Mobile Cloud Computing: Issues, Applications and Scope in COVID-19

Hariket Sukesh Kumar Sheth[1[0000-0001-5283-7716]], **Amit Kumar Tyagi**[2,3[0000-0003-2657-8700]]
[1,2] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamil Nadu, India.
[3] Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamil Nadu, India
shethhariket@gmail.com, amitkrtyagi025@gmail.com

Abstract. As the world is transitioning into a tech-savvy era, the twenty-first century is evidence of many technological advancements in the field of AI, IoT, ML, etc. Mobile Cloud computing (MCC) is one such emerging technology, providing services regardless of the time and place, contours the limitations of mobile devices to process bulk data, providing multi-platform support and dynamic provisioning. Not only there is an enhancement in computation speed, energy efficiency, execution, integration, but also incorporates considerate issues in terms of client-to-cloud and cloud-to-client authentication, privacy, trust, and security. Reviewing and overcoming addressed concerns is essential to provide reliable yet efficient service in nearing future. Mobile Cloud Computing has the potential to bring wonders in the fields such as education, medical science, biometry, forensics, and automobiles, which could counter the challenges faced in the ongoing COVID-19 Pandemic. To combat the prevailing challenges due to COVID-19, it has become critical that more efficient and specialized technologies like Mobile Cloud Computing are accepted that enable appropriate reach and delivery of vital services by involving gamification, cloud rendering, and collaborative practices. This paper provides a detailed study about MCC, mitigated security and deployment attacks, issues, applications of MCC, providing developers and practitioners opportunities for future enhancements.

Keywords: Mobile Cloud Computing; Data Processing; Security; Authentication System; Issues in MCC; COVID-19; Smart Applications.

1. INTRODUCTION

Cloud Computing is an ever-growing technology, incorporating the potential to attract most organizations because of its incomparable efficiency to provide services like Virtual Machines, storage custom networks, Middleware, and resources to their customers and users. Now the question arises, how Mobile Cloud Computing is different. Entitling Mobile Cloud Computing

(MCC) as an inheritance of Cloud Computing would not be wrong. Incorporating the services offered by Cloud Computing, with the presence of a Mobile Computing Environment, MCC has proved to be the potential technology of the future. The Cloud Services are made available via wireless media, responsible for successful communication between mobile devices and clouds. There is a need for interfacing between Mobile Devices and Cloud so that the computational phases of any application can be offloaded and resources are received whenever re-quested. MCC is not only smartphone-specific but is implementable for a wide range of devices. [1]. It enables the delivery of applications and services from a remote cloud server or environment. The spike in the number of mobile users and contouring the issues faced in mobile devices like slow processing power, limited storage space, low bandwidth – MCC anticipates reaching USD 118.70 billion by the end of 2026, recording a compound Annual Growth Rate (CAGR) of 25.28% during the forecast period (2021 - 2026) [2]. Mobile computing involves how mobile devices learn the context related to their mobility and networking, access the Internet in an ad havoc communication environment. Despite the benefits offered by MCC, the proportion of new users switching to this technology is not equivalent and comparatively less. Since the world is now transitioning to an era where paradigms such as IoT, and Artificial Intelligence (AI), are consistently researched for integrating with mobile computing technologies, it is the need of the hour to review the challenges, issues, and solutions that are being addressed and proposed till date. The foremost reason for the same is crucial issues in disciplines like Client-To-Cloud and Cloud-To-Client authentication, security, communication channels, and protecting resources. Apart from this, there is a need for ensuring QoS (Quality of Service) provisions, standard protocol, signaling, Context-Aware Mobile Cloud Services, and Service integration.

2. MOTIVATION AND STRUCTURE OF WORK

Artificial Intelligence, IoT (Internet of Things) integration with Mobile Cloud Computing can propose solutions for real-world problems. Additionally, give practical solutions in the ongoing COVID-19 Pandemic in various sectors such as Healthcare, Education, logistics, management by addressing the research gaps, comparing the solutions proposed till now, and analyzing the contributions made in this field. The structure of this paper is as follows: Section 3 would be discussing the applications of Mobile Cloud Computing (MCC) in various domains. Section 4 would be highlighting the implementation of various models for the discussed applications. Section 5 would be stating the current challenges and issues faced in MCC and the solutions given to challenges by other researchers. Sections 6 would be discussion on the scope of Mobile Cloud Computing in COVID-19 Pandemic in the mentioned applications. In Section 7, the authors would be concluding the paper, along with highlighting the research gaps and topics for future research.

3. APPLICATIONS OF MOBILE CLOUD COMPUTING

The number of databases can make it difficult to find accurate and appropriate information from the available resources. Even when we have well-defined needs, they may not be accessible from our current location, with mobile cloud computing, access to any database with an internet connection, and a device that supports cellular data or wifi where available.

- **Blockchain:** Specifically, in this pandemic time, we have witnessed a transition to Electronic Health Records (EHRs) [4] [5] rather than the traditional printed Medical Reports on mobile cloud environments. This new shift also raises concerns about data privacy and network security. We have frameworks that combine blockchain and decentralized interplanetary file systems (IPFS) [3] on a mobile cloud platform. Using Ethereum blockchain with Amazon cloud computing can provide an effective solution for reliable data exchanges on mobile clouds, eliminating the need for specialized and centric storage systems.

- **Artificial Intelligence (AI):** Artificial Intelligence (AI) tools handle large workloads and, organizations are selling products with improved abilities, enabling users to access inordinate functionalities of the software. Integrating AI with the cloud-based application will suggest services based on a behavioral study. Provide live and automated services like chats and emails, prediction of user tone.
  Cloud-based AI is an asset enabling many organizations to deliver the utmost in this digitalizing era.

- **Internet of Things (IoT):** Mobile IoT Cloud Computing is the intersection of fields like Cloud Computing, IoT Cloud Computing, IoT, Mobile IoT Computing, Mobile Computing, and Mobile Cloud Computing [6]. IoT follows the principle of multiple data offloading schemes to increase smartphones, devices applications performance, energy efficiency, and execution support. Machine Learning-Based Mobile Offloading Scheduler (MALMOS), [7] having a novel approach to using online machine learning algorithms. It assumes attributes as independent of each other and also has a drawback of biasing towards earlier observations. The computing models proposed for the MCC can not only be limited to the field of IoT. It also extends to branches such as Nano Things (IoNT) and Under Water (IoUW).

- **Internet of Mobile Things (IoMT)** – IoMT is one abused, misunderstood thing. As previously mentioned about Mobile IoT Cloud Computing – IoMT deals with challenges faced by devices such as mobiles, smartphones, smartwatches, and wearable technologies put forward. Such mobile devices include smartphones, vehicles, wearable devices, and smartwatches. Internet of Mobile Things [8] is mainly referred to as the Internet of Moving Things [9], Internet of Medical Things [10], Internet of Multimedia Things [11], and the Internet of Manufacturing Things.

- **Machine Learning:** Machine learning and the code offloading mechanism in the Mobile Cloud Computing concept enables the operation of services to be optimized, among others, on mobile devices. This technology will enable hybrid applications to be built with code transfer that runs on different operating systems (such as Android, iOS, or Windows), which decreases the amount of work required from developers, as the same code is executed on a mobile device and in the cloud.

- **DevOps:** App Development faces challenges such as handling multiple screen sizes and variant operating systems. Deployment of apps with cross-functional capabilities by transferring program data and moving servers on the cloud. Both the Development and Operations team processes can be tremendously speeded up.
  The storage capabilities with added computing power have played a vital role in the advancement in app development. There are several pros of using MCC like Multi-Platform Support for Cloud-based applications, Faultless integration of database, expeditious app development, Comprehensive Data Recovery and, secure data storage.

- **Healthcare:** Healthcare and patient care are very important applications to be adapted via the mobile cloud computing approach. The shifting from traditional healthcare model to consumer-driven healthcare model is a very important aspect of this approach in which is moving forward to establish a direct private connection to the consumer patient model. This approach achieves a respectable performance of healthcare services anytime anywhere for both privacy and security of protecting the confidential information of the consumer (patient). This issue opens a new future field of computing that lacks resources, including flexible architecture, adapted protocols, real-time processing, huge storage, online services, privacy, and security.

- **Education:** Mobile cloud computing system that has widespread applications in the Educational Domain. Mobile cloud computing will help students, teachers, staff, and also learners from rural areas. Mobile cloud computing is changing how students are learning. Applications can be created in a form that can be used with smartphones and hence enabling students to access the learning module in a quicker and faster way with this cloud computing system. This modern technology encourages students and helps them to meet their academic goals. Various Institutes are benefiting from cloud computing due to its low cost, easy monitoring of data, centralized storage of data, and universal accessibility. The Mobile Hybrid Cloud discussed above provides versatility and improved overall security and reliability which is a must in mobile cloud computing.

4. MOBILE CLOUD COMPUTING MODELS

After the discovery and evolution of personal computers, Mobile Cloud Computing is one such paradigm that has changed how data is stored and shared. It disregards the process followed by the traditional computational models (Distributed Computing), Von Neumann Architecture, and Turing machines. The present proposed computing models are human-machine and machine-

machine interactions based. Even though it is future technology, MCC capital costs are more or less the same as estimated for the traditional computational systems. Combining the plethora of fields catering to accessibility, authorization, accounting, and efficiency, amalgamizing wireless web technology, cloud, and mobile processing.
In MCC, the data from the mobile devices intended to be sent to a cloud-based platform is moved to a central processor via a base Transceiver. Similar to the Version Control technologies present like Git and BitBucket, information about user identity, location, and network statistics and routes are stored and maintained. MCC thus ensures the maintainer to have an appropriate check on the authenticity of the changes being made. Before any transfer, MCC also certifies that a legible copy of the data files sent over the channels is created (which are used for re-transmission / transfer faults). As explained in Figure 1, MCC extends its services by catering to authorization, accessibility, accounting, and efficiency.

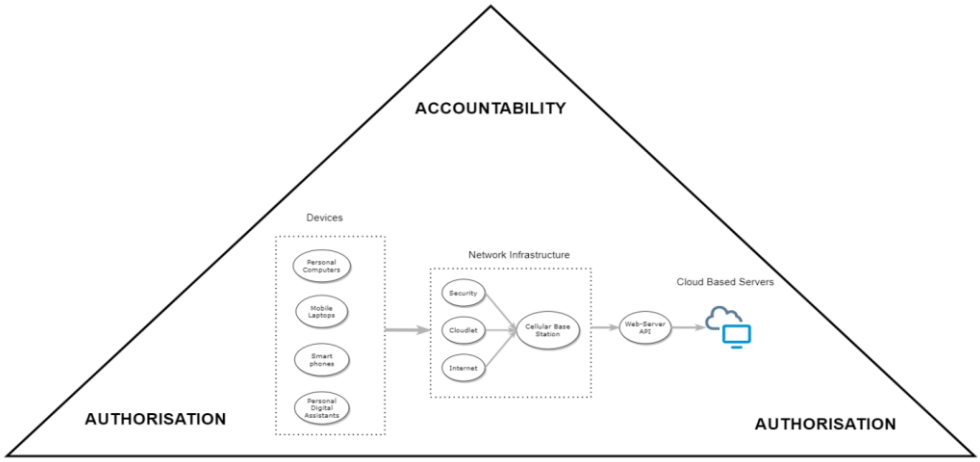

Figure 1: Mobile Cloud Computing Infrastructure

4.1. Service and Deployment Models:

4.1.1 Service Models

- **Infrastructure as a Service (IaaS):** IaaS provides access to resources like networks, data storage, and computers. However, the user is not authorized to have control over the resources or any sort of deployment. These are the basic building blocks of the cloud. It allows the user to pay only for the resources utilized and have limited control over the network components.

- **Platform as a Service (PaaS):** It grants resources for the development and management of applications. User is allowed to access these resources by Programming Language, tools, libraries, and services. It includes testing and deploying the software application. It facilitates the users to not focus on the underlying architecture.
- **Software as a Service (SaaS):** SaaS is a software application delivery to the end-users. SaaS focuses on an easily reachable application that is accessed from web browsers or any program interface. In this service, a user is not supposed to be concerned about the architecture and maintenance of the underlying infrastructure.
- **Virtualization:** It is the procedure of decoupling the hardware from the system on the machine. Virtual machines are the illustrations of the physical machines, which are maintained to run on some host by the monitor software or a hypervisor [7]. These hypervisors are responsible for implementing virtualization on the physical machine, and it can be of one or two varieties. Variety 1 type hypervisors are native hypervisors that run on bare metal or can directly control the host's hardware and monitor the guest operating systems. On the other hand, type 2 types of the hypervisor are hosted hypervisors and run within an environment of OP.
- **Computing as a Service (CaaS) –** In this, the main focus, is on investing less on the hardware related services and rather opt for the services structured and designed according to your needs and requirements. Hence, computing as a Service gives the real essence of the cloud based computing systems, removing the hassle of any sort of maintenance and installations but at the same time availing a lot of features and benefits. In this, the computations are handled on the virtual servers. For ex: EC2 service. [27]
- **Security as a Service (SECaaS) –** Security as a service is simply a model in which an external organization or third-party service is responsible for handling and managing the security of the services offered by the host. SECaaS is suited best for the corporate infrastructures and provides subscription-based services. SECaas outsources cybersecurity services along with added advantages such as getting the latest security tools, Identity and Access Management (IAM) , Security Information and Event Management (SIEM). [28]

4.1.2 Background Models

Public Cloud: Public clouds are owned and managed by third-party cloud service providers delivering their resources like storage and servers. The software, hardware, and other infrastructure are owned and controlled by the cloud service provider. The user can use the services by logging into their account on a browser.
Private Cloud: Resources are utilized mainly by an organization or a company. The resources can be limited to an on-site data center for that particular company. The private network is responsible for the Maintenance of the complete infrastructure.

Hybrid Cloud: Public and Private Clouds are combined and bound together using technology enabling data and applications sharing. Such a combination in hybrid clouds offers more flexibility, deployment options, and efficient optimization of resources.

5. CHALLENGES IN MOBILE CLOUD COMPUTING-BASED SYSTEMS

Mobile Cloud Computing broadly focuses on offloading the two vital processes of data processing and data storage. The issues are specifically in energy, QoS (Quality of Service), application, and Security. Because of the numerous advancements in MCC, industries and a wide range of sectors are resorting to MCC. Nevertheless, of the benefits, MCC brings a substantial increase in the number of security hacks, breaches of data privacy, malicious attacks. Any attack intended on the Cloud systems/architectures with malicious intentions to access the resources illegally or without proper permission, acquiring unsecured data, modifying or deleting the resources, etc are termed as cloud attacks. Figure 2 broadly specifies the challenges faced by MCC.

5.1 Analysis of Issues in Mobile Cloud Computing

1. Issues related to Energy: The cause of these issues is mostly the low battery lifetime. Mobile Devices aren't efficient in terms of energy. The solution proposed for dealing with the issues raised was to offloading specific complex computational tasks. Specific frameworks are adopted where the devices offload such tasks by dynamically resorting to the application content, with the use of Virtual Machines using the concept of virtualization and parallelization [13]. The frameworks were tested for different types of networks were in the results were recorded and analyzed based on the performance metrics set.

The models proposed by the authors of Dynamic Energy-aware Cloudlet-based Mobile cloud computing model for green computing [14], Mobile Cloud offloading Architecture (MOCA) [15], and Performance Evaluation of Remote Display Access for Mobile cloud computing (PERDAM) [16] have addressed the issues of low computation power, issue of remote display access, restrictions of wireless bandwidth and latency delays. The authors of [14], [15], and [16] implemented and proposed solutions for the above-mentioned issues by giving an implementation on the lines of setting up AlterNet, Testbed, user-developed simulator (DECM-Sim), and OpenStack Cloud Platform.

2. Issues related to Security: Security and Privacy are some of the most abused words used in the literature because it is misapprehended. Security mainly covers maintaining confidentiality, integrity, and availability whereas, Privacy only concerns access to personal information and ensuring data quality. The Mobile Cloud Computing issues are further divided into Cloud Data Center Security, Mobile Data Security. Authors of [17], [18] have discussed extensively, the RMTAC, EACDAC, and PADMC, the issue stressed out by the authors of the mentioned contributions and related to Lack of Proper system for authentication, absence of fine-grained secure access.

3. **Security issues related to Dynamic Offloading:** Offloading is the formal process of transferring the computational tasks that are complicated and hard to handle on the web servers. In [18], the author has evaluated the cost by taking execution time as one of the primary parameters consumed in making the offloading decision. The cons in the proposed models are that offloading disregards the status of both the device and the cloud. Even though security is disregarded in [18], but it enhances mobile device resource consumption. The computations are classified such that the trusted cloud is mainly used for critical operations, whereas requests to the offloaded data are processed in parallel by the modified cloud on encrypted data. The research paper [19] focuses on the fundamental issue of deployment decisions, Battery life of the mobile device. Experiments on Android devices for individual components were performed.

5.2 Mobile Cloud Computing Protocols

The challenges faced by MCC are summarized in Figure 2 as well:

- Multifactor Authentication
- Client to Cloud Authentication
- Encryption key, Data Security
- Privacy
- Cloud to Client Authentication
- Denial of Service (DoS)
- Unsecure Protocols
- Attacks Related to IaaS
- Internal and External Attacks
- VM (Virtual Machines) Attacks

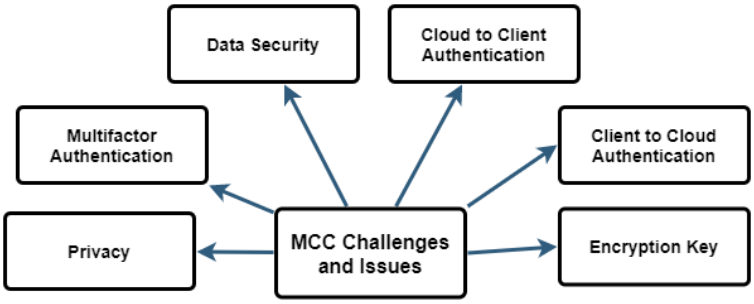

Figure 2: Challenges faced by Mobile Cloud Computing

1. **Hyperjacking:** Hyperjacking is a type of Virtual machine attack (VM Attack) that is very rare, but has the potential of creating great havoc to the virtualized environment and servers. Because of the fatal effect, Hyperjacking can have on the system, it is considered a real-world threat. In hyperjacking, the Hackers /Attackers gain complete control over the processes and activities happening in the virtualized cloud environments by targeting the vulnerable hypervisors. If the attacker succeeds, then all the services associated with the Hypervisor would be affected and can be manipulated. Hence, Hypervisor is one of the foremost issues in which the researchers should stress more upon.

2. **Denial of Service (DoS) Attacks:** A method is proposed in [20] that considers the advantages and pros of Virtual Machines (VM's) along with the CPU. This method identifies the Denial of Service (DoS) attacks and in data cloud centers. The information entropy mentioned by the authors in [20] needs to be applied in the monitoring stage to stay updated about the malicious Virtual machines. Such malicious Virtual Machines exhibit a particular VM status, which is similar to launching a DoS attack. Distributed DoS Attacks (DDoS), where the conventional traffic of the virtual environment is disturbed by overburdening the server by transmitting an immense amount of spam or bogus data, resulting in a DoS attack

3. **Cache Side-Channel Attacks (CSCA):** A cache attack is a kind of side-channel attack, which uses the time information leaked at the interface. The CSCA attack is system-centric rather than an attack. Any protocols/algorithms used for ensuring the security and privacy of the data transmitted. [21] For the CSCA attack, the intruder or the hacker needs to have a good idea about the internal architecture of the system. Even though various mitigation techniques are proposed or implemented, the probability of facing a CSCA attack remains the same. Processor caches are often shared globally or used by multiple cores. Processor caches consider the execution time taken by the cache. It tends to bypass some of the essential common security isolation mechanisms. [21]

4. **Internal and External Attacks:** An attack executed by a cloud service provider, customer, or third-party provider, basically anyone authorized to access the system. Internal attacks can also occur because of any existing privileges given to the users in the near past, who are directly / indirectly dependent on third parties for the task execution. It can pose critical threats like Data Leak, etc. Internal attackers do not resort to similar or one type of attacks, making it difficult to build a robust system, safe from all such attackers. The range of attacks can be from accessing sensitive or private data, overwhelming the servers, and introducing viruses in the network. Internal Attacks like DoS, ICMP, and UDP Flood Attacks are becoming prominent. External Attacks are the vulnerabilities where the attackers get unauthorized access over the resources from the outside environment.

5.3 Analysis of MCC Security Models Proposed

The open issues and challenges faced in the MCC (Mobile Cloud Computing), are broadly mentioned in sub-section 5.2. The security models proposed by the authors will be summarized and discussed in this section. A free-pairing incremental re-encryption model mainly revolves around certificateless file modification operations. In this model, all the users are allocated a specific partial secret key. The data owner further generates a Full private and public key. Encrypted EHR is sent and uploaded to the cloud. If the user requests downloading the EHR, it is fetched from the cloud using the private key. Decryption starts once the data is received. The proposed scheme in [24] is an improved model for Tsai et al's protocol. [24] gives a robust authenticated key agreement protocol in the formal security analysis. Tsai et al's proposed protocol has some the vulnerabilities, such as more probable desynchronization and server-based attacks. In [25], the main contributions are for maintaining the integrity of the data and ensuring data security. Outsource ciphertext attribute-based encryption (SO-CP-ABE) scheme and the probable data possession (PDP) scheme.

The model proposed in [26] uses the IMEI Number of mobile devices for authentication. One of the most common issues faced in the MCC is experiencing an overhead of communication. [26] delegates extensive tasks to the cloud and complex methods, which becomes the main reason for communication overhead between the mobile device and the cloud.

Authentication is one of the open challenges to MCC. Some of the security models have completely excluded the use of the Authentication module. Recent models focus on adopting only one dimension for authentication. But a potential issue in adopting to one dimension level of authentication, the mobile devices to overcomes their resource capabilities. Even though authentication modules are added. [23] and [26] have proposed requiring the second level of authentication, known as the cloud to client authentication. In MCC Based System, there is a need for passing all the user requests via the attack detection module. The user requests, once approved, are passed to the security Module. After this, the user requests are safe to handle access to the requested data from the cloud.

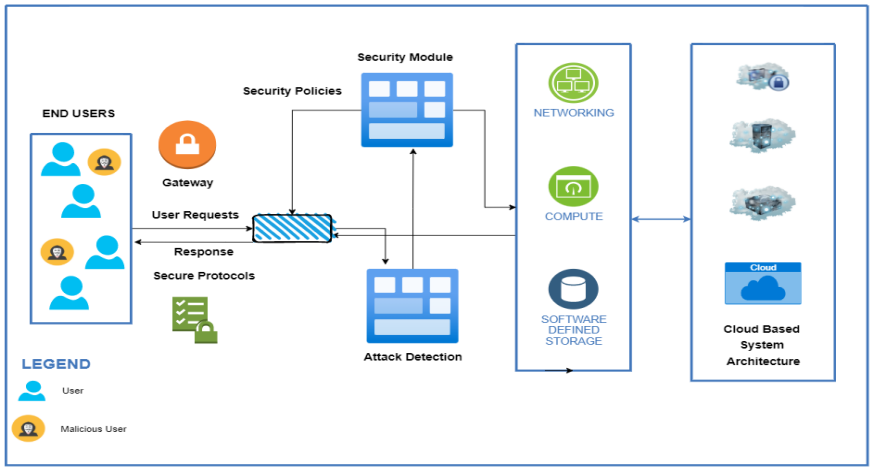

Figure 3: Proposed System for Mobile Cloud Computing Based Systems

6. MOBILE CLOUD COMPUTING IN COVID-19

1. **HealthCare:** The first and foremost industry of critical importance is health care. During this COVID-19, the world has seen a tremendous increase in Online Video Conferencing Services such as Zoom, Microsoft Teams, Google Meet, having cloud-based facilities that have helped the physicians and doctors to monitor the patients and conduct a virtual checkup. It does not violate any Social Distancing guidelines, which are indirectly violated in physical checkups. Apart from Online Video conferencing, Other Services such as the Amazon Web Services and Microsoft Azure offer features that can ease the process and include automation in tasks. During this COVID-19, Electronic Health Reports (EHRs) and epidemiology tools [29] are used extensively. Even though many new novel approaches are published. But the issues regarding security and maintenance still are a matter of concern.

2. **Education:** Education is one of the sectors, which came to a halt abruptly because of this COVID-19 Pandemic. Even though some of the schools, universities, and institutions were utilizing some of the digital resources and services, the transition from an offline mode of teaching to online teaching was quite burdensome for the academicians, faculty, and students. Not only there was also a need for a platform that handles the needs of the students. But also ease the process of management and evaluation for the teachers and faculties. MCC not only can save hefty costs. But also

is highly efficient in the proper functioning of the E-Learning platforms, archiving the student data, assignments, and works on the cloud. The challenge of conducting sessions online are resolved by the Video Conferencing Services. But there is still a challenge in terms of conducting assessments and exams in the online mode.

3. **Artificial Intelligence:** Artificial Intelligence, an advancing technology that has a lot of unexplored potentials. Similarly, in [31] the author proposed a novel voice analysis model that helps in the early detection (Asthama and COVID-19) by analyzing the change in the voice patterns. The main aim of this model was to be able to distinguish between the COVID-19 and Asthama detections. The mobile application proposed in these records and stores the user/patient's voices regularly to the cloud storage. That, in turn, helps in quick and accurate analysis. Even the models combine Machine learning and Artificial Intelligence to analyze and do image processing to detect the COVID-19. Since an adequate number of photos need to be stored for analysis. Hence a cloud-based infrastructure would be in need.

4. **Blockchain:** Blockchain is a versatile field because it has applications in almost all of the other sectors, be it healthcare, education, governance, management, transportation, etc. Applications such as sharing of Patient Information, Contactless delivery, Online Education, surveillance, automations and contact tracing. Blockchain ensures that privacy is maintained, while the data is shared over the network or any platforms. Such as in Patient Sharing Information, since the data of the COVID-19 affected patients have to shared nationally as well as internationally so as to conduct specific research and analysis in terms of the identification. Blockchain ensures that the patient personal information are safe. Apart from these Blockchain technology can help in linking stakeholders and developing chains that have provenance and transparency [32].

7. CONCLUSION AND FUTURE REMARKS

In this paper, we analyzed that how Mobile Cloud Computing plays an ideal role in increasing the functionalities provided by mere devices such as Mobile, smartphones, and PDA's. MCC widely accepted lately in the cloud and mobile computing communities because of its cost-effectiveness, accessibility, availability, and it can have a wide variety of applications in the sectors such as Blockchain, Education, Healthcare, IoT, Artificial Intelligence. But, even though MCC has scopes to address the real-world challenges and problems faced during the lockdown and COVID-19 pandemic, MCC still faces several challenges in security, authentication, data encryption and security, assurance, and interoperability.

In this paper, the models proposed by various authors and researchers are reviewed in terms of technicalities and methodologies followed for contouring the issues present in the MCC technology. The paper discusses the models, challenges faced by MCC. The number of mobile users has witnessed an exponential increase, one of the prominent

reasons to research and adopt MCC. MCC not only provides access to complex computational processes irrespective of the device configuration and the location from which the user raises requests. But addresses processing and resource constraints.

The findings concluded after reviewing the proposed models by various researchers and authors are:

There is a need for a comprehensive model that addresses all the issues. Disregarding any of the aspects in such an architecture can pose critical threats and attacks. The issues of the authentication process, specifically cloud-to-client authentication haven't been addressed widely. It is advisable not to disregard cloud-to-client authentication because it calls Man in the Middle Attacks. Future researches should be done considering real-world scenarios like COVID-19. It can give insights into underlying issues and possible benefits.

8. ACKNOWLEDGEMENT

We thank our management of Vellore Institute of Technology, Chennai for their constant support and encouragement. Authors acknowledge the scholars whose articles are cited and included in references to this manuscript. The authors are also grateful to authors/editors/publishers of all those articles, journals and books from where the literature for this article has been reviewed and discussed. All the diagrams/ figures / illustrations used and added in the paper are made using Open-Source software, ensuring no copyright issues.

9. AUTHORSHIP STATEMENT

All persons who meet authorship criteria are listed as authors and took the public responsibility for the content, including participation in the concept, analysis, writing, and revision of the manuscript. All authors revised and gave final approval for the version submitted.

10. CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Abid Shahzad1 and Mureed Hussain 2, 2013, Security Issues and Challenges of Mobile Cloud Computing, International Journal of Grid and Distributed Computing, Vol.6, pp.37-50, www.sersc.org

[2] Mobile Cloud Market – Growth, Trends, COVID-19 Impact, and Forecasts (2021-26), https://www.mordorintelligence.com/industry-reports/global-mobile-cloud-market-industry

[3] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in *IEEE Access*, vol. 7, pp. 66792-66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[4] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc. 2018 Apr 16;2017:650-659. PMID: 29854130; PMCID: PMC5977675.

[5] Hölbl, Marko, Marko Kompara, Aida Kamišalić, and Lili Nemec Zlatolas. 2018. "A Systematic Review of the Use of Blockchain in Healthcare" *Symmetry* 10, no. 10: 470. https://doi.org/10.3390/sym10100470

[6] Hanan Elazhary, Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions, Journal of Network and Computer Applications, Volume 128, 2019, Pages 105-140, https://doi.org/10.1016/j.jnca.2018.10.021.

[7] H. Eom, R. Figueiredo, H. Cai, Y. Zhang and G. Huang, "MALMOS: Machine Learning-Based Mobile Offloading Scheduler with Online Training," *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2015, pp. 51-60, doi: 10.1109/MobileCloud.2015.19.

[8] L. E. Talavera, M. Endler, I. Vasconcelos, R. Vasconcelos, M. Cunha and F. J. d. S. e. Silva, "The Mobile Hub concept: Enabling applications for the Internet of Mobile Things," *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2015, pp. 123-128, doi: 10.1109/PERCOMW.2015.7134005.

[9] Hernandez, L., Cao, H., Wachowicz, M., 2017. Implementing an Edge-fog-cloud Architecture for Stream Data Management. Cornell University Library, https://arxiv. org/abs/1708.00352.

[10] UST Global, 2017. Internet of Medical Things (IoMT) Connecting Healthcare for a Better Tomorrow. https://www.ust-global.com/sites/default/files/internet_of_medical_things_iomt.pdf

[11] S. A. Alvi, G. A. Shah and W. Mahmood, "Energy efficient green routing protocol for Internet of Multimedia Things," *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2015, pp. 1-6, doi: 10.1109/ISSNIP.2015.7106958.

[12] Tyagi, Amit Kumar and M, Shamila, Spy in the Crowd: How User's Privacy Is Getting Affected with the Integration of Internet of Thing's Devices (March 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019, http://dx.doi.org/10.2139/ssrn.3356268

[13] Kosta, S., Aucinas, A., Hui, P., Mortier, R., & Zhang, X. (2012). ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. *2012 Proceedings IEEE INFOCOM*, 945-953.

[14] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, "Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing," Journal of Network and Computer Applications, vol. 59, pp. 46–54, 2016.

[15] A. Banerjee, X. Chen, J. Erman, V. Gopalakrishnan, S. Lee, and J. Van Der Merwe, "MOCA," in Proceedings of the Eighth ACM International Workshop on Mobility in the Evolving Internet architecture, pp. 11–16, ACM, Miami, FL, USA, 2013.

[16] Y. Lin, T. Kam¨ ar¨ ainen, M. Di Francesco, and A. Yl ¨ a-J ¨ a¨aski, ¨ "Performance evaluation of remote display access for mobile cloud computing," Computer Communications, vol. 72, pp. 17–25, 2015.

[17] A. N. Khan, M. M. Kiah, M. Ali, and S. Shamshirband, "A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach,"

[18] Sukhpreet Kaur, & Sohal, H. S. (2016). *Hybrid Application Partitioning and Process Offloading Method for the Mobile Cloud Computing. Proceedings of the First International Conference on Intelligent Computing and Communication, 87–95.* doi:10.1007/978-981-10-2035-3_10

[19] Yan Gu, Verdi March, Bu Sung Lee,"GMoCA: Workshop on Green and Sustainable Software GREEN Zurich, 3-3 June 2012, pp 15-20, Print ISBN: 978-1-4673-1833-4, DOI: 10.1109/GREENS.2012.6224265.

[20] Cao, J., Yu, B., Dong, F., Zhu, X., and Xu, S. (2015) Entropy-based denial-of-service attack detection in cloud d center. *Concurrency Computat.: Pract. Exper.*, 27: 5623– 5639. doi: 10.1002/cpe.3590.

[21] Z. Tong, Z. Zhu, Z. Wang, L. Wang, Y. Zhang and Y. Liu, "Cache side-channel attacks detection based on mach learning," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing a Communications (TrustCom), 2020, pp. 919-926, doi: 10.1109/TrustCom50675.2020.00123

[22] Donald, A. Cecil & Arockiam, L. & Kalaimani, Suresh. (2018). ORBUA: An effective data access model MobiCloud environment. International Journal of Pure and Applied Mathematics. 118. 79-84.

[23] Bhatia, T, Verma, AK, Sharma, G. Towards a secure incremental proxy re-encryption for e-healthcare data shar in mobile cloud computing. *Concurrency Computat Pract Exper*. 2020; 32:e5520. https://doi.org/10.1002/cpe.55

[24] Irshad, A, Chaudhry, SA, Shafiq, M, Usman, M, Asif, M, Ghani, A. A provable and secure mobile u authentication scheme for mobile cloud computing services. *Int J Comm Syst*. 2019; 32:e3980. https://doi.org/10.1002/dac.3980

[25] H. Yadav and M. Dave, "Secure data storage operations with verifiable outsourced decryption for mobile clo computing," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 20 pp. 1-5, doi: 10.1109/ICRAIE.2014.6909236.

[26] Rashidi Othman, Fatimah Azzahra Mohd Zaifuddin, Norazian Mohd Hassan, Carotenoid Biosynthesis Regulat Mechanisms in Plants, Journal of Oleo Science, 2014, Volume 63, Issue 8, Pages 753-760, Released July 2014, [Advance publication] Released July 14, 2014, Online ISSN 1347-3352, Print ISSN 13 8957, https://doi.org/10.5650/jos.ess13183,

[27] Mathew, Saju Mathew. (2012). Implementation of Cloud Computing in Education - A Revolution. Internatio Journal of Computer Theory and Engineering. 4. 473-475. 10.7763/IJCTE.2012.V4.511.

[28] Agrawal, Somya. (2020). A survey on recent applications of cloud computing in Education: COVID-19 perspect

[29] Dadhich, Priyanka & kavita, Dr. (2021). Cloud Computing Impact on Healthcare Services During COVID- Pandemic.

[30] A. O. Popadina, A. -M. Salah and K. Jalal, "Voice Analysis Framework for Asthma-COVID-19 Early Diagnosis a Prediction: AI-based Mobile Cloud Computing Application," 2021 IEEE Conference of Russian Young Research in Electrical and Electronic Engineering (ElConRus), 2021, pp. 1803-1807, d 10.1109/ElConRus51938.2021.9396367.

[31] A. O. Popadina, A. -M. Salah and K. Jalal, "Voice Analysis Framework for Asthma-COVID-19 Early Diagnosis a Prediction: AI-based Mobile Cloud Computing Application," 2021 IEEE Conference of Russian Young Research in Electrical and Electronic Engineering (ElConRus), 2021, pp. 1803-1807, d 10.1109/ElConRus51938.2021.9396367.

[32] Sharma, A., Bahl, S., Bagha, A.K. et al. Blockchain technology and its applications to combat COVID-19 pandemic. Res. Biomed. Eng. (2020). https://doi.org/10.1007/s42600-020-00106-3