I.J. Modern Education and Computer Science, **2020, 2, 30-35**
Published Online April 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2020.02.04

Data Security in Mobile Cloud Computing: A State of the Art Review

Rida Qayyum
Department of Computer Science, Government College Women University Sialkot, Pakistan
Email: ridaqayyum6@gmail.com

Hina Ejaz
Department of Computer Science, Government College Women University Sialkot, Pakistan
Email: hinaejaz299@gmail.com

Received: 01 January 2020; Accepted: 19 February 2020; Published: 08 April 2020

***Abstract*—**Due to tremendous use of smartphones the concern of cloud computing in mobile devices emerges, which is known as Mobile Cloud Computing (MCC). It involves the usage of mobile devices and cloud computing to perform resource intensive tasks using the internet with minimum impact on cellular resources. Nowadays, people are relying on mobile devices due to their small size and user friendly interface but due to its limited storage capacity, people can no more rely on internal RAM. Therefore, this promotes a drastic need for technology to make it possible for anyone to access their data anywhere anytime. As a result, Mobile Cloud Computing facilitates mobile users with its enticing technology by providing its on-demand and scalable services. But privacy and security are the main concern for a mobile user in the modern era. Thus, issues regarding security can be divided into cloud security and mobile network user's security, respectively. However, the primary focus of this study is to analyze how to secure the user's data in a mobile cloud. Leading to objectives, the current study presents a comprehensive analysis of existing techniques that can be considered for securing data in MCC efficiently. Moreover, this work will contribute a state-of-the-art roadmap to research and development communities for the right selection of proposed approach.

***Index Terms*—**Mobile Cloud Computing (MCC), data security, Secure Data Sharing in Clouds (SeDaSC), Homomorphic Encryption, data integrity, confidentiality, data storage

I. Introduction

Nowadays, technology is rapidly increasing due to the fast growth of the internet and mobile devices. People are depending on mobile devices due to their small size and user-friendly interface. But due to its limited storage capacity, people can no more rely on internal RAM provided by the device providers. However, there is a lot of work to do in order to spend life peacefully. Therefore, this raises a drastic need for technology to make it possible for anyone to access their data anywhere anytime. As a result, Mobile Cloud Computing facilitates the mobile user with its emerging technology [2].

There are many cloud computing services that are being offered to consumers. Mobile Cloud Computing is one of them. MCC comes in combination with cloud computing due to its essential features such as self-service, elastic, on-demand, pay per user, and the group of resources. Fig. 1 gives a basic idea of Mobile Cloud Computing in which the information is delivered by the user to the cloud vendor's server for using on-demand storage services, then the mobile user loses its physical control of data. As the user is unaware of its data location so there is a higher possibility that some malicious user gains access to its data and utilize it in an unauthorized way [3].

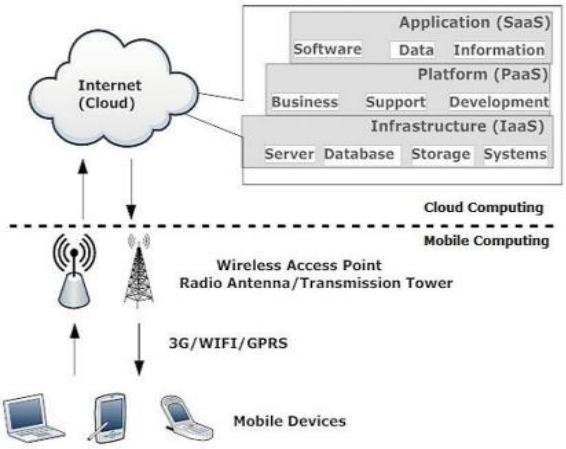

Fig. 1. A basic idea of Mobile Cloud Computing

The issues and challenges associated with Mobile Cloud Computing are a 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, security and privacy issues, etc. With the evolution of

Mobile Cloud Computing (MCC), some of the issues are the loss of the data confidentiality and security of mobile phone user, where primary impediments must be overcome with the rapid adoption of mobile cloud computing. Though it is a very diverse field so our focus one of its basic issues "Lack of Data security in MCC" [4]. Further, to address these issues we concentrate on the existing approaches that are securing user data in MCC. In the current study, we compare and analyze all the existing solutions under this category. After comparison, the most suitable schemes could be Secure Data Sharing in Clouds (SeDaSC) and data storage security scheme as they both are highly scalable. Hence, these promising solutions help us to achieve security for a mobile user's network.

The remaining paper is structured as follows: Section II describes the security architecture of Mobile Cloud Computing. Related work of the concerned issue is discussed in Section III. In section IV, we have presented a comparative analysis of proposed approaches with their strong points and security features. Section V provides a discussion for this paper and finally, section VI presents the conclusion of the work.

II. Security Architecture of Mobile Cloud Computing (MCC)

Basically, Mobile Cloud Computing security architecture comprises of three main parts, they are mobile devices, mobile internet, and cloud computing. Hence, mobile user trust and confidence in offered services are retained only by preserving user privacy from the attacker [5]. An underlying architecture of Mobile Cloud Computing can be explained in Fig. 2.

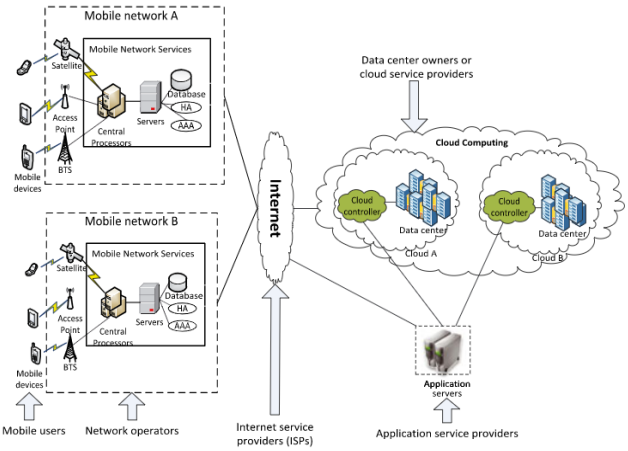

Fig. 2. Security Architecture of MCC

III. Related Work

Alqahtani and Kouadri-Mostefaou (2014) proposed a framework for ensuring the security of user's data in Mobile Cloud Computing. This framework makes use of data compression, data encryption and distributed multi-cloud storage schemes. At the initial step, data is divided according to user preferences into various sections and then it reserves distributed multi-cloud. However, to improve the security the mobile user can store one section of its data on its storage [6].

Abdalla and Pathan, (2014) work on the same framework and introduced data scheme for secure storage over Multi-clouds. The mobile users upload their data on the provider's server through data protection manager-consisting of two parts i.e. data merger and data fragmenter. Data merger is used to merge the user's uploaded data in such a way that it can be downloaded anytime from the stored data. On the other hand data fragmenter aims to make the fragments of data to forward them to multiple servers for storage. This framework is securing user's data in such a way that if one cloud is compromised then another one protects user's data against the unauthorized/unknown person from being alteration or misuse of data [7].

Another framework is presented by Wang et al. (2014) to provide data security on the cloud. This technique consists of three parts including scalable watermarking, secure sharing, and Reed-Solemon coding. Hence, in the context level, the watermarking technique is deployed to perform authentication. Besides conventional authentication done at the packet level, context level provides less operating cost. The multimedia content is forwarded to different clouds by fragmenting it into different chunks using secure sharing. Furthermore, the Reed-Solemon coding guarantees that the transmission of multimedia elements is accomplished reliably [5].

The security scheme for data storage is presented by Louk and Lim et al. (2015) that ensures the confidentiality of user's data in MCC. It could be regarded as the most appropriate and robust scheme for securing mobile users' data at mobile cloud by providing support for homomorphic encryption. Homomorphic encryption is a form of encryption that allows computation on ciphertext, generating an encrypted result which decrypted, matches the result of the operations as if they had been performed on the plaintext. [8].

Khan et al and Abdul Nasir Khan (2014), presented cryptography based Block Based Sharing (BBS) technique which establish the data integrity and confidentiality of mobile user's that is stored in cloud. In this technique, security operations of mobile device side include reasonably partitioning data into numerous chunks, apply encryption and decryption on those chunks and reorganization to make the actual form. Service providers of cloud only present storage of data. BSS provide better security than cloud, authors implement the performance which result that block based sharing scheme (BSS) has lower computational demanding security operation than current techniques [9].

The innovative data encryption technique titled as Dynamic Data Encryption Strategy (D2ES) is presented by Gai et al (2016). The technique employs the concerned encryption strategy by keeping in mind the required time for execution. [5].

A proxy-assisted technique utilizing the benefits of attribute-based encryption scheme is proposed by Yang et al (2015). It provides the fine-grained sharing of data and helps to maintain the scalability in the cloud environment. [9].

An auditing protocol for public use is proposed by Yu et al (2014) that protects the shared data from compromising its integrity in cloud environment. This protocol makes use of proxy re-signature and asymmetric group key agreement scheme. The Asymmetric group key scheme allow publically sharing secret keys between members of group and tags are created for files. When group members are changed, the proxy re signatures allow user to upgrade the tags. Furthermore, this technique protect identity of mobile user and related information by providing anonymousness to the group members and auditors [10].

A remote data auditing scheme is presented by Sookhak et al (2017) that ensures the integrity of the client's data stored on the cloud platform. This scheme makes use of algebraic signatures through which auditor can easily check the possession of mobile user's data. Author develop a new data structure to extend the method that divide and conquer the table (DCT) and support update operation of dynamic data. By using DCT at block level user can implement update operation of data without loading the complete data. At the end, author implement and analyze the work that result in which DCT and algebraic signature have less computational operation on cloud rather than traditional auditing data methods [11].

Yu et al (2016) proposed auditing data technique which apply the systems of zero knowledge proof, authenticators of linear homomorphic and proxy re-signatures [10].

Tian et al (2015) presented a scheme of public auditing which is Dynamic Hash Table (DHT) based 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 auditor from service provider. In the result, there is a minimization in computational and communication overhead. This Scheme uses homomorphic authentication that is public key and random masking based develop by auditor to protect the privacy [12].

A P2DS scheme called dynamic secure data scheme is presented by Qiu et al (2016) that is used to protect the data of the mobile user from the access of unauthorized users. This technique used semantic and proactive determinative access algorithms. To protect from unauthorized access Odelu et al 2016 and Jin et al (2015) presented ciphertext policy which is encryption (CP-ABE) based. These scheme grant access control in MCC and allow user to source fully computational processing from devices to cloud within lower encryption and decryption operation. Furthermore, the mobile users get control of flexible access to data [13].

A 2SBM model called IntercroSsed Secure Big Multimedia Model is presented by Li et al (2016) for guaranteeing secure access in cloud environment. This depends on recognition of ontology access and matching semantic information algorithms. [14].

An efficient multi-keyword ranked search (EMRS) scheme introduces by Hongwei Li et al. (2015) that makes use of relevance score and k-nearest neighbor algorithm to perform organized searching using multiple keywords over the secured mobile cloud data. Besides this, an efficient index is employed to improve search response. Furthermore, the blind storage system in this scheme is utilized to hide the pattern used by the user to access the data from the cloud server [15].

Guo et al. (2016) propose a different technique for controlling access and ensuring the security of searched data. It is based upon a public key attribute-based encryption technique having user's secret key and the ciphertext both depend upon specific aspects. The ciphertext cannot be decrypted unless the user key's attributes match with those of ciphertext [16].

D Liu et al. (2015) proposes personalized search-customization of search engine results that practices relevant information such as the user's history, location and preferences protecting data in Mobile Cloud. It makes use of the k nearest neighbor algorithm, bloom filter, vector-space based search and advanced attribute-based keyword search system. Firstly, k nearest neighbor and bloom filter methods are used for relevance based result ranking and effective multi-keyword searching. Furthermore, Vector-space based search and advanced attribute-based keyword search algorithms support searching controlling multiple users requesting large data [17].

An attribute-based data scheme proposed by Zhang et al. (2016). It combines Ciphertext-Policy attribute-based encryption (CP-ABE) with symmetric encryption to provide a secure mobile cloud environment. As CP-ABE is experiencing certain performance shortcomings concerning large ciphertext size and high computational, fit to only cloud computing not appropriate for MCC due to its restrained resources. But the addition of symmetric encryption to CP-ABE providing the consistent cost for computation over the mobile cloud [5].

JK Liu et al. (2015) introduce a support providing mobile users with the facility of sharing and searching video data on mobile cloud securely. It takes advantage of cryptographic algorithms including Searchable Symmetric Encryption (SSE) Ciphertext-Policy Attribute-Based Encryption (CPABE), Advanced Encryption Standard (AES) and Digital Signature (DS). For sharing video the user is required to register with an attribute-based secret key and with cloud server for controlling the access of data. Searchable keywords are attached to the video before outsourcing it to the cloud server. Ultimately video is secured employing AES, Symmetric Encryption (SSE) is employed to secure searchable keywords and CP-ABE to secure AES keys [5].

Mollah et al. (2017) present a secure scheme for searching and sharing the data on the cloud using remote mobile devices. This scheme applies advanced security

mechanisms including digital signatures, searchable secret key encryption, public key encryption and secret key encryption to secure the data on mobile cloud [18].

A Secure Data Sharing in Clouds (SeDaSC) scheme is introduced by Ali et al. (2015) having three components including the cryptographic server (CS), the user and the cloud. The data, access control and group members list is outsourced by the user to the cryptographic server. The encryption, decryption, access control and key management is done at CS end. First of all, to secure the data, the cryptographic server produces the symmetric key. This key is divided into two parts by the cryptographic server, one part is assigned to group members and another is allocated for access control. Ultimately the cloud saves the encrypted data by the permission of the user. Whenever data is required from the mobile cloud, a group member forwards its key with the request to the cryptographic server. The data then could be decrypted and retrieved from the cloud whenever the cryptographic server completes its authentication process [19].

IV. Comparative Analysis

In this section, we have made a comparative analysis of all the techniques that are securing the data on the Mobile Cloud Computing. We have described the proposed approaches with its strong points and security features including data confidentiality, authentication, data integrity, data privacy, identity privacy protection, access control, secure data sharing and searching. Most of approaches have still missing features to achieve a high security for MCC. To review the proposed approaches and its strong points and security features, follow the below Table 1.

Table 1. Evaluation of proposed techniques and framework

Ref	*Proposed Approaches*	*Strong Points*	*Security Features*
[5]	Secure data storage and sharing in mobile cloud	This technique consists of three parts including scalable watermarking, secure sharing, and Reed-Solemon coding.	Authentication and Data Confidentiality
[5]	Dynamic Data Encryption Strategy	This technique apply a careful encryption scheme within appropriate requirement of execution time.	Data Confidentiality
[5]	Attribute based data in MCC	It combines Ciphertext-Policy attribute-based encryption (CP-ABE) with symmetric encryption to provide a secure mobile cloud environment.	Secure Data Sharing
[5]	Secure real time video sharing and searching in MCC	Introduce a support providing mobile users with the facility of sharing and searching video data on mobile cloud securely.	Secure Data Sharing and Searching
[6]	Multi-clouds for secure data storage	At the initial step, data is divided according to user preferences into various sections and then it reserves on distributed multi-cloud.	Data Confidentiality
[7]	Data scheme for secure storage over Multi-clouds	Through data protection manager, the mobile user uploads their data to the service provider. First is data merger and second is data fragmenter.	Data Confidentiality
[8]	Security of data storage	In this framework, homomorphic encryption is used to provide security.	Data Confidentiality
[9]	Block based sharing scheme (BSS)	In this technique, security operations of mobile device side include reasonably partitioning data into numerous chunks, apply encryption and decryption and reorganization to make the actual form.	Data Confidentiality
[9]	Extended Proxy-Assisted	Technique which is depend on encryption of attributes to maintain scalability and grained data which shared with cloud.	Data Confidentiality
[10]	A public auditing protocol	It protects the shared data from compromising its integrity in cloud environment.	Data Integrity, Identity Privacy protection
[10]	Cloud Data Auditing	Apply the systems of zero knowledge proof, authenticators of linear homomorphic and proxy re-signatures.	Data Integrity
[11]	Remote data auditing	This scheme is algebraic signature based in which auditor can easily check the possession of mobile user's data.	Data Integrity
[12]	Dynamic hash table	It is a two-dimensional storage medium in which the auditor registers audit the data more rapidly and dynamically.	Data Integrity and Data Privacy
[13]	Proactive dynamic secure data scheme (P2DS)	This technique used semantic and proactive determinative access algorithms to protect from unauthorized access.	Access Control
[13]	ciphertext policy	These scheme allow user to source fully computational processing from devices to cloud within lower encryption and decryption operation.	Access Control
[14]	IntercroSsed Secure Big Multimedia Model (2SBM)	It is used to protect access with various platforms in cloud by depending on recognition of ontology access and matching semantic information algorithms.	Access Control
[15]	Efficient multi-keyword ranked search (EMRS)	Makes use of relevance score and k-nearest neighbors' algorithm to perform organized searching using multiple keywords over the secured mobile cloud data.	Secure Data Searching
[16]	Fine-grained Data	It is based upon a public key attribute-based encryption technique having user's secret key and the ciphertext both depend upon specific aspects.	Secure Data Searching
[17]	Personalized search over encrypted data and secure updates (PSU)	It makes use of the k nearest neighbor algorithm, bloom filter, vector-space based search and advanced attribute-based keyword search system.	Secure Data Searching
[18]	Secure data sharing and searching at the edge of cloud network	This scheme applies advanced security mechanisms including digital signatures, searchable secret and public key encryption to secure the data.	Secure Data Sharing and Searching
[19]	Secure Data Sharing in Clouds (SeDaSC)	This technique has three components including the cryptographic server (CS), the user and the cloud.	Secure Data Sharing, Access Control

V. Discussion

Cloud Computing is considered to be the most engaging technology in the modern era due to its on-demand and scalable services. Mobile Cloud Computing is another enticing technology that connects modern cloud computing markets by omnipresent smartphone technology. Both mobile users and cloud-based service providers have supported and appreciated the benefits of using mobile cloud.

MCC framework involves the usage of cloud computing model to endeavor resource intensive jobs using the internet with minimum influence on cellular resources. It depends upon erroneous wireless channel due to the limited processing power and memory provided by the mobile devices. Due to limited battery life, Mobile devices provide little support for an advanced reliable security layer. Moreover, security and privacy are the most crucial challenges to address in Mobile Cloud Computing. In the modern era of mobile cloud computing, these security threats are going to be the major obstacle.

To overcome these security challenges, there is a demand for reliable communication medium connecting the cloud and mobile devices. The security threats should be analyzed and examined to establish a robust and secure MCC framework. Therefore the current study focuses upon studying and comparing different approaches proposed so far by the different researchers to provide data security in MCC.

In this paper, after critically analyzing all the approaches proposed so far, we have observed that data storage security technique providing support for homomorphic encryption and Secure Data Sharing in Clouds (SeDaSC) scheme could be regarded as the most appropriate and robust scheme for securing mobile user data at mobile cloud by providing high level of encryption. If we try to find out more ways to improve the performance of above mentioned techniques then security could be enhanced and these both schemes could be considered promising for securing data in mobile cloud computing.

VI. Conclusion

We conclude from the above discussion that mobile computing has provided mobile users' the facility to store their data easily on mobile cloud and made their jobs more comfortable as they can access the cloud services from anywhere over the internet. But still, numerous issues need to be considered while moving towards MCC i.e. availability, data security, identity & location privacy, browser security, lock-in, heterogeneity, access control, mobile device security, virtualization security, partitioning and offloading security challenges. The most important challenge that needs to be addressed in MCC is the data security issue. In this paper, we have conducted a comprehensive survey on the technique that is securing user data in mobile computing. Based on a critical analysis, the current study suggested that the data storage security scheme and Secure Data Sharing in Clouds (SeDaSC) scheme could be a promising model that can be taken into consideration for securing user data on Mobile Cloud Computing more efficiently. This research area is too big, we discuss some problems in this manner but still many security issues need to be analysed and solved. We hope this paper will help you regarding state of the art challenges in Mobile Cloud Computer Security. In future, the work can be done on the proposed scheme for providing data security, authentication, and data confidentiality with data integrity so that Mobile Cloud Computing will be widely accepted.

Acknowledgment

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 insightful, and constructive suggestions throughout the research.

References

[1] Rupinder Pal Kaur, A. K. “Perspectives of Mobile Cloud Computing: Architecture, Application and Issues”, International Journal of Computer Applications, pp. 9-14, 2014.

[2] S M Shamim, A, S, and Ali Newaz Bahar, M. A. “A Review on Mobile Cloud Computing”, International Journal of Computer Applications, pp. 4-9, 2015.

[3] Sudhanshu Maurya, D. K. “A Literature Review on Mobile Cloud Computing”, International Journal of Applied Engineering Research, Vol. 10 No.79, pp. 329-334, 2015.

[4] Nirbhay K. Chaubey, D. M. “Security, Privacy and Challenges in Mobile”, International Journal of Innovative Research in Computer, pp. 1259-1266, 2016.

[5] Muhammad Baqer Mollaha, M. A, and Vasilakosb, A. “Security and privacy challenges in mobile cloud computing”. Journal of Network and Computer Applications, pp. 38-54, 2017.

[6] Hassan Saad Alqahtani, G. K.-M. “Multi-Clouds Mobile Computing for the Secure Storage of Data”, IEEE/ACM 7th International Conference on Utility and Cloud Computing, pp. 495-497, 2014.

[7] Abdul Nasir Khan, M. L, and Mazhar Ali, S. A. “BSS: block-based sharing scheme for secure data storage services in mobile cloud environment”, Springer the Journal the Supercomputing, 2014.

[8] Louk M., Lim, H. “Homomorphic encryption in mobile multi cloud computing, in Information Networking (ICOIN)”, 2015 International Conference on, pp. 493-497, 2015.

[9] Rahul Neware, A. K., and Dandige, V. “Survey on Security issues in Mobile Cloud Computing and Preventive Measures”.

[10] Yong Yu, L. N. “On the security of auditing mechanisms for secure cloud storage”, 2013

[11] Chandni Patel, S. C. and Patel, B. “A Data Security Framework for Mobile Cloud”, International Journal of Advanced Research in Computer and Communication Engineering, pp. 254-257, 2015.

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

[13] Ibtihal Mouhib, El Ouadghiri Driss and Khalid Zine-Dine "Encryption as a service for securing data in mobile cloud computing", 15th International Conference on Intelligent Systems Design and Applications (ISDA), pp. 546-55, 2015.
[14] Muhammad Baqer Mollaha, M. A and Vasilakosb, A. "Security and privacy challenges in mobile cloud computing: Survey and way", Journal of Network and Computer Applications, pp. 38-54, 2017.
[15] Hongwei, Li. Dongxiao, Liu. Yuanshun, Dai. Tom, H. Luan, Xuemin. Sherman, She "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", pp.127-138, 2015.
[16] Cheng Guo, R. Z, and Yingmo Jie, Y. R. "Fine-grained Database Field Search Using Attribute-Based. Journal of Medical Systems", pp. 235-244, 2016.
[17] Hongwei Li, D. L, and Yuanshun Dai, S. Y. "Personalized Search Over Encrypted Data With Efficient and Secure Updates in Mobile Clouds", IEEE Xplore, pp. 1-12, 2015.
[18] Muhammad Baqer Mollah and M. A. "Secure Data Sharing and and Searching at the Edge of Cloud-Assisted Internet of Things". IEEE Cloud Computing, pp. 34-42, 2017.
[19] Mazhar Ali, R. D, and Eraj Khan, S. "Secure Data Sharing in Clouds". IEEE SYSTEMS JOURNAL, pp. 1-10, 2015.

Authors' Profiles

Rida Qayyum was born in Sialkot, Pakistan in 1996. She is currently Student of Bachelor of Science in Information Technology (BSIT), Department of Computer Science from Government College Women University, Sialkot. She attended seminar on Cyber Secure Pakistan organized by PISA at National Library of Pakistan Islamabad and also certified as Microsoft Office Specialist. Her research interest including Location based services (LBS) System, Network Security, Cloud Computing and Computer Communication Network.

Hina Ejaz was born in Sialkot, Pakistan in 1997. She is currently Student of Bachelor of Science in Information Technology (BSIT), Department of Computer Science from Government College Women University, Sialkot. Her research interest including Location based services (LBS) System, Network Security, Telecommunication System and Computer Communication Network.

How to cite this paper: 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

