International Journal of Science Engineering and Advance Technology

Secured Framework for Data Outsourcing using ABE in Cloud Computing

V. Sri Ramya[1], A.P.V.D.L. Kumar[2]
[1]M.Tech Scholar, Department of Computer Science & Engineering,
[2]Assosc.Professor, Department of CSE, BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.

Abstract

Cloud has been around for two decades and it comprises of the tremendous measure of data from everywhere throughout the world. The vast majority of the general population at an individual level and association level have moved their data to the cloud and share data over all around the globe. The fundamental test looked by everybody is to share the data everywhere throughout the world or at hierarchical level safely without giving endlessly the essential data to any exploiters. To beat the test to share the data safely finished 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 Algorithm for scrambling the data previously sending it to the cloud. This will push the client to safely store and share the data in encoded shape. Additionally we utilize the AES (Advance Standard Encryption) calculation for data encryption and decryption reason.

Keywords: Attribute-Based Access; Access Control. Mobile Cloud Computing.

I. Introduction

With the rapid augmentation in the data sharing over the Internet, the cloud processing framework is every now and again utilized as a part of the numerous data proprietor situation. The cloud registering framework offers different kinds of administrations. Stage as a Service (PaaS) is a cloud-based administration that gives more decisions to the supporter for picking the processing stage. Foundation as a Service (IaaS) gives an indistinguishable highlights from the PaaS, yet the client is totally in charge of controlling the leased framework. Programming as a Service (SaaS) permits the business undertakings to access the usefulness at a lower cost than the cost of authorized applications, as the SaaS estimating is based on a month to month expense. Because of the remote facilitating of the product, the clients don't have to put resources into the extra equipment. The SaaS diminishes the exertion of establishment, setup and support by the business endeavors. Subsequently, it is alluded as basically facilitated applications. The data proprietor can transfer the data to the cloud specialist organization and access the put away data utilizing the product gave by the specialist co-op. As the data got from the data proprietor isn't sufficient to fill the storage room of the server, it prompts a considerable measure of capacity squander. The data got from various data proprietors is put away in a similar server to build the use rate of server storage room. There is a need to secure the private data for keeping the burglary of classified data by unapproved individual or other data proprietors. Thus, the private data is scrambled and put away. The data proprietor and cloud client ought to acquire the security keys from the specialist co-op. On the off chance that the data proprietor and client access a tremendous measure of data, there is a need to deal with countless. The lightweight key administration approach is the ideal answer for the key administration issue. In different data proprietor situation, it is expected that the quantity of keys increments with the expansion in the quantity of data proprietors and clients. In Single-layer Derivation Encryption [1-5] plans, there is a need to store a solitary key relating to the data proprietor. In Double-layer Derivation Encryption [6-8] plans, the quantity of cryptographic keys utilized for the data encryption process is twofold than the Single-layer encryption conspire. The Attribute-based Encryption (ABE) [9-10] plan acknowledges a broad key identified with an arrangement of attributes applicable to the data proprietor and cloud client. The encryption plans are utilized to deal with the approval, in which every client ought to deal with an arrangement of decryption keys comparing to the arrangement of data proprietors. The Ciphertext Policy-ABE (CP-ABE) [7] is a compelling cryptographic based access control system with better data security in the cloud condition. The attribute expert issues an arrangement

of attributes to produce an access approach for scrambling the data record. Just the clients having attributes that fulfill the access arrangement can decode the document. The unauthenticated or outsider individual can't access the record. The CP-ABE based access control plans [1-2] are adaptable and versatile. The primary issue is key denial administration. The attributes are shared by various clients. On account of client or attribute renouncement, the non-disavowed clients should refresh their keys. On the off chance that the renounced attribute shows up in the access arrangement, the records ought to be re-encoded under the new strategy to keep the unapproved decryption of the keys containing denied attributes. It requires denial cost and computational many-sided quality. In the vast majority of the current techniques, the client needs to deal with an arrangement of keys.

II. Related work

Cooperation among mobile gadgets: As the mobile gadgets have certain asset limitations, there emerges a need to get assets from outside sources. One of the approaches to conquer this issue is getting assets from a cloud, yet the access to such stages isn't generally ensured or/and is excessively costly. Huerta-Canepa in [6] presents the rules for a structure that mirrors a conventional cloud supplier utilizing mobile gadgets in the region of clients. The system recognizes close-by hubs that are in a steady mode, implying that will stay on a similar territory or take after a similar development design. On the off chance that hubs in that state are discovered, at that point the objective supplier for the application is changed, mirroring a virtual supplier made onthe-fly among clients. In situations like downloading a portrayal record at a historical center, collocation builds the odds of individuals willing to perform basic tasks[7]. To spare the assets like vitality and preparing power, the arranged mobile gadgets can cooperatively go about as a nearby cloud and split the undertaking into littler subtasks to be performed on various devices[8]. The outcomes would then be able to be collected and shared. The proposed approach permits staying away from an association with foundation based cloud suppliers while keeping up the primary advantages of offloading. Fernando et'al in [9] then again propose to utilize a wide range of nearby assets (cell phones, PDA, even PCs) to be utilized to team up in framing the neighborhood cloud to accomplish a shared objective. Their approach is to defeat the asset meager condition, vitality utilization and low availability problems [10] looked in customary mobile cloud figuring. Sharing of workload is dynamic, proactive and relies upon cost model to profit all members. The design comprises of predominantly a Resource Handler, a Job Handler and a Cost Handler. The asset handler finds the assembled assets, the cost handler at that point figures the expenses to perceive what conveyance of employments will have most advantages and afterward the activity handler distributes [1] the sub-assignments, run the occupations and gather them back on sender. At long last the cost handler handles micropayments among the taking an interest gadgets. SpACCE idea in [2] giving estimation limit of PCs is proposed to encourage disseminated joint effort. A SpACCE is an advanced impromptu cloud registering condition that can be worked by the requirements that happen at any given time on an arrangement of individual, i.e., non-committed, PCs and progressively move a server[3] for application sharing to another PC. By moving the server, excess computation limit of PCs can be used for making a SpACCE, where the reaction time of the application shared among clients is progressed. A SpACCE gives the accessible estimation limit of a PC as the server for coordinated effort to different PCs which have no application as well as insufficient count ability to be the server on request.

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.

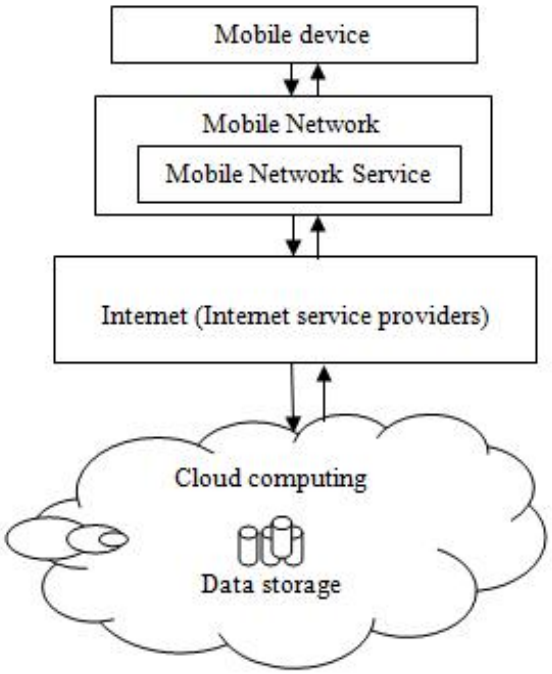

Fig. 1 Architecture of MCC

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.

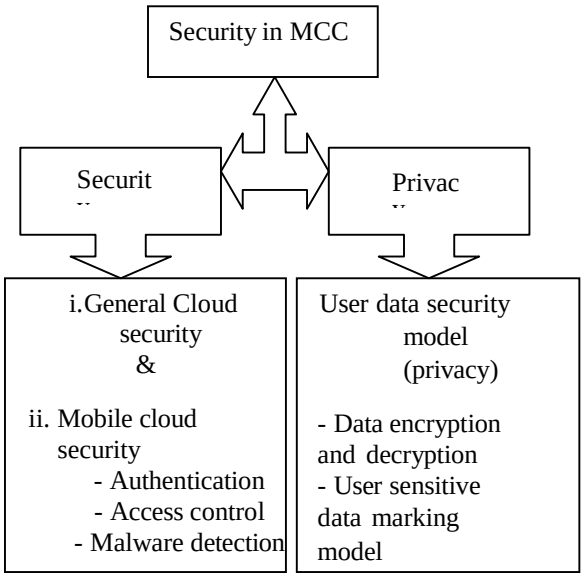

Fig. 2. Mobile Cloud Computing security and privacy classification.

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.

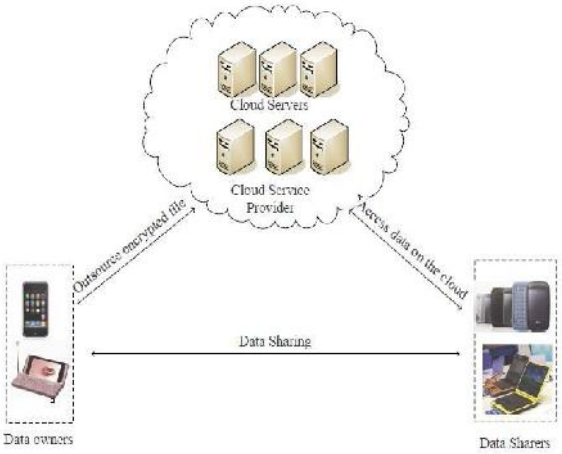

Fig.3. Network model for our protocol

V. 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 identity based 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.

Authors

V. SRI RAMYA is pursing M.TECH (CSE) in the Department of Computer Science and Engineering from BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.

A.P.V.D.L. Kumar is working as Associate Professor in Department of Computer Science & Engineering, BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.