Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol. 7 No. 2, 2018, pp. 80-85

DOI: https://doi.org/10.51983/ajeat-2018.7.2.1003

Mobile Cloud Computing: A Literature Survey

Lakshna Arun[1] and T.N.Ravi[2]
[1]Research Scholar, [2]AssistantProfessor
Department of Computer Science, Periyar E.V.R College, Tiruchirappalli, Tamil Nadu, India
E-Mail: proftnravi@gmail.com
(Received 3 July 2018; Revised 25 July 2018; Accepted 12 August 2018; Available online 20 August 2018)

***Abstract* -Mobile cloud computing (MCC) is the availability of cloud computing services in a mobile environment. By providing optimal services for mobile users, MCC incorporates the elements of mobile networks and cloud computing. In mobile cloud computing, all the data and complicated computing modules can be processed in clouds, and mobile devices do not need a powerful configuration like CPU speed, memory capacity, etc. However, the mobile devices are facing up with many struggles in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., privacy, mobility, and security). These challenges have a significant effect on the improvement of service qualities. In this paper, a literature survey on the MCC and security issues in MCC has presented.**
***Keywords*: Mobile Cloud Computing, Mobile Environments, Mobile Networks**

I. INTRODUCTION

In recent years, propels in the field of network-based computing and applications mobile cloud computing (MCC) has been presented as a potential technology for mobile administrations. It is the blend of mobile computing, cloud computing and wireless networks to convey astounding computational assets to network administrators, mobile clients, and cloud computing suppliers. MCC is another stage for consolidating the mobile gadgets and cloud computing to make another foundation. It alludes to a framework where both the information stockpiling and the information preparing occur outside of the mobile gadget. In this design, the cloud plays out the challenging work of computing-concentrated errands and stores much information. The quick rise of mobile computing (MC) turns into a great pattern in the improvement of information technology.

Because of real application display in the time of Internet, mobile cloud computing has turned into a vast research subject of the logical and mechanical networks. Its application is winding up a more important. Along these lines, distinctive applications of mobile cloud computing have been produced and served to clients, for example, Google's Maps, Gmail and Navigation frameworks for Mobile, Voice Search, and different applications on an Android stage, MobileMe from Apple and MotoBlur from Motorola. The expanding utilization of mobile computing is apparent in the investigation of Juniper Research, which expresses that the purchaser and venture advertise for cloud-based different mobile applications is $9.5 billion [1]. The primary objective behind the cloud computing is the conveyance of various administrations, programming, and handling limit over the Internet, expanding capacity, decreasing cost, robotizing frameworks and decoupling of network conveyance from basic technology, and giving adaptability and portability of information in various purposes.

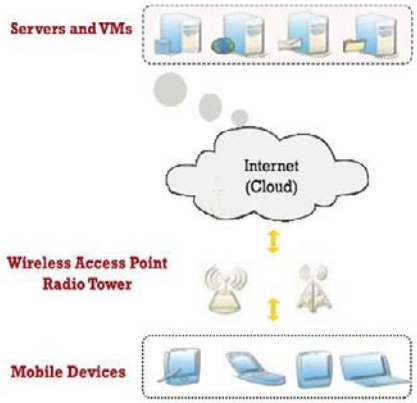

Fig. 1 Overview of Mobile Cloud Computing

The general design of MCC can appear in Figure 2. The basic engineering of MCC is formed from the parts: mobile clients, mobile administrators, internet service providers (ISP), cloud service providers, individually [2]. The Mobile gadgets primarily mobile telephones speak with the mobile networks with the assistance of base stations, passageways as well as satellite.

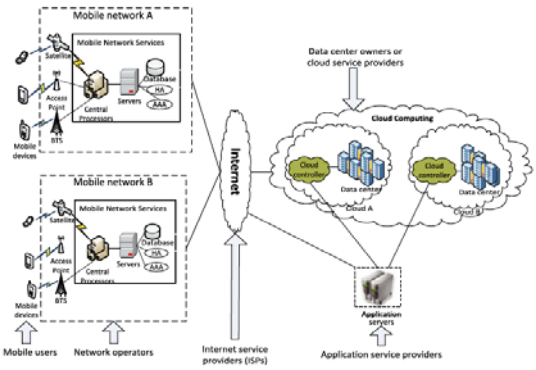

Fig. 2 Architecture of Mobile Cloud Computing

The information's are transmitted from the mobile gadgets, and these information's are worked on the focal processors unit, servers, and database on the mobile network supplier side. Here, mobile network administrators can give essential services to mobile telephone clients as an approval,

verification, and bookkeeping in light of the home operator and endorsers information put away in the databases. From that point, the endorsers' solicitations to the cloud through the internet. Cloud controllers process the solicitations to explore the relating cloud services. The mobile cloud computing design gives viability by utilizing the upsides of the cloud computing.

II. SECURITY ISSUES IN MOBILE CLOUD ENVIRONMENT

In mobile cloud computing applications security and privacy are the key issues and still face some enormous challenges [3]. User's privacy and integrity of data or applications are one of the key issues in securing mobile cloud computing. It is the combination of cloud computing and mobile networks. For this, the security-related issues have divided into two categories: cloud security and mobile network user's security; [4][5][6][7].

A. Mobile Network User's Security

A large number of security vulnerabilities and threats such as malicious codes are known to the different mobile devices such as cellular phones, Smartphone's, PDAs, laptops, etc. Some of the applications to these mobile devices can cause privacy issues for users [6]. There are the two major issues concerning the subscriber's security.

1. Security for Mobile Applications

The least demanding approaches to discover security issues will introduce and running security programming and antivirus programs on mobile gadgets. All the mobile gadgets are settled with handling and power restrictions. To shield gadgets from these dangers could be more difficult contrasted with compatible PCs. A few methodologies have been produced to discover security tools in the cloud. Before utilizing a specific mobile application on mobile, it might experience some level of risk assessment. First, it will be check, and if malicious is not recognize, the document is sent to the client mobile gadgets. Mobile gadgets are performing just lightweight exercises, for example, execution follows transmitted to cloud security servers as opposed to running opposition of plague programming or risk identification programs locally.

2. Privacy

By providing private information including indicating the current location and user's important information creates scenarios for privacy issues. To illustrate, the use of location-based services (LBS) which are provided by a global positioning system (GPS) devices. Various threats for exposing private information can be reduced by selecting and analyzing the enterprise needs and needs only specified services to be acquired and moved to the cloud network instead of running anti-virus software or threat detection programs locally.

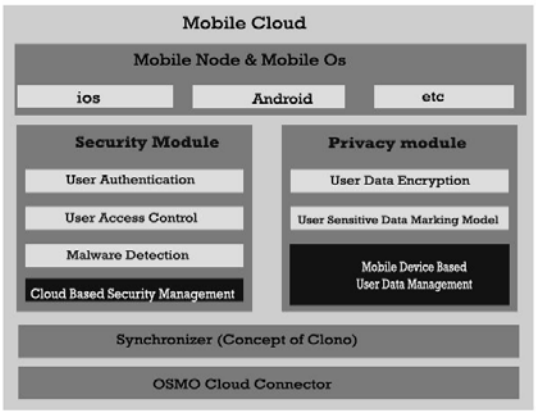

Fig. 3 Overview of Security Architecture of Mobile Cloud Computing

B. Securing Information on the Cloud

For storing a large amount of data or applications individuals and enterprises may take advantage over the cloud. However, integrity, authentication, and digital rights of data or application have to ensure during processing.

1.Integrity

The entire mobile cloud user must ensure the integrity of their information stored on the cloud network. All access must be authenticated and verified. In order to preserve integrity for one's information that is stored on the cloud is being proposed by giving different approaches. For example, complete information stored by each individual or enterprise in the cloud network is tagged or initialized to them wherein they are the only one to move, update or delete information.

2.Authentication

To secure the data access suitable for mobile environments using cloud computing a large number of authentication mechanisms has been proposed. Some use the open standards and support the integration of deferent authentication methods. Such as illustrating the use of access or log-in IDs, password or PINS, an authentication request, etc.

3. Digital Rights Management

Piracy of various digital contents such as image, audio, video, and e-book programs becomes more and more popular day by day. A numerous solution has been proposed to protect these contents from illegal access are implemented such as the provision of encryption and decryption keys to access these digital contents. Before accessing such digital contents on mobile devices coding or decoding platform must be done.

III. LITERATURE SURVEY ON MOBILE CLOUD COMPUTING

Many scientists have researched the mobile cloud computing and its security issues.

Bowen Zhou and RajkumarBuyya [8], the target of their paper is to give a guide on what accessible increase strategies can be received in mobile cloud computing frameworks and also supporting instruments, for example, central leadership and adaptation to internal failure approaches for acknowledging solid mobile cloud services. The authors likewise give a dialog on the open difficulties and future research bearings in the field. AndrzejWilczy 'nski and Joanna Kołodziej [9], built up a layer that empowers virtualization of touchy information, guaranteeing that they are transmitted securely finished the network and broke down with deference the insurance of individual information. An arrangement has been checked in good utilize case for transmission sports information to the specialists who send the determination as a reaction. Fan-Hsun Tseng *et al.* [10], proposed two calculations in light of use situated for least execution time, i.e., the Minimum Offloading Time for Mobile gadget (MOTM) calculation and the Minimum Execution Time for Cloud server farm (METC) calculation. This MCC offloads the assignments and occupations of mobile gadgets to cloud and mist conditions by utilizing the offloading plan. Maryam Sajjad, Aakash Ahmad, AsadWaqar Malik, Ahmed B. Altamimi, and Ibrahim Alseadoon [11], introduced a paper and their goal is to deliberately distinguish, systematically order and guide the condition of-explore on versatile security (a.k.a. self-assurance) for mobile computing.

Huber Flores, VassilisKostakos, SasuTarkoma, Pan Hui and Yong Li [12], the authors investigate the difficulties and chances of another sort of mobile engineering, to be specific proof mindful mobile cloud design, which depends on swarm detecting to analyze the ideal setup for moving mobile usefulness to cloud. The key point is that by utilizing the large parallel support of the cloud process, it is conceivable to gather offloading proof from an extensive measure of gadgets that is later dissected in conjunction to assume a practical design to execute a mobile phone application for a specific gadget.Qian He, Ning Zhang, Yongzhuang Wei, Yan Zhang [13], proposed a Lightweight Attribute-Based Encryption Scheme (LABE) for mobile cloud-helped CPS because of intermediary service design and another ciphertext arrangement ABE. Individually, mobile gadgets will exclusively perform symmetric encryption by joining validation and encryption intermediary services typified in RESTful. Encryption will not require matching, and afterward, the ciphertext can be decoded with one blending. Gabriel Orsini, Dirk Bade, Winfried Lamersdorf [14], the authors present the idea of Generic Context Adaptation (GCA), an information mining process that encourages the adjustment of (mobile) applications to their present and future setting. Geeta C M, Raghavendra S, RajkumarBuyya, Venugopal K R, S Iyengar, L M Patnaik [15], the creator exhibited an extensive overview on the condition of-craftsmanship methods in information inspecting and security are talked about. Testing issues in information archive inspecting and security are exhibited.

Li Yang, Ziyi Han, Zhengan Huang, Jianfeng Ma [16], the authors proposed another plan called FREDP (File Remotely keyed Encryption and Data Protection). This plan includes three-party communication among a mobile terminal, private clouds, and open clouds. The private clouds share the ciphertext document to people in general clouds until the mobile terminal and the confided in an outsider, the private clouds, complete the encryption of the plaintext record utilizing a remotely keyed encryption calculation. To guarantee security when a mobile terminal uses information, the private clouds as the outsider consistently check the uprightness of the information in general society clouds.Dazhi Li, Minglu Li, Jianhua Liu [17], this paper model the collaborations among virtual verification organizers, the confirmation agent and mobile clients as a three-arrange diversion, where each player goes for expanding its utility, and the trust\ designation is accomplished by G esteem learning. Numerical outcomes have demonstrated that the proposed authentication mindful structure is compelling, as it empowers all players to expand their utilities and enhance the level of the trust of mobile computing frameworks. Yi Liu, Yinghui Zhang, Jie Ling, Zhusong Liu [18], the authors proposed a fine-grained EHR get to control conspire which is demonstrated secure in the standard model under the decisional parallel bilinear Diffie-Hellman example suspicion. In the proposed plot, an EHR proprietor can create disconnected ciphertexts before knowing EHR information and access strategies, which plays out a more significant part of calculation undertakings. Moreover, the online stage can quickly collect the last ciphertexts when HER information and access arrangements end up known.Cong Zuo, Jun Shao, Guiyi Wei, MandeXie, Min Ji [19], the authors proposed the CCA security show for ABE with outsourced decoding, and after that present, a solid CCA-secure ABE conspires with outsourced unscrambling.

FushanWei, Ruijie Zhang [20], in this paper, the authors condensed the security prerequisites and set forward a formal security show for Two-factor verified key trade (TFAKE) conventions for cloud computing. The authors show a productive TFAKE convention without utilizing costly uneven cryptology instruments to accomplish high effectiveness. DurbadalChattaraj, MonalisaSarma, Ashok Kumar Das [21], in this paper, the authors expect to propose a validation convention which beats these security provisos in the current conventions. In the proposed convention, another powerful secret word based on two server verification and key trade component are proposed with the assistance of both open and private key cryptography. Also, to accomplish stable client namelessness property, another multifaceted validation plot with personality protection has been additionally presented. The security examination utilizing both the formal security utilizing the comprehensively acknowledged Real-Or-Random (ROR) display and the casual security demonstrate that the proposed convention ensures a few surely understood assaults. Furthermore, the formal security check utilizing the generally utilized Automated Validation of Internet

Security Protocols and Applications (AVISPA) guarantees that the plan is strong against replay and also man-in-the-middle attacks.Yinhao Jiang, Willy Susilo, Yi Mu, FuchunGuo [22], In this paper, the authors acquaint another instrument with upgrade Ciphertext Policy-Attribute based Encryption (CP-ABE) plans that give insurances against this key-assignment mishandle issue. The authors formalize the security necessities for such a property, and thusly develop a CP-ABE plot that fulfills the new security prerequisites. Alberto Ceselli, Marco Fiore, Marco Premoli, Stefano Secci [23], the authors propose a general information driven system for our application including an advancement center, an information pre-preparing module, and an approval module to test designs exactness. This enhancement center involves a combinatorial issue that is a multi-period variation of the Generalized Assignment Problem: this work outline a Branch-and-Price calculation that, albeit correct, performs well likewise as metaheuristics when joined with early halting. Broad investigations on both engineered and right datasets show that the proposed approach is both computationally viable and exact when utilized for prescriptive examination.

Li Xu*et al.* [24], the authors proposed sharable ID-based encryption with a catchphrase look in cloud computing condition, which empowers clients to seek in information proprietors' shared stockpiling while at the same time-saving security of information. For the execution examination, the creator shows the contrasted resultant and others ID-based or ID-relative encryption. PelinAngin, Bharat Bhargava, RohitRanchal [25], in this paper, the authors introduce a setting subordinate calculation offloading model for MCC, which depends on application fragments pressed into independent specialists. This approach requires secluded execution holders in the cloud to give a runtime domain to the operators, and insignificant association of the mobile stage amid the calculation procedure. The operators in the proposed show can shield themselves from altering utilizing respectability checkpointing and a confirmed encryption-based correspondence component.

AnimeshHazra, SoumyaGhosh and SampadJash [26], this paper gives a concise outline of DNA cryptology alongside another calculation in light of the combination of symmetric-key cryptography, DNA nucleotides, and XOR activity is proposed. This calculation is especially productive, and one fundamental striking component of the calculation is the security which can be set according to sender prerequisites. YiranShen, ChengwenLuo, Dan Yin, Hongkai Wen, Rus Daniela, Wen Hu [27], propose another cloud-empowered and Privacy-safeguarding short portrayal order (P2-SRC) framework to secure the protection of both the "information givers" and "application clients" when a cloud server is untrusted. Not quite the same as the best in class approaches which consider the assaults on information esteems, our proposed framework, P2-SRC, addresses various kinds of security assaults including Content Privacy Attacks, Source Privacy Attacks, and Label Privacy Attacks.

Yuan Xue, Yu-a Tan, Chen Liang, Yuanzhang Li, Jun Zheng, Quanxin Zhang [28], the proposed plot guarantees the security of established Android gadgets and improves the security of mobile terminal gadgets. This decreases the danger to cloud foundation from root-abused Android gadgets. Also, a model is actualized to assess its adequacy, effectiveness, and overhead. Jing Li, Xiong Li, Licheng Wang, Debiao He, Haseeb Ahmad, XinxinNiu [29], the authors exhibit a productive outsourced Ciphertext Policy-Attribute based Encryption (CP-ABE) plot with checkability, where the quantity of the exponential activities in the encryption can be lessened to a consistent by presenting a blinding calculation. Then, the ciphertext estimate is not expanded. Moreover, to ensure the accuracy of proposed conspire, the authors give the confirmation component in light of a crash opposition hash work, which enables the clients to check the legitimacy of messages and outsourced calculation results productively. Also, the proposed conspire is secure against replayable picked ciphertext assaults in light of Green's outsourcing security demonstrate. Wei Wu *et al.* [30] in this article, the writers, recommend a protected and financially savvy fluffy access control convention in mobile cloud computing. It is mainly intended for little and medium ventures (SMEs) giving business-to-clients services. The proposed convention enables the SME to outsource its services to a cloud to decrease the running expense. In the meantime, it does not require any correspondence between the cloud and the SME amid client validation arrange. That is, SME can be disconnected after clients have been enlisted. Clients individually manage the cloud for getting entrance. This causes the SME to spare a considerable measure of assets, including an extensive data transfer capacity interfacing with the cloud and a solid firewall framework.F. Lordan, J. Jensen • R. M. Badia [31], this paper presents chip away at actualizing MCC applications with secure interchanges. For that reason, we based on COMPSs-Mobile, an overhauled execution of the COMP Superscalar (COMPSs) system expecting to MCC platforms. COMPSs-Mobile naturally misuses the parallelism characteristic in an application and arranges its execution on approximately coupled conveyed condition.

K. S. Arvind, R. Manimegalai [32], the authors display a prevalent innocent classifier for secure information characterization in specialist based mobile cloud computing is proposed in this paper. The operator arranges the client's information into three distinct gatherings in particular, low, medium, high. At that point, the information is scrambled utilizing Advanced Encryption Standards (AES). The encoded information is exchanged to the representative for choosing for appropriate service specialist. In any case, the intermediary has numerous to one association with service operators. At that point, the information is sent to the cloud service supplier for capacity. The put away information is then homomorphically scrambled which empowers the cloud supplier and cloud client to process the information without the requirement for unscrambling. Suleman Khan, Muhammad Shiraz, LalehBoroumand, Abdullah Gani,

Muhammad Khurram Khan [33], his paper audits existing port-thumping verification strategies by dissecting the component and ordering the techniques into a topical scientific categorization. Current port-thumping verification techniques are looked at given static or dynamic thumped groupings, which tend to tackle the Network Address Translation (NAT) thump and Denial of Service (DoS) thump assaults. At last, we talk about the issues and difficulties in executing port-thumping for MCC. VangaOdelu, Ashok Kumar Das, SaruKumari, Xinyi Huang, Mohammad Wazid [34], the authors proposed a provably secure confirmation conspire for conveyed mobile cloud computing services. Through the thorough security examination, we demonstrate that our plan accomplishes Session Key (SK) - security and solid certifications' protection and keeps all notable assaults including the pantomime assault and vaporous insider facts spillage assault. ProsantaGope and Ashok Kumar Das [35], in this paper, the authors plan to propose another vigorous mysterious shared verification conspire for mobile cloud condition. Through this plan, both the mobile client and the service cloud need to demonstrate their authenticity, and it, in the long run, assists the real mobile cloud client with enjoying n times all the omnipresent services in a protected and proficient way, where the estimation of n may contrast in light of the vital he/she has paid for. The security of the proposed plot is altogether investigated utilizing both formal and besides casual security examination.

V. Suresh Babu, Maddali M. V. M. Kumar [36], this paper proposes a framework for security sensitive information sharing in the cloud, including secure information movement, amassing, utilize, and pulverization on a semi-trusted in cloud condition. The authors display Kerberos tradition over the framework and a customer method protection procedure in perspective of a virtual machine screen, which offers assistance for the affirmation of structure limits. Jin Li, Yinghui Zhang, Xiaofeng Chen, Yang Xiang [37], the authors proposed another trait based information sharing plan appropriate for asset constrained mobile clients in cloud computing. The proposed conspire kills a more significant part of the calculation undertaking by including framework open parameters other than moving halfway encryption calculation disconnected. What's more, an open ciphertext test stage is performed before the decoding stage, which dispenses with the vast majority of calculation overhead because of ill-conceived ciphertexts. For information security, a Chameleon hash work is utilized to produce a prompt ciphertext, which will be blinded by the disconnected ciphertexts to acquire the last online ciphertexts. The proposed conspire is demonstrated secure against adaptively picked ciphertext assaults, which is generally perceived as a standard security thought.

IV. SURVEY FINDINGS AND FUTURE DIRECTION

Research work has contributed immensely to the success of mobile cloud computing. However, there are still some issues, which need to be addressed to take this technology to the next level and make sure that it is used by a majority of the population. Through this survey, the following works to be carried out in future.

1. Improving the authentication scheme between the cloud and the users by using soft computing techniques.
2. Enhancing the security of the user data in the cloud environment.
3. Improving the technique to detect the intrusion in the cloud and mobile users.

TABLE I MEASURES TO IMPROVE THE SECURITY OF SERVICES IN MOBILE CLOUD COMPUTING

Security service	Consideration
Data backup	Useful backup, verification processes, policies, and procedures are needed
Encryption	Secure and effective key management and distribution policy is needed to control the generation of encryption keys, specific to an organization or country
Communication network	Prevent wiretapping. Encryption needs to be employed; Protect from repudiation, any transmitted or received data must be prepared; Check identity and authenticate users' needs to be employed; Protect against interlocking in a heterogeneous network; Protect against service refusal attacks;Protect the system from network hindrance.
System software	Protect the integrity of data and the installed software; Software updates to protect against any bugs or vulnerability in the software; Maintain operating systems and virtual systems vaccinations; Maintain software proficiency by applying service patches.
System virtualization	Control virtual machine resources; Apply and maintain service patches to prevent malignant code from becoming a problem; Define clear boundaries between the host operating system and the virtual machine; Maintain log and image histories of virtual instances.
The data center, disaster recovery policies	Policies to cover for all eventualities and risks, such as floods, fires, and earthquakes
Access management and authentication - Wireless access	Encrypt communication sessions; Control mobile terminal authentication and log session management
Access management and authentication - Login sessions	Implement mechanisms to verify user identity; Minimise user authority
Access management and authentication – Account	Implement an organization policy with restrictions on the number of attempts in case of login failure

V. CONCLUSION

Mobile cloud computing (MCC) as the development and extension of mobile computing and cloud computing has inherited mobility and scalability. Due to the large-scale response, it has become the hot topic of research in recent years. Within a year, it is expected to observe a fierce competition among PaaS players to become the market leader in mobile cloud computing.With this vital importance, this paper has provided an overview of mobile cloud computing and its security. In this paper, an extensive survey of current research on the mobile cloud computing and its security issues. The measures to improve the security of services in Mobile Cloud Computing have been figured out through this literature survey.

REFERENCES

[1] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Ganiand R. Buyya,"Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges",*Communications Surveys and Tutorials, IEEE,*Vol. 16, No. 1, pp. 337-368, 2014.

[2] Qian (Andy) Wang,"Mobile Cloud Computing", A Thesis Submitted to the College of Graduate Studies and Research in Partial Fulfillment of the Requirements, Feb. 2011.

[3] H. Suo, Z. Liu, J. Wan andK. Zhou,"Security and privacy in mobile cloud computing",*In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, IEEE,* pp. 655-659, 2013.

[4] D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, Secure data processing framework for mobile cloud computing,*In Computer Communications Workshops (infocomwkshps), 2011 IEEE Conference, IEEE,* pp. 614-618, 2011.

[5] R. Buyya, J. Broberg, and A. M. Goscinski, "Cloud computing: Principles and paradigms", Vol. 87, John Wiley and Sons, 2010.

[6] H. T. Dinh, C. Lee, D. Niyato, andP. Wang,"A survey of mobile cloud computing: architecture, applications, and approaches", Wireless communications and mobile computing, Vol. 13, No. 18, pp. 1587-1611, 2013.

[7] A. N. Bahar, M. A. Habib, andM. M. Islam, 2013. Security architecture for mobile cloud computing. International Journal, Vol. 3, No. 3, pp. 2305-1493.

[8] Zhou, Bowen, and RajkumarBuyya, "Augmentation Techniques for Mobile Cloud Computing: A Taxonomy, Survey, and Future Directions", *ACM Computing Surveys (CSUR),* Vol. 51, No. 1, pp. 13, 2018.

[9] Wilczyński, Andrzej and Joanna Kołodziej, "Virtualization Model for Processing of the Sensitive Mobile Data", *Modeling and Simulation in HPC and Cloud Systems, Springer,* Cham, pp. 121-133, 2018.

[10] Tseng, Fan-Hsun, *et al,*"Application-oriented offloading in heterogeneous networks for mobile cloud computing", *Enterprise Information Systems,* Vol. 12, No. 4, pp. 398-413, 2018.

[11] Sajjad, Maryam, *et al,* "Classification and Mapping of Adaptive Security for Mobile Computing", *IEEE Transactions on Emerging Topics in Computing*, 2018.

[12] Flores, Huber, *et al,* "Evidence-Aware Mobile Cloud Architectures", *Mobile Big Data, Springer*,Cham., pp. 65-84, 2018.

[13] He, Qian, *et al,* "Lightweight attribute-based encryption scheme for mobile cloud assisted cyber-physical systems",*Computer Networks*, 2018.

[14] Orsini, Gabriel, Dirk Bade, and Winfried Lamersdorf, "Generic context adaptation for mobile cloud computing environments", *Journalof Ambient Intelligence and Humanized Computing,* Vol. 9, No. 1, pp. 61-71, 2018.

[15] C. M. Geeta, *et al,* "Data Auditing and Security in Cloud Computing: Issues, Challenges, and Future Directions",*International Journal of Computer (IJC),* Vol. 28, No. 1, pp. 8-57, 2018.

[16] Yang, Li, *et al,* "A remotely keyed file encryption scheme under mobile cloud computing", *Journal of Network and Computer Applications*, 2018.

[17] Li, Dazhi, Minglu Li and Jianhua Liu, "Evolutionary trust scheme of certificate game in mobile cloud computing", *Soft Computing,* Vol. 22, No. 7, pp. 2245-2255, 2018.

[18] Liu, Yi, *et al,* "Secure and fine-grained access control on e-healthcare records in mobile cloud computing", *Future Generation Computer Systems,* Vol. 78, pp. 1020-1026, 2018.

[19] Zuo, Cong, *et al,* "CCA-secure ABE with outsourced decryption for fog computing", *Future Generation Computer Systems,* Vol. 78, pp. 730-738, 2018.

[20] Wei, Fushan, Ruijie Zhang and Chuangui Ma, "A Provably Secure Anonymous Two-Factor Authenticated KeyExchange Protocol for Cloud Computing", *FundamentaInformaticae,* Vol. 157, No. 1-2, pp. 201-220, 2018.

[21] Chattaraj, Durbadal, MonalisaSarma and Ashok Kumar Das, "A new two-server authentication and key agreement protocol for accessing secure cloud services", Computer Networks, Vol. 131, pp. 144-164, 2018.

[22] Jiang, Yinhao, *et al,* "Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing", *Future Generation Computer Systems,* Vol. 78, pp. 720-729, 2018.

[23] [23] Ceselli, Alberto, *et al,* "Optimized assignment patterns in Mobile Edge Cloud networks", *Computers and Operations Research*, 2018.

[24] Xu, Li, *et al,* "A shareable keyword search over encrypted data in cloud computing", *The Journal of Supercomputing,* Vol. 74, No. 3, pp. 1001-1023, 2018.

[25] Angin, Pelin, Bharat Bhargava and RohitRanchal, "A Self-Protecting Agent Based Model for High-Performance Mobile-Cloud Computing", *Computers and Security*, 2018.

[26] Hazra, Animesh, SoumyaGhosh and SampadJash, "A New DNA Cryptography Based Algorithm Involving the Fusion of Symmetric-Key Techniques", *Advanced Computational and Communication Paradigms, Springer*, Singapore, pp. 605-615, 2018.

[27] Shen, Yiran, *et al,* "Privacy-preserving sparse representation classification in cloud-enabled mobile applications", *Computer Networks*, Vol. 133, pp. 59-72, 2018.

[28] Xue, Yuan, *et al,* "RootAgency: A digital signature-based root privilege management agency for cloud terminal devices", *Information Sciences,* Vol. 444, pp. 36-50, 2018.

[29] Li, Jing, *et al,* "Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption", *Soft Computing,* Vol. 22, No. 3, pp. 707-714, 2018.

[30] Wu, Wei, *et al,* "Towards secure and cost-effective fuzzy access control in mobile cloud computing", *Soft computing,* Vol.21, No. 10, pp. 2643-2649, 2017.

[31] F. Lordan, J. Jensen, and R. M. Badia, "Towards Mobile Cloud Computing with Single Sign-on Access", *Journal of Grid Computing*, pp. 1-20, 2017.

[32] K. S. Arvind and R. Manimegalai, "Secure data classification using superior naive classifier in agent-based mobile cloud computing",*Cluster Computing,* Vol. 20, No. 2, pp. 1535-1542, 2017.

[33] Khan, Suleman, *et al,* "Towards port-knocking authentication methods for mobile cloud computing", *Journal of Network and Computer Applications*, Vol. 97, pp. 66-78, 2017.

[34] Odelu, Vanga, *et al,* "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services", *Future Generation Computer Systems,* Vol. 68, pp. 74-88, 2017.

[35] Gope, Prosanta and Ashok Kumar Das, "Robust anonymous mutual authentication scheme for n-times ubiquitous mobile cloud computing services", *IEEE Internet of Things Journal,* Vol. 4, No. 5, pp. 1764-1772, 2017.

[36] Babu, V. Suresh and Maddali MVM Kumar, "An Efficient and Secure Data Storage Operations in Mobile Cloud Computing",*IJSRSET,* Vol. 4, No. 1, pp. 1385-1390, 2018.

[37] Li, Jin, *et al,* "Secure attribute-based data sharing for resource-limited users in cloud computing", *Computers and Security,* Vol. 72, pp. 1-12, 2018.