International Journal of Research in Engineering, Science and Management
Volume 5, Issue 9, September 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

A Comparative Study of Significance of Mobile Cloud Computing in the Modern World

Dheeraj Pal[1*], Chandra Shekhar Yadav[2], Rahul Kumar Sharma[3]
[1,2,3]*Department of Computer Science and Engineering, Noida Institute of Engineering and Technology, Noida, India*

***Abstract*: Mobile Cloud Computing (MCC) is the combination of cloud computing and mobile computing to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. In mobile cloud computing brings an additional significant benefit. Mobile devices are restricted to fulfill the importance and need of smaller sizes, lighter in terms of weights, less power consumption, hand-held and carrying ease, toughness, water resistant etc. The two types of cloud computing, general-purpose mobile cloud computing (GPMCC) and application-specific cloud computing (ASMCC) which allow users to extended storage and hardware resources to performed expensive tasks on the cloud respectively. Privacy, data access and security are the major areas to work on, encryption, minimum-necessary exposure, effective and make data clean up the part of execution task will be the approach at this level.**

***Keywords*: Mobile cloud computing.**

1. Introduction

Mobile Cloud Computing (MCC) is the combination of cloud computing and mobile computing to bring rich computational resources to mobile users, network operators, as well as cloud computing providers. Some of the key reasons that cloud computing is implemented to substantially minimize or entirely eliminate downtimes and to cut costs for computer hardware systems allowing computation. A company must have a minimum number of hardware systems that can handle the maximum load on its system.

The load and the flow are extremely unpredictable, which contributes to difficult equipment maintenance and expensive time and energy. Remote cloud storage provides a major added value. Smart devices are confined to the need and value of smaller models, weight lighter, fewer power use, simple manual and transportation, locking, waterproof etc. Such issues are at the core of cell app hardware and software growth. Cloud storage allows access to these limited and left-off pieces, enabling users to manage cloud queries and execute cloud activities and deliver the results to their computer. Cloud storage is also strongly needed for mobile apps. Cloud computing is a general mobile cloud computing (GPMCC) that offers general ways of enabling extended storage, sharing, etc. and application-specific cloud computing (ASMCC) allowing applications to perform costly tasks regarding cloud hardware. Analysis and analyst reports demonstrate the breadth of these developments in the world's industrial environment. An proliferation in smartphone and handheld computers often adds greatly to the world's Internet application flow. Cloud storage appears to be the best option to meet this data demand, because of their quick scalability, seamless network connectivity, on-demand self-service and other functionality. The ICT sector is switching to a digital technological environment for development and investment once every 20-25 years. It is recognized as the 3rd framework focused on smart devices and applications, cloud computing, wireless internet networks, big data processing and new technology. By 2020, when the industry of ICT hits $5 billion — $1.7 billion greater than at this stage — the proliferation of innovative technologies based on the current technology and fast-growing adoption of all of these in emerging markets would drive at least 80 percent of the industry's growth. We realize that their computing capacity, battery life and bandwidth constrain mobile devices. Cloud infrastructure, though, creates an impression of limitless computational power. Mobile cloud networking is a modern technology that incorporates mobile apps with cloud storage to build a digital network, where the cloud raises operational functions significantly with retains vast volumes of data. Data transmission and data management take place beyond handheld devices under this modern design.

Mobile apps utilize this IT infrastructure to deliver the following benefits:

1) Extended lifespan of battery
2) Enhanced data collection and transmission power
3) Better data replication by "file it in one location, access from anywhere"
4) Reliability and scalability enhanced
5) Simple to incorporate

Remote cloud computing is supported by the following factors:

Trends and requests: consumers demand ease from everywhere and at any time for the services or apps of businesses. This comfort can be given by mobile devices. Business customers often need exposure to enterprise software and shared resources to improve their efficiency, particularly while on the path.

3G and 4G, Wi-Fi, femtocells, wired wireless and so on have greater internet access, enhanced and expanded network coverage. Enabling technologies: HTML5, CSS3, mobile app hypervisors, web lets and Web 4.0 accelerate virtual cloud

*Corresponding author: thesisworks2022@gmail.com

computing growth. Find mobile cloud computing as a combination of smartphone growth and cloud computing. This provides a smartphone customer with a feature-rich application that is operated by a cloud-backed network. Intensive computer power and mobile framework support for device deployment is needed for most apps designed for smartphones. Most handheld users with low-end, browser- enabled apps cannot afford such applications. With the advent of mobile cloud computing, resources in computing, storage and support for platforms are available through the cloud and more devices can, in theory, be supported. The "in theory" aspect of the mobile cloud must be stressed. Mobile cloud computing is a methodology or paradigm under which mobile apps are created, driven and hosted using cloud technologies, though there is a great deal of opportunity in this field.

A mobile cloud solution helps developers to build apps for mobile devices without being bound to the mobile operating system and to the smartphone's device or battery space. Mobile cloud-centric computing is normally accessible from a remote webserver through a smartphone device, typically without the need to install a consumer program on the receiver computer.

Mobile subscribers have risen dramatically lately because of the continued growth of mobile phones, cellular communication and networking.

TechNavio analysts estimate that, in 2011–2015, the Enterprise Mobile Cloud Computing business in North America would expand by 18.12 percent at CAGR. The rising need for market versatility is one of the major contributing factors to this development. Amazon, Terremark Worldwide, IBM, and Salesforce.com are the main vendors that control this market. Cloud computing advances today bring significant benefits for mobile users, as cloud infrastructures and platforms provide virtually large-scale computing power with elastic scalability and greater resource sharing and utilization. For mobile computing, we will solve other conventional drawbacks. Digital cloud infrastructure provides the following special benefits across the advantages of mobile networking with universal, easy internet connectivity and position data services.

- *Computation and storage efficiency:* The mobile computer can reduce the amount of computational power and data storage needed by transferring challenging workloads and high data into the cloud.
- *More powerful mobile applications:* Since mobile devices now have background access to a powerful cloud, we have the capacity to create more powerful mobile apps than before.
- *Power savings:* Most resourced research in mobile devices can be discharged into the cloud, ensuring that mobile users can focus more on energy consumption reduction without betting on results.
- *Thin mobile clients:* Less space demand for a smartphone app ensures that, paired with a cloud network, we can create less expensive mobile apps that increase overall performance. This allows them to "stumble down" smartphone users, so that they simply manage consumer contact and transfer all client research and knowledge to the cloud.

2. Literature Survey

A. General-Purpose MCC Solutions

Could be a promising facet of MCC. 2.2 MCC Software Application-specific.

Unlike GPMCC, technologies unique to MCC involve the creation of different apps for cloud-based mobile devices. While any mobile computer can without doubt enable for more complex operations than just maltreatment of native execution, ASMCC has the added benefit that it enables cloud storage applications that need more than just enhanced machine capacity. For an case, chat-shoppers or e-mail-shoppers ought to use ASMCC as the site is used because a contact tool and not only for the storage or extra computer power. There are several avenues and technologies developed to promote mobile cloud storage for apps in particular. We 're going to cowl them throughout this segment.

3. Problem formulation, Need and Significance of Proposed Research Work

Cloud computing has other problems which might cause reluctance or concern within the user base. A number of these issues area unit particularly relevant to mobile devices. During research, we formulate ways to minimize these problems, as well as each incidents involving them and techniques accustomed combat them.

A. Research Gap

The user privacy has to compromise with any limitation to security and encryption. For applications that use cloud computing usually store theuser's data remotely to execute remotely. Any remotely stationed data is still vulnerable if security of the cloud is compromised or breached.

B. Problem Statement

1) Privacy

One important concern for cloud computing normally is privacy. For applications that use cloud computing usually store the user's data remotely to execute remotely. This results in issues that firms can use or sell this info without user's permission or knowledge. We formulate a technique which clean the encrypted data as soon as it get processed.

Privacy in Mobile Cloud Computing:

The Oxford Dictionary says that privacy is "a condition in which one is not noticed or disrupted by another." Thus, in daily communications obtained from you, promotional emails become an violation or an intrusion of your privacy, whether requested or accepted. However, all these junk e-mails can hardly be stopped.

Cloud providers collect a lot of personal information quickly to the MCC. It is equivalent to (or even exploited) a gold mine that is waiting for discovery. The harm to personal privacy has just begun and its long- term consequences are still unclear.

Each cloud has a silver lining, however. During the past, confidential information is collected on a computer's hard disk or USB drive, so the data held will be corrupted whether it is transferred or discarded or whether a Flash drive is misplaced or robbed. Sensitive personal details were sometimes contained

on a hard drive used. Luckily, this won't happen with cloud-specified results. However, cloud contributes to many forms of privacy issues:

Users do not necessarily provide their own data storage, thus cloud services are liable for data security.

For details keeping publicly, the cloud service has data protection concerns.

Whenever a customer switches the cloud service, the transfer of data is a challenge. Must fresh data be done on the cloud site? Can old data on the web platform be completely cleared?

Even if a cloud provider leaves business? How should the details go? Who's going to own the data?

Besides these privacy problems in the cloud, MCC introduced new mobility problems. The biggest problem is that there will be numerous applications, but are they safe? Do they collect private information from other parties from mobile devices? Have they any disgusting functions?

The issue of mobile cloud protection became more complex and severe with the explosion of prepaid smartphones. The US Senate is seeking to pass laws to secure internet devices. Yet free smartphone apps typically require publicly identifying details on ads and advertisement. However, so much security is not sufficient and certain demands will move from free to fee-based. The approach is to provide consumers with more controls and options. Mobile apps will notify consumers about the details they are gathering and sharing, i.e., problems surrounding openness in mobile applications.

The default resource for company mobile apps has been the starting point for fast, just- in-time services. Many MCC solutions have been developed to provide consumers with security software and utilities over mobile networks. The benefits of cloud infrastructure in tracking, intrusion identification and malware protection may be used by mobile cloud provisioning. It does not assume, though, that cloud-based software and utilities are completely clear of the danger of ransomware. This just means that the management of online service companies and their infrastructure are already more complicated for hackers than only delivering malicious programs. For cloud-based systems and utilities, the deployment and management of sophisticated antivirus and malware apps on computer devices is redundant, even if such on-device security can also be deemed extra security.

The main protection issue in the mobile cloud is mainly the attacks against smartphones and tablets. Those challenges may be classified into three major categories:

1) actual menaces,
2) cell network vulnerability risks and
3) intrusion attacks

Physical menaces:

The development, failure or misuse of a computer introduces physical risks to mobile apps, allowing anyone else to access data or software without the necessary authorization. While mobile devices are fitted with a pin or password-based lockout system, the owners still do not use this function. Even if such a feature is enabled, it can be subverted in numerous ways. Apps built on mobile devices also have links to cloud infrastructure and data directly and automatically.

Challenges: Subscriber identity (SIM) cards can quickly be disabled and obtained by anybody, from certain mobile devices.

Possible solutions: Developers should attach an extra protection layer at program level if their applications will reach confidential data. Developers will insure that these data is not retained on SIM cards. In the server side, backups are required to erase the data from the storage center when a cell phone is misplaced. More complex verification methods, such as speech recognition and fingerprints, may also be used to secure mobile devices as a second authentication tool.

Mobile network vulnerability risks:

Smartphones can be reached through 3 G or 4 G, Wi-Fi and Bluetooth wireless networks. Users will connect mobile, Web and Short Messaging Services (SMS) via smartphones. From a protection point of view, both interfaces threaten revealing confidential and harmful material. In addition, eavesdropping and spoofing are easier on wireless networks than on wired networks. Significant threats include eavesdropping, middle guy assault and access denial. Certain risks from cell network risk prevention, such as connectivity risk and billing fraud are also current. Real- time fraud identification is also important to track the actions of users in real-time and to change the user profile depending on the monitoring. Challenges: Challenges are a big problem. If it's in the web, device interfaces or cell network networks, telecom service companies are primarily liable for stopping a range of protection breaches by supplying network and end-users. Obviously, the Mobile Cloud is fully virtualized and federated. An approach to control and manage identities across different clouds must therefore be developed.

Possible solutions: Several measures should be taken to avoid unwanted access to mobile devices and to secure cloud storage. The first aspect is also ensuring consumers are trained and that any smartphone device learns the best approach to use the networks. Policies to govern the use of wireless devices should also be established. Additionally, one-time passwords will be saved on the computers. A customized software profile may be generated on-mobile device to facilitate the installation of a personal protection token or app credential. Only users with trustworthy devices that conform to the security policy can then access applications and data in the cloud. iOS and web need additional protection monitoring, which resides below and above iOS devices and cloud providers. Finally, the flow of knowledge between mobile devices and cloud services must be managed and secured.

The threats of malware:

Smartphones are increasingly advanced and thus growing focus has been given to the developers of malware. With growing millions of internet-enabled mobile apps, web-based attacks are becoming a major security issue, not just in terms of botnets and malware, but also in terms of hostile domains and social networks, identity robbery and spam. Challenges: Mobile apps communicate directly with each other and with the real environment from a technology standpoint across a broad variety of innovations. Therefore, mobile Internet consumers ought to be secured from other advanced security risks. Cloud-based systems vary in many respects from traditional applications. The layer of identification is far more complicated

as there are more apps per device than ever before and utilities are becoming just as relevant internally and externally as ever. Potential solutions: Authorized cloud services should be pre-installed and spread. If malware is detected, smartphone software from trusted cloud backups should be restored. Firstly, it is necessary to change the behavior of users through education. A business will warn its staff about risks in the wild to ensure that workers consider what to do through the usage about their cell network or apps. Second, we have to continue to develop network connectivity to ensure that all smartphone devices are safe from unwanted connections to inappropriate pages to spam filter by utilizing anti-malware, anti-spyware and other protection tools. MCC is a prominent developing market for smartphones and tablet computers. As more electronic apps on the market, the amount of safety concerns can undoubtedly rise and appropriate protection measures must be constantly created.

2) Access to and protection of data

When AN device relies on remote information storage and network connectivity to function the least, then the impact on the customer would be important. For example, if a user stores all of his calendar and calls on-line, outages will affect his ability to run from day to day.

MCC is especially fragile as several connection points may be disrupted. Reception and high-speed connectivity for handheld devices can differ tremendously. We create the mechanism to hold data protected such that the data can only be opened and interpreted by authorized people, not even the service provider.

4. Objectives

- To study and formulate the various technique to ensure the privacy of the users.
- To study and formulate the effective technique to access the data and security of the data. The security and access should not come at the cost of speedy accessibility of the data and requirement of higher hardware systems.

5. Methodology/ Planning of Work

1) Collecting the data from user.
2) Encryption of the data using proper encryption algorithm.
3) Transferring data to cloud application/storage in order to process and store.
4) Decryption of the data using secure algorithm and based on minimum access principle for processing.
5) Re-encryption of the data before transferring result back to user's mobile device.
6) Providing result to user in human readable form with accuracy.

Mobile cloud computing encompasses numerous research fields and subjects. Here are some interesting research subjects in MCC.

MCC architecture – The innovation analysis work for MCC will concentrate on how the cost-effective modeling, design, testing, and evaluation of the creation of virtual clouds and networks can be used in a well-defined way. Close attention should be given in this regard to the architecture and testing of mobile application scalability, multi-tenant enterprise SaaS, mobile computing energy consumption, device usability and mobile protection.

MCC Wireless Networking — Monarch of virtual cloud networks covers multiple cellular networks and the Cloud. The primary research emphasis in the networking field will be creative protocols and communications techniques for the management of attractive requirements of energy effective communications, scalable network technology scalability and intelligent network access between networks, applications and computers.

Mobile cloud infrastructure – Analysis on this subject focuses on how mobile cloud infrastructure creates cost-effective and energy-efficient to serve three core classes of services: (a) computing services; (b) network resources; and (c) storage resources. Typical subjects cover information maintenance, virtualization, management and control, load balancing and user profiles.

Mobile apps and technology – In academia and business, the development of successful and easy-to-use web applications on mobile devices has concentrated. When smartphone applications grow increasingly advanced, they may choose to be completely automated, but simpler and easier to use than their standard equivalents. Two prominent device manufacturers (Apple and HP) realize what that means: a possibly massive disruption from a gradual convergence between mainstream desktop and smartphone platforms.

Mobile computer protection in MCC – Safety concerns and requirements at the different levels within MCC, including mobile cloud systems, networks, frameworks and software implementations, are discussed by analysis. Mobile data and cyber protection, mobile device end-to - end communications, safe mobile cloud access, network monitoring and security assessment on mobile clouds are usually granted focus. Some recent research can be found on this subject.

Mobile SaaS – According to a new Forrester Estimates survey, the mobile SaaS industry would grow by more than $92 billion annually by 2016. Existing SaaS application implementations include MobileMe by Apple, Funambol and LiveMesh by Microsoft. We anticipate fascinating research topics on mobile SaaS reference infrastructures and technologies, mobile protection platforms] and systems, facilities and innovation for large-scale mobile SaaS applications.

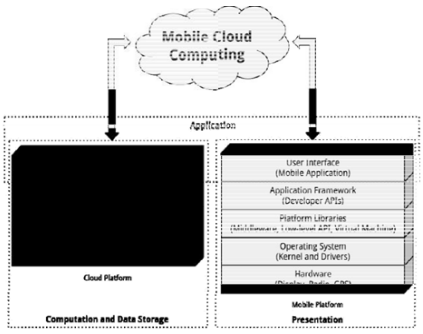

Fig. 1.

First generation model– Personal mobile cloud:

In recent years, a range of vendors have been supplying their smartphone customers with specific web clouds. A variety of examples are mentioned in Table 1. These are also known to provide smartphone users with smartphone data, information, storage and certain personal resources such as m uses and video clips, schedules and calendars, images and documents. These personal clouds offer the first wave of private cloud infrastructure for smartphone devices.

Third generation model and implementation:

As Virgin Media Industry CEO Mark Heraghty pointed out, the explosiveness of mobile internet use has contributed to drastic improvements in client connectivity, handheld plastics substitute for transfers, new innovations including SDNs and Network Virtualization. It is an extremely creative and revolutionary age, as Lee Chooking suggested in [12], and believes that today's ICT operators look radically different from now for a decade. The smoothing is dedicated to Fixmo, Guardtime and Joyent. Switch. Switch. Therefore, the recent growth in mobile access involves a major change in the usage of cellular network networking systems in order to overcome existing cellular networks and services' severe limitations:

- Reduced network coverage scalability and protection for traffic.
- Carrier-oriented broadband network.
- Reduced portability and synchronization between different wireless networks controlled and hosted by wireless service providers.

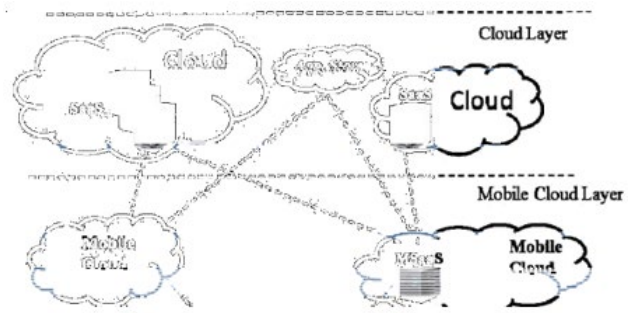

Fig. 2. Third-Generation: Mobile Cloud Service infrastructures

Agent-based Application Partitions:

An agent-based application partition is a chunk of application code packed in a mobile agent, that is executable in a cloud host. Agent-based application partitions provide great advantages over existing mobile-cloud program partitioning techniques due to their autonomous computing capabilities. Autonomy of these application partitions is particularly useful in the context of mobile-cloud computing due to the capability of transparently moving between cloud hosts without requiring management by their caller and self-cloning in different cloud hosts, which can help boost performance in the case of changing runtime conditions in the cloud.

The transformation from a regular application partition to the corresponding agent-based partition is achieved through a behaviour. In the current framework, application partitions have either class-level or method-level granularity, but the same arguments would apply to finer granularity application components as well (such as part of a method). Figure 3a shows a sample application partition and Figure 3b shows the corresponding agent-based partition.

```
public class Queens {

    int[] x;
    public static ArrayList<int []> solutions;

    public Queens(int numQueens) {
        x = new int[numQueens];
        solutions = new ArrayList<int []>();
        callplaceNqueens();
    }

    public void callplaceNqueens() {
```

```
public class QueensBehaviour extends OneShotBehaviour {

    int[] x;
    public static ArrayList<int []> solutions;
    int numQueens;

    public QueensBehaviour() {
        DataStore ds = getDataStore();
        int numQueens = (int) ds.get( "numQueens" );
    }

    public void action() {
        x = new int[numQueens];
        solutions = new ArrayList<int []>();
        callplaceNqueens();
    }

    public void callplaceNqueens() {
```

(a) Application partition for N Queens puzzle. (b) Corresponding agent-based partition

Fig. 3. Application partition transformation to an agent-based partition

Execution Manager:

This component is a service running on the mobile device, responsible for probing the network for bandwidth and latency measurement and making the decision regarding the execution platform of the different agent-based application partitions. In order to decide where to execute the application partitions, the execution manager contacts the cloud directory service to get a list of cloud hosts (virtual machine instances) that are available for use. After choosing the most promising cloud hosts, the execution manager uses the following cost model to make offloading decisions for each off loadable application partition (Note that a sub-partition s of an application partition p is a partition invoked by p):

Let,

td_p: time to execute application partition p on the device less the time to execute its sub-partitions.

tc_p: time to execute application partition p wholly in the cloud with all of its sub-partitions.

s_p: size of the data that is sent to partition p from its super-partition for a single invocation of p np: the number of consecutive invocations of partition p by its super-partition.

An Agent-based Optimization Framework for Mobile-Cloud Computing Angin, and Bhargava

cd_p: the cost (in terms of execution time) of executing application partition p locally on the device.

cc_p: the cost (in terms of execution time) of executing application partition p in the cloud.

b: the network bandwidth available to the application

p_s: the set of sub-partitions of p.

Then cd_p and cc_p are calculated as follows:

$cd_p = td_p + å\ argmin(cd_i; cc_i)$ (1)

i2ps

$cc_p = tc_p + s_p\ n_p=b$ (2)

In order to determine td_p and tc_p, we currently use a static application profiler measuring the execution time of each application partition and record the results as metadata of the application, so they are available for use by the execution manager during application execution.

When the execution manager is making decisions regarding the execution location of agent-based application partitions, it

uses the following two heuristics.

If a partition is migrated, all of its sub-partitions (partitions called by this partition) will too: This is based on the assumption that the cloud hosts always have more computing power than the mobile device, i.e., the sub-partition execution time in the cloud will be shorter than on-device execution for every sub-partition. As the sub-partitions will involve data communication with the offloaded partition, keeping them together will prevent the penalty to be incurred by network latency during communication.

6. Conclusion

Application partitions with frequent communication should be kept together if the time savings from offloading the sub-partition is below a certain threshold: Frequent communication between application partitions on different platforms could actually hurt performance under variable net- work conditions if the estimated time savings for executing the sub-partition in the cloud is low. Furthermore, there is a cost associated with processing (saving state etc.) due to offloading the sub-partition, which justifies the use of this heuristic. -- This eliminates capital costs for improving multiple mobile network infrastructure enabling a number of connectivity systems as well as business models for diverse sectors of the industry.\-- Reduces operational expenses by reducing electricity options and maximizing the usage of distributed services because of various service offers. -- Reduces mobile device production costs by back-end infrastructure elasticity and centralized connectivity. So far as the cloud layer of this design model is concerned, the main research problem for the smartphone device is the availability of substitution database resources. Indeed, cloud infrastructure management and con tent and distribution networks are problems shared in standard cloud service provision and are also critical to the success of mobile cloud applications. A special feature of mobile clouds is the need to reduce the computational charge placed on mobile resource devices for tasks like voice recognition or image processing. Under these scenarios the creation of secure and reliable adaptive strategies for managing this trade-off during runtime is one of the key component of competitive mobile cloud service delivery depending on the balance between connectivity and technical delay tolerance for the particular application. Owing to high costs opportunities for cell network providers, analysis of the view of the mobile network framework was already underway. In fact, network sharing at the stage of the Radio Access Network is widespread among middle-size operators worldwide. The rise of mobile virtual network operators (MVNOs), who specialize in catering for unique, mostly small and consumer markets, has been a noteworthy trend over the past five years. However, these approaches are stagnant and require significant management and operating expense from a technological perspective. For e.g., by improving base station visualization strategies and growing usage of digital radios, such a simulation is anticipated to become a key function of systems in future. The new advances in application technologies however preclude the core tasks conducted on the mobile app layer from being transferred to the cloud. Instead, we anticipate that the major developments in this layer will affect access, in the sense that services enabled by cloud technology in the mobile network and cloud layers of the model will be accessed in a consistent and relatively transparent manner. With this in mind, the key goal is to formulate articulate and effective frameworks for flexible exposure to mobile cloud systems and resources.

References

[1] Steve Ranger, “Everything you need to know about the cloud” ZDNet Online, December, 2018.

[2] Emma Simmonds, “How Cloud Computing Will Transform Traditional IT in 2019,” Compare the Cloud, Jan, 2019.

[3] Samimi et al., “Mobile Service Clouds: A Self-Managing Infrastructure for Autonomic Mobile Computing Services,” Self-Managed Networks, Systems, and Services, 2006.

[4] Zhang et al., “Securing elastic applications on mobile devices for cloud computing,” Proceedings of the 2009 ACM workshop on Cloud computing security, 2009.

[5] Christensen, “Using RESTful web-services and cloud computing to create next generation mobile applications,” Conference on Object Oriented Programming Systems Languages and Applications, March 2010.

[6] Cheng et al., “Preserving User Location Privacy in Mobile Data Management Infrastructures,” Proc. of the 6th Workshop on Privacy Enhancing Technologies, 2006.

[7] Pragya Gupta, Sudha Gupta, “Mobile Cloud Computing: The Future of Cloud.”

[8] L Guan, X Ke, M Song, J. Song, “A survey of research on mobile cloud computing,” 2011 10th IEEE/ACIS Sanya, China.

[9] H. Qi, A Gani, “Research on mobile cloud computing: Review, trend and perspectives,” 2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP).

[10] Victor C.M. Leung, Min Chen, “Cloud Computing,” 4th International Conference, Cloud Comp 2013, Wuhan, China, October 17-19, 2013.

[11] Ruay-Shiung-Chang, Jerry Gao, Volker Gruhn, Jingsha He, George Roussos, Wei-Tek Tsai, “Mobile cloud computing research-issues, challenges and needs,” 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering.

[12] Xu Yang, Xinyi Huang, Joseph K. Liu, “Efficient handover authentication with user anonymity and untrace ability for Mobile Cloud Computing,” Future Generation Computer Systems Volume 62, September 2016

[13] Keke Gai, Meikang Qiu, Hui Zhao, Lixin Tao, Ziliang Zong, “Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing,” Journal of Network and Computer Applications Volume 59, January 2016

[14] Wenzhong Li, Yanchao Zhao, Sanglu Lu, Daoxu Chen, "Mechanisms and challenges on mobility-augmented service provisioning for mobile cloud computing," IEEE Communications Magazine, Volume: 53, Issue: 3, March 2015.

[15] Keke Gai, Meikang Qiu, Lixin Tao, Yongxin Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," Security and Communication Networks Volume 9, Issue 16, November 2016.

[16] Mehdi Sookhak, F. Richard Yu, Muhammad Khurram Khan, Yang Xiang, Raj kumar Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," Future Generation Computer Systems, Volume 72, July 2017.

[17] Vanga Odelu, Ashok Kumar Das, Sar Kumari, Xinyi Huange, Mohammad Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," Future Generation Computer Systems, Volume 68, March 2017.

[18] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, "Secure integration of IoT and Cloud Computing," Future Generation Computer Systems, Volume 78, Part 3, January 2018.