https://doi.org/10.31871/IJNTR.7.3.6
International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-7, Issue-3, March 2021 Pages 07-15

A Survey of Mobile Cloud Computing Challenges and Solutions

Ghadeer Alwafi, Mona Alrougi, Rahaf Alsulami, Shaimaa Salama

***Abstract*— In the last few years, mobile devices support different types of applications, many of which require high computing power. This is considered a problem since mobile devices provide limited computing power, storage, and energy. Fortunately, cloud computing (CC) is rapidly becoming known as the computing world's latest technology. CC allows users to use unlimited dynamic resources when required. Mobile Cloud Computing (MCC) integrates the concept of cloud computing within the mobile environment, which removes barriers associated with mobile devices' performance. These benefits of MCC are not completely problem-free. But there are still many challenges facing MCC that must be addressed in order to enable ubiquitous deployment and adoption. This survey paper has done a comprehensive review of the research papers through search engines such as Google Scholar, IEEE, ScienceDirect, SCOPUS, and Research Gate to find MCC's challenges and solutions exist in the field. The survey paper intended to present the most common challenges including computation offloading, energy consumption, heterogeneity, bandwidth, security, and privacy with solutions proposed by various researchers. The paper finds that most of the solutions presented in 2016 and earlier. Computation offloading solutions focused on energy consumption and vice versa, privacy solutions focused on authentication mainly, heterogeneity and bandwidth solutions are old and require further research and new solutions.**

***Index Terms*— Mobile cloud computing; computation offloading; energy consumption; heterogeneity; bandwidth; security; privacy.**

I. INTRODUCTION

The use of mobile devices has grown globally, and it became an essential part of our lives. The number of users across the world for mobile devices such as smartphones reached up to 3.2 billion in 2019 [2]. Nowadays, users can edit their documents, do shopping and social networking without using computers. Unlike computers, mobile devices have limitations like limited battery life, little bandwidth, less storage capacity, and restricted processing [3]. As a solution for these limitations, Mobile Cloud Computing (MCC) was introduced [3].

MCC is "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage, and mobility to serve a multitude of mobile devices anywhere, anytime through the channel of Ethernet or the Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle." [4]. MCC is a combination of cloud computing, mobile computing, and wireless networking, that aims to provide cloud-based services to the mobile device's customers [5]. When MCC is fully deployed, mobile devices do not require high resources, such as random access memory (RAM), storage and Central Processing Unit (CPU), because the entire data or complex computing are transferred to remote cloud-based resources [6]. Besides, MCC has other advantages as flexibility, multiple platform support, data availability, cost efficiency, data backup and recovery. For instance, mobile apps like Amazon, Facebook, Gmail, and Uber, store and process user data and other information by hiring storage space and platform from cloud service providers [3].

Each technology brings new opportunities along with several challenges. MCC has several challenges, including computation offloading, energy consumption, limited bandwidth, security, trust, and privacy. The goal of this survey is to discuss these challenges of MCC and propose existed solutions to give insights and define the gaps founded. The survey paper will be organized as following, Section II introduces background on MCC including architecture, service models and benefits. Section III discusses each challenge followed by the solutions. Some gaps and insights will be in Section 4. Finally, Section 5 draws some conclusions.

II. Background

The following sections will give an overall background of MCC. It shows MCC architecture including three layers: mobile user, network, and service provider. Define the most common service models which are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Then, illustrates the benefits of MCC.

A. MCC Architecture

The general architecture of MCC shown in Figure 1. It includes three main layers: mobile user layer, mobile network layer and cloud service provider layer [7]. Each layer illustrated as following:

- **Mobile User Layer.** This layer consists of cloud service users. Users use mobile devices such as smartphones, tablets, and laptops to connect to Mobile Network Layer via Wireless Access Points (WAPs), Base Transceiver Station (BTS), or satellite.
- **Mobile Network Layer.** This layer handles mobile users' requests and information by mobile network operators.

Ghadeer Alwafi, Information systems, King abdulaziz university, faculty of computers and information technology
Mona Alrougi, Information systems, King abdulaziz university, faculty of computers and information technology
Rahaf Alsulami, Information systems, King abdulaziz university, faculty of computers and information technology
Shaimaa Salama, Information systems, King abdulaziz university, faculty of computers and information technology

After receiving the users' request, the mobile network operator provides services such as authentication, authorization, and accounting (AAA) based on the home agent (HA) and users' data stored in databases [8]. If authentication and authorization succeed, the mobile network operator delivers the mobile users' requests to the cloud through the Internet.

- **Cloud Service Provider layer.** This layer consists of multiple cloud service providers that process the users' requests to provide the corresponding cloud services. Cloud services provided to users include IaaS, PaaS, and SaaS, which will be explained in detail in Section B.

B. MCC Service Model

The most common mobile cloud service models are IaaS, PaaS, and SaaS. Each model offers different services:

- **IaaS.** This model offers an infrastructure to users such as storage, servers, and networking components and delivers it as a service over the network [1]. Amazon Elastic is an example of IaaS.
- **PaaS.** This model offers an advanced integrated environment for users to build, test, and deploy their applications [8]. Some examples of PaaS are Google App Engine and Microsoft Azure.
- **SaaS.** This model provides applications to multiple users as a service on-demand [1]. Examples are Google Apps such as email and word processing.

C. MCC Benefits

MCC is a term that rise exponentially in the last 10 years, mobile cloud applications move the computing power and data storage from mobile phones into the cloud [9], which open new way to service and application on mobile devices. MCC is a very important technology since it combines the advantages of both mobile technology and cloud computing, to be able to give the best services to mobile user, MCC support reached a wide range of applications as in mobile commerce, mobile banking, and healthcare and other areas [10]. In this part, we will enlist some of the benefits in having MCC.

- Overcome the limitations of mobile devices in particular of the processing power and data storage [9].
- extend the battery life and processing power of mobile devices [11].
- Maximize the resource sharing and reuse of existing computing resources in cloud infrastructures and Internet-based applications and services [11].
- A number of new technical functionalities might be provided by mobile clouds. In particular, provisioning of context and location-awareness enables personalization of services is an attractive functionality [9].

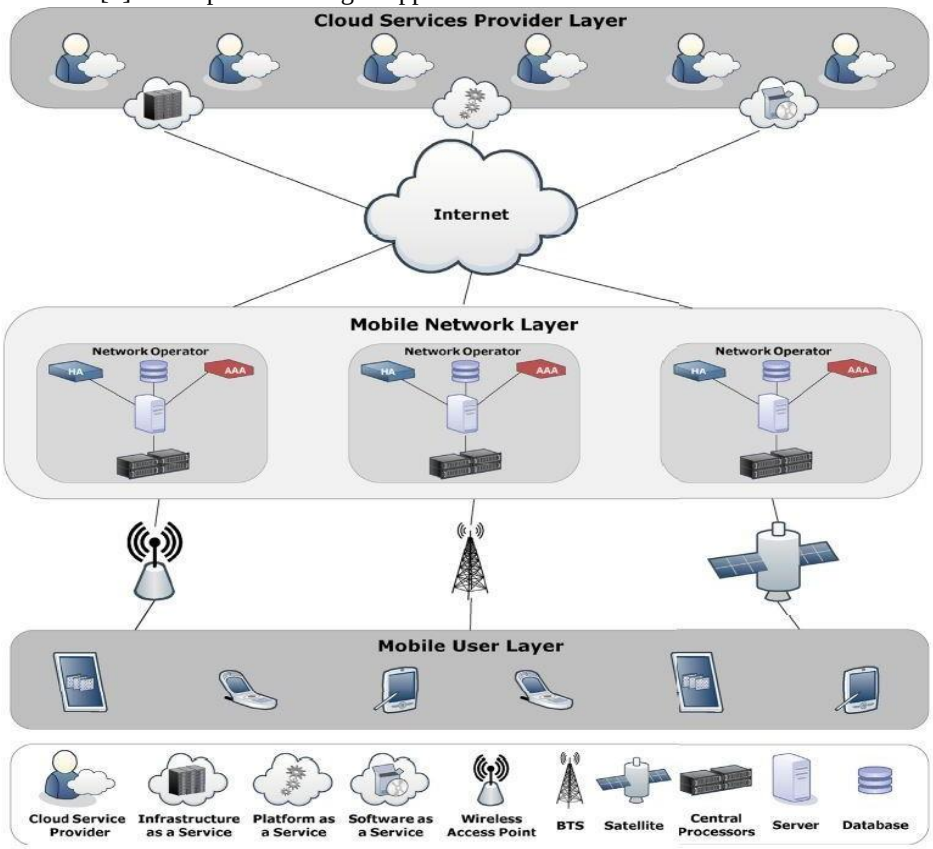

Figure 1: Mobile cloud computing architecture [7]

I. challenges and solutions of mcc

Several issues concerning the MCC environments need to be addressed due to the connection limitation, energy sufficiency, dynamics, and distributed nature of mobile cloud computing environments. This section illustrates the most common challenges including computational offloading, energy consumption, heterogeneity, bandwidth, security, and privacy. Then provide the solutions for each challenge including frameworks, algorithms, and models. Table 1 summarizes the

MCC challenges, solutions, year, and objectives of each solution

A. Computation Offloading

With mobile devices' limited capabilities and computationally intensive applications, cloud computation offloading comes as a solution. Computation offloading is the task of sending/offloading computationally intensive applications and heavy tasks from mobile devices to the cloud for execution, then send back the result [12]. This technique provides more resources and capabilities for execution and increases performance. However, the computation offloading technique has its challenges as well. To address the computation offloading challenges, offloading steps must be explained first. These steps include application partitioning, preparation, taking decisions, migration, and execution [12, 13]. The mobile device makes decisions based on its resources about how to execute the application and how much computation needs to be offloaded [12]. Therefore, divides the application into off-loadable and not off-loadable components, to determine which components will be migrated to the cloud and which are kept on the mobile device [13]. Then, execution and processing are transferred from the mobile device to the clouds. These steps may change depending on the offloading type, static offloading, or dynamic offloading. Static offloading means that the program partitioning happens before execution and the components migration decision is taken at the beginning of the execution [14]. In dynamic offloading, the offloading decision is taken based on the current situation at runtime [14]. Many challenges may arise during performing these steps such as the overhead of components migration at runtime, amount of time taken to receive offloading results, coordination of partitioning, and lost connection during components migration.

Solutions: Reference [15] proposed a computation offloading strategy for service workflow to minimize execution time and energy consumption. This strategy addressing three main issues which are mobile service workflow, users' mobility, and fault tolerance. These issues must be considered before making computation offloading decisions. Multiple services composed in a workflow may execute in parallel and depend on each other, so the order of the execution is very important and must be considered. With the users' mobility, mobile network bandwidth and data exchange rates may vary, and users may occasionally lose their connection during receiving a service that may cause some failures. The proposed strategy includes an offloading strategy for workflow services with interdependency among their components. Then, incorporate a mobility model with a fault-tolerance mechanism into the proposed strategy to consider users' mobility and network variation during the execution.

Reference [16] proposed a context-aware offloading decision algorithm with a general cost estimation model and a prototype. Context-aware offloading decision algorithm takes into consideration context changes that include network conditions, device information, and the availability of multiple types of cloud resources such as mobile ad-hoc networks, cloudlets, and public clouds. It helps in making offloading decisions about which wireless medium to use and which cloud resources to offload to at runtime. A general cost estimation model was proposed for cloud resources to estimate the task execution cost including execution time and energy consumption. Then, a prototype system was designed and implemented considering the three types of cloud resources. The results of the proposed system lower the cost of execution time and energy, and provide suitable offloading decisions based on mobile device context.

Reference [17] study the interaction between multiple users and the cloud by jointly improve tasks offloading decision and communication resource allocation to minimize the cost of energy, computation, and delay. The proposed multi-user multi-task offloading (MUMTO) algorithm uses semidefinite relaxation (SDR) and binary recovery to jointly compute the offloading decision and communication resource allocation. The result shows that the MUMTO algorithm almost gives optimal performance.

Reference [18] proposed an agent-based MCC framework to enable the device to receive a quick response about offloading results and provide an offloading strategy to achieve maximum energy saving for multi-user. The framework consists of distant cloud, agents, and multiple mobile devices. Request filtering is adopted on the device and the agent to effectively.

B. Energy Consumption

Mobile devices have a relatively limited battery capacity. Energy consumers in mobile devices include the CPU, screen, Global Positioning System (GPS), Bluetooth, wireless, and sensors. For example, the use of location services like GPS consumes a lot of energy because it involves extensive use of sensors. Mobile cloud computing solves this issue which is the hardware limitation in mobile devices. Particularly, offloading discussed in Section 3.1 illustrates many solutions that involve improving offloading and energy efficiency. However, the use of wireless networks in offloading to deliver cloud services and the use of sensors and advanced technology consumes a lot of energy [19].

Solutions: Reference [20] presented a system architecture that helps in profiling user's energy usage per application to build a predictive model about energy consumption for future use. The proposed system profiles user applications depend on their resource consumption and then if more resources are required, negotiate with an external cloud. This system architecture is useful for constrained resource clouds because of the need to choose between several clients. It helps to determine when it is required for mobile devices to use more resources from the cloud.

Reference [21] Energy Efficient Computational Offloading Framework (EECOF) studies the issue of additional energy consumption in computational offloading. The framework deploys a distributed architecture and employs a simple procedure to minimize the overhead of runtime component offloading, thereby minimizing energy consumption. EECOF is used for intensive applications and leverages the SaaS model and the IaaS model. The results show that the size of data transmitted over the network is reduced by 84 % and the cost of energy consumption is reduced by 69.9 %.

Reference [22] studied the energy-efficient dynamic

offloading and resource scheduling (eDors) to reduce energy consumption and application completion time. The proposed eDors algorithm consists of three sub-algorithms: computation offloading selection, clock frequency control, and transmission power allocation. The results show that the computation offloading selection depends on the computing workload, the maximum completion time of the previous task, the clock frequency, and the transmission power of the mobile device. The eDors algorithm adjusts the CPU clock frequency of smartphone devices and adapting the transmission power for the wireless channel to effectively reduce the energy efficiency cost.

C. Heterogeneity

Heterogeneity in mobile cloud computing is the existence of distinguished hardware, infrastructure, architectures, and technologies of mobile devices, clouds, and wireless networks [23]. This Heterogeneity could lead Mobile Cloud Computing to fail to fulfill its proposed advantages as being effective in mobile device energy usage, always connected, and scalability of wireless on-demand connection and could cause complication of mobile cloud computing and slows down its success [24].

Heterogeneity in Mobile Devices: The technological differences among mobile devices in terms of hardware, software, operating systems, and platforms such as Android, iPhone, Windows, etc., lead to heterogeneity in this area [23]. Furthermore, smartphones recently increased in popularity and created a dynamic and demanding market that disperse them to different dimensions, for instance, hardware, brand, operating system, feature, and communication medium [23]. Hence, collaboration at the device-level becomes more challenging in MCC [23].

Heterogeneity in Clouds: Many cloud vendors provide various services with custom-built policies, platforms, infrastructure, and APIs that make the cloud heterogeneous [23]. These differences cause portability and interoperability as major challenges in cloud computing [23]. **Heterogeneity in Wireless Networks:** In mobile cloud computing, most communications occur in the wireless network environment, which is a heterogeneous communication medium, which can be cellular, WLAN, or Satellite-based [25]. Differences in wireless networks and their related technologies influence the delivery of cloud service and affect mobility, augmentation, and smartphone usability [23].

Solutions: Reference [26] proposed a cloud OS kernel called Mirage to mitigate the impact of hardware variety in the cloud and smartphones, which is based on virtualization technology. Mirage enables development applications that are neutral and cross-platform and can operate on mobile devices and cloud servers. Mirage compiles and connects mobile applications into the kernel installed and operates directly on ARM-based mobile devices and Xen-based clouds. Mirage wrote from scratch through an open-source programming language called OCaml. Using Mirage, the developers can produce rich, multi-tier applications on normal OSs like Linux and port them to many mobile phones and cloud resources.

Reference [27] proposed an architecture to provide an intelligent network access strategy for mobile users to satisfy the application requirements. This architecture was built based on the concept of Intelligent Radio Network Access (IRNA). IRNA is an effective paradigm for dealing with the dynamics and heterogeneity of available access networks. The authors suggest a context management architecture for acquiring, managing, and distributing context information, to apply IRNA in the MCC environment. This architecture consists of three major components which are: context provider, context broker, and context consumer, as shown in Figure 2. However, the context quality enabler is as well required to smooth the operations of other components. In this architecture, when a context consumer needs to communicate with a context provider, the context consumer will request the Uniform Resource Identifier (URI) of context providers at the context broker. Using this URI, the context user will connect directly to the context provider and demand the context data. This process, thus, increases the speed of transmission of context data. Moreover, when a context quality enabler receives the requirement about the context quality from the context consumer, the context quality enabler will filter out URIs of the context providers that are not suitable with the required quality level. Therefore, this architecture can be controlling context quality according to the demands of the context consumers.

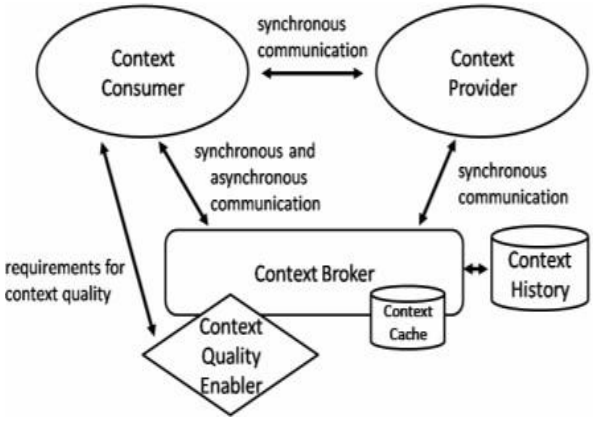

Figure 2: Context Management Architecture [27]

Reference [28] proposed a parallel programming standard for heterogeneous computing devices, called OpenCL. It allows developers to create desktop applications that be executable on different types of computing elements such as GPU, CPU, multicore, and other accelerators. In the cloud, the same approach can be maintained, which reduces hardware heterogeneity. Applications developed using OpenCL for certain architectures may be ported to other architectures with correct and guaranteed functionality. Utilizing multiple programming strategies, the application can query hardware specifications and host machine capabilities and choose an appropriate kernel to increase correctness and compatibility.

Reference [29] proposed a Tree Like Structure protocol to solve the heterogeneity in mobile devices. It is a straightforward and efficient routing protocol. That enables users to be self- organized and configuring. As well as it has followed the on-demand method. If a node has to connect to the internet and wants to transfer the data over the link, it requests to connect first and then send data. This method can decrease the traffic on the link because the medium will

remain free when the nodes did not want to transmit the data. Therefore, this method can address the issue of heterogeneity.

D. Bandwidth

When signals are travel from various sources in parallel at high speed, that is known as bandwidth [29]. The bandwidth in wired networks such as LAN is fixed, and users enjoy the high connection speed without any interruptions [30]. However, this is not the case in mobile devices that typically use wireless networks [30]. In wireless networks, the bandwidth is less than wired systems, often, there could be congested network, which will impact the wireless service [30] as the network capacity depends on the network users, and this capacity is measured by the

bandwidth per cubic meter [29]. The number of mobile phone users increases over time, and they want to use more applications on their mobile phones [29]. This affects the performance as the available bandwidth is insufficient that can be used for these services [29]. Therefore, bandwidth is considered a major problem in mobile communications.

Solutions: Reference [31] proposed an architecture to solve the bandwidth problem in which limited bandwidth can be shared between mobile users based in the same location (e.g. workplace and station) and engaged in the same content like a video file. The authors model the interaction as a coalition game between the users. For instance, the users form a coalition where each user is responsible for a piece of video files (e.g., images, captions, and sounds) and transmits/exchanges it to other coalition users. This results in the quality of the video being enhanced. However, the solution proposed is only used in cases where users in a given area are interested in the same content. It also does not consider a distribution policy (e.g., who receives how much and which part of contents), which results in a lack of fairness about the contribution of each user to a coalition. Meanwhile, the sharing, distribution policy needs to be applied [32]. Reference [33] considered the data distribution policy, which specifies when and how pieces of available bandwidth are shared between users from which networks (e.g., WiFi and WiMAX). It periodically gathers user profiles (e.g., calling profile, signal strength profile, and power profile) and uses the Markov decision process algorithm to creates decision tables. The users decide based on the tables whether or not to assist the other users in downloading some contents that they cannot receive themselves because of the bandwidth constraint and how much it should help (e.g., 10% of contents). The authors built a framework on the cloud, called RACE (Resource-Aware Collective Execution), to take advantage of the computing resources to maintain user profiles. For users who share the limited bandwidth, this approach is suitable for them to balance the trade-off between benefits of the assistance and energy costs.

Reference [34] proposed a bandwidth conservation framework in order to reuse the bandwidth which was not utilized. The framework proposed can adjust the bandwidth allocation and reschedules the bandwidth dynamically. A certain amount of bandwidth is allocated to users according to the Service Level Agreement (SLA) between the customer and the service provider, but it is up to the user how efficiently he uses the allocation of bandwidth. The framework contains four components: the cloud, apps or services running on user device, dynamic scheduling of bandwidth, and bandwidth conservation system. This proposed system can help the bandwidth-constrained user to use the available bandwidth while banking the unutilized bandwidth for future use.

Reference [29] proposed a protocol to solve the bandwidth issue based on 5G technology called Dynamic Hash Table (DHT). It is a decentralized distributed system such as a hash table. In the DHT, stored a pair of key and value in it. A map between the keys and values can be maintained through the nodes. When a node is altered, minimal disruption is produced. As the hash table buckets are a network's independent nodes, then hashing is applied to it when a key is needed to find the hash table.

E. Security

MCC gained a lot of popularity among mobile users. However, according to [35] CEOs and IT Executives were not interested in adopting MCC services as result of the risks related with security and privacy. Since MCC provides mobility as main service along with other services as it is easy to access whenever and wherever the user is, it also raises the concern of data security, mobile device security and offloading security along with various other factors [35]. Almost all of security challenges in MCC are inherited from cloud computing. Indeed, it is not convenient to run anti-malware application in a mobile device that it computationally intensive, due to the lack of computational processing capability to execute complicated algorithms [12]. As a result of resource limitation, the algorithms proposed to secure the mobile cloud computing environment cannot run directly on the mobile device [35]. To be able to evaluate the MCC as secure environment, it should follow a few requirements confidentiality, integrity, availability [12]. However, it is not easy to implement all the requirements as there is a tradeoff between the energy consumption on the device and the cost of using cloud resources while implementing a secure environment [35]. Moreover, mobile node signals suffer from interference and eavesdropping in mobile networks which make security increasingly more important [36].

Solutions: Due to the limited mobile device resources as mentioned before, it is not possible to run anti-malware applications, security applications, or monitoring tools on these devices [12]. However, to address these issues the authors in [37], propose a new approach to provide cloud-based security functions for mobile devices. In this model, during mobile devices connecting and communicating with remote destinations, all the data passes through an OpenFlow controller. the OpenFlow switch is integrated with mobile device for redirection purposes. A security manager and OpenFlow controller module are installed on the cloud side. In [38], the authors proposed an architecture which is consists of components installed in mobile device side and cloud side. In installed components each one has it own particular functionalities. This architecture is presented to assure the integrity of application and the communications among same application parts in both sides. optimization

manager, mobile security manager and mobile manager are components on the mobile device side. While application manager and cloud security manager are components on the cloud side.

In [39] authors believed that each cloud layer has its vulnerability. One of the challenges that faced the authors were to identify the attacks from normal virtual machine operations in cloud virtual environment. With the rise of new technologies, the usual way to protect the user data by adopt end-point encryption, firewalls and antivirus solutions is no longer enough, now the targets of attackers have shifted from the network layer to the application layer. As a result, the authors presented an alternative option to incorporate intrusion detection techniques into the cloud computing model. The authors also explored the locations in cloud service delivery models where these IDS can be deployed for efficient detection and prevention.

F. Privacy

Lately privacy has raised many concerns since people understood the risks related to having their personal information stolen which might subject them to identity theft. Authentication became the main topic when talking about privacy challenges in MCC along with others concern as data privacy, location privacy and identity privacy. Authentication is the process of identifying the user, user's data or application [36, 40]. In fact, privacy in MCC is quite different from traditional cloud computing since it involves more sensitive data such as location information from the GPS when various location-based services or application are used [7].

Now the user's data are processed and moved from mobile devices to the cloud servers. These servers are located at various places that are owned and maintained by the service providers only, who is usually a third party. Since the users cannot physically reach nor store their data, the service providers are responsible for user's data privacy and protection [12].

Solutions: There are several researches have been done towards mobile user authentication to cloud. [41] proposed a privacy-aware authentication model to use a single private key to ensure security to cloud service users so that mobile users can access many services from different service providers. the security in this approach is strengthens since utilized bilinear crypto system and dynamic nonce generation. In addition, it supports user anonymity and untraceability, mutual authentication and key exchange. However, it does not require any verification tables to implement a trusted Smart Card Generation (SCG) and service provider end. Here, the keys distribution to different clouds and mobile users is done through the trusted SCG, but it does not take a part in the individual mobile user authentication process. This approach reduces the authentication processing time and usage of memory spaces, due to having the targeted cloud server only interacts with the requested user in each user authentication session.

Efficient privacy preserving approach for outsourced data, the solution focused on data security, using a probabilistic public key encryption and ranked keyword searching algorithm. In [42] the authors propose an efficient privacy preserving approach for outsourced data. The approach used a probabilistic public key encryption technique and ranked keyword searching algorithm. Frist, the mobile user makes an index for file collection, and then encrypt both the data and index. Also, the user produces trapdoor for keywords and sends to the cloud. So, it would be able to access the stored data in the cloud, When the cloud receives the trapdoor, the cloud starts to search for it is match data. Second, after collecting, the matched data entries and its corresponding encrypted relevance scores it is sent back to the user in ranked sequences which are based on the relevance scores. Lastly, the user can get the original data retrieved by decryption operation.

In [43], a lightweight cryptographic method for mobile device is proposed to store data on clouds. This method is based on pseudo-random permutation operation. As it is lightweight, the permutation operation is done on mobile device instead of cloud in order to protect data privacy.

II. Discussion

Most of the MCC challenges' solutions conducted in 2016 and earlier. The focus of most solutions in computation offloading is toward energy consumption and vice versa. It was focused on improving offloading decisions, selections, and migration to increase energy efficiency. Moreover, there was not much attention given the heterogeneity, especially heterogeneity in cloud, and bandwidth over the past years. Most of the research proposed solutions for heterogeneity and bandwidth in 2010. After this year, a few researches proposed new solutions, while other research mentioned the same solutions. Also, most of the research in the privacy field focused on authentication solutions.

III. Conclusion

In the last few years, MCC has become a highly used trend since it combines mobile technology and cloud computing benefits. As a result, it catches the attention of many researchers to overcome it is challenges. This survey presented a comprehensive survey of mobile cloud computing challenges. It highlighted challenges of computation offloading, energy consumption, heterogeneity, bandwidth, security, and privacy with their proposed solutions.

Table 1: Mobile cloud computing research challenges and solutions

MCC challenges	Solutions	Year	Objectives
Computation offloading	Service workflow in mobile cloud computing [15]	2014	Computation offloading strategy for interdependence services with respect to user mobility and fault tolerance to minimize execution time and energy consumption
	A context sensitive	2015	Algorithm to make suitable offloading decisions based on network

	offloading scheme for mobile cloud computing service [16]		condition, device information, and the availability of cloud resources to minimize the execution time and energy.
	Joint offloading decision and resource allocation for multi- user multi-task mobile cloud [17]	2016	Algorithm to compute offloading decision and communication resource allocation for multi-user and multitask situation that optimizes the performance by minimizing the cost of costs of energy, computation, and waiting time
Energy consumption	A quick-response framework for multi-user computation offloading in mobile cloud computing [18]	2018	Framework that uses agent between mobile devices and the cloud to retrieve the offloading decision and results quickly, minimize energy consumption, and reduce communication burden
	User profiling for energy optimization in mobile cloud computing [20]	2015	System architecture to build predictive models for future energy consumption to help cloud and mobile devices in making decisions about required energy
	Energy efficient computational offloading framework for mobile cloud computing [21]	2016	Provide algorithm to reduce the energy- efficiency cost by considering computation offloading selection, clock frequency control, and transmission power allocation
	Multiscale not Multicore: Efficient Heterogeneous Cloud Computing [26]	2010	Mirage operating system aims to compiles applications directly into a high- performance and energy-efficient kernel that can run directly on mobile devices and virtual clouds

Heterogeneity	Access schemes for mobile cloud computing [27]	2010	Architecture that aims to provide an intelligent network access strategy for mobile users to satisfy the application requirements. It was built based on the concept of Intelligent Radio Network Access (IRNA), which is considered an effective paradigm for dealing with the dynamics and heterogeneity of available access networks
	OpenCL: A parallel programming standard for heterogeneous computing systems [28]	2010	A parallel programming standard for heterogeneous computing devices. It allows creating desktop applications that are executable on different computing elements
	Dealing Issues of Mobile Cloud Computing using 5G Technology [29]	2017	Protocol to solve the heterogeneity in mobile devices. it enables users to be self- organized and configuring
Bandwidth	Cloud assisted P2P media streaming for bandwidth constrained mobile subscribers [31]	2010	The proposed architecture allows mobile users located in the same location to share the limited bandwidth between them
	Bandwidth		Bandwidth Conservation System which can use unutilized bandwidth

	Conservation Framework for Mobile Cloud Computing: Challenges and Solutions [34]	2014	for future use.
	Dealing Issues of Mobile Cloud Computing using 5G Technology [29]	2017	Provide protocol based on 5G technology to increase bandwidth in heterogeneity in mobile devices.
Security	Towards Cloud-Based Compositions of Security Functions For Mobile Devices [37]	2015	The proposed module installed an OpenFlow controller (cloud side) and OpenFlow switch (mobile side) for redirection.
	A New Secure Mobile Cloud Architecture [38]	2015	An architecture proposed installed components on both sides the cloud and mobile. To guarantee the integrity of application and communication.
	On cloud security attacks: a taxonomy and intrusion detection and prevention as a service [39]	2016	presented a cloud computing model with alternative options to incorporate intrusion detection techniques in different layers.
Privacy	A Privacy-Aware authentication scheme for Distributed mobile cloud computing services. [41]	2015	The new approach uses a single private key to strengthens its security by utilizing bilinear crypto system and dynamic nonce generation. it results in reducing authentication processing time and usage of memory spaces.
	An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing [42]		Efficient privacy preserving approach for outsourced data, the solution focused on data security, using a probabilistic public key encryption, and ranked keyword searching algorithm.
	A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing, in Mobile Cloud Computing, Services [43]	2016	A light-weight data privacy preserving method, the solution focused on data security, using a pseudo-random permutation method

REFERENCES

[1] Kahoro, P. and G. Kanyi, Mobile Cloud Computing Models, Infrastructures, & Approaches, in Cloud Computing. 2015.

[2] Gu, T., Newzoo's Global Mobile Market Report: Insights into the World's 3.2 Billion Smartphone Users, the Devices They Use & the Mobile Games They Play. 2019.

[3] Sahu, M.I. and U. Pandey. Mobile cloud computing: Issues and challenges. in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). 2018. IEEE.

[4] Sanaei, Z., et al. SAMI: Service-based arbitrated multi-tier infrastructure for Mobile Cloud Computing. in 2012 1st IEEE International Conference on Communications in China Workshops (ICCC). 2012. IEEE.

[5] Abolfazli, S., et al., Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. IEEE Communications Surveys & Tutorials, 2013. **16**(1): p. 337-368.

[6] Ko, S.-K.V., J.-H. Lee, and S.W. Kim, Mobile cloud computing security considerations. Journal of security engineering, 2012. **9**(2): p. 143-150.

[7] Noor, T.H., et al., Mobile cloud computing: Challenges and future research directions. Journal of Network and Computer Applications, 2018. **115**: p. 70-85.

[8] Dinh, H.T., et al., A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 2013. **13**(18): p. 1587- 1611.
[9] Chetan, S., et al., Cloud computing for mobile world. available at chetan. ueuo. com, 2010.
[10] Arun, M.C. and K. Prabu, Advantages of mobile cloud computing. 2018.
[11] Gao, J., et al. Mobile cloud computing research-issues, challenges and needs. in 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. 2013. IEEE.
[12] Mollah, M.B., M.A.K. Azad, and A. Vasilakos, Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 2017. **84**: p. 38-54.
[13] Akherfi, K., M. Gerndt, and H. Harroud, Mobile cloud computing for computation offloading: Issues and challenges. Applied computing and informatics, 2018. **14**(1): p. 1- 16.
[14] Barbarossa, S., S. Sardellitti, and P. Di Lorenzo, Communicating while computing: Distributed mobile cloud computing over 5G heterogeneous networks. IEEE Signal Processing Magazine, 2014. **31**(6): p. 45-55.
[15] Deng, S., et al., Computation offloading for service workflow in mobile cloud computing IEEE transactions on parallel and distributed systems, 2014. **26**(12): p. 3317-3329.
[16] Zhou, B., et al. A context sensitive offloading scheme for mobile cloud computing service. in 2015 IEEE 8th international conference on cloud computing. 2015. IEEE.
[17] Chen, M.-H., B. Liang, and M. Dong. Joint offloading decision and resource allocation for multi-user multi-task mobile cloud. in 2016 IEEE International Conference on Communications (ICC). 2016. IEEE.
[18] Kuang, Z., et al., A quick-response framework for multi-user computation offloading in mobile cloud computing. Future Generation Computer Systems, 2018. **81**: p. 166-176.
[19] Judge, P., Cloud Wireless Access Burns More Energy Than Data Centres. 2013: UK.
[20] Benkhelifa, E., et al., User profiling for energy optimisation in mobile cloud computing.Procedia Computer Science, 2015. **52**: p. 1159-1165.
[21] Shiraz, M., et al., Energy efficient computational offloading framework for mobile cloud computing. Journal of Grid Computing, 2015. **13**(1): p. 1-18.
[22] Guo, S., et al. Energy-efficient dynamic offloading and resource scheduling in mobile cloud computing. in IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. 2016. IEEE.
[23] Sanaei, Z., et al., Heterogeneity in mobile cloud computing: taxonomy and open challenges. IEEE Communications Surveys & Tutorials, 2013. **16**(1): p. 369-392.
[24] Allam, H., et al. A critical overview of latest challenges and solutions of Mobile Cloud Computing. in 2017 Second international conference on fog and mobile edge computing (FMEC). 2017. IEEE.
[25] Tuli, A., et al., Exploring challenges in mobile cloud computing: An overview. 2013.
[26] Madhavapeddy, A., et al., Multiscale not multicore: Efficient heterogeneous cloud computing. ACM-BCS Visions of Computer Science 2010, 2010: p. 1-12.
[27] Klein, A., et al. Access schemes for mobile cloud computing. in 2010 eleventh international conference on mobile data management. 2010. IEEE.
[28] Stone, J.E., D. Gohara, and G. Shi, OpenCL: A parallel programming standard for heterogeneous computing systems. Computing in science & engineering, 2010. **12**(3): p. 66-73.
[29] Umar, M., et al., Dealing Issues of Mobile Cloud Computing using 5G Technology. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 2017. **17**(8): p. 246-250.
[30] Hakak, S., S.A. Latif, and G. Amin, A review on mobile cloud computing and issues in it. International Journal of Computer Applications, 2013. **75**(11).
[31] Jin, X. and Y.-K. Kwok. Cloud assisted P2P media streaming for bandwidth constrained mobile subscribers. in 2010 IEEE 16th international conference on parallel and distributed systems. 2010. IEEE.
[32] Khan, S., et al., Towards port-knocking authentication methods for mobile cloud computing. Journal of Network and Computer Applications, 2017. **97**: p. 66-78.
[33] ung, E., et al. User-profile-driven collaborative bandwidth sharing on mobile phones. in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond. 2010.
[34] Olanrewaju, R.F., A. Egal, and O.O. Khalifa. Bandwidth Conservation Framework for Mobile Cloud Computing: Challenges and Solutions. in 2014 International Conference on Computer and Communication Engineering. 2014. IEEE.
[35] Khan, A.N., et al., Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 2013. **29**(5): p. 1278-1299.
[36] Al-Janabi, S., et al. Mobile cloud computing: challenges and future research directions. in 2017 10th international conference on developments in esystems engineering (DeSE). 2017. IEEE.
[37] Hurel, G., et al. Towards cloud-based compositions of security functions for mobile devices. in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). 2015. IEEE.
[38] Olafare, O., H. Parhizkar, and S. Vem, A new secure mobile cloud architecture. arXiv preprint arXiv:1504.07563, 2015.
[39] Iqbal, S., et al., On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications, 2016. **74**: p. 98- 120.
[40] Alizadeh, M., et al., Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications, 2016. **61**: p. 59-80.
[41] Tsai, J.-L. and N.-W. Lo, A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal, 2015. **9**(3): p. 805-815.
[42] Pasupuleti, S.K., S. Ramalingam, and R. Buyya, An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Journal of Network and Computer Applications, 2016. **64**: p. 12-22.
[43] Bahrami, M. and M. Singhal. A light-weight permutation based method for data privacy in mobile cloud computing. in 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. 2015. IEEE.