www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Data sharing mechanism in mobile cloud environment

K.V.Priyadharshini[1], Mr.R.B.Ramesh M.E[2].

[1]M.E CSE, Department of CSE, Mahendra Engineering College, Mallasamudram, Tamil Nadu.
[2]Assistant Professor, Department of CSE, Mahendra Engineering College, Mallasamudram, Tamil Nadu.

ABSTRACT

Though the electronic technologies have undergone fast developments in recent years, mobile devices such as smart phones are still comparatively weak in contrast to desktops in terms of computational capability, storage, etc., and are not able to meet the increasing demands from mobile users. By integrating mobile computing and cloud computing, mobile cloud computing (MCC) greatly extends the boundary of the mobile applications, but it also inherits many challenges in cloud computing, e.g., data privacy and data integrity. In this paper, we leverage several cryptographic primitives such as a new Pay metric technology to improve the security, which provides data privacy, data integrity, data authentication, and flexible data distribution with access control. Compared to traditional cloud-based data storage systems, our system is a lightweight and easily deployable solution for mobile users since no trusted third parties are involved and each mobile user only has to keep short secret keys consisting of three group elements for all cryptographic operations. Finally, we present extensive performance analysis and empirical studies to demonstrate the security, scalability, and efficiency of our proposed system.

Keywords: AES, Access control, Data integrity, Authentication, security

INTRODUCTION

In cloud computing, many computing resources are provided as services over the internet. One of the main services provided by clouds is storage (e.g., Simple Storage Services—Amazon, which allows users to store their enormous amount of data to the remote clouds without bothering the complex management of storage hardware. Outsourcing big data to clouds provides many benefits, e.g., low costs, good reliability and availability, but the data security issues such as privacy and integrity brought by third party's cloud systems have been the major Concerns for users utilizing such services. According to the surveys, more than 90 percent of US consumers wants to be asked to give permission for their data to be shared, and 88 percent of all potential consumers are worried about the privacy of their data. Since the data is stored and managed in the cloud, the data security highly depends on the IT management of the cloud services providers, and any security loophole in the cloud system might damage the security of the users' private data [1-5].

Today, the market of mobile phones is growing at a very high speed. Everyone has a mobile phone which provides the facility to move anywhere and access the data anytime. With the emergence of cloud computing in mobile web, mobile users can use infrastructure, platform, software provided by cloud providers on on-demand basis. Emergence of cloud computing with mobile devices gave birth to mobile cloud computing [6-10].

Author for correspondence:
M.E CSE, Department of CSE, Mahendra Engineering College, Mallasamudram, Tamil Nadu.

RELATED WORK

Mobile Cloud Computing is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access. Aepona describes MCC as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds.

The mobile devices do not need a powerful configuration (e.g., CPU speed capacity) because all the complicated computing modules can be processed in the clouds. There are many limitations in mobile devices like limited processing power, low storage, less security, unpredictable Internet connectivity, and less energy. To augment the capability, capacity and battery time of the mobile devices, computationally intensive and storage demanding jobs should be moved to cloud [11-17].

LITERATURE REVIEW

Balakarishnan.S et al.has introduced TPA (Third Party Auditor) between client and cloud service provider, which acts as external auditor to audit the user outsource data. This scheme has provided secured and efficient dynamic operations like data updates, deletion and append on data blocks stored in the cloud.

Joshi Ashay.M et al argued that Asymmetric Cryptography Algorithms and Digital Signature techniques are reliable and efficient to provide more security user's data in Cloud Computing. The potentiality of the paper was that, the authors have seeded the idea of using two different keys algorithms but failed to give the model or methodology for implementations.

Richard Chow et al. described a framework for supporting authentication decision, which is named as Trust Cube. A proposal of a high-level architecture of authentication flows was made. The architecture has four participants: client devices, data aggregators, an authentication engine, and authentication consumers. Client device, data aggregators and authentication consumers must be authenticated themselves through authentication engine before exchange of data.

The strength of that paper was a model of cloud authentication. However this article only focuses on one threat (Authentication), facing Cloud Computing. Other threats in Cloud environment such as Repudiation, Denial of Services and Spoofing identity are probably ignored by the authors.

Hongwei Li et al. presented a Hierarchical Architecture for Cloud computing and proposed Identity-Based Encryption and Identity-Based Signature for that Hierarchical Architecture. Finally the author proposed Authentication Protocol for Cloud Computing (APCC). In the end a conclusion were made that, APCC is more light weight and efficient as compared to SSL Authentication Protocol, on the basis of performance analysis.

Yuefa et al.analyzed the basic problem of Cloud Computing that is data security. The author has got data security requirement of Cloud Computing and has given a mathematical model on the basis of these requirements. The data security model proposed, is a worth addition in world of Cloud Computing security. However, writers are not able to give a comprehensive solution for security of Cloud Computing.

Qiu-Xin.F et al. proposed a multi-layered and multi-level secured architecture for Cloud Computing according to the characteristics of mobile user. The author has proposed the idea of SaaS (Security as a Service). The advantage of this proposal is that when implemented, is flexible to different scaling system to different requirements and can integrate different operating system and heterogeneous network.

Cloud computing has developed as a widespread model in computing world in which resources of the computing infrastructure are provided as services over the Internet. A cloud computing scenario usually tailors the server as needed. Cloud computing pattern also brings out several new challenges in data security and access control when consumers outsource delicate data for sharing on cloud servers.

METHODOLOGY

In this paper, we propose a Pay metric technology to improve the security for mobile cloud computing environment. We design an algorithm called AES based on Advanced Encryption Standard method to offer efficient access control over cipher text. We use proxy servers for encryption and decryption operations. In our approach, computational intensive operations in AES are conducted on proxy servers, which greatly reduce the computational overhead on client side mobile devices.

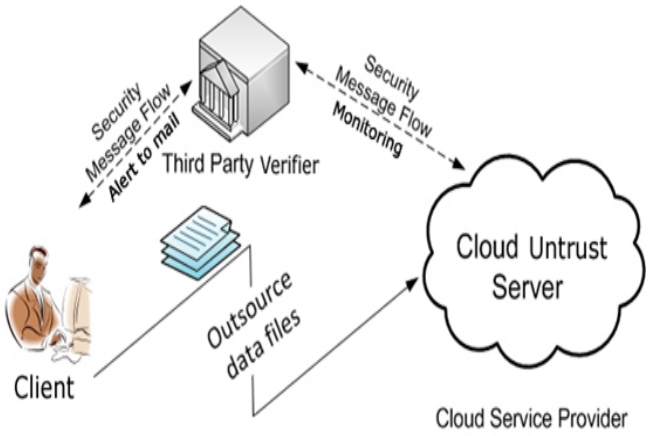
To address privacy issue in existing system we propose a crypto-system for secure sharing of data over the cloud, which uses combination Attribute Based Encryption and Byte Rotation Encryption Algorithm for secure encryption of the data over cloud.

The main three works are as follows:

1. Identify the issues in cloud system for data storage on cloud. Since data is not secure on cloud user can upload the data in encrypted format.
2. Propose a crypto-system which can run on all limited resources devices. It can take data from the user and provide off-line-online service.
3. Apply Attribute Based Encryption Algorithm and Byte Rotation Algorithm for encryption of data to securely transfer the data between the users.

ADVANTAGES

- ✓ We are providing methods for efficient access of the data.
- ✓ Performance has been increased with the reduced cost.
- ✓ Here data can be transferred from one user to another securely over the cloud.
- ✓ The system cost will be decreased.
- ✓ It will work on all limited resource devices



Cloud service provider

RESULT AND DISCUSSION

System and security model

System model

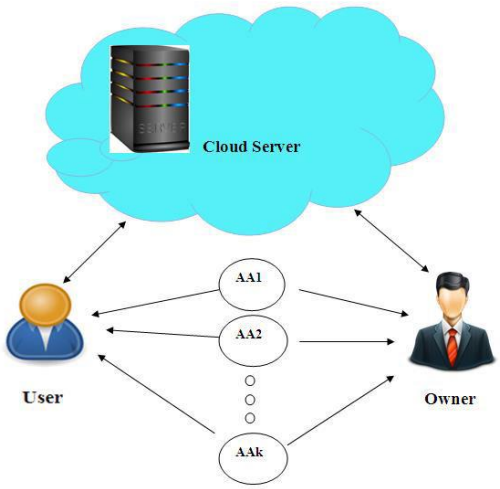
We consider a cloud storage system with multiple authorities. The system model consists of the following entities: authorities (AA), cloud server (server), data owners (owners) and data consumers (users).

Authority

The Authority delimits that, power is delegated formally. It includes the right to command a situation, commit resources and give orders. In previous works every authority is dependent with each other and is responsible for managing attributes of users in its own area. Here the secret key / public key pair is generated for each attribute in its domain and follows to generate the secret key for each user according to their attributes.

Cloud server

The A cloud server is a logical server that is built, compared and provided through a cloud computing platform over the Internet. Cloud servers possess and show similar capabilities and functionality to a typical server but are accessed remotely from a cloud service provider. A cloud server may also be called a virtual server or virtual private server. The cloud server stores the data for data owners and allows the data owners to access service to the users. The server is also in charge for updating cipher texts from old access policies to new access policies.



System Model

Data owners

There are other concerns with regards to storing data in the cloud such as backups, data security, privacy and transfer of data. So despite the advantages of cloud services an enterprise must answer the most crucial question when going for any cloud hosted service, that is 'who owns the data'. The actual ownership of data in the cloud may be reliant on the nature of data stored as well as where it was created. The data owners define access policies and encrypt data under these policies before hosting them in the cloud.

They also ask the server to update access policies of the encrypted data stored in the cloud. After that, they will check whether the server has updated the policies correctly.

Data Users

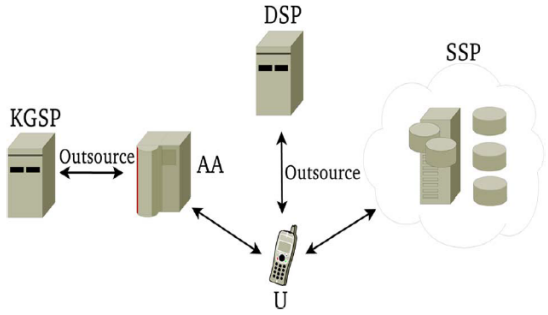
Each user is assigned with a global user identity with set of their corresponding attributes and can freely get the cipher texts from the server. The user can decrypt the cipher text, only when its attributes satisfy the access policy defined in the cipher text.

Data User

Data User is he who has successfully registered himself and having his own ID and password using which he can login to the website in order to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher-text and obtain the data.

Attribute Authority

Here Attribute Authority may also be known as data owner. He allows to upload it into the external data-storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. The data owner logins to the website using his credentials and then he can upload the file to the Storage Service Provider (SSP). While uploading the file the data owner will define the access policy which is based on attribute. Then the data owner also has the checksum of that file so that the CSP may not return results incorrectly. The redundant data is also attached to the ciphertext to fight against dishonest actions of KGSP and DSP.



System model for outsourced Pay metric technology to improve the security scheme

Key Generation Service Provider

Aiming at eliminating the most overhead computation at the attribute authority and the user sides, an outsourced ABE scheme is proposed that not only supports outsourced decryption but also enables delegating key generation. KGSP is to perform aided key-issuing computation to relieve AA load in a scale system when a large number of users make requests on private key generation and key update. It is in charge of issuing, revoking, and updating attribute keys for users. KGSP is in charge of generating the encrypted password and sending it to the mail-ID of the user. At the time of downloading the file, the session password is required which is generated by KGSP.

Decryption Service Provider

DSP is used for generating the decrypted key when the user requests for the decryption of the encrypted key. Then the DSP asks for the ID and encrypted key of the user and then sends the decrypted key to the user. It is used for decrypting the ciphertext which is obtained from the user. When the data owner uploads the file which is in encrypted format, then the DSP will decrypt it when the authorized user who satisfies the access policy and who have suitable attributes requests for downloading the file. The DSP will then send the file in the decrypted format to the authorized user so that the user can gain access to that data.

Storage Service Provider

SSP is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. All the uploaded data will be stored in Storage service provider. SSP will be in charge of controlling the access to that data from outside users. It will be storing all the data and provides the data only to authorized users. The files which are uploaded by the Data Owner will be stored in the SSP. When the authorized user wants to access that file, the SSP will then sends the file to the user so that user can download it by entering session password (OTP).

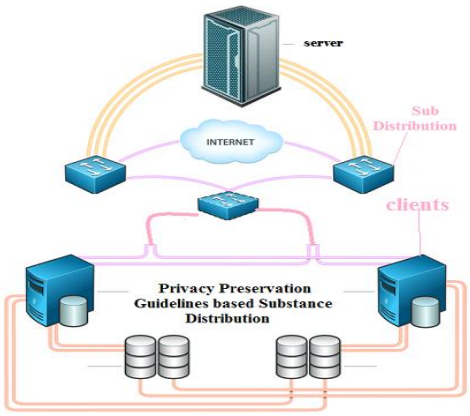
Proxy Re-Encryption

During a proxy re-encryption theme, a proxy server will transfer a cipher text beneath a personal key A to a replacement one beneath another public key B. The server does not grasp the plaintext throughout transformation. The information is initial encrypted with an interchangeable encryption key keep within the cloud storage server. The cloud storage server uses a re-encryption algorithmic rule to transfer the encrypted DEK into the format that may be decrypted by the recipient's personal key. The recipient then transfer the encrypted information from the cloud and use the DEK for coding. A re-encryption secrets generated from the information owner's personal key and a recipient's public key. A knowledge owner might share completely different files with different recipient teams. Therefore, a recipient cannot scan information for a gaggle it does not belong to. The cloud, on the opposite hand, acts as an intermediate proxy. It cannot scan the information because it cannot get DEKs. The system has information confidentiality and supports the information forwarding performs.

This system sketches the planning of PAST, a large-scale, Internet-based, world storage utility that has measurability, high availableness, persistence and security. PAST could be a peer-to-peer web application and is entirely self organizing. PAST nodes functions access points for purchasers,

participate within the routing of shopper requests, and contribute storage to the system.

- The Pastry location and routing theme, that faithfully and expeditiously routes shopper requests among the PAST nodes, has sensible network neighborhood properties and mechanically resolves node failures and node additions.
- The use of organization to confirm diversity within the set of nodes that store a file's replicas and to supply load balancing.
- The optional use of smartcards, that area unit control by every PAST user and issued by a third party referred to as a broker.
- Easy for the cloud atmosphere remainder a task in progress.
- Easy to sharing and distributed the shopper systems.



Proxy Server

CONCLUSION

The concept of cloud computing provides a great opportunity into users to utilize their services by on-demand basis. The requirement of mobility in cloud computing gave birth to Mobile cloud computing. Pay metric technology to improve the security provides more possibilities for access services in convenient manner. It is expected that after some years a number of mobile users will going to use cloud computing on their mobile devices. There are many issues in mobile cloud computing due to limitations of mobile devices. Security is the main concern in mobile cloud computing. In Mobile Cloud Computing data of owner is stored on the cloud, which is not secured. This paper has provided the description about the basics of Mobile Cloud Computing and issues associated with it. Mainly it discussed about security of data stored in cloud and importance of data security. This paper has explored a number of mechanisms for providing data security so that Mobile Cloud Computing can be widely accepted by a number of users in future. It also proposed a mechanism to provide confidentiality, access control as well as integrity to mobile users

REFERENCE

[1]. M. Armbrust et al., "Above the clouds: A Berkeley view of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[2]. G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, 598–609.

[3]. A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, 584 597.

[4]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. 28th Int. Conf. Distrib. Comput. Syst. (ICDCS), 2008, 411–420.

[5]. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high availability and integrity layer for cloud storage," in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, 187–198.

[6]. J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographically dispersed clouds," J. Comput. Syst. Sci., 78(5), 2012, 1345–1358.

[7]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proc. ACM Workshop Cloud Comput. Secur. Workshop, 2010, 31–42.

[8]. Sayi, T. J. V. R. K., Krishna, R. S., Mukkamala, R., & Baruah, P. K. Data Outsourcing in Cloud Environments: A Privacy Preserving Approach. In Information Technology: New Generations (ITNG), 2012 Ninth International Conference on 2012, 361-366.

[9]. Shah, M. A., Baker, M., Mogul, J. C., & Swaminathan, R. 2007, May. Auditing to keep online storage services honest. In Proceedings of the 11th USENIX workshop on Hot topics in operating systems (pp. 1-6). USENIX Association.

[10]. Yang, K., & Jia, X. Data storage auditing service in cloud computing: challenges, methods and opportunities. World Wide Web, 15(4), 2012, 409-428.

[11]. Chen, L., & Guo, G. An efficient remote data possession checking in cloud storage. International Journal of Digital Content Technology and its Applications, 5(4), 2011, 43-50.

[12]. Gohel, M., & Gohil, B. A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage. Trust Management VI, 2012, 240-246.

[13]. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. Enabling public auditability and data dynamics for storage security in cloud computing. Parallel and Distributed Systems, IEEE Trans. on, 22(5), 2011, 847-859.

[14]. Agrawal, D., Das, S., El Abbadi, A.: Big data and cloud computing: current state and future opportunities. In: Proceedings of the 14th International Conference on Extending Database Technology (EDBT/ICDT'11), 2011, 530–533

[15]. Assunção, M.D., Calheiros, R.N., Bianchi, S., Netto, M.A.S., Buyya, R.: Big data computing and clouds: trends and future directions. J. Parallel Distrib. Comput. **79–80**, 2015, 3–15

[16]. Batalla, J.M., Kantor, M., Mavromoustakis, C.X., Skourletopoulos, G., Mastorakis, G.: A novel methodology for efficient throughput evaluation in virtualized routers. In: Proceedings of the IEEE International Conference on Communications (ICC 2015)—Communications Software, Services and Multimedia Applications Symposium (CSSMA), London, UK, 2015, 6899–6905

[17]. Batalla, J.M., Mavromoustakis, C.X., Mastorakis, G., Sienkiewicz, K.: On the track of 5G radio access network for IoT wireless spectrum sharing in device positioning applications. In: Internet of Things (IoT) in 5G Mobile Technologies, 2016, 25–35. Springer International Publishing.