**IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 12 (December. 2018), ||V (I) || PP 89-94

# Secure Authenticated Storage Outsourcing Scheme with Secure Accessibility in Cloud Computing

Bhasuru Kishore Kumar[1], Dr.B.Giridhar[2],R.V.L.S.N.Sastry[3]
*[1]M.Tech Scholar, Department of Computer Science & Engineering,*
*[2]Professor, Department of Computer Science & Engineering,*
*[3]Assoc.Professor, Department of CSE, Sri Vekateswara College Of Engineering & Technology, Srikakulam, AP, India.*
*Corresponding Author:Bhasuru Kishore Kumar*

**Abstract-** Cloud has been around for two decades and it comprises of the huge measure of data from everywhere throughout the world. A large percentage of the general population at an individual dimension and association level have moved their data to the cloud and offer data over all around the globe. The fundamental test looked by everybody is to share the data everywhere throughout the world or at authoritative dimension safely without giving endlessly the imperative data to any exploiters. To beat the test to share the data safely over the cloud, a productive data encryption calculation for scrambling data before sending it to the cloud. In this proposed we are utilizing a mix of Attribute-Based Encryption and Byte Rotation Encryption Algorithm for scrambling the data previously sending it to the cloud. This will push the client to safely store and offer the data in encoded frame.

**Keywords:**Cloud computing, Mobile Cloud Computing, Privacy, Security, issues in Mobile Cloud Computing.

Date of Submission: 29-11-2018 Date of acceptance: 13-12-2018

## I. INTRODUCTION

Because of intrinsic difficulties of remote correspondences, for example, unreliable nature and issues identified with heterogeneity, security and protection issues are excessively unpredictable in mobile cloud computing. And furthermore because of vitality requirements in mobile gadgets, mobile clients need to lightweight security components. To illustrate the application scenario, let us consider a mobile remote health sensing scenario, where a doctor using a mobile device (e.g., smart phone) to inquiry the sensing data collected from a set of body sensors attached on a patient at home. It is convenient to encrypt the data and enforcing data access policies that only eligible users can decrypt it. To this end, the sensed data can be encrypted using the following policy: Verification is the most imperative factor to secure frameworks against assaults. Particularly in remote mobile correspondences, verification techniques ought to be lightweight, additionally calculation and correspondence expenses ought to be close to nothing. Initially lamport in 1981 proposed a confirmation plot over an open channel [1]. Chang and Wu proposed shrewd cards for remote client validation conventions [2]. At that point numerous two factor verification conventions have been proposed [3-7]. Chow et al proposed a verification structure for mobile cloud clients [8]. Their proposed confirmation plot was understood verification. Schwab and li proposed an element verification plot for mobile cloud condition [9]. They utilized fluffy secret phrase validation in their plan. Hoon and Euiin additionally proposed a confirmation plot utilizing profiling method in mobile cloud computing [10]. The heterogeneous mobile cloud condition contains distinctive sorts of computing assets, for example, remote clouds, cloudlets, and mobile gadgets in the region that can be used to offload mobile undertakings. Heterogeneity in mobile gadgets incorporates programming, equipment, and innovation varieties. In MCC, giving joint effort among different mobile and cloud hubs with various interfaces is a critical issue. Dynamic natural changes is one of the difficulties confronting the offloading basic leadership in mobile cloud applications. Mobile Cloud systems need to adjust to these progressions for proficient assignment apportioning and high QoS of the mobile applications running on end client gadgets. Existing mobile calculation offloading structures do not have the computerized straightforwardness include so the encompassing gadgets can be recognized and the calculation offloading happen in a consistent way [8].

## II. RELATED WORK

Mobile Computation offloading exchanges handling from the mobile gadget to other service suppliers. Mobile application is parceled and investigated so that the most computational costly activities at code level can be recognized and offloaded [9]. The goal is to enhance the calculation execution, empower propelled usefulness, and safeguard rare assets. In the mobile-to-cloud offloading model, most difficulties emerge from dividing the mobile application code to remote and nearby undertakings based on the conditions of each errand. All things considered, the present arrangements can be sorted by dividing system into static and dynamic. The creators at [10] deliver a versatile application model as weblets which can be stage free or ward. The choice of offloading is based on logical parts put away in the cloud including gadget status (CPU stack, battery level), execution proportions of the application for nature of experience and client inclinations. Thusly, the application model backings different running modes: control sparing mode, rapid mode, ease mode or disconnected mode. Mobile offloading beats the asset confinements of lower end gadgets by part asset concentrated undertakings and dispensing subtasks to other asset rich gadgets. Offloading might be performed at various granularities going from techniques and individual assignments [10] to applications [1] and virtual machines [2]. The mobile cloud structure created in [3] utilizes a similar interface of existing cloud APIs for the gathered virtual computing suppliers. This permits a consistent combination with the current cloud frameworks. Then again, Cuckoo structure [4] utilizes the local Android dividing to isolate the UI from the foundation computational code. This facilitates the structure and execution of MCC applications, as mobile application designers don't require any cloud computing information, for example, coordinating with offloading APIs. Most existing MCC proposition focus on single-site offloading [5] i.e., offloading application's parts from the mobile gadget to a solitary server. In any case, as the quantity of encompassing gadgets and cloud computing and storage expands, it is more typical that an application can be executed on different servers [6]. It is demonstrated that we can get better execution from multisite offloading. In this way, multisite offloading is considered as a for the most part sensible model in this work. In any case, settling on choice for multisite offloading issue is a NP-finish issue, and henceforth, getting the ideal arrangement is tedious. Thus, we utilize a straightforward close ideal choice calculation to locate the most ideal dividing for offloading to multisite clouds/servers.

## III. MOBILE CLOUD COMPUTING ARCHITECTURE

Fig. 1 shows the general architecture of Mobile Cloud Computing. Where mobile devices are connected to the mobile networks via base stations (e.g., base transceiver station (BTS), access point, or satellite) that establish and control the connections (air links) and functional interfaces between the networks and mobile devices. Requests and information (e.g., ID and location) of Mobile users‟ are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as AAA (for authentication, authorization, and accounting) based on the home agent (HA) and subscribers‟ data is stored in databases. After that, the subscribers‟ requests are delivered to a cloud through the Internet. In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services.

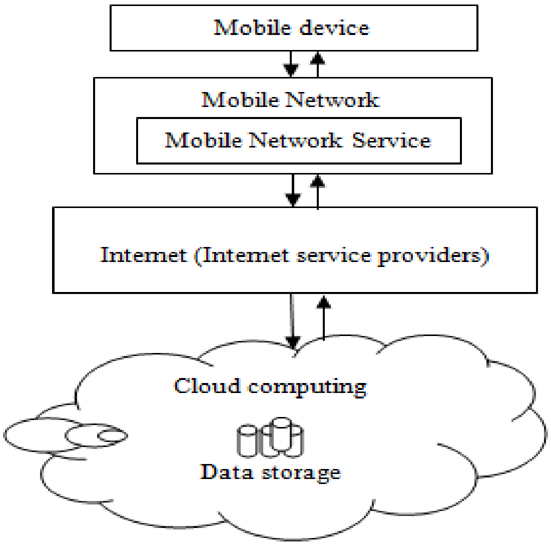

**Fig. 1** Architecture of MCC

Features of Mobile Cloud Computing

- Network latency and limited bandwidth
- Different radio access network
- Energy and resource constraint mobile device
- Different Mobile device operating systems and hardware

- Input - output interface of mobile device
- Fluctuating network condition

***Application of Mobile Cloud Computing***

Because of more demand of processing and storage capability for mobile devices, Mobile Cloud Computing is gaining popularity. Some Mobile Cloud Computing applications are discussed below.

*Mobile Commerce:*

Mobile commerce has made the market available in customer's hand-anywhere anytime. According to Bangalore based management consulting firm Zinnov, e-commerce is expected to increase from US$6.3 billion in 2011 to US$23 billion by 2016 [6].The buzz is growing around mobile transactions. M-commerce is creating ripples in the business world by providing instant access to customers. The sales have grown phenomenally because of the introduction of m-commerce in business which is evident in business companies like e-bay, snapdeal, mantra.com and many more.

*Mobile Learning:*

Traditional education system has certain limitations like in remote areas quality education is not easily accessible, however mobile learning can bridge this gap. For example, Indian top educational Institutes IIT Kanpur [7] [8] and NIIT have launched their own cloud to facilitate research and educational activities.

*Mobile Healthcare:*

Better health services can be provided with mobile healthcare by having ubiquitous access to patients, clinical data and clinical knowledge. A patient can be kept under observation without specialized doctor being physically present with the help of Mobile Healthcare. Even, authenticity of the drugs can be checked by accessing cloud database of the company through mobile [8] [9].

*Image processing:*

We can give more features to Smartphone in gesture recognition, like image process applications through Mobile Cloud Computing by processing their data through cloud.

*Speech recognition and synthesis:*

Speech Recognition application like language translator can help mobile user to feel comfortable in a country where language is not known or understood by the mobile user.

*Mobile Banking:*

Now a day's mobile banking is gaining more popularity than e-banking because of more mobile users than internet users

*Social Networking:*

Social networking like face book, what's up help in staying connected with people with Mobile Cloud Computing.

*Mobile Gaming:*

As we know games demand more processing and graphic hardware, with Mobile Cloud Computing it is possible to use high end gaming application on mobile phone.

*Mobile Security:*

Mobile cloud computing can provide more security to the mobile device by proving security through cloud.

## IV. MOBILE CLOUD COMPUTING SECURITY AND PRIVACY CLASSIFICATION.

Mobile devices are exposed to numerous security threats like malicious codes and their vulnerability. GPS can cause privacy issues for subscribers. Security of mobile cloud computing is divided into two main parts security modules and privacy modules. Security module mainly concern with security of mobile network and security for cloud. Security module secure the device by using authentication, access control and malware detection, whereas privacy module determines user data encryption/decryption and sensitive data management model, as shown in fig.3. Now we will see the concept of general cloud security, mobile cloud security and privacy in detail.

A) Security in Mobile Cloud Computing

Security for mobile application, one way to protect the device from installing the threat by running security software

.Mobile devices are resource constrained, protecting them from the threats is more difficult than that for resourceful devices. Oberheide et al.[9] present an approach to move the threat detection capabilities to clouds. It is an extension of the CloudAV platform consisting of host agent and network service components. Host agent runs on mobile devices to inspect the file activity on a system. If an identified file is not available in a cache of previous analyzed files, this file will be sent to the include network service for verification. The second major component of CloudAV is a network service that is responsible for file verification. Portokalidis et al.[10] present a paradigm in which attack detection for a smartphone is performed on a remote server in the cloud. The smartphone records only a minimal execution trace, and transmits it to the security server in the cloud.

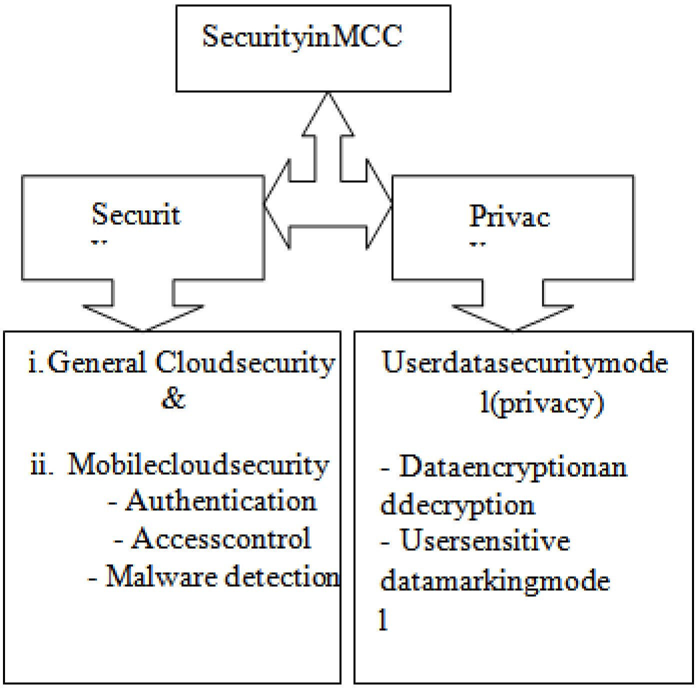

**Fig. 2.** Mobile Cloud Computing security and privacy classification.

B) General cloud security:

J. Brodkin, Gartner[9] summarize seven security risks that users need to consider in mobile Cloud computing;

1. Privileged user access: uploading sensitive data to the cloud would raise the problem of loss of direct physical, logical and personnel control over the data.
2. Regulatory compliance: the cloud service providers should be willing to undergo external audits and security certifications.
3. Data location: the exact physical location of user‟s data is not transparent, which may lead to confusion on specific authorities and commitments on local privacy requirements.
4. Data segregation: since cloud data is usually stored in a shared space, it is important each user‟s data is separated from others with efficient encryption schemes.
5. Recovery: it is imperative that cloud providers provide proper recovery mechanisms for data and services in case of technological failure or other disaster.
6. Investigative support: since logging and data for multiple customers may be co-located, inappropriate or illegal activity should they occur may be very hard to investigate.
7. Long-term viability: assurance that users data would be safe and accessible even if the cloud company itself goes out of business.

C) Mobile cloud security:

The simplest ways to detect security threats will be installing and running security software and antivirus programs on mobile devices. But since mobile devices are constrained with processing and power limitations, protecting them from these threats could be more difficult compared to regular computers. Several approaches have been developedtransferring threat detection and security mechanisms to the cloud. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it is malicious or not. Instead of running anti-virus software or threat detection programs locally, mobile devices only performs lightweight activities such as execution traces transmitted to cloud security servers. Security in mobile cloud computing, between mobile device and user is determine by three main parts authentication, access control and malware detection. To make the secure communication between mobile device and cloud, X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, S. Jeong,[8] propose the Securing elastic applications on mobile devices for cloud computing, name as „weblet‟.‟ Weblet‟ is use to migrate the data/information to and from mobile device and cloud. So as far as security concern, it include 3 main parts, they are explain as follows.

1. Authentication between the „weblets‟ that would be distributed between the cloud and the device,

2. Authorization for weblets that could be executing on relatively untrusted cloud environments to access sensitive user data.
3. Establishment and verification of trusted „weblet‟ execution of cloud nodes.

The secure elastic application framework for weblet is based on the assumption that the cloud elasticity service (CES), including the cloud manager, application manager, cloud node manager, and cloud fabric interfaces (CFI), is honest. The security threats are categorized as threats to mobile devices, threats to cloud platform and application container, and threats to communication channels. So that the authors propose a framework with the following security objectives: Trustworthy weblet containers (VMs) on both device and cloud, authentication and secure session management needed for secure communication between weblets and multiple instantiation concurrently, authorization and access control enforcing weblets on the cloud to have the lowest privileges, and logging and auditing of weblets.

Privacy Issues in Mobile Cloud Computing: In [2], M. Fahrmair, W. Sitou, B. Spanfelner, Security and privacy rights management for mobile and ubiquitous computing, presents the following requirements of a mobile and ubiquitous system that satisfies user privacy for both mobile device and cloud, they are as follows protection against misuse, identification of pirated datasets, adjustment of laws (to provide additional security under certain circumstances), and ease of use.

Location based services (LBS) faces a privacy issue on mobile users‟ provide private information such as their current location. This problem becomes even worse if an opponent knows user‟s important information. Zhangwei and Mingjun [1] propose the location trusted server (**LTS**) approach. After receiving mobile users‟ requests, LTS gathers their location information and cloaks the information called “cloaked region” to conceal user‟s information. The “cloaked region” is sent to LBS, so LBS knows only general information about the users but cannot identify them.

Digital Rights Management(DRM): DRM is used to protect digital contents from illegal access. Phosphor is a cloud based mobile digital rights management (DRM) scheme with improved flexibility and reduced vulnerability at a low cost. A License State Word (LSW) located in a sim card and the LSW protocol based on the application protocol data unit (APDU, the smart card comm. std) command are provided. When a mobile user receives the encrypted data, he/she uses the decryption key from a sim card via APDU command to decode.

## V. PROPOSED SYSTEM

This paper, proposes another ensured data sharing arrangement for Mobile Computing as a move up to A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing Model by planning the twofold structure encryption development with particular confirmation technique. While the introduced plot supporting any standard access structures is worked in the composite structure bilinear social affair, it is checked adaptively CCA secure in the standard framework without undermining the expressiveness of access approach. In this paper, we try despite make an overhaul for the model to get greater profitability in the re-encryption key age and re-encryption stages.Then using registration norms, data owner is easily registered within the few steps and by logging it through the data owner list. This diagram represents the data owner and data user transaction method with light weight deriving scheme like proxy re encryption and attribute based encryption method. Using this encryption method, data owner can easily able to upload the file to cloud with encrypted format. And based on the trusted authority access, attribute key is generated based on the key matching through the ESP. Date user must be register to process the data stored in the cloud that are provided by the data owner. If both the ESP and DSP verified the key value then there is no restriction to access the file through the cloud. Finally using the DSP, the uploaded file can be easily downloaded from the cloud.The cloud servers not only provide storage but enforce access control policies on the stored data. In our access control mechanism, the DO forwards the encrypted file to the cloud servers.

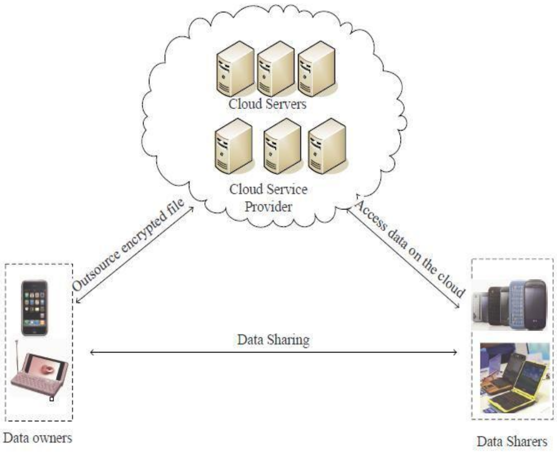

**Fig.3.** Network model for our protocol

## VI. CONCLUSION

Mobile Cloud Computing is a new paradigm since 2009 and it is still in nascent stage. The security and privacy issues in mobile cloud computing are inherited from cloud computing, however, it is difficult to resolve these issues because of resource constraint in mobile devices like energy, storage, processing etc. However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices has limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CPABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can help in solving the secure data sharing problem in mobile cloud. The experimental results show states that LDSS can ensures data privacy in mobile cloud and reduce the overload on users' side in mobile cloud. In future work, we will design the new approaches to ensure data integrity. To further tap the potential of mobile cloud, and also ensure how to do cipher text retrieval over existing data sharing schemes. To address the security and privacy issues, we will have to develop efficient security and privacy framework with the objective of lesser resource requirement in mobile device and minimize the communication cost and network latency while ensuring privacy, authenticity and integrity of user's data in cloud.

## REFERENCES

[1]. A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing Ruixuan Li, *Member*, *IEEE*, Chenglin Shen, Heng He, Zhiyong Xu, and Cheng-Zhong Xu, *Member*, *IEEE*.

[2]. A. Agarwal, S. Siddharth, and P. Bansal. "Evolution of cloud computing and related security concerns," Symposium on Colossal Data Analysis and Networking, pp. 1-9, IEEE, 2016.

[3]. Y. Ren, J. Xu1, J. Wang, and J.U Kim, "Designated-Verifier Provable Data Possession in Public Cloud Storage," International Journal of Security and Its Applications , Vol. 7, No. 6 , pp.11-20, 2013.

[4]. J. Wei, W. Liu, X. Hu, " Secure data sharing in cloud computing using revocable-storage identitybased encryption," IEEE Transactions on Cloud Computing, 2016, Mar 23.

[5]. J. Hong , K, Xue, Y, Xue, W, Chen, DS, Wei , N, Yu, P, Hong, "TAFC: Time and attribute factors combined access control for time-sensitive data in public cloud," IEEE Transactions on Services Computing, 2017 Mar 14.

[6]. Li, Ruixuan, C. Shen, He, Heng, Z. Xu, and Cheng-Zhong Xu. "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," IEEE Transactions on Cloud Computing , 2017.

[7]. K. Fan, Q. Tian, J. Wang, H. Li, and Y. Yang, " Privacy protection based access control scheme in cloud-based services," China Communications, 14(1), pp.61-71.

[8]. X. Wu, R. Jiang, and B. Bhargava, "On the security of data access control for multiauthority cloud storage systems," IEEE Transactions on Services Computing, 10(2), pp.258-272, 2017.

[9]. G. V. Kapse, V. M. Thakare, S. S. Sherekar, and A. V. Kapse," Multi-Authority Data Access Control For Cloud Storage System With Attribute-Based Encryption.

[10]. Z. Mahmood, " Data location and security issues in cloud computing. In Emerging Intelligent Data and Web Technologies (EIDWT)," International Conference ", pp. 49-54, IEEE, 2011 September.

Bhasuru Kishore Kumar. "Secure Authenticated Storage Outsourcing Scheme with Secure Accessibility in Cloud Computing. "IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 12, 2018, pp. 89-94.