I.J. Wireless and Microwave Technologies, **2020, 6, 36-46**
Published Online December 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2020.06.05

A Critical Survey on Privacy Prevailing in Mobile Cloud Computing: Challenges, State of the Art Methods and Future Directions

Rida Qayyum
Department of Computer Science, Government College Women University Sialkot, 51040, Pakistan
Email: ridaqayyum6@gmail.com
ORCID ID: 0000-0001-5332-6133

Received: 22 September 2020; Accepted: 03 November 2020; Published: 08 December 2020

Abstract: With the explosive growth of mobile applications and extensive praxis of cloud computing, mobile cloud computing has been introduced to be a potential technology for mobile services. But privacy is the main concern for a mobile user in the modern era. In the current study, we address the privacy challenges faced by mobile users while outsourcing their data to the service provider for storage and processing. However, a secure mobile user is required to protect these fundamental privacy factors such as their personal data, real identity, current location and the actual query sent to the cloud vendor server while availing different cloud services. Under these privacy metrics, we evaluated the existing approaches that are counting privacy challenge in mobile cloud computing. The primary focus of this study is to presents a critical survey of recent privacy protection techniques. Leading to objective, the current study conduct a comparative analysis of these state of the art methods with their strong points, privacy level and scalability. After analysis, this paper suggests the pseudo-random permutation method could be a promising solution that can be taken into consideration for preserving user personal information and data query privacy in MCC more efficiently. Primarily, the purpose of the survey was to focus on further advancements of the suggested method. Furthermore, we present the future research directions in the mobile cloud computing paradigms.

Index Terms: Mobile Cloud Computing, MCC Challenges, Privacy, Protection Goals, Permutation, Ranked keyword Searching Algorithm, Encryption, Mobile User Anonymity.

1. Introduction

Current technological landscape and its constant development have led to a new era in computing, where smart mobile devices are seamlessly used for daily activities with sophisticated operating systems and advanced hardware features [1]. Despite significant hardware and software improvements, these cellular phones pose certain limitations that are not going to be mitigated by producing more powerful smart devices [2]. Although, these devices are not suitable for performing compute-intensive tasks because of the limited storage and processing capabilities. Due to these constraints, people can no longer rely on internal RAM provided by the device providers [3].

With the growing use of applications and mobile phones in our everyday lives, devices such as smartphones, PDAs, tablets, palmtops, etc. have become a must for almost everyone. But due to their small size and portability, mobile devices cannot run all types of applications and still remains a low computational entity [4]. Computing industry manufacturers are continuously improving the battery life, storage space, weight, and computational capability of smartphones to cope-up with computation intensive applications. Still, the restrictions such as size, weight, cost, and energy make considerable bumps in the improvements infeasible [5].

Mobile Cloud Computing can, therefore, be viewed as a life-saver and can be described as a combination of two well-established computing paradigms, cloud computing, and mobile computing [6]. Here, mobile computing allows users to perform computational tasks seamlessly, regardless of their location and mobility. In MCC, mobile devices themselves act as a resource provider of the cloud making up a mobile peer-to-peer network and run an application on a remote resource rich server. Cloud computing, however, is a way to enable mobile users to access the shared pool of remote computing resources, including storage, and virtualized computing services through the internet. Briefly, mobile cloud computing provides data storage and processing services to mobile users in the cloud [7]. These computing resources can be acquired on-demand with the least management efforts. Thus, mobile users facilitate based on pay per use. Basically, it has been introduced to empower the storage and processing capabilities of mobile devices.

The general architecture of the mobile cloud computing can be shown in Fig. 1. The mobile devices are connected to the cellular networks via base stations (e.g., base transceiver station, access point, or satellite) that establish and manage the connections and interfaces between the networks and mobile devices. Mobile users' requests and information (e.g., ID and location) are transmitted to the central processors connected to servers providing mobile network services [8]. Then, the subscribers' requests are delivered to a cloud infrastructure using the internet. Afterwards, the cloud controllers process the request to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization, and service-oriented architecture, e.g., web application, and database servers. However, the adoption of the cloud service enables smart mobile devices to perform compute-intensive tasks by neglecting limited storage and processing capabilities provided by the device providers. Also, it aims to empower mobile terminals to access robust and reliable cloud services that facilitate the optimal utilization of resources [9].

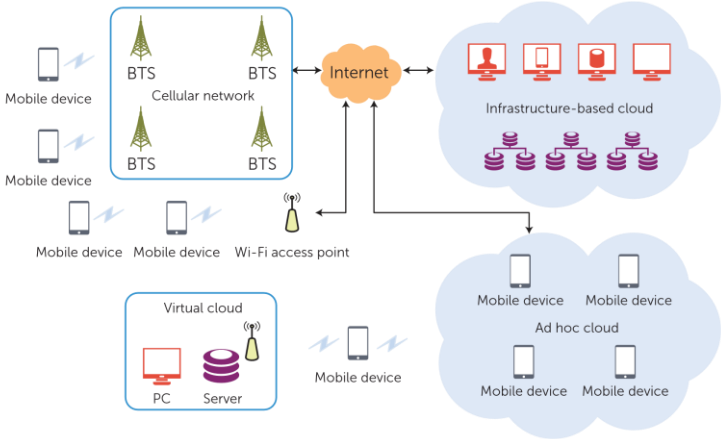

Fig. 1. Architecture of Mobile Cloud Computing.

Although there are several issues and challenges associated with mobile cloud computing which causes a barrier in its rapid evolution and advancement [10]. These problems and challenges include the number of finite resources in consumer mobile phone, availability, mobility management, network access charges, shortage of channel bandwidth, stability, process offloading, elasticity, trust, application services issues, heterogeneity, ensuring the quality of service, security and privacy issues, etc Among these, privacy becoming more challenging issues than others due to several reasons like resource constraint mobile devices, distributed cloud storage and processing, and heterogeneous environments [11]. As shown in Fig. 2, when mobile user deliver their data to cloud vendor server for using on-demand storage services, they ultimately lose the physical control of their data. Here, the mobile terminal uses the open-source operating system and third party software in the mobile network. Under these circumstances, the attacker exposes the privacy of the user and can misuse its information without their knowledge which ultimately results in privacy leakage, information loss and devices damage through all kinds of attack methods [12]. Whereas, the mobile user is concerned about the vulnerability to attacks when personal information and critical IT resources are outside the firewall. Here, software vulnerabilities involve data transfer with phone and computer using FTP [13]. Therefore, this promotes a drastic need for technology to resolve privacy issues of the mobile user while storing and processing their confidential data to the cloud environment where they lose physical control of their data.

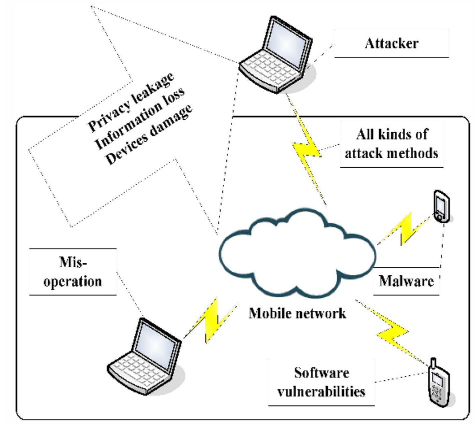

Fig. 2. Overview of Privacy Leakage.

A secure MCC user is required to protect these fundamental privacy factors including their personal data, real identity, current location and the actual query to access the data from the cloud. These objectives preserve the privacy directly or indirectly for the cloud service user in mobile devices [14]. The mobile user is said to be fully protected when these privacy factors fully secure them. In the current study, we aimed to investigate the privacy challenges and protection goals related to MCC. Further, we concentrate on the existing approaches that are preserving mobile user privacy in MCC. Then, we compare and analyze all the existing state of the art methods concerning privacy factors. Based on findings, the current study has come up with a promising solution that reduces privacy risks for MCC. After comparison, the most promising approach could be the pseudo-random permutation method due to its privacy level and high scalability. At the end of this paper, future research directions are presented which may help in providing a fully safe environment and reduce the privacy issues between the mobile user and server provider for wide acceptance of mobile cloud computing.

The remaining paper is structured as follows: Section 2 highlights the privacy challenges and protection goals of the mobile cloud computing. Related work of the concerned issue is discussed in Section 3. Section 4 explains the research methodology of this paper in detail. In section 5, we have presented a comparative analysis of the existing state of the art models with its strong points and privacy levels. Section 6 provides a discussion and recommendation for this paper and finally, Section 7 presents the conclusion of the work.

2. MCC Privacy Challenges and Protection Goals

In mobile cloud computing, privacy and data protection, are the biggest challenge for the mobile user as their confidential data is stored and relocated from mobile devices to heterogeneous distributed cloud servers leveraging various cloud services [15]. These servers are situated in different places that are owned and maintained by the service providers only. For instance, Google's cloud servers are nearly everywhere, with seven locations in the Americas, two in Asia and three in Europe. Therefore, cloud storage and processing in multiple locations pose serious privacy concerns where mobile user personal information stored remotely [16], which may be disclosed without their permission e.g. update about user current location, real identity, and the data regarding actual query sent to the service provider. Furthermore, location-aware applications and services raise privacy concerns for mobile devices [17]. They take user location information to deliver location-based services [18]. Therefore, LBS also raises privacy challenges as they need to collect, store, and process the personal information of the user such as hobbies, locations, and other credentials [19]. Thus, privacy concerns related to data protection are in the hands of the service providers, and the mobile user is not responsible for the lack of privacy.

To reduce the privacy risk for MCC users, four privacy metrics are needed to preserve. The attributes include data privacy, identity privacy protection, location, and query privacy. The challenges that are focused on this paper are depicted in Fig. 3. The mobile user is said to be fully protected when these privacy factors fully secure them.

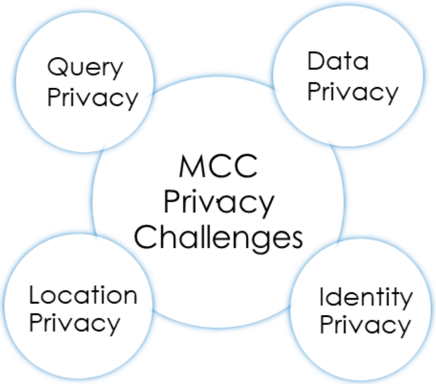

Fig. 3. MCC Privacy Challenges and Protection Goals.

2.1. Data Privacy

Mobile user facing problems when their confidential data shifted from mobile devices to the heterogeneous distributed cloud servers as they lose physical control of their data. It is essential to ensure this private information not exposed to an unwanted individual who might be an intruder/adversary.

2.2. Identity Privacy

Mobile user identity information includes user ID, address, contact number, or any aggregation of the related key terms that are used to uniquely identify the user. The aim is to hide user identity when they are availing different services from cloud vendors.

2.3. Location Privacy

The absence of location privacy can lead to the disclosure of important information about the mobile user. Location privacy refers to hiding current and past information from the attacker and preserving the level of detail influences the potential misuse of information.

2.4. Query Privacy

It is important to ensure a complete and fully safe environment when mobile users make a query to the service provider and retrieve their stored data. The primary objective is to preserve data query privacy when the user accesses their data.

3. Related Work

The authors in [20, 21, 22, 23] introduced several methods to preserve mobile user's data privacy in mobile cloud computing. In [20], the author proposed a privacy-preserving framework that ensuring the protection goals of MCC. It preserves the privacy of data shifted from mobile device to the service provider. This framework makes use of probabilistic pubic key encryption and ranked keyword searching algorithm. At the initial step, the mobile user creates an index for available files, and before sending for storing in the cloud vendor server, it encrypts both the data and index. To retrieve the saved data, a trapdoor is created by the user as a keyword and forward to the service provider. When the service provider takes trapdoor, it searches a list of matched data entries and its corresponding encrypted results. Based on the relevant result, matching data is returned to the user in the ranked series. Ultimately, the user can restore the original data through decryption. This framework is highly scalable in terms of data protection of mobile users but it doesn’t provide adequate protection against attribute disclosure.

In [21], the authors proposed a novel cryptographic method that ensures the data privacy of a mobile device. For storing data on clouds, this method is titled a pseudo-random permutation operation where permutation operation is done on mobile devices instead of the cloud in order to protect data privacy. Its scalability is considerably high. This method also preserves identity and location but doesn’t employ query privacy. This method has the capability of protecting all information pertaining to the personal sphere of mobile users except query privacy.

In [22], the author proposed privacy assured data utilization approach in the cloud. Here, a private cloud is used that is introduced as a trusted proxy server to reinforce the keyword searching method for privacy-preservation and access control over encrypted data on the public cloud. Its scalability is moderate. This approach is highly suitable in terms of data protection of mobile users but it doesn’t provide adequate protection against attribute disclosure.

In [23], the author presented a scheme of public auditing which is the dynamic hash table (DHT) scheme. It is a two-dimensional storage medium in which the auditor registers the information of data property in order to audit the data more rapidly and dynamically. In this technique, metadata extract the transfer of block tags to auditors from the service provider. As the result, there is a minimization in computational and communication overhead. This scheme uses homomorphic authentication that is a public key and random mask developed by the auditor to protect privacy but doesn’t guarantee all protection goals required to protect all personal information of mobile users.

The authors in [24, 25, 26, 27, 28] present approaches to protect mobile user's identity privacy in MCC. In [24], the authors presented the public auditing protocol to guarantee identity privacy of mobile user. It could be regarded as the most appropriate scheme for protecting mobile users’ identity information at the mobile cloud by providing support for the chameleon hash signature algorithm. However, this protocol allows the user to randomly extract a pseudo-key pair and modify the data tag with this pseudo-key pair to conceal their identity information. The cloud server therefore cannot distinguish the actual source of the outsourced data. This method is highly suitable in terms of identity protection of mobile users but it doesn’t provide adequate protection against other privacy attributes such as location disclosure, data and query protection.

In [25], the author proposed an auditing protocol for public use that protects the shared data from compromising its integrity in the cloud environment. This protocol makes use of proxy re-signature and asymmetric group key agreement scheme. Here, the asymmetric group key scheme allows publicly sharing secret keys between members of the group and tags are created for files. When group members are changed, the proxy re-signatures allows users to upgrade the tags. Furthermore, this technique protects the identity of the mobile user and related information by providing anonymousness to the group members and auditors but couldn’t provide location and query protection.

In [26], the author proposed an improved identity management protocol (I2DM) that uses pretty good privacy (PGP) based on public key infrastructure (PKI). It facilitates interactions based on mutual dependency and proper management of mobile user identities. It provides the fine-grained sharing of data and helps to maintain the scalability in the cloud environment. Thus, this protocol is highly scalable in terms of identity protection of mobile users but it doesn’t provide adequate protection against other privacy factors such as location disclosure, data and query protection.

In [27], the author presented consolidated identity management (CIDM) architecture that protects mobile user identity from many possible vulnerabilities such as privacy leakage from the identity management server, compromising mobile devices, and interception of network traffic in MCC. Here, IDM is a third party server that administers the digital identifications of mobile users on behalf of service providers under this CIDM architecture. The protection procedure includes three steps such as (1) Separating the user, IDM server and service providers authorization credentials to preserve unauthorised access against IDM misuse or interception (2) Provided an additional authentication layer to avoid compromising mobile device and (3) To increase the safety of the CIDM and cloud service provider, communication channel has added among them, this reduces the risk of a successful breach of this communication. This scheme provides moderate level scalability and hence ignore location and query privacy.

In [28], the author proposed a method which is based on dynamic credential generation instead of the digital credential method. The dynamic credential method means outsource data to third-party entities to reduce the computational overhead of mobile devices. Here, dynamic credentials are created based on communication between mobile devices and the cloud to provide greater protection against credential thefts. This scheme has three entities such as mobile users, service providers, and managers. In order to ensure authenticated smartphones, the agent first allows users to connect and then forwards the dynamically generated credentials, and these credentials are encrypted with user public key to guaranteeing confidentiality. This architecture is ensure user identity privacy and neglect remaining fundamental factors such as current location privacy, data and query protection.

The authors in [29, 30] proposed schemes to protect mobile user's query privacy in MCC. In [29], the author introduced a privacy assured substructure similarity query (PASSQ). This proposed technique implies three algorithms say secure index construction, trapdoor generation, and query processing. The secure index turns the original into an encrypted form to hide the details. And the last two algorithms are used to measure privacy and to create trapdoor similarities. However, this proposed solution protects the query related information of the mobile user and doesn't guarantee identity, location, and the data query protection.

In [30], the authors propose a solution to protect data query privacy for the mobile user in MCC. In this method, two ways are presented, one is for the server-side and another is for the mobile client-side. In the server-side method, dynamically generated VMs act as proxies for data protection within communication between the server and mobile device. While in mobile client-side, live migration from VMs at the application level is carried into the cloud to cover eavesdropper's data collection as well as aggregation procedures. Although, this mechanism has low scalability in terms of data query protection. Also, it doesn't provide adequate protection against other privacy factors which may put the privacy of mobile user at risk.

To protect location privacy, several approaches have been proposed. Among them, caching aware dummy selection algorithm (CaDSA) is the most popular model. The authors in [31, 32, 33, 34] introduce the techniques to preserve mobile user's location privacy in MCC. In [31], the author present a caching aware dummy selection algorithm (CaDSA) to improve the location privacy of mobile users. In this algorithm, the mobile device sends false location information with their real spatial data to LBS providers as a query parameter. In this way, the service provider unable to understand the user's primary agenda in the wrong way. However, this approach is highly scalable for protecting location related information of mobile user but unable to preserve user identity, data and query protection.

In [32], the author propose LP-doctor, a fine-grained location access control tool to preserve location privacy risk from location access of MCC user. It's a mobile device level tool that allows the users to use OS based location access control without any change in the application layer. It has several modules with specific functions such as application session manager, policy manager, place detector, mobility manager, threat analyzer, and anonymization actuator. The first module supervises application launch and exit events to anonymize location. The second module sustains a privacy policy for currently visited places and launched applications. The third module observes the user's current location, and the next module updates the user location profile when the user changed its location. The threat analyzer module decides whether the user is detected or not based on the user's policies manager. If this module decides to protect the location information, then the last module takes necessary actions by adding a fake location to ensure location anonymity. Finally, this LP-doctor preserves location related information of the mobile user with moderate scalability but it ignores the identity and query protection that may disclose the user information.

In [33], the author introduce location privacy preservation scheme (LPPS) to conceal the location privacy of the MCC user. This approach displays a distributed cache proxy to store commonly visited locations in clusters, and transfer the requested location data to individual mobile users from the group. If data is available in the cache, the user does not communicate with the LBS service provider to send out location related queries. In this way, this scheme preserves the location privacy of the mobile user. Moreover, this scheme provides high scalability and hence ignore identity-related information and data query privacy.

In [34], the author present a privacy protection method named location-based information survey applications (LB-ISA). It uses the mobile device clone-level samples in the cloud. The computation of the delivery function across a peer-to-peer network is shared to cloud clones. The cloud clone provides greater access to system services than mobile devices [35], which protect privacy. This scheme offers a strong load balancing, low overhead and cost connectivity with increased privacy level in LB-ISA. Thus, this scheme doesn't provide adequate privacy to identity-related information and data query protection [36].

4. Research Methodology

In order to achieve our objectives, our research will include the following phases. The steps of research methodology adopted in this research study are shown in Fig. 4 and their detailed description is given below.

4.1. Set Aims and Objectives of Research

The primary focus of this research was to critically analyze the various proposed approaches and strategies in the related work to suggest the most effective approach for preserving mobile user privacy on MCC by taking into account the efficacy and certainty of the approach.

4.2. Preparation of Proposal

For the preparation of the proposal, random research papers were selected from ACM and IEEE digital libraries in order to study the current issues in the domain. Based on these articles, proposal was written to define the problem statement and propose research topic.

4.3. Compilation of Research Papers in the Relevant domain i.e. Privacy in Mobile Cloud Computing

Afterwards, it was decided that systematic review of literature will be followed. In order to perform the systematic review, different digital libraries were searched out for the research articles under Privacy in Mobile Cloud Computing keyword.

4.4. Search for Research Papers

While searching articles, it was found that IEEE digital library contains most relevant research articles. With the keyword of “Privacy in Mobile Cloud Computing” total 65 articles were found.

4.5. Selection of Relevant Research Papers and Division of Research Papers

Selected research articles were divided into four major categories by taking into account the different approaches related to our privacy issue in MCC. From these categories, there were different techniques for privacy protections goals and the articles which did not lie under these techniques were discarded.

4.6. Literature Writing

Literature review was performed based on the selected articles and the main focus remained on the techniques that were related to privacy protection and other techniques were ignored for the sake of this research.

4.7. Comparative Study of Approaches

Comparative study of all the surveyed techniques was performed in order to come up with comparative analysis. Once the critical analysis performed, suggestions were given for improvement of the most robust approach.

4.8. Selection of the most Suitable Scheme

After critical survey, we have analyzed these approaches to move toward a right solution in current study. Therefore, most suitable and effective techniques has been selected on the basis of the comparative study.

4.9. Discussion and Recommendation

The improvement in the selected technique and suggestions have been discussed in the detail so that efforts can be made in future to make our suggested scheme more efficient.

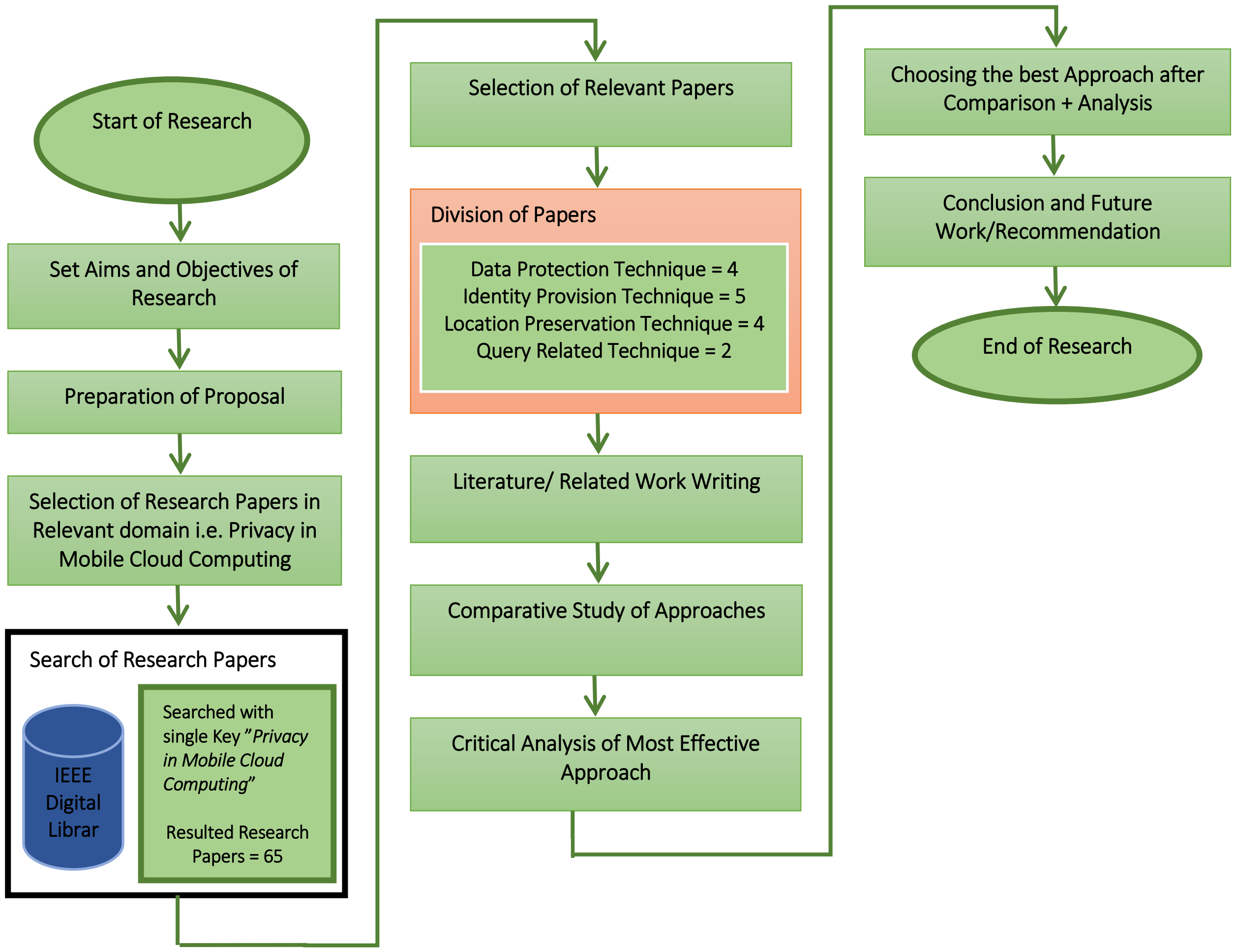
Start of Research
Set Aims and Objectives of Research
Preparation of Proposal
Selection of Research Papers in Relevant domain i.e. Privacy in Mobile Cloud Computing
Search of Research Papers
IEEE Digital Librar
Searched with single Key "*Privacy in Mobile Cloud Computing*"
Resulted Research Papers = 65
Selection of Relevant Papers
Division of Papers
Data Protection Technique = 4
Identity Provision Technique = 5
Location Preservation Technique = 4
Query Related Technique = 2
Literature/ Related Work Writing
Comparative Study of Approaches
Critical Analysis of Most Effective Approach
Choosing the best Approach after Comparison + Analysis
Conclusion and Future Work/Recommendation
End of Research

Fig. 4. Research Methodology

5. Comparative Analysis of Existing State of the Art Methods in Mobile Cloud Computing

In this section, we have made a comparative analysis of all the techniques that reduce privacy risk for the mobile user. We have described the proposed approaches with its strong points and privacy level with protection goals including data privacy, identity privacy protection, location, and query privacy. We also highlight the scalability of the presented work. Most approaches have still missing features to ensure a fully private environment for MCC user [37, 38]. Hence, the conclusive summary of related works is presented as the tabular format in Table 1 containing five columns which are described below:

- **Ref. No** is the first column showing reference to the proposed schemes presented in this paper.
- **Strong Points** is the second column presenting the short description of each state of the art method.
- **Protection Goals** is the third column containing the privacy factors measured by proposed scheme.
- **Privacy Level** describes the current level of existing methods counting privacy issue in MCC. It contains various entities, namely excellent, good better, bad and worst.
- **Scalability** describes to what extent the proposed schemes handle scalable service. It comprises four entities, namely high, moderate, medium and low.

Table 1. Comparison of existing methods counting privacy issues in MCC

Ref. No	Strong Points	Protection Goals				Privacy Level	Scalability
		Data Privacy	Identity Privacy	Location Privacy	Query Privacy		
[20]	Utilize probabilistic public-key encryption and ranked keyword searching algorithm to preserves the privacy of mobile user.	Yes	No	No	No	Good	High
[21]	Use Pseudo-random permutation method where permutation operation is done on mobile devices instead of the cloud to protect data privacy.	Yes	Yes	Yes	No	Excellent	High
[22]	Employ trusted proxy servers to support privacy-preserving keyword searching and access control over encrypted data on the public cloud.	Yes	No	No	No	Bad	Moderate
[23]	The two-dimensional data structure, homomorphic authentication provide privacy to the mobile user in the cloud.	Yes	No	No	No	Worst	Moderate
[24]	The chameleon hash signature algorithm used that allows the user to randomly extract pseudo-key pair to conceal their identity information.	No	Yes	No	No	Good	High
[25]	Use asymmetric group key agreement and proxy re-signature to protect the identity related information of the mobile user.	No	Yes	No	No	Bad	Medium
[26]	Employ pretty good privacy (PGP) based on mutual dependency and proper management of mobile user identities.	No	Yes	No	No	Good	High
[27]	Trusted third-party managers add an extra layer of authentication to protect mobile user identity from many possible vulnerabilities.	No	Yes	No	No	Good	Moderate
[28]	Dynamic credential generations used that outsource data to third-party entities to reduce the computational overhead of mobile devices.	No	Yes	No	No	Worst	High
[29]	Secure index construction, trapdoor generation and query processing are used to measure privacy for the mobile user.	No	No	No	Yes	Better	Moderate
[30]	Dynamically created VMs as proxies, live migration of application-level VMs are utilized to provide privacy to the mobile user.	No	No	No	Yes	Bad	Low
[31]	Creating fake locations and sends with original information to the LBS service provider for improving the location privacy of mobile users.	No	No	Yes	No	Good	High
[32]	Use trusted manager and analyzers that allows the users to use OS based location access control to preserve location privacy of the user.	No	No	Yes	No	Better	Moderate
[33]	Utilizes distributed cache proxy servers to store commonly visited locations in clusters to preserve the location privacy of the mobile user.	No	No	Yes	No	Bad	High
[34]	Use cloud infrastructure where the mobile device is system-level cloned to protect location privacy of the mobile user.	No	No	Yes	No	Good	Moderate

6. Discussion and Recommendation

Mobile cloud computing signifies immense advantages for individuals and the community by improving reliability, enabling computation offloading, extending battery life, enhancing the data storage capabilities and processing power of mobile devices. The evolution of cloud computing leads to a new era where different computing paradigms integrate through mobile wireless communication network systems such as cellular phones. MCC brings benefits for mobile users, network providers as well as cloud providers by combining cloud computing and mobile networks. Both data storage and data processing happen outside the mobile device. Thus, all resource-intensive computing performed in the cloud environment. MCC offers these services at low cost in on-demand fashion by providing reliability, availability, scalability, dynamic provisioning, multi-tenancy and ease of integration.

The mobile user is concerned about the vulnerability to attacks when personal information and critical IT resources are outside the firewall. Here, vulnerabilities involve data transfer with phone and computer using FTP. Mobile user personal information stored remotely, which may be disclosed without their permission e.g. update about mobile user actual location to an unwanted individual who might be an intruder/adversary. On the other hand, most of the mobile users avail Location-based services to obtain information by directly connecting their current location. Then, LBS provide desired data that has been extracted and processed taking account of the user's current location. The extensive utilization of these services poses major privacy issues such that the attacker can hack their credentials and use it for useless means. In consideration of privacy factors while defending mobile users' privacy when they outsourcing their data to service providers are their personal data, real identity, current location and the actual query sent to the cloud vendor server. To achieve all these goals, there is no state of the art method that achieves all these factors simultaneously to protect user privacy and fulfil privacy requirements for MCC user.

To overcome these privacy challenges, there is a demand for reliable communication medium connecting the cloud and mobile devices where user data and personal information could not be exposed to unauthorized people. Moreover, there is a need to protect data with proactive privacy plan where right policies, technologies and techniques should be considered to win the battle of privacy breaches. Thus, there is a need to focus on privacy threats to establish a robust and secure MCC privacy preserving method. Therefore, the current study analyzed and compare recent solutions and countermeasures techniques proposed so far by the different researchers to provide privacy in MCC. After critically analyzing all these approaches, we have observed that pseudo-random permutation method could be regarded as the most appropriate and robust scheme for preserving mobile user privacy at mobile cloud by utilizing ranked keyword searching and cryptographic methods. Hence, the suggested state of the art method encounters both privacy requirements as well as performance. If we try to find out more ways to improve the performance of the above mentioned techniques then privacy could be improved for preserving data and personal information in mobile cloud computing. However, the current study provides a promising roadmap to research and development community for the right selection of privacy approach so that enhancing any available algorithm or policy will help in accumulating more secured data and preserve personal information while storing or retrieving data between mobile and cloud. Although this research field is still unexplored in-depth, many challenges are still under consideration. In this paper, we mentioned some open research challenges of mobile cloud computing that require additional efforts and identify future research directions in this field.

7. Conclusion

Recently, mobile cloud computing has attracted significant attention to computing industries, promises to meet the requirement for richer mobile services. However, due to the integration of mobile computing with cloud computing infrastructure, privacy is a big concern in MCC. In the current study, we aimed to investigate the privacy challenges related to MCC. To address the problem, we analyze these issues from a mobile user perspective such as their personal information and data query preservation. Leading to the research challenges, we have conducted a comprehensive survey to investigate the existing state of the art approaches and analyzed them critically. Based on findings, the current study has come up with a promising solution that reduces privacy risks for MCC users. After a critical analysis, the current study suggests the pseudo-random permutation method could be a promising model that can be taken into consideration for preserving user data and personal information on MCC more efficiently. We hope this paper will help you regarding privacy challenge, their state of the art methods and future research directions in mobile cloud computer field. This research area is too big, we discuss some open research areas in this manner but many challenges are still under research and need to be analyzed and solved. It still requires further research efforts to enhance the suggested method to provide a fully private environment to the mobile user while availing different cloud services.

Acknowledgements

This work was performed under auspices of Department of Computer Science and Information Technology, Government College Women University Sialkot, Pakistan by Heir Lab-78. The Authors would like to thanks Dr. Muhammad Usman Ashraf for his continuous support, enthusiasm, insightful, and constructive suggestions throughout the research.

References

[1] Lane, N.D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T. and Campbell, A.T., A survey of mobile phone sensing. IEEE Communications magazine, 48(9), pp.140-150. 2010.

[2] Rahimi, M. Reza, et al. "Mobile cloud computing: A survey, state of art and future directions." Mobile Networks and Applications, pp. 133-143, 2014.

[3] Qi, Han, and Abdullah Gani. "Research on mobile cloud computing: Review, trend and perspectives." 2012 Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP). IEEE, 2012.

[4] Rida Qayyum, Hina Ejaz, "Data Security in Mobile Cloud Computing: A State of the Art Review", International Journal of Modern Education and Computer Science (IJMECS), Vol.12, No.2, pp. 30-35, 2020. DOI: 10.5815/ijmecs.2020.02.04

[5] Gao, Jerry, Volker Gruhn, Jingsha He, George Roussos, and Wei-Tek Tsai. "Mobile cloud computing research-issues, challenges and needs." In 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, pp. 442-453. IEEE, 2013.

[6] Buyya, Rajkumar, et al. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." Future Generation computer systems, pp. 599-616, 2009.

[7] Arpaci, I., Understanding and predicting students' intention to use mobile cloud storage services. Computers in Human Behavior, 58, pp.150-157.

[8] Amin, Mohammed Arif, Kamalrulnizam Bin Abu Bakar, and Haider Al-Hashimi. "A review of mobile cloud computing architecture and challenges to enterprise users." In 2013 7th IEEE GCC Conference and Exhibition (GCC), pp. 240-244. IEEE, 2013.

[9] Prasad, M.R., Gyani, J. and Murti, P.R.K., Mobile cloud computing: Implications and challenges. Journal of Information Engineering and Applications, 2(7), pp.7-15. 2012.

[10] Alizadeh, Mojtaba, and Wan Haslina Hassan. "Challenges and opportunities of mobile cloud computing." In 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 660-666. IEEE, 2013.

[11] Jana, Debasish, and Debasis Bandyopadhyay. "Efficient management of privacy issues in mobile cloud environment." In 2015 IEEE International Advance Computing Conference (IACC), pp. 481-486. IEEE, 2015.

[12] Suo, Hui, Zhuohua Liu, Jiafu Wan, and Keliang Zhou. "Security and privacy in mobile cloud computing." In 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 655-659. IEEE, 2013.

[13] Qureshi, Shahryar Shafique, Toufeeq Ahmad, and Khalid Rafique. "Mobile cloud computing as future for mobile applications-Implementation methods and challenging issues." In 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, pp. 467-471. IEEE, 2011.

[14] Lin, H., Xu, L., Mu, Y. and Wu, W., A reliable recommendation and privacy-preserving based cross-layer reputation mechanism for mobile cloud computing. Future Generation Computer Systems, 52, pp.125-136. 2015.

[15] Horrow, Susmita, Sanchika Gupta, Anjali Sardana, and Ajith Abraham. "Secure private cloud architecture for mobile infrastructure as a service." In 2012 IEEE Eighth World Congress on Services, pp. 149-154. IEEE, 2012.

[16] Zhang, H., Yu, N. and Wen, Y., Mobile cloud computing based privacy protection in location‐based information survey applications. Security and Communication Networks, 8(6), pp.1006-1025. 2015.

[17] Ashraf, Muhammad Usman, Rida Qayyum, and Hina Ejaz. "STATE-OF-THE-ART, CHALLENGES: PRIVACY PROVISIONING IN TTP LOCATION BASED SERVICES SYSTEMS." International Journal of Advanced Research in Computer Science (IJARCS), 10(2), 2019. DOI: 10.26483/ijarcs.v10i2.6396

[18] Muhammad Usman Ashraf, Kamal M. Jambi, Rida Qayyum, Hina Ejaz and Iqra Ilyas, "IDP: A Privacy Provisioning Framework for TIP Attributes in Trusted Third Party-based Location-based Services Systems" International Journal of Advanced Computer Science and Applications (IJACSA), 11(7), 2020. DOI: 10.14569/IJACSA.2020.0110773

[19] Rida Qayyum, Hina Ejaz "Provisioning Privacy for TIP Attribute in Trusted Third Party (TTP) Location Based Services (LBS) System", May 2019. DOI: 10.13140/RG.2.2.25631.59041

[20] Pasupuleti, S.K., Ramalingam, S. and Buyya, R., An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Journal of Network and Computer Applications, 64, pp.12-22. 2016

[21] Bahrami, Mehdi, and Mukesh Singhal. "A light-weight permutation based method for data privacy in mobile cloud computing." In 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, pp. 189-198. IEEE, 2015.

[22] Li, H., Liu, D., Dai, Y., Luan, T.H. and Shen, X.S., Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage. IEEE Transactions on Emerging Topics in Computing, 3(1), pp.127-138. 2014

[23] Hui Tian, Y. "Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", IEEE Computer Society, 2015.

[24] Zhang, Y., Su, S., Wang, Y., Chen, W. and Yang, F., Privacy‐assured substructure similarity query over encrypted graph‐structured data in cloud. Security and Communication Networks, 7(11), pp.1933-1944.2014

[25] Yu, Y., Niu, L., Yang, G., Mu, Y. and Susilo, W., On the security of auditing mechanisms for secure cloud storage. Future Generation Computer Systems, 30, pp.127-132. 2014.

[26] Park, In-Shin, Yoon-Deock Lee, and Jongpil Jeong. "Improved identity management protocol for secure mobile cloud computing." In 2013 46th Hawaii International Conference on System Sciences, pp. 4958-4965. IEEE, 2013.

[27] Khalil, I., Khreishah, A. and Azeem, M., Consolidated Identity Management System for secure mobile cloud computing. Computer Networks, 65, pp.99-110.2014

[28] Khan, A.N., Kiah, M.M., Ali, M. and Shamshirband, S., A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach. Journal of Grid Computing, 13(4), pp.651-675. 2015

[29] Zhang, J. and Zhao, X., Efficient chameleon hashing-based privacy-preserving auditing in cloud storage. Cluster Computing, 19(1), pp.47-56. 2016.

[30] Owens, Rodney, and Weichao Wang. "Preserving data query privacy in mobile mashups through mobile cloud computing." In 2013 22nd International Conference on Computer Communication and Networks (ICCCN), pp. 1-5. IEEE, 2013.

[31] Niu, Ben, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li. "Enhancing privacy through caching in location-based services." In 2015 IEEE conference on computer communications (INFOCOM), pp. 1017-1025. IEEE, 2015.

[32] Fawaz, Kassem, Huan Feng, and Kang G. Shin. "Anatomization and protection of mobile apps' location privacy threats." In 24th {USENIX} Security Symposium, pp. 753-768. 2015.

[33] Chen, Ming, Wenzhong Li, Zhuo Li, Sanglu Lu, and Daoxu Chen. "Preserving location privacy based on distributed cache pushing." In 2014 IEEE Wireless Communications and Networking Conference (WCNC), pp. 3456-3461. IEEE, 2014.

[34] Zhang, Y., Zheng, D., Chen, X., Li, J. and Li, H., Efficient attribute-based data sharing in mobile clouds. Pervasive and Mobile Computing, 28, pp.135-149. 2016.

[35] Rida Qayyum. "A Roadmap Towards Big Data Opportunities, Emerging Issues and Hadoop as a Solution", International Journal of Education and Management Engineering (IJEME), Vol.10, No.4, pp.8-17, 2020. DOI: 10.5815/ijeme.2020.04.02

[36] Rida Qayyum, Hina Ejaz. "A Comparative Study of Location Based Services Simulators". International Journal of Computer Engineering in Research Trends (IJCERT), Vol.7, No. 11, pp.1-12, November 2020. DOI: 10.22362/ijcert/2020/v7/i11/v7i1101.

[37] Suguna, M., and S. Mercy Shalinie. "Privacy preserving data auditing protocol for secure storage in mobile cloud computing." In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 2725-2729. IEEE, 2017.

[38] Lyu M., Li X., & Li H. Efficient, Verifiable and Privacy Preserving Decentralized Attribute-Based Encryption for Mobile Cloud Computing. In IEEE 2nd International Conference on Data Science in Cyberspace (DSC), pp. 195–204, IEEE, 2017.

Author's Profile

Rida Qayyum (born September 17, 1996) received BS-Information Technology (BSIT) degree in 2019 from Government College Women University Sialkot, Pakistan. She has awarded with Gold Medal and Roll of Honour for her academic performance in BS-Information Technology from GCWUS and certified as Microsoft Office Specialist. She has many publications in international journals. Her research on Location Based Services Systems, Mobile Cloud Computing, and Big Data has appeared in International Journal of Advanced Research in Computer Science, International Journal of Advanced Computer Science and Applications, International Journal of Computer Engineering in Research Trends, I.J. Modern Education and Computer Science, I.J. Education and Management Engineering and I.J. Wireless and Microwave Technologies. She has served as HPC scientist in High Performance Computing Research Centre.

How to cite this paper: Rida Qayyum, " A Critical Survey on Privacy Prevailing in Mobile Cloud Computing: Challenges, State of the Art Methods and Future Directions", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.10, No.6, pp. 36-46, 2020.DOI: 10.5815/ijwmt.2020.06.05