International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

Mobile Cloud Computing-Literature Review

Viraj Joshi, Rachit Mehta, Onkar Sanap, Vishant Mehta, Jai Mehta
IT Department KJ Somaiya College of Engineering Mumbai
IT Department KJ Somaiya College of Engineering Mumbai
IT Department KJ Somaiya College of Engineering Mumbai
IT Department KJ Somaiya College of Engineering Mumbai
IT Department KJ Somaiya College of Engineering Mumbai

Submitted: 05-05-2021 Revised: 17-05-2021 Accepted: 20-05-2021

ABSTRACT— The high-speed development and renaissance in mobile devices have produced a fast-growing market. The remarkable progress made within the mobile applications allows the users to accomplish most of their tasks such as shopping, social networking, information gathering and business through their mobile devices. However, there are some limitations in the mobile environment, which reduce the utmost benefits of using mobile devices. These devices are not as powerful as personal computers and lack high level computational storage capabilities. Therefore, mobile cloud computing has been introduced as a possible enhancement for mobile services. Cloud computing is integrated into the mobile environment in order to beat the restrictions of mobile devices. In the paper, we describe the privacy and security issues faced by the Mobile Cloud Computing (MCC) technology. The issue faced in integrating green computing technology is discussed in this research paper.

Keywords—Framework, Features, Privacy, Security, Green Computing, Service, Future.

I.INTRODUCTION

In the recent few years, there have been advances in the field of Mobile Cloud Computing. Mobile Cloud Computing has been introduced as a technology for Mobile services. It is essentially the mixture of mobile computing and cloud computing that has hardware, software and communication for performing different operations like accessing information, storing data and running different applications on mobile devices. Mobile Cloud Computing refers to a space or an environment where data and its processes are stored outside of the mobile device. The main aim of Mobile Cloud Computing is to supply accurate, real time and valuable information to the user or the client. The motive of Mobile Cloud Computing is to switch the execution of mobile phone's applications with an upscale to the user's experience thereby providing efficient results. It also provides business opportunities to both cloud providers and network operators. Mobile cloud computing technology unifies resources of cloud computing and different network technologies with functionalities like mobility, flexibility and scalability which in turn enhance the performance. MCC has gained a lot of popularity because of its applications. Different Mobile Cloud Computing applications such as Gmail, Google Maps and navigation systems for mobile voice search and android based applications have been developed and served to mobile users. These have certainly proved to be very beneficial to the clients. The motivation behind Mobile Cloud Computing is software processing, increasing storage capacity, automating systems, reducing cost and delivering different services from the underlying technology which essentially leads to ease of accessibility and eventually eliminates most of the limitations. Mobile Cloud Computing applications move data storage and computing powers from mobile phones into a cloud environment. It is the latest paradigm for mobile applications where storage and processing are moved from a mobile device to a centralized and powerful computing platform that is in cloud over the internet. These centralized applications are accessed by the assistance of a wireless connection.

Applications created for the mobile can be classified as online and offline. Offline could lead to have a negative impact on the cloud structure on emergence, since it has a reliance on the mobiles abilities unlike the online mode. In the online mode, Cloud enable the mobile to have an interaction with the servers and thus this will be beneficial as the mobile having limited resources or abilities will be able to able to execute operations without the need to carry them locally. This paper provides a comprehensive study of the Architecture of the Mobile Cloud Computing, Security, Challenges that the technology faces and solutions for the same, and discusses the Future of the technology. The paper is

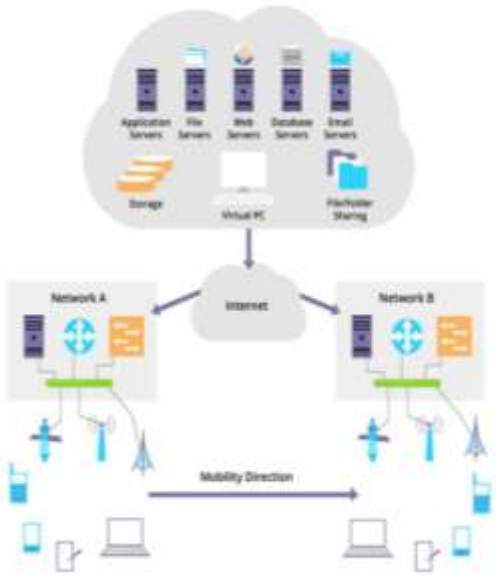
International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

organized into various sections from Introduction to Conclusion.

II.ARCHITECTURE

Mobile Cloud Computing basically consists of cloud service providers, internet service providers, application servers, web servers, database servers, network systems, etc. The devices are connected either to a satellite or a base station through a network. Hence, a connection is developed between the station, devices and their interfaces. The user transfers the information and requests through the internet to the cloud. This data is stored in the servers and can be accessed as and when the user makes requests.

There are four different models representing Mobile Cloud Computing. They are: Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud.



Mobile Cloud Computing comprises of mainly four layers namely Access Layer, Management Layer, Virtual Layer and Physical Layer.

1. The Access Layer provides interaction between the user and the cloud.
2. The Management layer provides services between the servers and devices.
3. The Virtual layer consists of virtualization of computation and network resources.
4. The Physical Layer consists of devices like laptops, computers, mobile phones, etc. which are physically available.

III MOBILE OFFLOADING

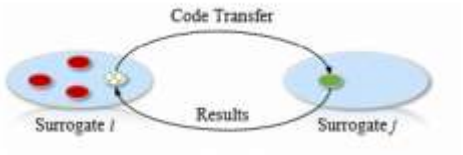
Mobile devices conduct computation offloading to balance the cloud's capacity, allowing apps to run faster and consume less energy.

Computation offloading is when a mobile computer shifts some of its processing to the cloud. This treatment entails

- partitioning of applications
- decision to offload
- job execution in a distributed manner

A mobile app may be broken down into different roles or service components.

Model is a service-oriented architecture in which mobile cloud services are made up of multiple functions or service components that are supported by multiple surrogates (a surrogate can be either a mobile device or an Internet cloud server).



Offloading

The process of transferring a code or process to a surrogate for processing. After being processed, the surrogate will transfer the results of function back to the offloading requester

Composition

Once the code is processed a service request is sent to surrogate in order to get back the results.

Mobile Cloud Application Partition and Offloading Decision

The following are three factors that are taken into account when modelling the application partition problem:

1. Device profile - The processing capacity of cloud virtual machines is normally several times that of mobile devices, which helps with execution time modelling.
2. Application profile - A directed acyclic graph (DAG) is used to model mobile applications, with the vertices representing application modules and the edges representing module dependencies or data flow.
3. Environment profile - In the partition strategy, the interaction between mobile devices and clouds is critical, especially the wireless connection such as WiFi or cellular connection is not always stable.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

Partitioning and execution of data stream applications

- The aim of the optimization is not only to achieve maximum speed/throughput in processing the streaming data, but also to achieve high throughput while minimising the makespan. (total duration of the schedule) i.e., the time it takes for all workers to be processed
- The architecture not only enables dynamic partitioning for a single user, but it also enables the sharing of computation instances across multiple users in the cloud, allowing for more efficient use of the underlying cloud resources.

Various mobile cloud offloading strategies:
Distributed abstract class graphs in mobile environments:
Although retaining abstraction elements for components in remote devices, the computer maintains a graph consisting only of components in its memory space.

Dynamic software deployment

A framework that adapts device partitioning decisions in real time. The framework works by continuously profiling the performance of an application and dynamically updating its distributed deployment to account for changes in network bandwidth, computer CPU consumption, and data loads.

Fine-grained, multisite computation offloading
This system allows portions of an application to be offloaded in a data-centric manner, even if that data exists at multiple sites.

Mobile Cloud Offloading Framework
A mobile cloud offloading framework has to solve two essential problems.

1. The surrogate environment must run the offloaded code bits. Offloaded code that is meant to be consistent with both the original and surrogate environments can be solved by synchronising both environments or code translation.
2. The original programme must invoke the offloaded code. An RPC-like mechanism between the original application and the offloaded code is needed to solve this issue.

Identity and Access management evaluation criteria for MCC

Extensive Authentication and Authorization Support

- User identification and access control on the wireless medium must be handled across all forms of cloud delivery models (public, private, and hybrid) and service models in MCC.
- Authentication and authorization requirements vary by distribution platform and service model.
- A one-time, certificate-based, risk-based, multi-factor, and multi-level authentication and authorization technique can be used to achieve this.

User-Friendly Single Sign-On Support

- There are a lot of providers and applications in the mobile cloud, and each one needs its own authentication.
- So memorizing several passwords, repeated login to the same service or app, frequent password change, phishing, and password recovery are all problems that arise as a result of this requirement. As a result, the organization's overall efficiency and productivity suffer.
- SSO can help solve this problem by providing a centralised, safe, simple, and user-friendly way to authenticate a user only once in a given environment.

Lightweight Standard/Protocol

- A cloud that is mobile For over-the-air mobile applications, the IAM standard should be a lightweight standard/protocol.
- They have a smaller overall scale, leave out unnecessary data, and can use a data compression technique to reduce network transmission overhead .

Platform Independent, Vendor-Neutral and Open Standard

- MCC is a multi-platform, multi-application, multi-service, multi-vendor, multi-IT infrastructure environment.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

- It incorporates a mobile environment, a desktop environment, and a number of other environments, an IAM specification should be a transparent, platform-independent, vendor-neutral industry standard that guarantees operability in all of them.

Scalable Standard

- It is always important to strike a balance between security and scalability.
- The rapid growth of the mcc industry, on the other hand, has necessitated the creation of flexible standards to cope with the growing number of users, services, and resources.
- As a result, an IAM standard should be able to accommodate more users, consumers, capital, and applications without compromising cost or efficiency.

Mobile Standard

- The extensive use of mobile devices is one of the main distinctions between MCC and other forms of cloud computing.
- As a result, traditional mobile entities, protocols, and specifications are used for authentication and authorization.

Many IAM standards may be acceptable for mobile devices, but they may be ineffective

IV SECURITY

Data Security in Mobile Cloud Computing:

Security of data is of paramount importance in mobile cloud computing since the data uploaded in the cloud is vital and shareable between multiple mirror servers of a particular organization. The data is sensitive and has private value and should be prevented from manipulation, undue access and abuse. Data theft has become very common as cloud computing technology has become the mainstay for multifarious businesses. Security is a must to prevent such untoward incidences.

Each cloud service provider has the onus for providing three very basic facets of data security, these include:

1. Tried and verified encryption scheme for protection of data.
2. Strong access control protocols to prevent unwanted and unauthorized access to personal or business data.
3. Periodic backup and storage of data in case of loss.

These 3 features form the major bulwark of any cloud provider; however, there are still some pressing issues yet to be resolved. The most important among them is the role of lessor of assets as contrasted with that of the cloud service provider. The development of a robust security model is important for the resolution of these issues.

AES (Advanced Encryption Standard) Algorithm:

The previously used Triple Data Encryption Standard was rendered obsolete by the newly developed AES that rectified the key size disadvantage prevalent in the TDES. The older key size of 56 bits was supplanted by the 128 bits size key of the new standard. Data being sent up for storage has to encrypted and secured using the algorithm and then decrypted upon request for access.

The main features of this system include:

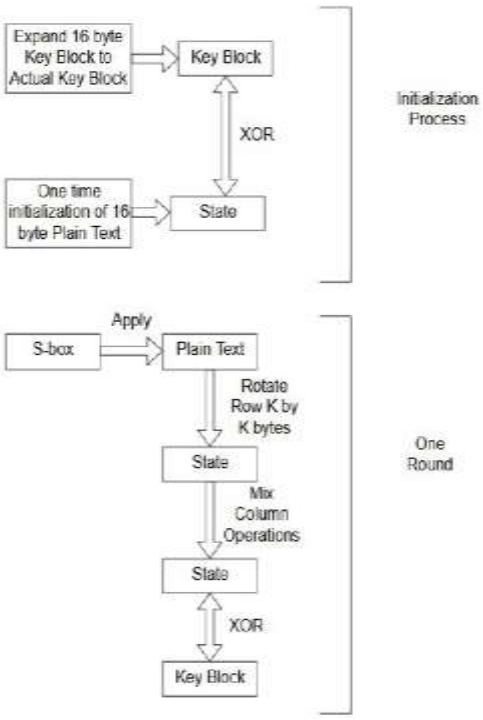
1. Presence of a symmetric and parallel framework allowing flexibility for the algorithm and bolstering it against cryptoanalysis attacks.
2. Adaptation to latest modern processors.
3. Efficient and smooth usage with smart cards.

The various sub parts of the AES algorithm have different bit sizes, each block comprises of 128 bits plain text and a key size of 128 bits. Two distinct versions of combination can be used in the implementation; the first one is the encryption of a 128-bit plain text with a 128-bit key while the second one encrypts the equivalent size plain text with a longer 256 bits key. The first case is predominantly used.

The AES algorithm consists of the following process executed in an orderly fashion. During the decryption the same steps are performed in a reverse fashion to mitigate the encryption results.

1) One-time Initialization Process.
a) Derivation of the Key Block from the rudimentary 16-byte key.
b) Production of the state from the 16-byte plain key text box.
c) XOR of the key block and state.
2) Steps for each round, the totality of rounds is 10.
a) Application of the Substitution Box to the plain text bytes.
b) Rotation of the kth row by k bytes.
c) A mixing of columns followed by repetition of the XOR operation performed between the state and key block.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

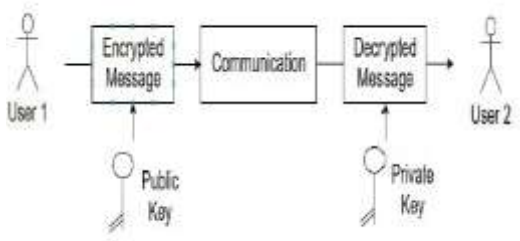


RSA Algorithm:

The RSA algorithm is most commonly used for the establishment of a secure data communication channel via the means of a digital signature. Its security is derived from the existence of two disparate keys; namely, the public key and private key. The public key is used for the encryption while the private key is used for decryption. The derivation of any one key while knowing the other is a difficult task. 1024 keys are used for the process but the doubling of the number of keys enhances the efficacy of the algorithm due to reduction in the proportion of symmetric key length.

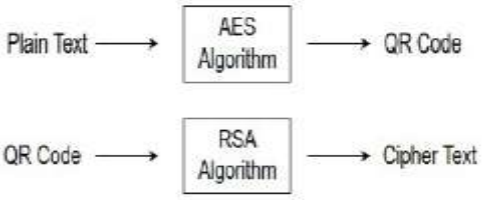
The step wise description of the RSA procedure is as follows:

1. Selection of two large prime numbers A and B.
2. Calculating N which is the product of A and B.
3. Choosing encryption key E, so that it is not a factor of (A-1) and (B-1).
4. Choosing decryption key D in such a way so that it is satisfies the given condition:
5. (D*E) mod (A-1) (B-1) = 1.
6. Encryption: CT=PTE mod N
7. Decryption: PT=CTD mod N



Proposed Data Encryption Model:

The proposed data encryption model is an amalgamation of the AES and RSA Algorithms. The plaintext is first encrypted using the AES system by the usage of a QR (Quick Response) Code. A second scanning of the code takes place and it is finally coded into ciphertext by the RSA system. The decryption process is the exact reversal of these steps.



The application of the proposed AES-RSA Encryption model can be in online ticket booking, payment for goods, information access and much more. The only prerequisite is a smartphone with a stable internet connection.

The advantages of the proposed system are as follows:

1) Robust security system with less chances of a brute force attack due to the prevalence of not one but two different cryptographic algorithms.
2) Data Integrity is maintained by the means of Cyclic Redundancy Check.
3) Usage of QR codes completely eliminate the need to carry paper documents.

V.CHALLENGES AND SOLUTIONS

In MCC there exists challenges in various parts like operations, services of the applications, management of data, security, privacy etc… In addition, the Quality of Service can be easily affected by the presence of the varying landforms, weather and buildings. In the following section, we will look at these challenges and discuss challenges and needs in different important areas stated below and further discussed in the paper:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

i) Privacy
ii) Threats
iii) Architecture and Infrastructure of Mobile Cloud
iv) Quality of Service
v) Green Computing

i) Privacy:

Unwanted or unscrupulous emails you receive everyday may constitute an attack or violation of your privacy. These emails are inexorable and they cannot be stopped. A large amount of personal information is collected by the cloud providers which is equivalent to a treasure of information that is yet to be explored. This information stored on cloud serves to be detrimental to the personal privacy and has long term effects, we have not come across yet.

Cloud has been efficient in solving the problem of storing the data on the initially used computer hard disks or the USB drives, thereby reducing the amount of data being compromised when the USB is lost or the computer is either sold or recycled. However, there are other problems that the cloud possess:

- The providers of the system are responsible for protecting the data as the users are do not physically possess the storage.
- If the users, wishes to change the cloud and wants to migrate to some other cloud provider, migration of this data can be a challenge. It cannot be verified too whether the data on the old cloud will be completely deleted.
- What if the cloud provider goes bankrupt? Or the cloud providers discontinue the service? In that case what would be done with the data? In addition to the above problems, another problem that arises is that there do not exist enough means to check the safety of storing data on the cloud and to select the safest cloud provider. There do not exist enough means for a general user to verify if their data is safe or is it being shared with unauthorized parties for any kind of hideous functions. With the growth of these mobile clouds, the privacy problem might become even more serious and detrimental. Governments are trying to impose laws, but the free service providers earn from advertisements, and these advertisements usually demand personal data. If too much protection is provided, it might even lead to change of the providers to fee based services.

The solution to the problem is, providing the users with more transparency about the process i.e. about eh information that is being collected, the information that is being shared or sent out. In addition to the transparency the users shall be given more controls and flexibility of choices, to select the privacy preferences.

ii) Threats:

Mobile loud systems can take advantage of the monitoring, malware protection, security detection etc… but this does not imply that that these applications are totally safe. It only implies that the difficulty of the violation or attack or invasion on the system has considerably increased, and its not easy to break into or cause any kind of breach.

The issue that concerns the cloud providers is about the security of these platforms. There can be threats to the system, which can be divided into three categories:

A. Physical threats:

- Challenge: The devices can be stolen, or lent to someone, which can result in access to the personal data or applications. Although, the devices are equipped with security systems, they can often be broken into by methods and applications stored in the devices, sometimes give direct access to the data stored on the cloud. The SIM(Subscriber-Identity-Module) cards can be easily removed from most of the phones thereby leaving the access to anyone who has the card.
- Possible Solution: Sensitive data is usually accessed at the application level, so to protect this data, the developers can add here an extra level of security. Also, the SIM cards should not be used to store too much data. Biometrics can be used in the security system of the device to keep the security of the device effective. Also there should be ways to take back up of data from the cloud, which has been lost in the device.

B. Mobile Network Security threats:

- Challenge: Smart are accessible using various access facilities like connection to internet using 3G, 4G or 5G cellular networks, Wi-Fi, Bluetooth. Using the above services, smartphones can use Internet Services, make phone calls, using Short Messaging Services (SMS) etc… These services have interfaces which possess dangers of breach of data and is susceptible to various attacks. They are all a part of wireless networking technology, unlike wired networks they are more susceptible to attacks likes eavesdropping, man in the middle attack, denial of service attack. There are other fraud related threats too which the wireless networks are vulnerable to. Dealing with them is a major challenge. The MCC is inherently federated and highly virtualized, thus there is a need of an

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

approach that is developed to manage identities across different clouds.

- Possible Solution: The primary solution will be to provide education to all the smartphone users about the correct ways of utilizing the networks. There is a need of established policies to govern the use of these devices and networks. An additional security benefit can be attained when we use One Time Passwords (OTP) for authentication instead of the stored passwords. There should be strict rules for the people who can access the data of the cloud, to prevent unauthorized access. There should be new security controls that stand above the cloud providers.

C. Malware threats:

- Challenge: As the number of the smartphone users is increasing, the Web based network is exponentially expanding, thereby attracting malware creators towards the highly sophisticated smartphones. These malwares pose a serious security issue in the form of phishing attacks, identity theft, viruses, botnets and spams. Mobile devices use a wide array of technology to interact with each other and thus there is a requirement of protection from sophisticated threats to the security. The increasing number of applications per user makes the identity layer harder.
- Possible Solutions: As a solution to this challenge, official software can be used authorized by the cloud providers, and they should be pre-installed on the devices. When the devices are attacked by the malwares this software would be used in effectively restoring the back up. These threats can be avoided by providing the users with the education to use the mobile networks or applications in a safe and conducive way. Network Infrastructure should be upgraded to help the user to restrict any type of malware, spyware and other unauthorized sites/spams using anti malware, anti-spyware and other security sites.

iii) Infrastructure of Mobile Cloud:

There are various papers available on the subject addressing mobile cloud infrastructures and architectures. On observing these papers, we found out that there are few issues and needs in the mobile cloud infrastructures. Two of them are:

- Cloud computing Infrastructures that are network oriented: Many challenges in network cloud infrastructure need to be addressed to meet the demands of the latest generation of cloud services, which provides auto resource provision, balancing the load, improvised standards of connectivity and green computing.
- There is a need for the new technology for connectivity and solutions: In the present systems, there are issues like limitations on the existing network bandwidth, speed in compatibility between the servers used for computing and networks. To resolve these issues, we need an improvised technology and infrastructure solutions.

iv) Quality of Service:

Unlike the wired networks, the MCC system is based on wireless networks, which do not use any physical connections. Thus due to the existing clearance in network overlay, the rate of transfer of data in the MCC environment is constantly changing and discontinuous. Additionally there is a large distance between the data centre present in large enterprises , the Internet service provider resources and the end users. In such kind of connections the latency delay might be 200 milli seconds in the last mile unlike that in the wired networks (which has latency delay of 50 milli seconds).

Various other factors like weather, varying application throughput, user mobility etc… lead to the changes in the bandwidth and network overlay, thereby increasing the handover delay in wireless networks.

v) Green Computing:

In past few years Green Computing has remained the most interesting and hot topic of the discussion and there are various research projects being taken up with respect to the conservation of the energy involved in the computing.

The protocols to support mobile communication in MCC need to be more energy efficient. There is a need for energy efficient migration and synchronization techniques. We need an upgradation using more efficient technologies for the future wireless connectivity infrastructure, which can deal with various and networks and technologies and make the consumption of energy more efficient. Infrastructure that is Energy Efficient and similar data centres are the necessary requirement for the future technology. The future infrastructure of cloud storage and networks must include energy efficient resource allocation and management methods and solutions. There is also a need of solutions that can cross different layers such as infrastructures, platforms, mobile SaaS (software development and deployment approach) to provide system-level energy monitor and analysis so that cost-driven and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 752-762 www.ijaem.net ISSN: 2395-5252

green-based resource allocations and management decisions can be made.

VI.APPLICATIONS

1. To share Internet Data: Data can be shared among different devices that are nearby each other using a local connection and a connection between the parties. This method is quite and low in cost.
2. Image Processing: If an individual faces difficulty in understanding the language or the objects of a certain region then he/she can click pictures of that particular place and use mobile cloud computing to interpret the language or the meaning of the objects.
3. Social Networking: Mobile Cloud Computing can be an effective tool for people to share information with each other using social networking websites and applications. The user information and content can be stored on the mobile cloud. Individuals can efficiently access and share resources with friends and family.
4. Applications related to sensor data: Nowadays, all the devices have sensor related applications that can read and analyse data. The data that is read using these applications can be stored for future use in the mobile cloud.
5. Language Processing: Translation of language is possible through Mobile Cloud Computing. When people visit different countries, they might find it difficult to understand the local language of that region. At such times, users can make use of the language processing application offered by MCC.
6. Mobile Cloud Computing also serves the purpose for mobile commerce. It has become easier for people to make transactions or buy commodities over the Internet.
7. Mobile Cloud Computing holds an important place in healthcare sector as well. Data can be accessed from time to time to assess the patients and improve the treatment. Errors can be avoided and accuracy can be improved. Solutions to complex medical conditions can be found within seconds through data stored in the cloud.
8. Another application of MCC is mobile gaming. The amount of data that the games require is quite a lot. Clouds play an integral role to store all this data, hence resulting into space optimization. This further improves the speed, performance and communication measure.
9. Mobile Cloud Computing has paved a path for learning. It has enhanced the processing speed, data capacity and battery life for all the students across the globe. Different cloud-based applications are used by the faculties to communicate with students.

VII.ADVANTAGES

1. Mobile Cloud Computing is quite advantageous as it helps to store and accommodate so much more data as compared to a personal computer. It basically is a gateway to unlimited data storage which can be accessed from anywhere in the world.
2. The users do not have to worry about the infrastructure or the maintenance of the cloud. The cost required for maintaining and upgrading a personal computer is eliminated in the case of cloud. It also minimizes the cost of other services like management.
3. Scalability is one of the features of cloud. All the instances are automatically deployed within the system. Mobile Cloud Computing is quite flexible. It is not dependent on any hardware or software components. It is mobile which means that it supports access anywhere and also provides all the available services irrespective of the location of the user. It is very easy to view, modify and update shared documents and files on mobile cloud.
4. Mobile cloud Computing provides efficient backup and data recovery techniques. In case of a corrupted hard drive or a device, cloud easily restores all the deleted data without any discrepancy.
5. In MCC, long execution time on applications is avoided which decreases the power consumption and in turn increases the performance measure.
6. Cloud and internet can turn out to be very useful for integration of various services from different service providers.

VIII.LIMITATIONS

1. Mobile Cloud Computing is not completely secure and safe as it can be exposed to external threats such as hacks and malwares. This might result into malfunctioning of the device and implementation of wrong operations.
2. When a cloud infrastructure is developed by a third party, the users have no alternative but to trust the party for privacy and confidentiality of their data. The service provider along with the third party gets access to the user data for management and protection. This can lead to concerns regarding the privacy, safety and security of information provided by the users.
3. Low bandwidth is one of the drawbacks in the mobile cloud environment.

4. The biggest limitation is that Mobile Cloud Computing is completely dependent on internet service provider for all the services.
5. As the services are provided and run by a third party, the user has limited control over the working and management of the system.
6. The cloud based mobile applications can corrupt the data and this can further affect its integrity. This can pose to be a threat to the privacy of the users.
7. There are challenges related to offloading and partitioning. During the offloading process, there is a possibility of data violation through unauthorized users.

IX.FUTURE

Mobile cloud computing, to put it plainly, is technology that enables data and computation to take place outside of the mobile device, allowing new forms of applications including context-aware mobile social networks. NIST defines the cloud architecture as having five essential characteristics, three service models, and four implementation models that facilitate availability.

Essential characteristics:

- On Demand Self Service: Without requiring human contact with each service provider, a client may arbitrarily provision computing capabilities, such as server time and network storage, as required.
- Broad Network Access: Capabilities are accessible over the network using standard mechanisms that allow heterogeneous thin and thick client platforms such as cell phones, laptops, and PDAs to access them.
- Resource Pooling: Using a multi-tenant model, the provider's computing services are shared to support many users, with separate physical and virtual resources dynamically delegated and reassigned based on customer demand. Processing, memory, network speed, and virtual machines are all things to remember.
- Rapid Elasticity: Capabilities may be provisioned and released easily and elastically, in some cases automatically, to quickly scale out and quickly scale in.
- Measured Service: Through using a metering capability at a level of abstraction suitable to the type of operation, cloud services dynamically monitor and maximise resource utilisation.

Service Models:

- Software as a Service (SaaS): The user is granted the right to access the provider's software, which are stored on a cloud platform. A thin client interface, such as a web browser, is used to view the software from multiple client computers. With the exception of restricted user-specific device configuration settings, the client does not access or monitor the underlying cloud infrastructure.
- Platform as a Service (PaaS): The customer is granted the freedom to launch consumer-created or purchased software onto the cloud platform using programming languages and software provided by the vendor. The user has no influence over the underlying cloud infrastructure, such as the network, servers, operating systems, or storage, but he or she does have control over the configured software and likely application hosting environment configurations.
- Infrastructure as a Service (IaaS): The user is given the right to provision processing, storage, networks, and other basic computational tools, from which he or she can deploy and run arbitrary devices, such as operating systems and applications. The user does not handle or monitor the underlying cloud technology, but he or she does have control over operating systems, servers, and deployed software, as well as potentially partial control over such networking elements.

Deployment Models:

- Private Cloud: The cloud technology is handled exclusively for the benefit of a corporation. It can be run by the company or by a third party, and it can be on-site or off-site.
- Community Cloud: Several organisations share the cloud platform, which represents a specific culture with similar interests (e.g., mission, security requirements, policy, and compliance considerations). It can be handled by the organisations themselves or by a third party, and it can be on-site or off-site.
- Public Cloud: The cloud technology is operated by a corporation that provides cloud software and makes it open to the general public or a wide business community.
- Hybrid Cloud: The cloud architecture is made up of two or more clouds (private, group, or public) that are separate but linked by standardised or proprietary technologies to allow data and device portability (e.g., cloud bursting for load-balancing between clouds).

Challenges and solutions for the future:

Several advances in the way we view computation and connectivity have occurred over the past decade. For a variety of factors, it has proven to be a promising mobile computing approach.

- Resource Poverty

- Data storage capacity and processing power
- Division of application services

There are a number of other problems that arise as a result of MCC implementation.

- Absence of standards
- Access schemes
- Security
- Elastic application models

Open Research Issues of the future:

A. Energy Efficiency: Since mobile devices have limited resources such as battery power, usable network bandwidth, storage space, and processing performance, researchers are constantly on the lookout for technologies that optimise the usage of those resources.
B. Security: The lack of standards poses a serious problem, especially in terms of the protection and privacy of data sent to and from mobile devices to the cloud.
C. Better service: MCC was developed with the aim of offering PC-like services to mobile devices. However, due to the many variations in functionality between fixed and mobile devices, service transformation from one to the other cannot be as straightforward.
D. Task division: Researchers are constantly looking for new ways to offload computation operations from handheld devices to the cloud. However, owing to the variations in computational criteria of different software available to consumers and the range of handsets on the market, an optimal approach is a field that needs to be studied.

CONCLUSION

The research paper covers the most important aspects and features of mobile cloud computing and establishes lucidly that it is a technology that has potential in a multitude of spheres. Technological development of the future will be incomplete without cloud computing playing an important supporting role in the storage and access of data.

The world has become data centric and the need to handle big data has never been more pivotal. In addition to this there has been an exponential proliferation of mobile phones, with the rapid development of applications serving all the needs of the consumers. It is imperative that mobile devices should be potent enough to encapsulate and effectively operate newer and more complex functionalities. These devices have certain limitations associated with them like the smaller screen size, variability of devices in the market and underlying network latency. Such impediments need to be overcome and the apex solutions available are via cloud computing. It stands alone in providing optimal services to mobile users.

Security, storage, recovery and backup of data form the pith of the functionalities directly affecting users and organizations. Not only do such issues need requisite scrutiny but emerging diagnostic tools should be simple enough to promote usage on a wider basis. Mobile Cloud Computing addresses each of these individual issues adequately. Recovery and Backup of data is simplified and no more does it occupy hard memory in mobile devices, freeing up the main memory for more paramount operations and boosting overall functioning of the device. Security of data is ensured by the utilization and amalgamation of latest standards in encryption and network security.

Mobile Cloud Computing occupies a unique place in technological trends due to its dual advantages derived from the mobile technology and cloud computing. It is projected to be an important revenue driver for businesses in the upcoming decades. With this central role that the technology is going to play, this research paper has presented a succinct and orderly overview of the architecture, security, advantages and future scope germane to the topic. The development of mobile offloading has also been addressed. We have extensively reviewed related work and selected the most recent research in this field. In conclusion, for seamless implementation of Mobile Cloud Computing, the aforementioned challenges need to be critically addressed, the solutions and technology made more robust. It is a promising paradigm, which is viable and technologically feasible in the pervasive computing research domain.

REFERENCES

[1] Sahu I., Pandey U S., 2018., “Mobile Cloud Computing: Issues and Challenges” in International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), IEEE. Link: https://www.scribd.com/document/483060612/sahu2018-cloud
[2] Alshehri A., Alshahrani H., Alzahrani A., Alharthi R., Alouf E., “The Potential of Utilizing Mobile Cloud Computing in Mobile Devices” in 2018 International Conference on Computational Science and Computational Intelligence, IEEE. Link: https://www.semanticscholar.org/paper/Mobile-Cloud-Computing-%3A-Issues-%2C-Security-%2C-%2C-

Tayade/0c0ac64a4d6296deb7d0a2a67133a935269103db

[3] Alakbarov R.G., Alakbarov O.R., "Mobile Clouds Computing: Current State, Architecture and Problems", IEEE, 2017. Link: http://www.mecs-press.org/ijcnis/ijcnis-v10-n2/v10n2-6.html

[4] Imad A. Elzein and Moustapha Kurdi, "Analyzing theChallenges of Security Threats and Personal information in Mobile Cloud Computing Infrastructure", 02 June 2020, IEEE Conference. DOI: 10.1109/ICD47981.2019.9105711Link: https://ieeexplore.ieee.org/abstract/document/9105711

[5] Imen Merdassi, Cherif Ghazel and Leila Saidane, "Surveying and Analyzing security Issues in Mobile Cloud Computing", 1-3 Dec. 2020, IEEE Conference. DOI: 10.23919/PEMWN50727.2020.9293077 Link: https://ieeexplore.ieee.org/document/9293077

[6] Ruay-Shiung-Chang, Jerry Gao, Volker Gruhn, Jingsha He, George Roussosand Wei-Tek Tsai, "Mobile Cloud Computing Research - Issues, Challenges and Needs", 10 June 2019, IEEE Conference. DOI: 10.1109/SOSE.2019.96 Link: https://ieeexplore.ieee.org/document/6525561

[7] Bakhtawar Aslam, Rabia Abid, Dr. Muhammad Rizwan (IEEE Member), Dr. Fahad Ahmad (IEEE Member), Mian Usman Sattar, "Heterogeneity Model for Wireless Mobile Cloud Computing & its Future Challenges", Proc. of the 1st International Conference on Electrical, Communication and Computer Engineering (ICECCE), 24-25 July 2019, Swat, Pakistan, 978-1-7281-3825-1/19/$31.00 ©2019 IEEE Link: https://ieeexplore.ieee.org/document/8940681

[8] Dr. Mahmoud Odeh, "Mobile Cloud Computing In The Technology Era: An Overview Of The Factors Influencing The Adoption Process", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 12, DECEMBER 2019, ISSN 2277-8616. Link: http://www.ijstr.org/final-print/dec2019/Mobile-Cloud-Computing-In-The-Technology-Era-An-Overview-Of-The-Factors-Influencing-The-Adoption-Process.pdf

[9] Ankul Sharma," MISSION SWACHHTA-Mobile application based on Mobile Cloud Computing", 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence),2020, 978-1-7281-2791-0/20/$31.00_c 2020 IEEE. Link: https://ieeexplore.ieee.org/document/9057926

[10] N. Chalaemwongwan and W. Kurutach, "Mobile Cloud Computing: A Survey and Propose Solution Framework" in 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, 2016. Link: https://ieeexplore.ieee.org/document/7561437

[11] Gopalakrishnan, "Cloud computing identity management," SETLabs briefings, vol. 7, no. 7, pp. 45–55, 2009.Link:https://www.researchgate.net/publication/316630606_Role_of_Identity_Management_Systems_in_Cloud_Computing_Privacy

[12] Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003. Link: https://crypto.stanford.edu/~dabo/papers/bfibe.pdf

[13] M. R. Momeni, "A lightweight authentication scheme for mobile cloud computing," International Journal of Computer Science and Business Informatics, vol. 14, no. 2, 2014. Link: https://www.researchgate.net/publication/281438784_An_Efficient_Authentication_Protocol_for_Mobile_Cloud_Environments_using_ECC

[14] Pingidentity.com. (2011) A standards-based mobile application idm architecture. [Online]. Link: http://www.enterprisemanagement360.com