricted cache imposes more I/O operation and increased energy consumption and processing time for data-intensive operations. Data transmission in intermittent wireless networks is an energy-consuming task. Intermittency due to the unreliability of a wireless link or a planned disconnection to save battery life are inevitable [25]. Therefore, data availability on mobile devices becomes a significant research direction. However, being nomadic, mobile devices cannot benefit from the vast data storage that is available to their immobile counterparts, which confines the amount of locally-stored data. Moreover, a mobile Database Management Systems (DBMS) functionality...
is influenced by the limited processing power and memory of the host mobile devices. The size-constraint screens and the gracile keyboards of mobile devices as visualization limitations are other impediments in the design of storage augmentation approaches.

Researchers endeavor to address aforementioned issues by major MSA approaches including caching [26], hoarding, and replication mechanisms [27] as well as broadcasting [28] and summarization [25] for mobile environment data.

B. Cloud-based Issues

Storage augmentation issues are not merely peculiar to the mobile environment. Advancements in data storage technology from magnetic tapes and disks, optical/magneto-optical storage media, and flash memory to a storage area network, network attached storage, and even storage virtualization approaches [29] cannot compete with the drastic growth of digital data to terabytes and petabytes [9], which calls for additional data-intensive computing and management mechanisms.

The advent of the cloud as a rich computing resource [30] has provided virtually infinite data storage to the industry and individuals. The cloud as proposed in [30] is “a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers”. Cloud computing exploits cloud resources to provide “ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [31].

However, reliability, Service Level Agreement (SLA), performance, portability, security, and data confidentiality [9] can be considered major cloud-related storage augmentation issues. Reliability can be realized with redundancy, which may jeopardize guarantees for Atomicity, Consistency, Isolation, and Durability (ACID) transactions. Active standardization to mitigate a customer’s data extraction as an approach for the data lock-in and portability issue, the concurrent execution of an application’s threads, optimized online scheduling [32] and the rich encryption as mechanisms for performance and security are among some of the effective approaches for addressing the aforementioned issues [33].

C. Converged Issues

The power of MCC originates from the convergence of mobile and cloud computing, which merges mobility, rich resources, and functionality as renowned advantages of each domain [15]. Resource poverty — processing power, storage capacity, and battery power — are inborn characteristics of mobile devices, and the consequent mobile device storage augmentation issues can be alleviated by leveraging MCC. MCC is “a rich mobile computing technology that leverages the unified elastic resources of various clouds and network technologies toward an unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere and anytime through the channel of the Ethernet or Internet regardless of the heterogeneous environments and platforms based on the pay-as-you-use principle” [19].

However, MCC is heterogeneous by nature because of inhomogeneous converged computing and networking technologies [19]. MCC heterogeneity is a consequence of diverse hardwares, operating systems, development languages, data structures and network technologies. Although mobile computing is augmented through rich resources of the cloud, the heterogeneity-based issues pose real challenges for storage amelioration in MCC. Data portability and interoperability, energy efficiency, long WAN latency, and data fragmentations are among the major issues of storage augmentation in MCC as identified in our proposed taxonomy. Addressing mobile data storage issues in MCC has leaded to several MSA approaches. In the next section, we critically review the state-of-the-art approaches.
III. MOBILE-CLOUD STORAGE AUGMENTATION APPROACHES

In this section, we review credible efforts that aimed to address storage amelioration and the I/O performance of mobile devices by leveraging cloud resources and lightweight methods. We analyze and synthesize the approaches from several aspects, including mobility, energy efficiency, latency, reliability, and architecture which are presented in II.

- **Attribute-Based Data Storage (ABDS)**
  The ABDS system [34] is part of the security framework presented in [34]. The framework encompasses two prominent components: namely, a privacy preserving CP-ABE (PP-CP-ABE) and an ABDS scheme. By leveraging PP-CP-ABE, the cloud handles encryption and decryption tasks that entail an excessive load on resource-poor mobile devices. Two core parts, the Encryption Service Provider (ESP) and the Decryption Service Provider (DSP), provide data confidentiality and security services without being aware of the encryption key and data contents. Similar to Phoenix [35], ABDS exploits the data partitioning mechanism. However, ABDS differs from Phoenix by outsourcing the encryption and decryption tasks to the public cloud. The ABDS scheme partitions data to a number of blocks and manages the encryption operations on the required blocks independently. Consequently, when modifying a file on the cloud, the update and encryption tasks are merely applied on specific blocks, which balance the storage and communication overhead through data storage and retrieval.

  Figure 2 depicts ABDS framework. The data owner refers to the mobile nodes in the framework. The data owner accesses the storage service provider services in a secure, energy-efficient, and optimized manner by utilizing outsourced services of two prominent components (i.e., DSP and ESP).

  Encryption through a data partitioning approach minimizes the data management and the cloud vendors’ charged costs. However, encryption requires additional control information for data blocks, which imposes extra overhead for the data management tasks. Moreover, the data block size should be identified optimally to satisfy the goal of minimizing data management overhead tasks.

- **SmartBox**
  SmartBox [21] is a solution for mobile storage capacity expansion through cloud resources. It employs cloud space referred to as shadow storage for storing and retrieving personal data by assigning a unique account for each mobile device. SmartBox is a rich personal repository and provides a public space as common storage for sharing data among associated mobile devices. Data access and navigation is provided via traditional hierarchical namespace and employs an attribute-based method for semantic query, which uses publisher-provider metadata.

  Nevertheless, the SmartBox design conforms to write once read many policy, which impedes its application as an enterprise solution. In addition, it requires a permanent connection to access data on the cloud, which is not feasible in many cases.

- **WhereStore**
  A location-aware data storage approach is considered by WhereStore [36] to enhance smartphones’ I/O performance by using cloud storage resources. The prediction and caching of adjacent place information through the replication of prominent data retrieved from the cloud is proposed in this solution to optimize data transfer time and to conserve energy.

  Although several human mobility models and routing techniques [37] are proposed to figure out movement plan of mobile users, predicting the user’s destination efficiently and specifying the appropriate state and time for caching are non-trivial tasks, which require further investigation.

- **Wukong**
  Wukong [13] is an additional I/O performance optimization and storage enlargement effort and is a cloud-based file service that provides user-friendly, transparent data access to inhomogeneous remote cloud storage services for mobile devices. By leveraging the Storage Abstraction Layer (SAL) and plugin procedures, cloud data and services, namely Dropbox and Amazon S3 can be accessed transparently and remotely via mobile applications as if they are available locally. Wukong realizes the provision of a uniform interface to access various cloud services simultaneously. The optimization stack, cache management, and pre-fetch mechanisms are utilized to improve the throughput and minimize long WAN latency. Moreover, the application of encryption and compression mechanisms enhances data security and communication, respectively, and completes the contribution of this approach.

  However, limited wireless bandwidth and I/O operation costs are impediments that hinder Wukong in minimizing long WAN latency. Moreover, the employment of efficient compression methods for multimedia files is required for
the success of this proposal. The proposed compression method is more beneficial for minimizing a text files size. These objects encompass file types with a high ratio of compression. In addition, the prefetching method is more efficient in sequential reading, which requires an improvement in random reading to enhance the performance of the work. However, in current prototype, defining large intervals among the open and read processes would save time during read operations.

- Phoenix
Phoenix [35] is a distributed communication and storage protocol that considers the power-aware storage sharing of eager nearby mobile devices in the cloud for one-hop networks. Unlike E-DRM [38], which utilizes a periodic broadcast of buffered data, Phoenix ensures data availability on participant mobile nodes by breaking each data content to a number of blocks and copying them on at least two or more mobile devices. Phoenix provides edge nodes with a true number of data blocks copied to maintain data availability and longevity in the self-organized cloud of mobile devices. Authors focus on the extending the data survival time by minimizing disconnections, by administrating node movement, and by leaving the support for the data update tasks to databases built on Phoenix’s platform.

In addition, autonomous management and maintenance is realized by utilizing an advertising model. When a node participates, it starts an asynchronous advertisement timer to decide whether to broadcast a block as a winner or to become a follower contributor as a loser. The Phoenix performance is evaluated through testbed and simulation experiments. Simulation is performed via TOSSIM in TinyOS. The number of data block copies as well as the effect of nodes failure and mobility are among the main factors examined in 100 simulations. The results show Phoenix support for data availability because the number of available block copies is rarely less than the number of nodes in the network where nodes are immobile. In the case of node mobility, it ensures data longevity by maintaining at least two copies of blocks in the network. However, the current evaluation considers only one-hop networks. The simulation in multi-hop networks [39] can improve Phoenix’s applicability.

Phoenix dependency on defining the number of participant nodes, the lack of authentication over a wireless network, and the overhead imposed on the network, in addition to the security, data safety, and privacy issues are among the challenging tasks that can hinder Phoenix’s application in a real scenario.

- Eager replication extended Database State Machine (E-DRM)
An E-DRM [38] is an energy-efficient replication approach for a Mobile Ad-hoc NETwork (MANET) [40]. A MANET encompasses a network of wireless mobile servers and clients. The nodes of a MANET are nomadic and have no permanent access to electricity. Hence, MANETs are restricted from an energy source. Eager replication maintains data consistency via the guarantee of an identical value for all copies on nodes. Unlike Phoenix [35] that focuses on preserving a true number of copies in the network, E-DRM minimizes the number of message broadcasts to conserve energy. In E-DRM, authors propose an eager replication scheme for application on a Database State Machine (DSM) approach introduced in [41]. The DSM supports atomic broadcasts in which nodes consent to the order and the set of delivered transactions.

E-DRM considers two mobile node types in the architecture of a MANET. Small Mobile Hosts (SMH) have restricted resources, and Large Mobile Hosts (LMH) have a rich resource capacity. SMHs contain only a part of the database to accomplish query tasks. Complete databases reside on LMHs and are responsible for broadcasting, certifying, and updating tasks. E-DRM minimizes message broadcasting overhead by buffering and periodic broadcasting at the beginning of the broadcast cycle. The broadcast cycle commences when a client requests a SMH to update or read data. SMHs commit the transaction to a LMH to be processed and broadcasted to other LMHs. LMHs commit or abort the transaction and certify it as a correct transaction. The cycle ends when a LMH broadcasts the result to a SMH to be transmitted to the client.

Figure 3 shows the broadcast cycle in detail. The E-DRM approach considers the start of the broadcast cycle for dispatching transactions to conserve energy. However, in real-time, all LMHs validate the transaction locally and conserve the energy that would be consumed for message broadcasting and consistency management.

- EECRS
EECRS [42] is an energy-aware content retrieval scheme
for mobile cloud. It proposes a directive-selective forwarding scheme for broadcasting interest packets in a MANET to obtain the contents. The EECRS approach is considered in an Information Centric Network (ICN). The contents of an ICN are characterized by a hierarchical-based naming strategy. Hence, names identify the requested contents. The EECRS improves energy efficiency and scalability by eliminating interest packets duplication to diminish traffic load. In addition, it searches multiple caches in parallel to fill the missing gap of the network’s node where interest packets fail to reach. Nonetheless, the inability of the EECRS to guarantee a 100% hit rate through the proposed approach hinders its full application. Authors develop an intelligent broadcast approach for content inquiry in case of missing nodes. Although this method ensures a content node hit, the imposed traffic overhead decelerates its performance and energy-efficiency.

- Market-Oriented Mobile Cloud Computing (MOMCC) MOMCC [43] is a service-oriented architecture-based mobile application development framework. The prominent engaging entities of the MOMCC architecture are the central supervisory entity as governor, service programmer, mobile host, and requester mobile node. In MOMCC, service developers create services and upload them in a central database for public availability. Individual mobile device owners who are interested in sharing their resources with nearby resource-poor mobile devices register their interest with the governor. The governor authenticates and authorizes the registered mobile devices that enter a request for hosting specific services. Moreover, the governor finds a secure proximate host for service execution in response to the service requester. The MOMCC overcomes the imposed overhead of code offloading in [44] by restricting hosting to services executed without offloading. The participating hosts as well as the governor, service programmer, and application developer will earn money on publishing, governing, hosting, and sharing services. The lack of direct attachment between the service developer and the requester enhances privacy in the proposed framework. The promise of this approach is the execution of services on a multitude of nearby mobile devices under the administration of a centrally trusted governing entity. The employment of adjacent mobile devices improves the availability of resources, which can be leveraged to alleviate mobile devices’ storage limitations. Moreover, the communication of mobile devices over a WLAN minimizes latency and conserves the energy, which would otherwise be dissipated on cellular networks. However, the MOMCC architecture shortcomings, such as the restricted computing of host devices, the necessity for fine-grained services, and the dependency on networking impede its employment for enterprise applications and in offline mode.

- UbiqStor UbiqStor [45] is an internet Small Computer System Interface (iSCSI) cache server that reduces the response delay time between mobile users and storage servers. The access to remote fixed storage servers via the nearest immobile UbiqStor server as a hybrid, multi-tier solution provides mobile clients energy-efficient access to rich storage capacity by eliminating long WAN latency in case of direct access to non-proximate storage servers. Initiator, target, and block management modules are components of UbiqStor, which handles iSCSI read and write mobile clients’ requests through a caching mechanism. Despite the enhancement of transfer latency and response delays, wireless network intermittency and cache server proximity factors can affect UbiqStor’s performance and can hinder its successful application.

- Service-based Arbitrated Multi-tier Infrastructure (SAMI) SAMI [15] is an Infrastructure as a Service (IaaS) hybrid model for mobile cloud computing that addresses storage augmentation issues in addition to its main purpose of data-intensive computations in MCC. It promotes the I/O performance as well as the storage capacity of resource-poor mobile devices through a hybrid architecture that encompasses three layers of an infrastructure, an arbitrator and a Service-Oriented Architecture (SOA). Mobile device users can benefit from SAMI’s multi-tier infrastructure, which provides access to distant fixed clouds, proximate MNOs, and adjacent MNO authorized dealers. SAMI’s Multi-tier infrastructure provides decreased communication latency and energy efficiency as a consequence, to latency-sensitive applications by MNO authorized dealers. In case of demand for security-sensitive services, MNOs are beneficial by providing access to their resources via more secure cellular network in comparison to Internet channel. When MNO’s resources are incapable of meeting data-intensive service’s demand or not accessible after operating hours, cloud infrastructures are exploited. Reducing latency, establishment of trust, alleviating portability, and preventing energy dissipation are among promising advantages of SAMI. Similar to UbiqStor [45], SAMI exploits a multi-tier architecture in its design. However, SAMI provides higher trust to mobile service consumers by leveraging resources of MNOs beside cloud and adjacent MNO dealers.

Furthermore, Table II summarizes the comparison results of the reviewed approaches based on the defined categories in the taxonomy presented in Figure 1. Table II advocates differentiations between mobile and immobile storage augmentation approaches. We deduce from Table II that the mobility factor plays an important role and affects other specified factors. Employing mobile cloud resources enhances energy efficiency, WAN latency, locality, and context awareness, while utilizing an immobile cloud back-end improves storage augmentation, data blocking, reliability, availability, data safety, security, and trust.

IV. CLOUD-BASED STORAGE CHARACTERISTICS

According to existing MSA approaches including the reviewed solutions in the previous section, we have devised a
<table>
<thead>
<tr>
<th>Mobility</th>
<th>ABDS</th>
<th>SmartBox</th>
<th>WhereStore</th>
<th>Wukong</th>
<th>Phoenix</th>
<th>E-DRM</th>
<th>EECRS</th>
<th>MOMCC</th>
<th>UbiqStor</th>
<th>SAMI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage augmentation</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Energy Efficiency</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Architecture</td>
<td>Client-Server</td>
<td>Client-Server</td>
<td>Client-Server</td>
<td>Client-Server</td>
<td>P2P</td>
<td>P2P</td>
<td>P2P</td>
<td>P2P</td>
<td>Hybrid</td>
<td>Hybrid</td>
</tr>
<tr>
<td>WAN Latency</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Hybrid</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Data Blocking</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Reliability</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Availability</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Security and Trust</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Data Safety</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Locality</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>I/O Performance</td>
<td>Varied</td>
<td>Varied</td>
<td>Varied</td>
<td>Varied</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Communication Platform</td>
<td>Internet</td>
<td>Internet</td>
<td>Internet</td>
<td>Internet</td>
<td>Ethernet</td>
<td>Ethernet</td>
<td>Ethernet</td>
<td>Internet/ Ethernet</td>
<td>Internet/ Ethernet</td>
<td></td>
</tr>
<tr>
<td>Context Awareness</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Client Networking</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
<td>Cellular / WLAN</td>
</tr>
</tbody>
</table>
cloud-based storage taxonomy. This classification is based on the prominent common characteristic and major differences between various cloud storage resources including the architecture, capacity, tiering, mobility, locality, security, back-end connectivity, and utilization cost factors. Figure 4 depicts the cloud-based storage taxonomy and will be explained in this section.

- **Architecture:** The variety in the cloud resources architecture arises from diverse roles of the cloud in augmenting resource-poor mobile devices. In a client-server architecture, a multitude of rich stationary servers owned by vendors and enterprises serve mobile devices as their clients to enhance their storage capacity. Public and private cloud resources fall into this category. Mobile Network Operators (MNO), stationary computers in public places as well as authorized MNO dealers, computing kiosks, and mobile devices are among other resources that have a server role and offers storage services to storage-constrained mobile devices [16]. Amazon S3, Amazon EBS, HP Cloud Object Storage, and HP Cloud Block Storage are well-known instances of storage services offered via the public cloud.

In peer-to-peer architecture, mobile devices are both a provider and consumer of services in a decentralized autonomous network of proximate non-stationary devices that form a mobile storage service. Conferences, coffee shops, and university campuses are scenarios in which ad-hoc networks can be formed among participants that generally share common interests. In this architecture, cloud storage services are exploited locally from the network of available mobile devices in the vicinity for a period of time [35], [38]. The storage capacity provided in a peer-to-peer architecture is incapable of competing with infinite storage that is accessible via the public cloud in a client-server architecture. Moreover, a peer-to-peer architecture leverages a decentralized management, on the contrary to a client-server architecture with centralized management. However, the exploitation of edge devices storage in a peer-to-peer network alleviates long WAN latency and device energy consumption. Moreover, caching information of same interest on participants’ devices is another advantage of this approach, which lessens the traffic over a cellular network. Nonetheless, a guarantee of the persistency and redundancy of data is a challenging task in this architecture due to node mobility and a participants disconnection, which may cause data loss when the participant leaves the network or powers off the device [46]. The researchers efforts are toward the application of power-aware, real-time-aware, or partition-aware [38], [47] approaches in wireless and ad hoc networks to conserve mobile devices’ energy, to minimize communication volume, and to maintain the availability of data in a well-timed manner.

- **Capacity:** Storage is one of the main services provided by the cloud as Storage as a Service (SaaS). The unlimited storage capacity of the cloud can augment resource-constrained mobile devices. SaaS capacitates keeping data and applications on the cloud resources and access them remotely. These unified, elastic, reliable, secure resources are usually located far from mobile nodes. Hence, mobile devices require crossing an Internet channel via a wireless network to access the unlimited storage of a distant public cloud. Dropbox, Google Docs, Amazon S3, iCloud, and SkyDrive are among the renowned cloud storage services that facilitate the storage, sharing, and synchronization of data for desktop and mobile device users. Several efforts such as UbiquStor [45] and MiSC [48] tried augmenting mobile devices using remote storage servers. The utilization of non-proximate cloud storage services over an Internet channel imposes increased WAN latency and decreased security. An alternative solution is the use of constrained transient storage capacity via nearby immobile cloud resources [49] and mobile devices [35]. Although leveraging this approach supplies limited storage to lightweight mobile devices in comparison to infinite storage capacity of the cloud, the reduced latency over cellular networks and Wi-Fi enhances performance and addresses mobile devices’ energy deficiency problem.

- **Tiering:** Tiering refers to the number of layers a mobile device passes over to exploit cloud services. Approaches such as [45] and [15] are referred to as multi-tier. For example, the three-tier infrastructure of SAMI [15] encompasses distant cloud resources, proximate MNOs, and MNO-authorized dealers in the vicinity. Conversely, the one-tier category approaches leverage one of the cloud resources for storage augmentation. Multi-tier infrastructure provides rich computing beside energy- and latency-aware communication. It is realized through the provision of several options for execution of services. While proximate cloud resources tier covers the requirements of latency-sensitive services, the choice of exploiting reliable and well known organizations’ resources tier is beneficial to the services with security and trust requirements. Service providers in the telecommunication are trustful options for the provision of resources over the secure cellular network as a cloud. The public clouds as the equipped tier with elastic, infinite storage.

4. https://docs.hpcloud.com/block-storage/
5. https://www.dropbox.com
7. https://www.icloud.com
8. www.skydrive.com
and computing resources are the choice for data-intensive services when resources of trustworthy, proximate tiers are insufficient.

- **Mobility**: Cloud resources are either mobile or immobile with respect to the mobility characteristic. When immobile, cloud resources are delineated by a richer source of computation and storage capacity and no energy shortcomings compared with mobile resources. Public and private cloud servers, MNOs, and fine-grained resources such as available desktop computers in coffee shops and airports and cloudlets are instances of immobile storage resources. A cloudlet is a proximate immobile cloud solution that concentrates on the computational augmentation of non-stationary neighboring devices. Similarly, it can be applied for storage enhancement in which the VM-based offloading method of the cloudlet is employed for more storage capacity to proximate mobile devices. On the contrary, mobile resources provide context-awareness and lower latency, which can adversely impact the energy consumption and transmission period.

- **Location**: Cloud storage resources are either located in the proximity or are distant. Approaches utilizing a multi-tier infrastructure can benefit from both and are referred to as hybrid resources. Distant resources, particularly public cloud storage, are accessible via an Internet channel over a wireless medium. Long WAN latency and low security are common challenges in wireless networks and are intensified through an Internet channel. However, proximate cloud resources are accessible via both Ethernet and Internet channel. Utilizing nearby mobile or fixed resources reduces latency, cost, and communication overheads [50]. Stationary computers in public places and nearby mobile devices specifically smartphones, laptops, and tablets are resources that can serve client mobile nodes in the vicinity.

- **Back-end Connectivity**: This category considers the connectivity of back-end storage resources to the Internet. They are either connected to a wired Internet connection or utilize a wireless medium. Mobile devices that play the role of servers to other mobile nodes or participate in a peer-to-peer architecture are supported via a wireless connection to the Internet. On the contrary, stationary servers, whether public or private cloud resources, or immobile computers in the neighborhood are equipped with a wired Internet connection.

**V. Open Issues**

In this section, we present crucial open issues on MSA in MCC as several thought-provoking future research directions.

**A. Energy-Awareness**

Energy conservation is one of the ultimate goals in mobile computing, cloud computing, and MCC domains. Although limitation of resources, processing, storage, and battery life of mobile devices can be alleviated through rich cloud-based resources [16], high pre- and post-offloading overheads of in/less-efficiently designed MCC solutions can remarkably intensify the energy limitations of mobile devices. Therefore, energy-awareness using lightweight mobile augmentation frameworks [51], communication-aware approaches [52], and fidelity adaptation [53] solutions are essential to meet the energy conservation in mobile devices. Lightweight solutions could mitigate the offloading overheads (processing and latency) [54] and ensure that the communication cost would not exceed the data computation benefits of mobile devices. Similarly, optimal communication-aware and fidelity adaptation solutions alleviate the energy efficiency issue by leveraging heterogeneous wireless networks (i.e., cellular and WLAN) for an energy-efficient trade-off for lightweight MCC solutions.

**B. Data Integrity**

Although the anywhere, anytime, any device principal of MCC is beneficial to mobile device users, the variation and inhomogeneity of storage services provided by varied cloud vendors cause data integrity issue and necessitates additional investigation of MCC storage augmentation approaches. Data integrity issue jeopardizes the reliability of cloud service providers and rises data retrieval issue as a consequence. To mitigate data integrity issue, efforts similar to [13] seek to provide a uniform interface to access various cloud storage services by exploiting middleware, SOA, and domain specific language approaches. Moreover, management of data,
which are distributed in various cloud storage services [30] is promising to overcome data integrity issues in MCC. However, further research is required for a unified, standard storage infrastructure and management of heterogeneity to alleviate data migration.

C. Trust

One of the most important concerns of the mobile end-users is to establish trust for the largely growing cloud vendors. Although several studies have been conducted for building trust in cloud resources [15], [55]–[57], the transmission of user data over insecure wireless networks (where stern supervision is lacking) and the Internet for storage of data in the cloud (where users do not have any control) is inevitable. Heterogeneity of cloud infrastructures as well as mobile devices’ resource poverty and intrinsic traits intensify trust issue. Protection of user data by leveraging encryption and decryption techniques [34], authorization, and authentication are among the approaches try to overcome trust issue in MCC. However, a necessity for novel trust establishment techniques similar to [58] exists which are required to be lightweight with respect to limited resources of mobile devices and wireless communication in MCC domain.

D. Data Portability

Harnessing cloud resources as a comparatively more reliable and safe storage for data has alleviated the data lock-in problem of mobile device users. Hence, the migration of data for messages and contact information between non-uniform mobile devices is facilitated. However, data portability is still an issue for cloud consumers and due to this problem, users are unable to transfer their data from Android-based to iOS-based mobile devices. Moreover, the heterogeneity of cloud services offered by diverse cloud vendors causes a vendor lock-in problem. Vendor lock-in is an attractive issue in business [59], but a real concern for customers. Vendor lock-in makes customers dependent on services provided by specific cloud vendors, as the incompatibility with other services or the consequence of cloud service providers’ policies.

Homogeneity between the existing cloud services architectures and programming languages is desired by end-users to overcome code and data portability concerns. Solutions including adapter and particularly middleware [60] as well as standardization such as Open Cloud Computing Interface (OCCI)\(^3\) are among approaches addressing portability issues in cloud computing. MCC data portability issues grant for further research that considers variant cloud’s policies, architectures, and storage structures to alleviate imposed challenges on the migration of data between dissimilar cloud storages and mobile devices.

VI. Conclusions

This paper surveys the crucial intrinsic restrictions of mobile devices and storage augmentation issues in three domains of mobile computing, cloud computing and MCC to devise a taxonomy of issues as the motivation for the emergence of effective and efficient MSA approaches in MCC. A number of approaches leverage data partitioning whereas other approaches exploit data replication, cache management, or SOA. Based on a review of the credible MSA approaches, the paper proposes a taxonomy of cloud-based storage.

A mobile devices local resource conservation, computational augmentation, and storage extension have been realized through the convergence of mobile and cloud computing that has produced state-of-the-art MCC. This association and all its inestimable privileges originate multi-dimensional heterogeneity in various domains, including platforms, operating systems, networks, and data structures. Pivotal sources of variations produce the generation of several non-trivial challenges for mobile data, including portability, interoperability, integrity, and security. Therefore, the need for lightweight, energy- and communication-aware MSA approaches is vital for the successful adoption of mobile computing. Mobility is one of the prominent factors affecting other factors in taxonomizing cloud-based storage resources in a positive or negative manner. Hence, additional efforts are required to address a number of crucial MCC storage augmentation open issues. Energy-awareness, data integrity, trust, and data portability are open issues, which specify future research directions in this area.

REFERENCES


\(^3\)http://occi-wg.org/


