LITERATURE REVIEW
MCC is the conceptual structure that mixes three technology, including mobile net, mobile computing, and cloud computing, to allow cell users to offload records processing and store onto clouds via wireless networks and cell devices. The finest motivation of making use of MCC is gaining benefits of cloud computing technology by way of leveraging cell strategies. The dynamic networking surroundings results in greater complex provider deployments and implementations, evaluating with primary cloud computing. In subsequent phase we can see distinct approaches for handling computation extensive applications that are nevertheless challenging for executing at mobile side. According to the survey cloud computing includes various technology “distributed computing”, “parallel computing” and “grid computing”. It emerged in autumn 2006 by means of Google engineer Christopher accountable for “Google one hundred and one” mission after that IBM has a joint mission with google on “cloud” and afterwards many groups released various plans on “cloud computing” emerged as the synonym for the subsequent era net revolution. Inside the recent years the important it giants for extraordinary cloud carrier vendors are amazon cloud for storing purpose, google cloud for development, fashion micro cloud for safety and security. The various 10 listed principal techniques of data generation the “cloud computing” continues to be the first-class. In keeping with a latest observe by ABI research, a New York-based firm, greater than 240 million corporations will use cloud services thru cell devices by using 2015.
Cloud computing era affords (EAAS) the entirety as a service; garage, sources, computing sources, development surroundings, testing, security and many others. Many formal definitions were proposed in each academia and industry, the only provided by way of U.S. NIST (National Institute of Standards and Technology).

With the explosive boom in cellular applications, platforms and end user needs, disadvantages at the cell device end (e.g., computation and garage capability, energy, shared wi-fi medium) considerably hinder further enhancements in application quality of service (QOS)- typical measures of QOS encompass consumer experienced put off, provider reliability/availability and information privateness. Mobile cloud computing (MCC) goals to triumph over those boundaries by means of integrating cloud computing into the mobile environment to enable cell customers and mobile software vendors to elastically make use of resources in an on-demand fashion.

In cellular cloud computing, assets are commonly assigned to a group of computers, which give these sources to clever cell gadgets. Cellular cloud computing concept percentage two most important viewpoints, considered one of them is processing and storage is inside the cell tool different is the whole thing is done at the cloud out of doors the cellular devices. At the same time as both of them have their advantages and downsides however cloud computing offer platform-unfastened packages, consequently, all the application can run within the cloud even as they may be no longer restrained to any unique cellular emblem or operating machine.

2.2 Various Mobile Cloud Computing Algorithms

Since the mobile devices have some constraints, there arises a need get sources from outside assets. One of the methods to overcome this trouble is getting sources from a cloud, but the right of entry to such systems isn't always assured or/and is just
too high priced. Huerta-canepa in [36] provides the tips for a framework that mimics a traditional cloud company the use of cell devices inside the region of users. The framework detects nearby nodes which might be in a static mode, which means to be able to continue the same location or follow the same movement sample. If nodes in that state are determined, then the target company for the application is modified, reflecting a virtual issuer created on-the-fly among users. In situations like downloading an outline report at a some places, collocation increases the probabilities of humans willing to carry out commonplace tasks.

To store the resources like electricity and processing electricity, the collocated cell gadgets can collaboratively act as a nearby cloud and break up the project into smaller subtasks to be finished on one of a kind devices [37]. The effects can then be aggregated and shared. The proposed method allows heading off a connection to infrastructure-based cloud companies whilst preserving the principle blessings of offloading.

Fernando et’al in [38] on the other hand proposed a methods to use all forms of nearby assets (smart phones, PAD, even computers) which can be used to collaborate in forming the nearby cloud to acquire a not unusual intention. Their approach is to triumph over the aid sparseness, power intake and low connectivity problems faced in traditional mobile cloud computing. Sharing of workload is dynamic, proactive and relies upon on price model to gain all individuals. The structure includes especially an aid handler, a activity handler and a value handler. The resource handler discovers the collocated assets, the price handler then calculates the values to find the distribution of jobs could have maximum advantages after which the job handler distributes the sub-tasks, run the roles and acquire them back on sender. Finally the cost handler handles micropayments a number of the taking participated gadgets.
SPACCE idea in [39] supplying calculation capacity of PCs is proposed to facilitate distributed collaboration. A SPACCE is a complicated adhoc cloud computing environment that can be built according to the needs that arise at any given time on a set of private, i.e., non-dedicated, computers and dynamically migrate a server for utility sharing to another computer. By using migrating the server, redundant calculation capacity of computers can be utilized for developing a SPACCE, in which the response time of the software shared among customers is progressed. A SPACCE provides the parameters that had calculation capacity of a laptop because the server for collaboration to different pcs which have no application and/or now not sufficient calculation ability to be the server on demand.

Collaboration [39] of cell gadgets to work as a unit in a networked environment is a good solution for a common mission. However occasionally work cannot be dispensed among mobile gadgets and needs to be offloaded to a useful resource rich platform. For that migration of executable block needs to be performed.

Rickyet’al in [40] has proposed stack-on demand asynchronous exception (SOADA) execution mechanism for offloading of work to a nearby cloud. On this mechanism, a stack is being maintained for the storing of execution state and only the current execution country this is on top of the runtime stack can be migrated. So on this technique irrespective of how large the image is, SOD migrates best the required part of the statistics to the vacation spot website. Taking pictures states in mobile gadgets in a transportable way has been executed the usage of asynchronous exception and is saved the use of dual method hierarchy technique which will minimize the overhead. However offloading to cloud introduces latency as a parameter.
A cloudlet [41] architecture proposed by using M.Satyanarayan, advocates a two tier method to decrease the latencies. Proposed structure states that in preference to counting on a far off “cloud”, we is probably capable of deal with the cell device’s resource poverty via a close-by resource-rich cloudlet. Cloudlets are decentralized and extensively dispersed internet infrastructure additives whose compute cycles and storage sources can be leveraged by using close by cell computer systems. Accessing to a cloudlet may be provided by way of wifi that saves energy as well as has greater bandwidth in comparison to other internet services.

Hyrax is also a similar kind of concept, proposed by e. marinelli in [42]. This architecture deploys mobile devices as nodes to create a cell cloud computing platform. On the way to enhance the performance of hyrax, an extended model of Hadoop, cell gadgets act as slave but grasp continues to be deployed on a laptop (useful resource rich platform in comparison with smartphones). Disbursed facts processing is provided through Hadoop’s map reduce implementation, which divides jobs submitted by means of the user into impartial “tasks” and distribute these tasks to slave nodes.

V. Balasubramanian [42] has mentioned various service fashions of cloud computing focusing on TAAS model, its architecture numerous service additives and the important thing capabilities of the TAAS structure. They discussed greater approximately mobile cloud computing structure and applications and additionally various issues related to the cloud surroundings, safety and the privacy of the records and the performance.

The definition, Scope, importance and the mobile testing process on cloud and different approaches with comparison to conventional mobile testing approaches is enlightened by Jerry GAO [43].
The advantages discussed includes lesser test environment cost due to multiple virtual machines (VM) for test environments on one host server, isolated VM so that if one VM crashes would not affect the other VM’s and stored VM image files that can be freely copied or moved.

Riungu and Taipale [44] discussed that testing of software’s on cloud is influenced by conditions such as level of domain knowledge needed to test an application, flexible and cost effective, security and economy of scale and cloud computing as a booming paradigm and the software testers to polish their skills.

**Table 2.1 Survey of Different Cloud Computing Algorithms**

<table>
<thead>
<tr>
<th>Name of the approach</th>
<th>Performance matrix</th>
<th>Application</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| Virtual cloud computing framework                         | Energy consumed      | Optical character recognition software | 1. Lightweight architecture  
2. Lesser energy consumed  | 1. No fault tolerance  
2. Very basic frame work                                   |
| Ad hoc and Opportunist is Job Sharing                     | Cost and device capabilities | Speech recognition and synthesis      | 1. Benefit to all participants.  
2. Includes all types of local resources                      | No fault tolerance                                      |
| SpACCE                                                    | Calculating capacity of PCs | CollaboTray                          | 1. Server can be migrated according to available calculating capacity.  
2. Even with no high-spec PC, acceptable response time is maintained. | Required network infrastructure.                        |
In analysis with vengattaraman [45] in cloud surroundings for software program checking out there are wide variety of clouds having specific checking out strategies. So it's far the responsibility of service supervisor to oversee and co-ordinate between the center activities of respective layered entities of standard cloud surroundings and outline the set of required clouds relying at the trying out strategies required via any manufactured from the consumer.

What's the importance of cloud primarily testing of cellular programs and what are the various sorts of CBT are discussed by means of mohata [46]. Cloud checking out which offers a shared check surroundings so that user want not to installation and maintain diverse trying out platforms to make sure internet site or cell application portability and compatibility and different issues like functionality , interoperability, performance and so on. Check scripts are recorded by means of the user from the local browser or with any of the OS in case of a cellular utility .The scripts are then submitted to the cloud for testing to be achieved mechanically with the today's testing tools available there.

Although cloud trying out is imparting a huge variety of static and dynamic testing and different services but applications hosted on faraway clouds have lower controllability, uncertainties and observability in comparison to conventional in house hosted programs. Automation has made an responsible effect in the checking out area is mentioned with the aid of fuyangpeng [47] i.e. implantation and architecture of cloud primarily based automatic software program test environment (CASTE).

To test a software on cloud it has conditions the device beneath test is access through online and testing infrastructure is hosted within the cloud. The automatic
testing surroundings is to be had all of the time round the clock as the principal advantage.

2.3 Various Offloading Algorithms

Wei et al. [48] furnished suitable definitions of important elements and offering efficient algorithms and processes. Their simulation results discovered that after the burden of the system is heavy, HACAS algorithm can pick those programs with maximum energy and power intake. With the parameters placing in the simulation, the profit of HACAS algorithm is set 30% higher than that of FCFS set of rules. Besides, while the load of the machine is light, the provider choice scheme followed in HACAS can successfully balance the load of the devices inside the system. Concretely speaking, HACAS algorithm’s load variant is set 60% higher than that of the random provider choice scheme.

Lin et al. [49] studied the MCC challenge scheduling trouble and came up with the primary project scheduling works that minimizes power intake under a difficult time constraint for the task graph in the MCC surroundings, contemplating the joint mission scheduling at the nearby cores in the cellular device, the wireless communication channels, and the cloud. They proposed a unique set of rules that starts from a minimal-postpone scheduling and subsequently performs strength reduction by migrating tasks some of the neighborhood cores and the cloud. A linear-time rescheduling set of rules become also proposed for the venture migration such that the overall computation complexity is successfully decreased. Simulation outcomes tested widespread power discount with the overall completion time constraint satisfied.

Wua et al. [50] proposed a scheduling set of rules that computes the concern of the duties through the use of their attributes primarily based on QOS-pushed in cloud
computing. This algorithm minimize the tasks according to their precedence after which schedules every task onto a service which has minimum completion time. The experimental consequences showed that the algorithm finished suitable overall performance. Though the set of rules based totally on QOS-driven could attain load balancing, it did not recall power intake.

Yamauchi et al. [51] considered mobile gadgets’ battery power, mobility and imbalanced load as three critical components and proposed a disbursed parallel scheduling technique for cellular cloud computing. As in line with this system a grasp tool observes the above cited parameters of the gadget and the opposite gadgets are its slaves. If the parameters are not sufficient for parallel processing to take vicinity, the master device will pick out different slave gadgets for processing the ones threads. The overall performance of cellular gadgets become stepped forward and unlike different algorithms it taken into consideration community high-quality in addition to load balancing too. It decreased the battery intake of cellular gadgets however not the entire energy of the overall gadget.

Mishra and jaiswal [52] designed a heuristic load balancing algorithm primarily based on ant colony optimization idea considering various performance parameters which include both CPU and community load, and available reminiscence. The pheromone update mechanism proved to be an effective tool for reaching load balancing of cloud assets and minimizing lifespan. It does not consider the fault tolerance issues in cloud environment.

Suryadevera et al. [53] proposed a load balancing algorithm for grid computing using ant colony optimization. High pheromone cost of a route method it is shorter. It considers various resource parameters (mips, verbal exchange bandwidth, variety of
processors and reminiscence) for calculating pheromone i.e. the resource capability for executing diverse jobs therefore allocating the first-class useful resource for the process and additionally stability the load of all of the assets. The algorithm is anticipated to reap higher throughput and subsequently increase the general overall performance in the grid environment. But, it does now not keep in mind qos requirements.

Yang et al. [54] proposed and defined a service for offloading heavy cell applications from aid-limited MHS to nearby surrogates with rich resources. Those packages may be downloaded from the net. The carrier changed into capable of correctly offload only those applications that were applied in java. The experimental and simulation effects showed that the offloading provider changed into very effective.

B.Chun in [55] has defined a technique clone cloud, with aim of offloading execution blocks from mobile tool to the cloud dynamically to adjust the execution performance of a mobile device. This method describes that clone are made on the cloud aspect at every initiation of a provider, which are replicate the image of the smart phone. In assessment with smart telephones, clones are useful resource and do not have the battery constraint as well. Primary gain of the clone cloud implementation is stated because the performance enhancement. Chun has taken virus scanning, photo seek and behavior profiling programs which are computation in depth for performance assessment. A few issues includes the software manage may be at both access stage or at exit degree handiest. Additionally local techniques cannot be migrated.

Another related technique is being proposed via l.yang in [56], which plays the offloading decision dynamically based at the resources available at cellular tool. This method is based totally on elasticity of an utility, which states that issue can be offloaded to cloud and vice versa at any specific time.
Gao et al. [57] proposed an approach wherein time and power are evaluated for both nearby and offloading computations. The mission is authorized to be offloaded while offloading is less time and electricity consuming than nearby computing. After taking an offloading selection for a task, a clustering algorithm is called. The clustering algorithm aims at taking similar selections for the obligations that communicate with each different, a good way to reduce communication power consumption. Despite the fact that each electricity and time are selection parameters, memory requirements and availability, and computation complexity are absolutely not noted.

Kovachev et al. [58] considered strength, memory, and execution time in a multi-standards application feature. However, introducing a multi-standards utility function to lessen the optimization trouble complexity generates an engineering trouble of the weights related to every parameter on this function.

clone2clone [59] allows users to create their own clone within the cloud or to request cloneds, the clone2clone directory carrier, to create a clone on their behalf. This introduces a new paradigm wherein there is dedicated vm within the cloud for each mobile tool. Clones can shape secure peer-to-peer networks for content material sharing, searching, and allotted code execution. This gets rid of the quandary of having unpredictable and electricity inefficient wi-fi networks, considering that clones inside the cloud have strong usually-on, excessive-bandwidth networks. Other mechanisms can be used to offload computationally heavy obligations to the cloud [3,4,14,15], for which the structure is likewise restrained to networks with low bandwidth and excessive latency.

Cdroid [59] makes use of some other MCC method in which a secured tunnel is installed between a mobile tool and its cloud clone for all net site visitors. The cloud
clone appears as a neighborhood aid for the cellular tool. This improves net navigation, compression and caching of internet pages, and blocking off unwanted marketing and virus scanning applications previous to set up. The main disadvantage is that cdroid requires a constantly-on connection to the cloud clone and all traffic ought to go through the clone, which isn't always energy-efficient.

Vm-based cloudlets [60] are decentralized and broadly dispensed net infrastructure additives whose computation and garage resources can be leveraged by way of nearby mobile gadgets.

Satyanarayanan et al. emphasized the need of physical proximity of the cloudlet to the wi-fi connection so that mobile devices gain from handiest having to traverse one hop the usage of high-bandwidth, low latency wireless networks.
Table 2.2 Survey of Various Energy Aware Algorithms

<table>
<thead>
<tr>
<th>Name of the approach</th>
<th>Performance metrics</th>
<th>Applications used</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone cloud</td>
<td>Total execution time and energy expanded</td>
<td>Virus Scanning, Image processing, Behavior modelling</td>
<td>1. Better execution results 2. Less energy consumed</td>
<td>1. Does not virtualize access to native resources</td>
</tr>
<tr>
<td>Application partitioning problem for mobile datastream applications</td>
<td>Throughput</td>
<td>Tasks with different computation to communication ratio.</td>
<td>1. Throughput achieved is about 2X.</td>
<td>1. Energy consumption not being taken into account. 2. Resources at cloud end are assumed to be abundant</td>
</tr>
<tr>
<td>MACS</td>
<td>Execution time and Energy consumed(in joules)</td>
<td>N-Queens problem and face recognition</td>
<td>Better cost function (consists of cost of transfer, cost of memory, cost of execution) in contrast with locally execution</td>
<td>This approach is lagging in parallelism between threads.</td>
</tr>
</tbody>
</table>

Kimberley [61] is the current reference for cloudlet implementation. It uses two approaches to introduce the VM state to the infrastructure.
1. The VM is suspended and its processor, memory, and disk states are transferred to the cloudlet, then the VM resumes at the exact point at which it was suspended.

2. In dynamic VM synthesis, the mobile device delivers a small VM overlay to the cloudlet infrastructure, which already possesses the base VM from which this overlay was derived. Parallelized VMs can be spawned on demand on the cloudlet side to achieve faster execution. Kimberley does not consider energy utilization on the mobile side, but resource-heavy operations can drain the battery of a mobile device.

2.3.1 VM Migration Based Offloading

S. Goyal found cyber foraging framework to make use of computation sources of computing gadgets (desk bound or cellular) in close proximity of SMD. The framework implements customer/server structure. Cell devices request for system offloading and surrogate server affords the offerings on demand. The framework supports configuration of more than one surrogate servers concurrently and employs virtual machine technology for far off software processing. A single surrogate server is capable to run a configurable wide variety of independent virtual servers with isolation, elasticity, equipment manipulation and simple cleanup mechanism.

Every offloaded software executes on remote digital server. The framework ensures secure communication by using deploying cryptographic measures for communication between smd and surrogate server. The framework consists of the advantages of low latency, nearby accessibility of remote surrogates and fewer issues of protection and privacy. The vital components of such method is the deployment of template based virtualization technique that is a noticeably time ingesting and assets
starving mechanism for vm deployment. The framework requires the annotation of manual components of the software as neighborhood or remote that is an additional attempt for application builders. Similarly, surrogate based cyber foraging is constrained to the availability of services and resources on nearby servers.

Bahl et al., delivered VM based totally cloudlets framework that's differs from current cyber foraging by way of migrating image of the loading application to the explicitly special faraway server. A cloudlet is a trusted aid wealthy computer or cluster of computer systems this is linked to internet and is available for SMDS. The mobile tool serve as a thin patron providing most effective person interface while actual processing is done at the cloudlet in distributed environment.

The proposed framework is based upon transient customization of cloudlet infrastructure using hardware VM technology in which VM encapsulates and detaches the temporary guest software environment from the cloudlet infrastructures permanent host software environment. The framework employs variant procedures for VM migration. The critical aspects are that the framework requires additional hardware level support for the implementation of VM technology and is based on cloning mobile device application processing environment to remote host which involves the issues of VM deployment and management on SMD, privacy and access control in migrating the entire execution environment and security threats in the transmission of VM.

Clone cloud based framework proposed with the aid of maniatis et al., which is a significant approach for offloading software of diverse nature in unique manners. Clone cloud differs from different approaches by means of employing 3 specific offloading algorithms for specific kinds of applications. However, the attribute of offloading image of the running status of the software to remote server resembles to the
The framework reduces the dynamic transmission overhead of utility code by deploying a simple technique for synchronization. Clone cloud employs primary functionality outsourcing by way of offloading computational in depth duties to remote host while easy obligations such as person interfaces are carried out on cell gadgets. Examples of the packages include speech recognition, photograph processing and video indexing.

Background augmentation offloads the entire software to remote host and communicates outcomes from historical past technique to the cellular device. Examples of the applications include; antivirus and file indexing for faster search.

Mainline augmentation policy is deployed for applications having mixing nature; having some computational intensive computational load and need to engage with other components of the programs inclusive of debugging programs. Clone cloud is a significant framework for offloaded processing which incorporates an easy approach for synchronization among smd and remote server.

The critical aspect of the Clone cloud is the migration of execution environment to remote server which involves the issues of security, privacy, access control, VM deployment and management on SMD. The deployment of variant strategies for application migration on the basis of application nature results in enlarged overhead on mobile devices. Clone cloud deploys a single thread approach which increases jitter in the execution time of the application components.

### 2.4 Various Security Algorithms in MCC

According to a report [the number of new susceptibilities in mobile operating systems increased 42 percent from 2009 to 2010. The number and sophistication of
attacks on mobile phones is increasing speedily as compared to the countermeasures. Data transmission over the wireless networks is highly vulnerable to network security threats. For example, using radio frequencies, the risk of interruption is higher than with wired networks therefore attacker can easily compromise confidentiality.

Similarly, in cloud datacenters the security threats are associated with the transmission between physical elements on the network, and traffic between the virtual elements in the network, such as between virtual machines within a single physical server. Therefore, in order to leverage the application processing services of computational clouds, a highly secure environment is expected at all the three entities of MCC model.

In current approaches, transmission of the running states of mobile application which is encapsulated in VM or binary transfer of the application code at runtime is continuously subjected to security threats at mobile device, wireless medium and cloud datacenters.

Therefore, secure transmission of the entire components of the application is a challenging issue for MCC. It is imperative to implement reliable security measures for the data transmission, and synchronization between SMD and cloud datacenters in distributed processing platform.

Similarly, access control, fidelity and privacy of distributed application components in the remote cloud datacenters is an important consideration for the distributed application processing in MCC. Cloud datacenters provide augmentation services which are unapproachable to mobile users. Therefore, it is highly demanding to ensure the privacy of data and computing operations in remote server nodes. A trustworthy distributed application model is highly expected to cope with such
important issues and ensure the trustworthiness of remote computing environment. A reliable distributed environment is expected to provide authentic access to authorized mobile user for legitimate operations on cloud server nodes. Considering the aforementioned research issues and challenges for distributed application deployment in MCC, lightweight and optimal distributed application deployment solution is extremely important. Such a solution should incorporate optimal procedures for the development, deployment and management of runtime distributed platform for MCC.

G. Shaik Abdullah and B. Muthulakshmi [62] have following finding, the method of applying steganography in conjunction with cryptography, referred to as twin steganography, develops a durable model that adds a lot of challenges in distinguishing any hidden and encoded information. Therefore using steganography within steganography, create to better interpretation of twin steganography which is able to give higher security in cloud.

A Proof Less Public Key Encoding (PL: PUKE) clears the key written agreement drawbacks in identity free-based encoding and certification annulment drawbacks in PU Key cryptography. A tends to (PL: PUKE) design while not exploitation matching operations. Each Data owner first register in the cloud service provider. It can submit Thumb Finger Print and Aadhaar Card Number. Both Finger Print and Andhra Card Number are stored in the Security-as-a-Service (SEaaS).

The Key Provider as a Service (KPaas) to provide key to Cloud data owner. The cloud is applied as safe compute storage as well as Key Creating Center as a Service (KCCaaS). The data owner encrypts the sensitive data using the cloud, KCCaaS making user key (UR Key) based on its data owner public key (PU Key) and upload the encoding data store to the Storage-as-a-Service (STaaS) in the cloud.
Upon successful authorization, the cloud partly decipherment the encoding data for the users by using Security Negotiation Host – as – a - Service (SNHaaS). The users subsequently fully decoding the partially decrypted data using their private key (SEC Key) as well as UR Key. A method for concealment knowledge with two level of security to plant knowledge at the side of sensible sensory activity transparency and high payload capability. A tend to carry out a CL-PUKE theme and the overall cloud primarily based system and assess its security and performance.

GarimaSaini and Naveen Sharma [64] worked for research work titled “Triple Security of Data in Cloud Computing”, in their proposed work they provide security by implementing three algorithm DSA, DES and steganography together to cloud network. To implement these three algorithm we use Asp.net as a platform.

In proposed system for encryption first apply DSA for authentication of data. Then apply AES algorithm for encryption and then hiding data within audio file for provide maximum security to the data.

Receiver can get original plain text by reversing the steganography, AES and DSA. They implements Digital signature Algorithm, Data Encryption Standard and Steganography to provide maximum security in cloud computing.
By implementing these three algorithm provide authenticity, security and data integrity to the data. Then find that the time complexity is high because it is a one by one process but in future this time complexity could be reduced.

Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al. Proposed Cloud AV platform, malware detection system for mobile device by moving detection capabilities to network service or cloud. Zhang et al. Present security framework for elastic mobile application model by dividing an application into easily configurable Weblets. Xiao and Gong proposed scheme for mobile cloud environment to generate a dynamic credential for mobile user for their identity protection from hackers. Wang and Wang8 have proposed privacy preserving framework for mobile devices while using location based scheme by spatial cloaking.
Huan et al., presents framework Mobile Cloud to enhance the functionality of MANET and cover security aspect in terms of risk management and secure routing. G. Portokalidis et al. proposed scheme for threat detection in a smart phone with Mobile Cloud Computing. H. Zhang and X. Mingjun proposed distributed spatial cloaking protocol for location privacy.

P. Zou et al., propose Phosphor, a cloud based mobile digital right management scheme with Sim Card by designing License state word. R. Chow et al. present policy based cloud authentication platform using implicit authentication for solving privacy issues. Itani et al. proposed an energy efficient framework for mobile devices by using incremental message authentication code to ensure integrity of mobile users.

Jia et al., presents proxy re-encryption (PRE) scheme and identity based encryption (IDE) scheme to achieve secure data service.

Huangs et al., proposed secure data processing framework for Mobile Cloud addressing issue of authentication on cloud. Yang ET al. 18 extended the public provable data possession scheme with Diffie-Hellman Key Exchange, Bilinear mapping and Merkle Hash Tree (MHT).

Chen et al. present security framework for location based grouped scheduling services for identity privacy and authentication. Ren et al. proposed three schemes; encryption based, coding based and sharing based to ensure the confidentiality and integrity of user’s file stored at cloud. Zhou and Huang proposed a privacy preserving framework by offloading the processing and storage intensive encryption and decryption on cloud based on Cipher text Policy attribute. Current research initiatives seem to address only one or two parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy. These research approaches favor static security algorithms without considering changing demand for security, quality of service, and resource usage of mobile users.
### Table 2.3 Analysis of Various Security Algorithm

<table>
<thead>
<tr>
<th>Author name</th>
<th>Methodology used</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
</table>
| Liu., Y. Lee, M.J   | The request for using cloud resources by a mobile is classified according to the level of security requirement of a novel resource allocation algorithm proposed. | 1. The problem of resource allocation in a secure way for mobile cloud computing system is formulated with a finite state SMDP under the average cost criteria.  
2. SMDP (Semi Markov Decision Process) is a form of Markov Decision process in which the time of transition between decisions is a continuous time random variable having same probability distribution. | 1. The SMDP-RAS strategy was evaluated in terms of request blocking probability and system reward.  
2. As the arrival rate increases, the system blocking probability becomes higher.  
3. For same arrival rates but increasing number of VMs the block probability decrease.  
4. The system reward increases as the traffic becomes heavier. |
| Liang, H., Huang, D., Cai | 1. The request for using cloud resources by a mobile is classified according to the level of security requirement of a novel resource allocation algorithm proposed.  
2. SMDP based resource allocation model is also described in this paper | 1. The problem of resource allocation in a secure way for mobile cloud computing system is formulated with a finite state SMDP under the average cost criteria.  
2. SMDP (Semi Markov Decision Process) is a form of Markov-Decision process in which the | 1. The SMDP-RAS strategy was evaluated in terms of request blocking probability and system reward.  
2. As the arrival rate increases, the system blocking probability becomes higher. For same arrival rates but increasing number of VMs the |
2. In order to achieve security cloud security services is classified into two categories namely Critical Security Services (CS) and Normal Security Services (NS). CS gives strong security protection but at the cost of consumption of more resources. CS users need to pay more than NS users. | Time of transition between decisions is a continuous time random variable having same probability distribution.  
3. At each step decision is taken regarding accepting the request or not and if accepted then efficient resource allocation for the request. | Block probability decreases.  
3. The system reward increases as the traffic becomes heavier. |
|---|---|---|---|
| Khan, A.N., Mat Kiah, M.L., Khan | 1. Many application providers outsource their database (ODB) because of powerful storage capacity and scalability of cloud. So, a secure framework focusing on location information of mobile terminals is used. | In order to maximize the system reward due to increasing number of CS and NS users, a Security Service Admission Model (SSAM) is proposed.  
2. Semi-Markov Decision process is used to model the system reward | The blocking probability which is an important QoS parameter for mobile cloud is compared for various defined security services.  
2. Blocking probability gets lower as the number of network resources such as Vis increases.  
3. Also blocking probability increases with increase in arrival rate. |
| | 1. LBS security model using ODB based system is framed comprising of users, service providers and cloud databases.  
2. The authentication processor is activated after the verification of user identity and device identity. | | 1. The comparison of different key generation functions indicates the superiority of network coding for small data set as compared to popular hash Functions. |
| Khan, A.N., Kiah, M.L., Khan, | 1. As the resource constraints of mobile devices are limited, the confidentiality of the data to be uploaded on the cloud must be checked.  
2. Most of the available security schemes execute complex security operation remotely on cloud or trusted third party.  
3. An incremental cryptographic version of the EnS, CoS and SnS are compared with original version on the basis of TAT (Turn Around Time) and energy consumption. | 1. To decrease TAT and energy consumption of a file modification operation, the original file is divided into equal sized blocks of \( n \) bits.  
2. Mobile users provide a password which is then transformed decryption and integrity keys. | 1. Performance is evaluated in terms of TAT and energy consumptions for different operations.  
2. For uploading and downloading operations, the system takes more time to complete.  
3. For block modification operation, the proposed methods only encrypt and upload the modified block which in turn improves TAT and energy consumption of the device. |
| Zhou, Z., Huang, D | 1. Due to the browsing of malicious websites, the security of mobile users is at a great threat.  
2. In order to achieve security against | 1. SSE comprises of different components like SSE Service, SSL Verifier, Phishing filter, SSE crawler, URL Service, DNS Service and Storage Service,  
2. Performance is evaluated for false positive and false negative Parameters.  
2. The percentage of false negative of the |
| phishing websites and SSL Strip-based MITM (Man In The Middle) attack anew secure web referral service called Secure Search Engine (SSE) for mobile devices is Proposed. | 2. The crawler picks up an unprocessed URL from the set of URLs in the URL Service and then sends HTTP request. Crawler derives the IP address in the URL with the help of DNS Service and passes them to storage service. | browser reduces as the time frame increases.  
3. The false positive of all the techniques are low and the result from SSE phishing Filters are the lowest. |
2.5 Various Dynamic Energy Saving Algorithm

The method proposed [65] by Mati B. Terefe et. al., differentiates the data intensive and computation intensive components of an application and it performed a multisite offloading in a data and process-centric manner.

A novel model has been presented which describes the energy utilization of a multisite application execution and used a discrete time Markov chain (DTMC) in modeling fading wireless mobile channels. A Markov decision process (MDP) framework has been adopted to develop the multisite partitioning problem as a delay constrained, least-cost shortest path problem on a state transition graph. The proposed EMOP (Energy-efficient Multisite Offloading Policy) algorithm that has been built on a Value Iteration Algorithm (VIA), founds the efficient solution to the multisite partitioning problem. The numerical simulation results reveal that the proposed algorithm considered the different potentials of sites in distributing the suitable components to achieve a lower energy cost for data transfer to the cloud from the mobile. A multisite offloading execution using the proposed EMOP algorithm attained a greater reduction on the energy utilization of mobiles when compared to a single site offloading execution. The performance of the proposed EMOP algorithm has been evaluated in terms of energy saving by comparing the results to a single site offloading execution. The energy consumption of an application has been observed with nodes ranging from 10-150, in single site execution and multi site execution.

From the simulation results, the proposed EMOP algorithm has been found to be an efficient multisite computation offloading approach for mobile devices. It has also been found outperforming the mobile and single site execution with respect to both energy consumption and execution time.
Radhika Loombaa et. al., [66] addressed the trade-off between the quality of the sensed data received by applications and the required energy to transfer data from the mobile handsets, by considering a scheme in which a collaborative sensing middleware intervene between multiple applications requiring sensed data and the mobile handsets located within a particular physical area. An algorithm, Info-Aggregation, has been presented which seeks to maximize the degree to which sensed data transferred from a mobile device can be served to more than one application. The performance has been evaluated in terms of energy consumption. A simulation study was made to assess the performance of the No-Aggregation and Info-Aggregation algorithms, and as a result, the Info Aggregation algorithm effectively reduced the number of active mobile devices and also the volume available for offloading from the sensing environment. The number of applications varied between 50 and 200, varied the number of sensor types requested by applications between 10, 15, 20 and 25, and varied the number of mobile devices present in the environment in the range of 300–1000 in the experiments. Each experiment has been run 30 times using different random number generator seeds. For each test-case the performance of the Info-Aggregation algorithm has been compared with the No-Aggregation algorithm in terms of the gain in mean battery values of all mobile devices, the difference in volume of data available for offloading and the difference in the mean number of active mobile devices in the sensing area during the planning prospect.

The simulation results showed that the number of active devices can be reduced up to more than 50% when sensed data from mobile devices is shared between multiple interested applications.

The mean increase, due to the decreased number of activated mobile devices needed by the Info-Aggregation algorithm to provide the required sensed data to the
applications and to the impact of fewer message transmissions due to the use of aggregation, in cumulative residual energy stored in mobile device batteries at the end of the simulated time interval for the Info-Aggregation algorithm has been compared with the No-Aggregation algorithm. As the number of applications increases this effect is improved, as the same sensor data is requested by multiple applications.

The evaluation showed that the proposed scheduling algorithm, Info-Aggregation, succeeded in delivering a significant improvement in terms of energy utilization in comparison to a technique that does not employ aggregation. It has also been found that the using truncated Levy Walk mobility model mean improves the performance even when devices move around within the physical area to be sensed.

Partially processed apps in the cloud to minimize the overall energy consumption of smart phones will not necessarily save energy if there is no methodical mechanism to evaluate the effect of offloading an app onto the cloud. A mathematical model has been presented [67] by Salwa Adriana Saab et. al., which represents this energy consumption optimization problem. They proposed dynamic minimum-cut algorithm to dynamically solve the problem while taking security measures into account.

They also proposed the free sequence protocol (FSP) which allows for the dynamic execution of apps according to their call graph. The experimental setup is configured with an Amazon EC2 Windows cloud instance with the specifications of 1.7 GB memory, 1 virtual core with 1EC2 compute unit, 160 GB instance storage, 64-bit platform, and moderate I/O performance, a Java server in the cloud, and the modified application has been installed on HTC Nexus One Android smart phone.
The experiment studied the effect of the factors: Workload size, Network type, Computation cost, Security measures such as encryption/decryption and offloading constraints, Signal strength, and Call graph structure. The results reveal that the proposed approach saves battery lifetime and enhances performance. The results also depicts the effects of computation cost, network type, security operations, signal strength, workload amount and call graph structure on the optimized overall energy consumption.

K.Huanget. al.,[68] proposed a set of, schemes for controlling CPU cycles for the model of local computing, time division between MPT and offloading for the other model of offloading and model selection. The CSI and CPU cycle information is used to maximizing the probability of successfully computation given data called computing probability under deadline constrains and minimization of energy consumption. The simulation result shows that the proposed method maximizing the energy saving for offloading.

2.6 ADHOC Based Cloud Computing Modeling

Mobile cloud computing was defined in many ways as presented in many literatures. In [69] Fan defines that mobile cloud computing expands cloud computing with mobility through providing the ability of storing data and processing services on demand by using a cloud computing platform to the mobile devices users. Mobile cloud computing is still in its early stage. So, several problems might be faced when delivering cloud service in mobile environment. Mobile devices native characters resulting in that mobile devices can’t hold complicated applications. In addition, these devices can’t be always online .Various literatures in this field are taken into account to get more understanding, and realizing their ideas in order to create our own idea.
In [70] the authors analyzed running an application for mobile on a remote resource rich server, while the mobile device performs in the vein of a thin client connecting over to the distant (enterprise) server through 3G (e.g. Facebook’s location aware services, twitter for mobile).

Fernando et al., [71] suggested a new approach of mobile cloud computing by utilizing mobile devices to act as resources provider by building up a cloud environment in a peer-to-peer network way. Therefore, the shared resources of the various mobile devices locality will be utilized for offloading jobs to local mobile resources.

A cloudlet concept presented by Quwaider et al., [72] show that the mobile device’s workload is offloaded to a nearby cloudlet. Each cloudlet is consisted of a number of multi core computers that would be placed in common regions such as universities and airports so that mobile devices can benefit the low latency offered by connecting as a thin client to the cloudlet.

Hong et. Al.in14 Explored energy efficiency of mobile devices when transferring data securely over various communication networks including high-speed 4G networks such as LTE and Wipro. We based on the Benchbee speed measurement of Galaxy S2 LTE14 to get our parameters for calculating the time need to transmit a file either via Wi-Fi or via 3G.

Although number of researches in wireless networks [73] have been done in location management, we want to focus on managing and supporting mobility in mobile cloud computing systems. To achieve this, we need to have proper information about the mobile device to find out this device’s recent location if it’s moving away
from or on the way to the range of the cloud. A possible technique could be the infrastructure based methods- that use technology such as Wi-Fi with GPS.

2.7 Security Protocols in MCC

In these context [74], the major leads and the main shortcoming occurs in the mobile cloud computing would be clearly declared. This paper concluded the architecture of the MCC and the main issues that arises in that environment.

In this research, the mobile applications which are integrates within the cloud service and their work survey where defined. By using these mobile applications, there would be some issues occurs due to the openness and also this paper examined the unique approaches to get rid of these issues. The challenges over the mobile cloud service which integrates with mobile applications. IPv6 is the novel version of Internet Protocol next to the IPv4. The features and benefits of the IPv6 are referred in [75].

The next generation of the Internet Protocol (IPv6) is developed to implement and improve the communication between the different networks. This context involved in the research of the IP to move on to the next version named IPv6. The key issues occurred in earlier version IPv4 and the refinement of the issues by the novel version of IPv6 is defined in this paper. The IPv6 have many of the features which acclimatize to the different networks [76] such as wireless, sensor networks, and rooftop networks. The key dilemma of the wireless networks occurs due to its mobility and dynamicity, the mobile cloud service hindrance with the many challenges and issues [77]. To defeat over these challenges the mobile cloud needs a narrative version of Internet Protocol known to be IPv6. IPv6 builds an overlay architecture for a wireless networks [78] to deals with major issues and challenges over the MCC with the assist of IPv6. The major security issues and the security refinement can be clearly defined in the context
The security challenges of various network environments have been overcome by one of the features of IPv6 named IP Sec (IP Security).

The features of IP sec and its application leading have been declared and concluded the IP sec in mobile applications would provide good performance. Ren-Hung Hwang et al., strategy design for IPSec in IPv6 protocol, and established by the network security of IPSec afforded. The performance analysis and the application revelation were examined.

In this paper [80] depicts an investigation of the recital overheads caused by the dispensation and hole necessities of IPSec when defending mobile IPv6 (MIPv6) signalling. Signalling between the mobile nodes and the home agent (HA) in a large-scale reference scenario is considered. The other issues of MCC will be discussed by Michelle X. Gong et al., the link detection within the wireless networks would be clearly defined.

The major involvement of the offered work in this paper was introduced a new approach for a route link detection in wireless networks. The successful hardware implementations using cross-layer approach will extends the battery life of the mobile nodes in the networks.

In the context of [80] the preferred protocols are evaluated on the source of multiple parameters, which include packet delivery ratio, packet loss, network lifetime, and control overhead using variable number of nodes and speeds.

The intention of this paper [81] is to generate classification of the ad hoc routing protocols, and to review and compare delegate examples for each class of protocols. We attempt to expose the requirements considered by the different protocols, the
resource limitations under which they operate, and the design decisions made by the authors.

### 2.8 Cryptographic Algorithms for MCC

Hung-Min Sun et al. proposed dual RSA algorithm and also analyzed the security of the algorithm. The new variants of RSA were presented by them whose key generation algorithms output two distinct RSA key pairs having the same public and private exponents.

Two applications for Dual RSA were blind signatures and authentication. The security of Dual RSA was raised in comparison to RSA when there were small values of \(e\) and \(d\). The main disadvantage of using dual RSA was that the computational complexity of the key generation algorithms was also increased.

P.Saveetha & S.Arumugam worked on the Network Security. According to them the network security as a mean to protect data during their transmission over channel of networks similarly Internet Security also to protect data during their transmission over a collection of interconnected networks in all over the world. Cryptography is the way of hiding information during transmission over a channel. There are lots of cryptographic algorithms available to protect our data from intruders. RSA also one of effective the public key cryptographic algorithm which needs time and memory.

B. Persis Urbana Ivy et al. worked to secure data or information by a modified RSA cryptosystem based on 'n’prime. This is a new technique to provide maximum security for data over the network. It is involved encryption, decryption, and key generation. Prime number used in a modified RSA cryptosystem to provide security.
over the networks. In this technique we used ‘n’ prime number which is not easily breakable. ‘n’ prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this paper we are used a modified RSA cryptosystem algorithm to handle ‘n’ prime numbers and provides security.

CRS Bhardwaj discusses the modification of DES algorithm, which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange. PN Generator produce the infinite random numbers which can be used to modify the DES algorithm to make it more critical to decipher.

The modified encryption of data cannot be deciphered by DES algorithm. It enables you to send the secure data between two computers on private wireless link.

![Security Manager Diagram]

**Figure 2.2 Security Manager**

Shah Kruti R. & Bhavika Gambhava give the principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of
digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection.

The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another.

Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm is introduced here. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

Mary Cindy Ah Kioon et al. analyses the security risks of the hashing algorithm MD5 in password storage and discusses different solutions, such as salts and iterative hashing. We propose a new approach to using MD5 in password storage by using external information, a calculated salt and a random key to encrypt the password before the MD5 calculation. We suggest using key stretching to make the hash calculation slower and using XOR cipher to make the final hash value impossible to find in any standard rainbow table.

Priyanka Walia & Vivek Thapar discusses that there have been significant research advances in the analysis of hash functions in past few years and it was shown that none of the hash algorithm is secure enough for critical purposes whether it is MD5 or SHA1. Nowadays scientists have found weaknesses in a number of hash functions, including MD5, SHA and RIPEMD so the purpose of this paper is combination of
some function to reinforce these functions and also increasing hash code length up to 512 that makes stronger algorithm against collision attests.

Chong Hee Kim improved differential fault analysis on AES key schedule. Proposed advanced encryption standard for which the main target is known DFA. Implementation of AES is known to be vulnerable to DFA which could be split into two categories depending on the fault location that has the DFA on the state and the DFA on the key schedule.

The major limitation is that if the key schedule is not redone for recomputation then it cannot prevent DFA on the AES Key Schedule. The major problem was that if
the key schedule was not done again for recomputation then it cannot prevent DFA on the AES Key Schedule.

Abid Shahzad and Mureed Hussain discusses Security Issues and Challenges of Mobile Cloud Computing. Cloud computing is proving itself an emerging technology in IT world which provides a novel business model for organizations to utilize software’s, applications and hardware resources without any upfront investment. Few years later with the broad development in mobile applications and advancements in cloud computing, a new expansion is being expected in the form of mobile cloud computing (MCC). MCC provides a platform where mobile users make use of cloud services on mobile devices. The use of MCC minimizes the performance, compatibility, and lack of resources issues in mobile computing environment. Despite the astonishing advancement achieved by MCC, the users of MCC are still below expectations because of the associated risks in terms of security and privacy. These risks are playing important role by preventing the organizations to adopt MCC environment. Significant amount of research is in progress in order to reduce the security concerns but still a lot work has to be done to produce a security prone MCC environment. This paper presents a comprehensive literature review of MCC and its security issues and challenges.

Rajkumar Buyya et al. analyze Cloud computing and its aim is to power the next generation data centers and enables application service providers to lease data center capabilities for deploying applications depending on user QoS (Quality of Service) requirements.
Cloud applications have different composition, configuration, and deployment requirements. Quantifying the performance of resource allocation policies and application scheduling algorithms at finer details in Cloud computing environments for different application and service models under varying load, energy performance (power consumption, heat dissipation), and system size is a challenging problem to tackle. To simplify this process, in this paper we propose CloudSim: an extensible simulation toolkit that enables modeling and simulation of Cloud computing environments. The CloudSim toolkit supports modelling and creation of one or more virtual machines (VMs) on a simulated node of a Data Center, jobs, and their mapping to suitable VMs. It also allows simulation of multiple Data Centers to enable a study on federation and associated policies for migration of VMs for reliability and automatic scaling of applications.

Cong Wang et al. Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service.

To ensure the correctness of users’ data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior
works, the new scheme further supports secure and efficient dynamic operations on
data blocks, including: data update, delete and append. Extensive security and
performance analysis shows that the proposed scheme is highly efficient and resilient
against Byzantine failure, malicious data modification attack, and even server colluding
attacks.

Joshi Ashay Mukundrao worked on Cloud computing which is emerging field
because of its performance, high availability, least cost and many others. In cloud
computing, the data will be stored in storage provided by service providers. But still
many business companies are not willing to adopt cloud computing technology due to
lack of proper security control policy and weakness in safeguard which lead to many
vulnerability in cloud computing. This paper has been written to focus on the problem
of data security. Service providers must have a viable way to protect their clients’ data,
especially to prevent the data from disclosure by unauthorized insiders. To ensure the
security of users’ data in the cloud, we propose an effective and flexible scheme with
two salient features, opposing to its predecessors. Avoiding unauthorized access to
user’s data by signaling user by sending message to his/her mobile number at the start
of transaction. Displaying fake information in case of unsuccessful login for avoiding
further login trials by intrusion (Honeypot).

Mohit Marwaha and Rajeev Bedi discuss Cloud computing as it is the next big
thing after internet in the field of information technology; some say it’s a metaphor for
internet. It is an Internet-based computing technology, in which software, shared
recourses and information, are provided to consumers and devices on-demand, and as
per users requirement on a pay per use model. Even though the cloud continues to grow
in popularity, Usability and respectability, Problems with data protection and data
privacy and other Security issues play a major setback in the field of Cloud Computing.
Privacy and security are the key issue for cloud storage. Encryption is a well-known technology for protecting sensitive data.

Use of the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval. The paper analyzes the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage. Xiaorui Chan and Guangzhong Liu [18] had devised one 160 bits improved hash algorithm based on MD5 and SHA1. And in additional, we also introduce four assistant functions named F(X,Y,Z), G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) to do 4 rounds of 16 steps iterative operation with 32-bit data as input and 32-bit as output, saving in A, B, C, D respectively. Then we use one new extending function K(X,Y,Z) to expand 32-bit A, B, C, D to 40-bit. At last, by combining the result from low-bit AA, we realize the 160-bit hash algorithm. By analysis, we have found that: without increasing the time complexity, the improved algorithm has increased the security better compared with MD5 and SHA1 algorithms.

Dr. Smith Jones worked on Cloud Computing that has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering.

The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16 billion in 2008 and will rise to $42 billion/year by 2012. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications. According to a Gartner press release from June 2008, Cloud Computing will be “no less influential than E-business”. Cloud computing evokes different perceptions in different people. To some, it refers to accessing software and storing data in the “cloud”
representation of the internet or a network and using associated services. To others, it is seen as nothing new, but just a modernization of timesharing model that was widely employed in 1960s before the advent of relatively lower-cost computing platforms.

This development eventually evolved to the client/server model and to the personal computer, which placed large accounts of computing power at people’s desktops and spelled the demise of time-sharing systems.

This paper proposes and implement a new algorithmic approach for cloud security using key based cryptography. This work can be enhanced using hybrid approach by integrating multiple cryptography algorithms.

2.9 Energy-Aware Mobile Application Using Scheduling Method

Wei et al. [82] introduced a new model called HLMCM by modifying the cloudlet architecture. HLMCM has low response latency but scheduling becomes a problem. So HACAS algorithm is proposed to solve this problem. The load balancing scheme of this algorithm is 60% efficient than normal scheme.

Shakkeera et al. [83] focused on energy conservation and purposed a new EMACS algorithm to minimize energy consumption in cloudlets.

EMACS make the use of local mobile cloud and has efficient task scheduling criteria. The makespan of EMACS is 70% better than the HACAS and ACO. It also improves average latency, load balancing and resource utilization.

Fernando et al. [84] considered various problems and suggested solutions to tackle them. An architecture is also purposed for mobile computing to improve privacy, security and cost factors. The architecture has three main components: Resource
handler, Cost manager and Job handler. It helps to manage resources, minimize cost and handle jobs easily.

Wua et al. [85] introduced a new algorithm for scheduling. This algorithm sort all the tasks according to their priority and then calculate their completion time with respect to different services. Then it executes the best suited service. This algorithm focuses to improve QoS factor.

Lin et al. [86] proposed a new algorithm to minimizing the energy consumption by mapping the tasks to local cores or by migrating them to cloud. The experimental results show that the energy consumption reduces with a factor of 3.1. It also satisfies the completion time constraint.

Mishra and Jaiswal [87] introduced a new method based on Ant Colony Optimization to improve load balancing. In this method, every node has a pheromone table which stored probability values for all possible destination nodes. Ants refer these probabilities to move to next node and also update its probability values corresponding to their source node. This method helps to separate load among many possible paths in network.

Yamauchi et al. [88] introduced a new methodology for Distributed Parallel Scheduling in mobile cloud computing. In the proposed methodology, a master device monitors some parameters of slave devices and if these parameters come out to be inadequate for performing parallel programming then master device selects other slave devices. This method improves load balancing and considers battery consumption, network quality which in result improves the overall performance of mobile device.
Karthik et al. [89] considered some of the problems of mobile computing and discussed Computation Offloading as a solution to it. In computation offloading, the heavy computations are offloaded to the external resource providers and results are returned back to mobile devices. Future work of different research areas in offloading is also highlighted.

Jaiswal et al. [90] described performance analysis of different cloudlet architectures. The conclusion of this comparison is that VM based cloudlet architecture is more efficient than other architectures.

Suryadevera et al. [91] purposed a new algorithm based on ACO for load balancing. This algorithm calculates pheromone value by considering various parameters. Higher pheromone trail represents shortest path. The pheromone represents the capability of resources to do various computations. The purposed algorithm improved the throughput of the system and helped to improve the overall system performance in grid computing.

Wang et al. [92] presented a survey of mobile cloud computing applications of existing and future generation. The challenges faced while building mobile cloud computing applications are discussed. A survey of existing solutions to these problems is provided and suggested a future search direction of combining trust management techniques to introduce a new method which can enhance QoS and security of mobile cloud computing.

Yang et al. [93] purposed a novel offloading service that helps to offload heavy tasks from mobile handsets to nearby extrinsic resource rich surrogates. The purposed service can efficiently offload the applications if they are implemented in java. The experimental results prove the effectiveness of the service.
Kianzad et al. (2005) use genetic algorithm to integrate task scheduling and voltage scaling under a single iterative optimization loop. Their technique searches the solution space to find an assignment and ordering of tasks on each processing element and generates a schedule such that deadline constraints are met and the power consumption is minimized. Further, their technique distributes the slack proportionately to different tasks and uses DVFS to save energy. They propose techniques for saving energy in both homogeneous and heterogeneous multiprocessor embedded systems. In several multimedia applications, missing some task deadlines can be acceptable since it remains unnoticed to human visual and auditory system.

Hua et al. (2003) utilise this fact, along with the information on statistical task execution time to propose techniques to save energy in embedded systems by dynamic voltage scaling. They have proposed two algorithms. The first algorithm ensures achieving highest completion ratio with lowest possible energy consumption. The second algorithm deliberately drops some tasks to create slack for saving additional energy, such that application-specific quality-of-service constraint is fulfilled. Thus, their algorithms provide opportunity to exercise trade-off between achieving high energy saving and achieving high task completion ratio (i.e., low deadline miss ratio).

Choi et al. (2004b) propose a DVFS technique which enables achieving a precise energy-performance trade-off. Their technique makes use of runtime information about the external memory access statistics and chooses the optimal CPU clock frequency and the corresponding minimum voltage level based on the ratio of the on chip computation time to the off-chip access time. Their technique lowers the CPU frequency in the memory-bound region of a programme to keep the performance degradation to a low value.
Quan and Hu (2001) propose two DVFS algorithms for saving energy in real-time embedded systems. The first algorithm finds the minimum constant speed that can be applied throughout the execution of the whole tasks set, such that the processor is shut down when idle. The second algorithm produces both the constant speed and schedule of variable voltage for minimizing energy. The second algorithm always saves more energy that the first algorithm.

Zhu et al. (2003) propose a technique for saving energy in multiprocessor systems. Their technique allows the processors to share the reclaimed slack which arises from a shorter execution time in one of the processors. Using this extra slack, the speed of future tasks can be reduced which results in energy savings.

They show that sharing the slack also helps in ensuring that all the deadlines are met. They show the effectiveness of their technique for both tasks with dependence (i.e., precedence constraints) and without dependence.

Kan et al. (2010) propose a DVFS technique for saving energy in soft real-time embedded systems. They find the optimal frequency for a task assuming availability of continuous range of frequencies. Afterwards, from the actually available frequencies, the closest frequencies which are smaller and larger than the optimal frequency are chosen and fraction of time each of them should be used to meet the deadline is decided.

They also suggest that difference in average-case and worst-case execution time gives rise to multiple deadlines and hence, if the first deadline is missed, the algorithm can try to meet the next deadline while conserving extra amount of energy.
Yang et al. (2002) propose technique for mapping concurrent tasks onto a heterogeneous multiprocessor platform in an energy efficient manner. On different processors, the execution time and energy consumption of the tasks are different and hence, their technique finds different task-ordering and processor-assignment possibilities, and generates a Pareto-optimal set, where every point is better than any other one in at least one way (i.e., either energy efficiency or execution speed). This information is used at runtime to save energy using dynamic voltage scaling and to find a global energy efficient solution.

Kim et al. (2008) discuss per-core DVFS technique for saving energy in embedded systems. Scaling CPU frequency slows down the CPU-bound operations but has little effect on memory-bound operations and based on this fact, the voltage and frequency are reduced during memory-bound intervals of an application. Their algorithm finds suitable voltage/frequency setting in an offline manner.

Use of on-chip regulators enables fine-grained voltage transitions using which the memory-bound intervals can be more effectively exploited. They also show that per-core DVFS scheme can better exploit the scaling opportunities in the individual threads and thus provides significant improvement over system-wide DVFS scheme. Further, they study the effect of voltage transition time, overhead and regulator losses on the benefit obtained from DVFS.

2.10 Homogenous and Optimal Distributed Platform

Homogenous and optimal cloud based application processing is an important research perspective in mobile cloud computing.
Heterogeneity of SMD architecture and operating platform is challenging for distributed application processing in MCC. Mobile device vendors employ different hardware architecture and operating system platforms for the specific mobile product. Traditional application offloading frameworks focus on the implementation of platform dependent procedures for outsourcing computational intensive loads.

For example, Weblets and MAUI are application offloading frameworks which are applicable for .Net framework, whereas virtualized execution framework and mirror server are suitable frameworks for android platform. Therefore, homogenous access to cloud services are highly expected wherein SMD are enabled to access widespread computing services of computational clouds irrespective of the concerns about operating hardware architecture and operating system platform. A homogenous distributed application deployment solution for the heterogeneous available SMDs platforms is a challenging issue for MCC. It describes important metrics such as heterogeneity, under this tripod which are crucial for the success of cloud mobile applications.

Similarly, the deployment of distributed application processing platform at runtime is a resources intensive mechanism. It uses computing resources on SMDs for the evaluation of computing resources utilization on SMDs and partitioning of intensive mobile applications at runtime. Current, approaches necessitate continuous assessment of application execution requirements on SMD which is a resource intensive operation.

Application Processing Framework employs runtime profiling and solving mechanism on SMDs periodically or casually to evaluate application processing requirements and the availability of computing resources on SMD.
The centralized distributed application deployment models require arbitration of SMD with centralized server for the selection of appropriate server node. As a result, computing resources (CPU, battery power) of SMD are exploited abundantly for the entire process of application profiling and solving. The deployment of distributed platform, management and operation of remote application processing in the optimal possible fashion is an important perspective of cloud based application processing. It is challenging to provide homogenous solution for heterogeneous devices, operating platforms and network technologies with minimum possible resources utilization on the SMDs.

2.11 Computing Issues in MCC

In mobile devices offloading the multimedia code increases the time for playing games by saving energy. Cuervo et al. [94] proposes a system that enables fine-grained energy aware offloading of mobile codes to a cloud. It is found that instead of offloading all codes to the cloud for processing, MAUI partitions the application codes at a runtime based on the costs of network communication and CPU on the mobile device to maximize energy savings given network connectivity. The results demonstrate that MAUI not only helps energy reduction significantly for mobile devices, but also improves the performance of mobile applications.

It is found that offloading the code is not always effective for saving energy. For a code compilation, offloading might consume more energy than that of local processing when the size of codes is small.

A framework was proposed by Li Z et al [95] to facilitate task partitioning, in which a program is divided into server and client tasks. Statically, under our execution model, a task corresponds to a procedure (or a function) call site. Dynamically, a task is
a single invocation of the corresponding procedure. After the partitioning, all the tasks
mapped to the same host can share the program state as they do in the original program.

The issue of coherence arises, however, when one deals with data shared
between two tasks which end up in different hosts. At the present, we maintain the
program state coherence in a conservative way. A piece of data can be shared by both
hosts only if the program transformations and message passing can guarantee the
correct dependence. Implementation of remote execution is predicted and we must
predict when the cost of performing remote execution will not outweigh its benefits.
The cost of a remotely executed operation consists of the time to transfer data (and
possibly code) from the device to the target, the time to transfer result information, e.g.,
data, status, rendered graphics, etc., from the target back to the device, and the time to
execute the operation at the target. The cost of a locally executed operation is the local
execution time. These costs can be decomposed or translated to consider other metrics,
e.g., battery consumption, response time, application fidelity. However, regardless of
their form, these values must reflect what the costs will be when the operation is
eventually performed.

A new framework was proposed and it was consists of three components [96]:
the mobile hosts, base station and a wireless channel. It is assumed that the server is
AC-powered and has a much larger computational capability than the client. We also
assume that the client services only its own local tasks and receives no request for
remote processing from the server.

This is a reasonable assumption since the AC-powered high performance server
is much more powerful from a processing point of view and has no energy limit, and
thus it will execute its own tasks (in addition, it will execute tasks sent to it by the mobile hosts.

This also means that the server has all the hardware and software resources required to execute the tasks that are sent to it by the remote clients. Furthermore, for the same reasons, the server does not turn down any request for remote processing. Dynamic offloading environment can cause additional problems due to changing connection status and bandwidth.

The analysis of performance in offloading in wireless environments [97] three cases was taken in executing an application, thereby estimating the efficiency of offloading. They are the cases when the application is performed locally (without offloading), performed in ideal offloading systems (without failures), and performed with the presence of offloading and failure recoveries. In the last case, when a failure occurs, the application will be offloaded. This approach only re-offloads the failed subtasks, thereby improving the execution time. However, this solution has some limitations. That is, the mobile environment is considered as a wireless ad hoc local area network (i.e., broadband connectivity is not supported). Also, during offloading execution, a disconnection of a mobile device is treated as a failure. Mobile devices already have wireless communication capabilities, and we expect most future systems to have such capabilities. There are two main differences between mobile and desk-top computing systems, namely the source of the power supply and the amount of available resources.

Mobile systems operate entirely on battery power most or all the time by Kremer U et al [98]. The resources available on a mobile system can be expected to be
at least one order of magnitude less than those of a “wall-powered” desk-top system with similar technology.

This fact is mostly due to space, weight, and power limitations placed on mobile platforms. Such resources include the amount and speed of the processor, memory, secondary storage, and I/O.

In implementing MAUI, Kremer U et al [98] discovered a number of unforeseen challenges to implementing program partitioning for mobile applications. One such challenge is that using power-save mode (PSM) when transferring state remotely can hurt the overall energy consumption of the application when the latency to the server is low. Moreover, PSM mode helps save energy but only when latencies approach the sleep interval (today’s hardware uses 100 ms). Another unforeseen challenge is related to using profiling to estimate the energy savings of code offload. On one hand, profiling the state transfer overhead of a method each time it is called can provide the freshest estimate; on the other hand, the cost of this profiling is not negligible and it can impact the overall application’s performance. Power dissipation has become one of the crucial design challenges of current and future computer systems. In a mobile environment, power savings are important to prolong battery life. Power and energy management addresses both of these issues. However, in the context, prolonging battery life is the main objective.

2.12 Routing Protocols in MCC

Table driven routing protocols are also known as proactive routing protocols. In this protocols network topology information is kept in routing table regardless of any use of it. Sometimes this information is useful for datagram traffic.
The routing tables need to be updated periodically whenever there is fluctuation in network topologies. This is difficult for any large network where different protocols need to maintain many number of routing tables. DSDV, WRP, OLSR are few examples for proactive routing protocols.

Bellman ford algorithm [modified slightly to develop DSDV protocol. DSDV routing protocol keeps routing table for each mobile node in the network. Routing table consists of topology information such as all available destination nodes and the number of hops for each node. Each routing table contains sequence number which is evolved from destination node. Updating routing information helps maintaining routing information of topologies. This updating might be either event driven or periodic. This is done by advertisement which may be done by broadcasting or multicasting periodically. DSDV protocol fails to work efficiently for fluctuating topologies.

Wireless routing protocol is path finding algorithm [101], it calculates the paths considering the information mentioned by nodes. Every node keeps four things for the purpose of routing which are a distance table, link cost table, routing table and message retransmission list (MRL). The wireless routing protocol uses the updates to transmit messages. MRL should acknowledge to response list. If there is no alteration of last update, then response list node should send an idle message to ensure its connectivity. A node itself can monitor whether to update its routing information after receiving updates from next neighbor node and it will always choose better path using new updates.

Cluster gateway switch routing [102] protocol (CGSR) operates by considering a clustered mobile wireless network. By developing several clusters distributed
processing mechanism is achieved however it is difficult to implement when there is frequent change or selection of cluster heads.

Dynamic source routing protocol (DSR) [103] is a simple reactive routing protocol skilled to utilize multi-hop mobile ad hoc network. Completely SON and self-configuring network enabled by use of dynamic source routing protocol without any base infrastructure. Route discovery and route maintenance are the two steps carried out in this protocol. First mechanism route discovery by which a source node willing to send a packet to a destination node. Route Discovery is used only when source attempts to send a packet to destination and does not already know a route to Destination. Second route Maintenance is the mechanism by which source node is able to detect, while using a source route to destination node, if the network topology has changed such that it can no longer use its route to destination because a link along the route no longer works. When Route Maintenance indicates a source route is broken, source can attempt to use any other route it happens to know to destination, or can invoke route discovery again to find a new route. Route Maintenance is used only when source is actually sending packets to destination.

ABR [104] protocol characterizes another kind of routing parameter "degree of association stability" for ad hoc network. In this routing convention, a route is chosen taking into account the degree of association stability of MANET nodes. Every node occasionally produces signal to declare its presence. After getting the signal message, a neighbor route refreshes its own routing table.

For every beacon each nodes are marked such that they are static and other nodes are reset when they travel out of neighboring range. This property of degree of association stability is difficult during when there is large network.
Battery preservation is one of the principle challenges for mobile gadgets and a level battery separates the user from MCC use. In the literature, a few proposed arrangements have been exhibited. The arrangements were intended to deal with the screen and the circle insightfully and to enhance CPU executional in endeavor to lessen power utilization. In any case, the proposed arrangements may be infeasible now and again, and the required equipment speculation is generally too high.

MCC is intended to permit the users a consistent service independent of area and time. Notwithstanding, assets, battery and network requirements are famous. With these limitations, computationally serious operations, for example, sensor use for GPS perusing, broad processing in computer games, discourse amalgamation, wearable computing and normal dialect processing has been unsuccessful. As indicated by previous works, the difficulties of MCC can be arranged into operational, end user, service level, privacy and security, connection mindfulness, and data management issues. At the point when a battery goes off, the user can't get to the MCC services, prompting low quality of service, refusal of service or an aggregate downtime.

Offloading is utilized to accomplish a stretched battery life, whereby applications requiring long execution time are processed on the cloud and conveyed on the mobile gadgets for power protection. The viability of offloading techniques to spare battery power of versatile gadgets has been assessed in previous works. The outcome uncovers that remote execution of complex errands can lessen power utilization by half.

The 915MHz AT&T Wavelon card was the wireless gadget utilized, propelled power management (APM) apparatuses were utilized, three applications were utilized as experiments and it was led on a Dell scope XP compact computer on Linux operating system.
The remote execution systems use complex expectation methods that aide computational offloading for proficient asset enhancement. An effective power management is accomplished by strategy streamlining utilizing a straight programming approach.

Likewise, the hypothesis of Markovian choice processes was utilized for great errand movement and remote processing to accomplish amplified battery life.

T. Xinget al., created Power Scope as a profiling apparatus for mobile applications, keeping in mind the end goal to dissect power depleting methodology; the instrument can help designers to change their software to be more successful in energy preservation. Utilizing Power Scope, 46% energy preservation was accomplished profiling a versatile video application running on Odyssey stage. After data gathering, profiling is done disconnected to dodge expansion of overheads to the examination. Battery levels can be questioned by software as done by Powers Spy, in windows OS it does two operations; occasion following (application run and followed for CPU time) information or yield action and energy utilization investigation stage (data obtained from occasion following is processed).

2.13 Data Storage Techniques in Cloud

A. Implicit Storage Security to Data in Online:

Providing implicit storage security to data in online is more beneficial in a cloud computing. The use of a data partitioning scheme for implementing such security involving the roots of a polynomial in finite field. In this scheme data is partitioned in such way that each portion is implicitly secure and does not to be encrypted. These portions are stored on different servers on the network which are known only to the user. Reconstruction of the data requires access to each server and the knowledge as to
which servers the data portions are stored. Several versions of this scheme are described, which include the implicit storage of encryption keys rather than the data and where a subset of the partition may be brought together to recreate the data.

B. Identify –Based Authentication:

An identify based encryption (IBE) and decryption and identity based signature IBS schemes for IBHMCC. Resources and services are distributed across numerous consumer. So there is a chance of various security risks. Therefore authentication of users as well as services is an important requirement for cloud security. When SSH Authentication protocol (SAP) was employed to cloud, it becomes very complex. As an alternative to SAP, proposed a new authentication protocol based on identity which is based on hierarchical model with corresponding signature and encryption scheme. Identify based authentication protocol constrains sequence of steps. In step (1) the client C sends the servers a client Hello message. The message contains a fresh random number Cn. Session identifier ID and c specification. In step (2) the server S responds with a server Hello message which contains new fresh random number Sn.

C. Public Auditing with Complete Data Dynamic Support:

Verification of data integrity at unreliable servers is the major concern in cloud storage with public audit ability trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to access the risk of outsourced data when needed.

It also provides a transparent yet cost effective method for data owners to gain trust in the cloud. To accomplish, dynamic data support, the existent proof read of PDF (or) POR scheme is improved by spoofing the basic Markel Hash tree (MHT).
D. Efficient Third Party Auditing (TPA):

Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. The data owners having huge amount of outsourced data and auditing the data correctness in a cloud environment can be difficult and expensive for data owners. To support third party auditing where user safely delegate in integrity checking tasks to third party auditors (TPA)[2] this scheme can almost guarantee the simultaneous localization of data error (i.e. the identification of misbehaving servers). A novel and homogeneous structure is introduced to provide security to different cloud types. To achieve data storage security, BLS (Bonch-Lynn-Sachems) algorithm is used to signing the data blocks before outsourcing data into cloud. Reed Solomon technique is used for error correction and to ensure data storage correction.

E. Way of Dynamically Store Data in Cloud:

Data storage is cloud may not be completely trustable because the clients did not have local copy of data stored in cloud. To address these issues proposed a new protocol system using the data reading protocol algorithm to check the data integrity services providers help the clients to check the data security by the proposed effective automatic data reading algorithm.

A flexible distributed storage integrity auditing mechanism (FDSIAM), these mechanisms utilizes the homomorphism tokens, blocking erasure and unblocking factors and distributed erasure coded data

F. Effective and Secure Storage Protocol:

Current trend is users outsourcing data into service provider who have enough area for storage with lower storage cost. A secure and efficient storage protocol is
proposed that guarantees the data storage confidentiality and integrity. This protocol is invented by using the construction of elliptic curve cryptography and sober sequence is used to confirm the data integrity [2]. Data and software process protocol step executed by cloud customers to add the privacy enforcement structure to the software and data before transferring them to the cloud. Challenge response protocol is protocol is credential so that it will not exposes the contents of the data to outsiders. Data dynamic operations are also used keep the same security assurance and also provide relief to users from the difficult of data leakage and corruptions problems.