ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Secure & Efficient Cloud Storage Middleware for Mobile Cloud Computing

Akanksha R. Patil [1], Vaibhav V.Sawant[2]

Asst. Professor, Department of Computer Engineering, PCP College, Pune, India[1]

Asst. Professor, Department of Computer Engineering, DYP Engineering College, Kolhapur, India[2]

ABSTRACT: Together with massive growth of the mobile applications and emerging of cloud computing concept, mobile cloud computing has been exotic to be a potential technology for mobile services. Although many users outsource their various data to clouds, data security and privacy concerns are still the biggest hurdles that restrict the widespread adoption of cloud computing. Using PP-CP-ABE, light-weight handheld devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content. Second, we propose an Attribute Based Data Storage (ABDS) system as a cryptographic group-based access control mechanism. Our performance assessments demonstrate the security strength and efficiency of the presented solution in terms of computation, communication, and storage. Simultaneously, it assimilates an effective structure for users to verify their data integrity, which relieves much load from mobile devices. Experimental simulations show that the proposed framework is secured and efficient to provide data sharing with minimum load on mobile devices.

KEYWORDS: Security Server (SS), Encryption Service Provider (ESP), Decryption Service Provider (DSP)

I. INTRODUCTION

Cloud computing security is an evolving sub-domain of computer network technologies and data security. Data security focuses on confidentiality, integrity & authenticity of information. More policies, technologies and controls are been deployed to protect data, applications, and the associated infrastructure for physical and logical security. Mobile Cloud computing is also emerging advancement, which is transforming the traditional Internet computing paradigm and IT industry into a new devastating era of computing. This new trend demand researchers and practitioners to construct a convincing architecture which includes a large numbers of lightweight, resource constrained mobile devices.

However, users worry about the data security is the main hurdle that impedes cloud computing from being widely adopted. These complexities are originated from the fact that sensitive data resides in public clouds, which are operated by monetary service providers that are not trusted by the data owner. Thus, new secure service architectures are needed to address the security concerns of the users for using cloud computing techniques.

In recent years, many people have realized that Cloud-based storage system is a very cost-effective for commercial applications. Since Mobile devices have limited computational capacity and run on small batteries, data storage and sharing is
difficult for these devices. With the spring of Cloud, storage platform can provide reliable and unlimited storage. They fulfill to the requirements of mobile computing environments very well & offer a flexible and low-cost solution to meet the unfolding storage requirements in such environments. This paper deals with the problems identified in regard to mobile devices cloud computing for data security.

The rest of this paper is organized as follows. Section II presents the literature survey. In Section 3, we briefly describe system architecture of the proposed system; In Section 4, experimental setup and simulated implementation details are presented. Finally, Section 6 concludes the paper with a brief discussion of future work.

II. LITERATURE REVIEW

A holistic security framework to secure the data storage in public clouds with the special focus on lightweight wireless devices store and retrieving data without exposing the data content to the cloud service providers is been

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

implemented by Zhibin Zhou and Dijiang Huang [1]. To achieve this goal, the solution focuses on the following two research directions: first, it presents a novel privacy preserving cipher policy attribute-based encryption to protect user data. Lightweight devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content and used security keys. Second, it proposes an attribute based data storage system as a cryptographic access control mechanism. Furthermore to facilitate key management and cryptographic access control in an expressive and efficient way Bethencourt and Sahai have associated user with multiple attributes. Multiple users may share common attributes allowing message encrypted to specify a data access policy by composing multiple attributes through logical operators such as AND, OR, etc [2].

A model for provable data possession is proposed by Antesia & Burns that can be used for remote data checking. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs [3]. In addition, as mobile cloud computing is a new model [4], it still has an opportunity for future research expansion in the three areas: First, Security issues are still frightening and there should be an appropriate solution for it, Second, architecture for the mobile cloud diverse wireless network should be investigated, Thirdly, A single access platform for mobile cloud computing via various operating systems platforms need to be established. In another article, research on cross-tenant trust models in Cloud computing is carried out through a systematic analysis of cross-tenant trust relations by *Tang & Ravi Sandhu* [5].

A) ABBREVIATIONS
I) Attribute Based Data Storage (ABDS)
II)Privacy Preserving – Cipher Policy – Attribute based Encryption (PP-CP-ABE)
III) Encryption Service Provider (ESP)

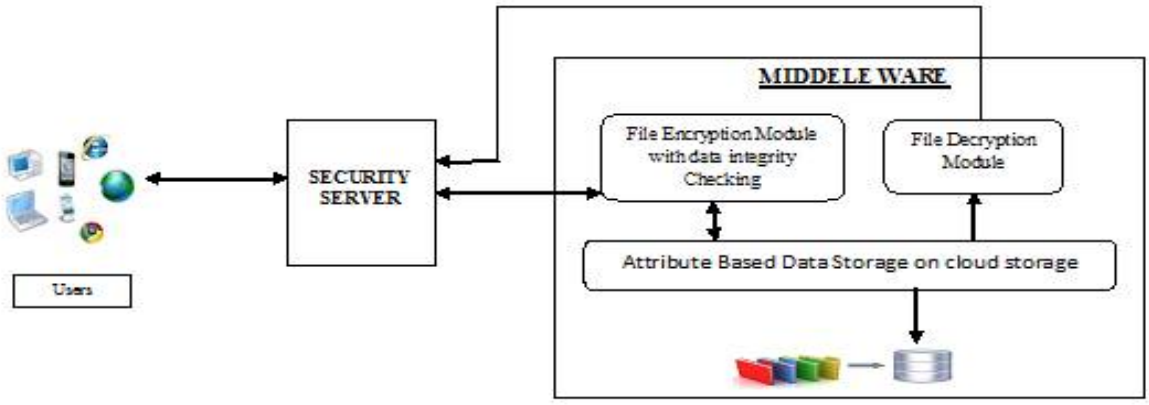


fig 1. System Architecture

III. SYSTEM ARCHITECTURE

The proposed system will provide a lightweight Cloud-based storage framework (middleware), which provides an effective mechanism for users to verify their data integrity, data security and secure network flexibility with PP-CP-ABE, ABDS, data integrity checking modules. Meanwhile it incorporates an effective mechanism for users which can relieve much burden from mobile devices.

In this proposed system mobile devices interact with middleware through a general web service portal. As shown in Figure 1, proposed system consist four major components: Users, Cloud Storage Service Provider (CSSP), Security Server (SS) and Middleware. The work is divided into following modules,
1. Authentication module with low cost

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

2. Attribute based Key Generation
3. Data Encryption and Security checking with PDP based Schemes
4. Attribute based file distribution
5. Attribute based retrieval and decryption

1. Authentication module with low cost

Whenever user wants to use cloud services, each user needs to register with the security server (SS). While registration to security server user specifies personal credentials with specific attribute which are further used at the time of key generation module. Also, at the time of registration users device is also registered for device authentication with its specific MAC address. If user wants to download owned data file then authentication will be verified with help of SS. User can download owned decrypted data if and only if the verification process is successful with right authentication of that device.

2.Attribute based Key Generation

Each user using cloud storage registers with the SS. After successful registration SS executes the key generation task. In this task user attributes will be authenticated and right private keys and public key for the user will be generated. An attribute can be any descriptive string that defines, classifies, or annotates the user, to which it is assigned.

In this module, the key generation algorithm takes a set of attributes(S) like user occupation, mail_id and MAC address of individual's device as input and outputs a set of private key and public key components corresponding to each attributes with help of Attribute based key generation algorithm.

3. Data Encryption and Security checking with PDP based Schemes

It will perform two operations Viz. encryption on uploaded file & data integrity checking

i] Encryption on uploaded file

To outsource the computation of encryption and preserve the data privacy, user must encrypt data files with help of ESP from middleware. The ESP then provides encryption service with PP-CP-ABE scheme [1] to the data owner without knowing the actual data encryption key.

ii] Data integrity checking

In Cloud storage system, most users are worried about data security and data integrity at unreliable and un-trusted storage servers. Therefore In this module PDP security protocol [3], [6] is used to provide data security. Data integrity checking process consists following steps:

i. The user uploads input files on cloud with help of SS.

ii. After successful encryption of that file the checksum related with that file is calculated and this checksum value is stored on SS in form of signature value and further this signature is used for verification operation.

iii. If user sends data integrity checking request to security server with a target filename, proof message is produced according the PDP based model and sent to SS.

iv. Security Server is responsible to verify the proof message by comparing original signature value with newly generated value, If verifying operation fails, it return false to users; otherwise, an Integrity Assurance procedure will be invoked by security service of middleware. Fig. 2 shows exact working of third module.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

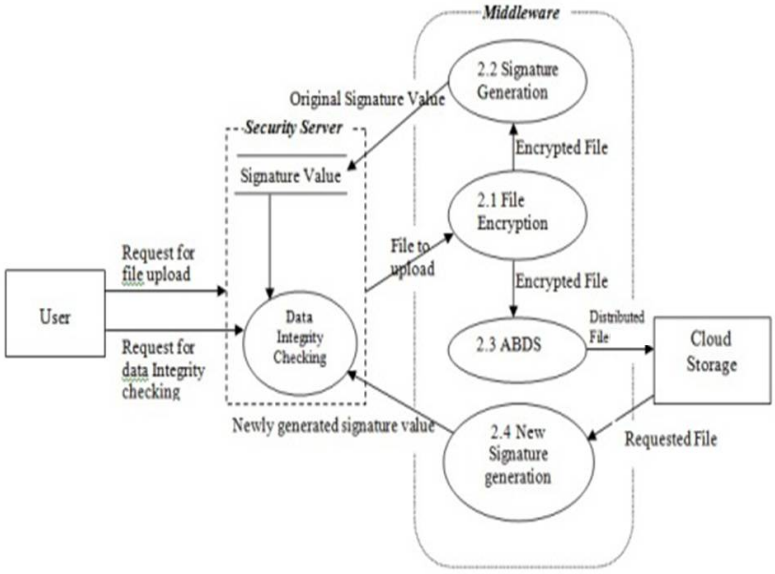


Fig2: Working of .Data Encryption and Security checking module

4. Attribute based file distribution Module

This module uses an Attribute Based Data Storage (ABDS) scheme that is based on PP-CP-ABE [1] to enable efficient, scalable data management and sharing. The ABDS system achieves scalable and fine-grained data access control, using public cloud services. Based on ABDS algorithm [1], user attributes are organized in a carefully constructed hierarchy so that the cost of membership revocation can be minimized. Moreover, ABDS is suitable for mobile computing to balance communication and storage overhead and thus reduces the cost of data management operations for both mobile as well as cloud infrastructure.

5. Attribute based retrieval and decryption

This module specifies the file retrieval and decryption process of middleware. This scheme achieves scalable and secured data access control using middleware's decryption services which is based on PP-CP-ABE decryption algorithm [1]. It will reduce the computation overhead for decrypting as we have done it for upload process data files.

IV. EXPERIMENTAL SET-UP

The project is implemented in Net Beans IDE 8.0.1. The experiment is carried out using multiple devices which are connected through same Wi-Fi network using IP. Different configuration mobiles and computers (client) are connected to the server. Server monitors all the tasks.

Table 1. System Configuration

Compnents	H/W Configuration	MAC ID
Server Node	Intel(R)Core(TM)i3 with 1.70GHz, RAM 4GB, HDD 1TB	AC-D1-B8-D3-C4-F7
Client Node	mobile Q- core1.2Ghz with Android K 4.4, RAM 2GB, Storage 8 GB	FC:64:BA:CB:3B:11
Client Node	Intel(R)Core(TM)i3 with 2.40GHz, RAM 3GB, HD 640GB	C0-CB-38-35-BD-EB
Client Node	mobile Q- core1.2Ghz with Android K 4.4, RAM 1GB, Storage 16 GB	44:91:DB:89:9C:0C

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

V.EXPERIMENTAL RESULT

In cloud computing important files can be stored in the cloud through different cloud service providers since, it is very necessary to ensure the security, so that no one can access our valuable data. With the help of encryption technique, we can ensure the security of these files. Hence to provide security we used encryption mechanism. Now-a-days, various client side encryption tools and cryptographic algorithms are available in market. For our result analysis we need to compare these tools with our system in form of efficiency and ensure more security.

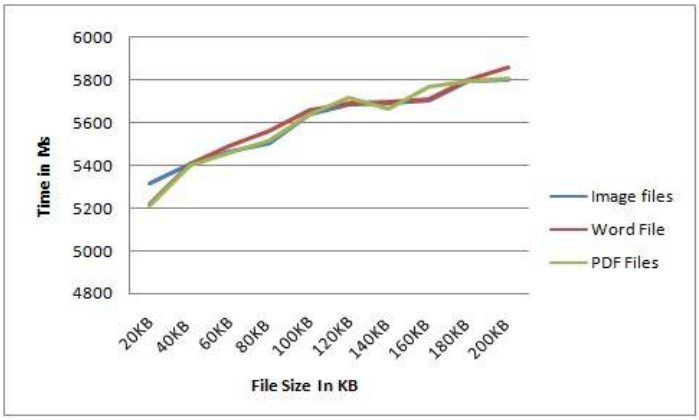
For analyzing our system we used three different mechanisms which are as follows:

- Find results of file encryption and uploading time for different file types and sizes
- Compare our system with different encryption and data uploading tools
- Compare our encryption algorithm with other encryption algorithms

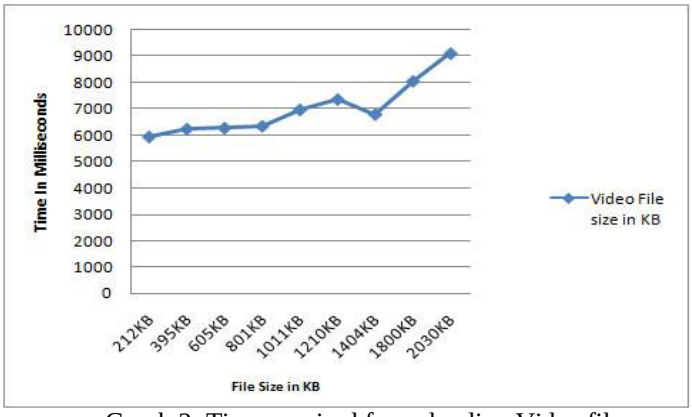
a. Find results of file encryption and uploading time for different file types and sizes

We have simulated the environment for the cloud and following results are generated with respect to *time* required for file encryption and uploading on cloud server.

Different files (image, word, PDF, video & audio) are inputted for uploading. File sizes are taken from 20 kb to 200 kb. With help of Graphs 1,2 & 3 we concluded that the whenever different types of files are uploaded on cloud the performance of our system will not affected because time required for file encryption and uploading will not changes drastically.



Graph 1: Time required for uploading Image, word , Pdf files



Graph 2: Time required for uploading Video files

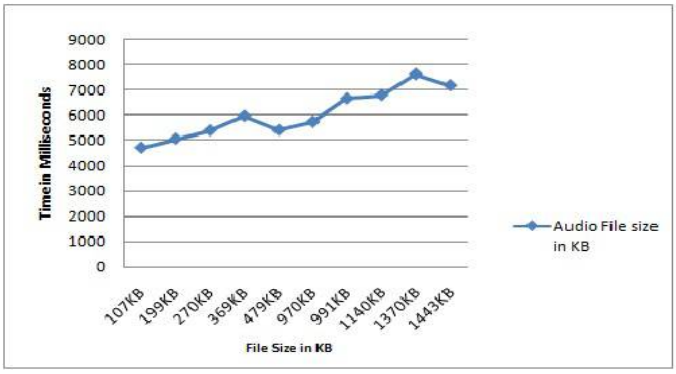
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

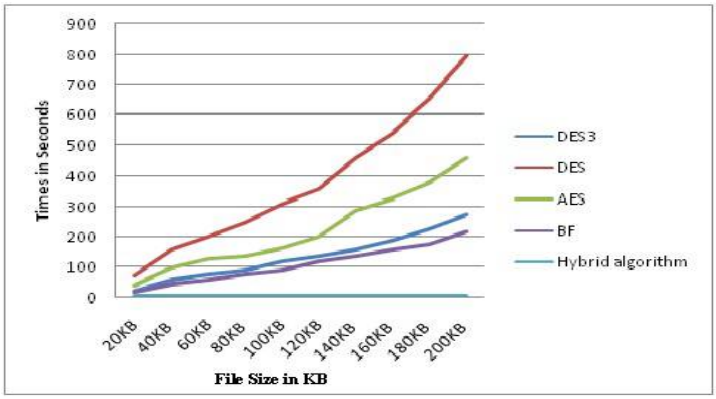
Vol. 5, Issue 10, October 2017



Graph 3: Time required for uploading Audio files

b. Compare our encryption algorithm with other encryption algorithms

To analyze proposed hybrid algorithm we used some popular Cryptography algorithms including DES, 3DES, AES (Rijndael) and Blowfish and their performance was compared by encrypting input files of varying contents and sizes. For this comparisons, we refer results of cryptographic algorithms from Paper "Performance Analysis of Data Encryption Algorithms" [2].



Graph 4: Comparison between Performances of Different Algorithms

From Graph 4 we can conclude that, using proposed Hybrid algorithm resultant performance for file encryption and uploading is better than other algorithms. So we can say that hybrid algorithm provide more security for user's data and keys in less time, i.e. performance of proposed algorithm is more efficient and faster than other cryptographic algorithm.

c. Compare our system with different encryption and data uploading tools

To analyzing performances of encryption tools we refer "Performance Analysis of Client Side Encryption Tools" paper [1]. In this paper authors measured the efficiency of different tools using performance of encrypting data and uploading the encrypted data in the cloud .They compared the performances of five client side encryption tools which are available in the market namely Boxcryptor, Ensafer, SharedSafe, SafeMonk and Cloudfogger.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

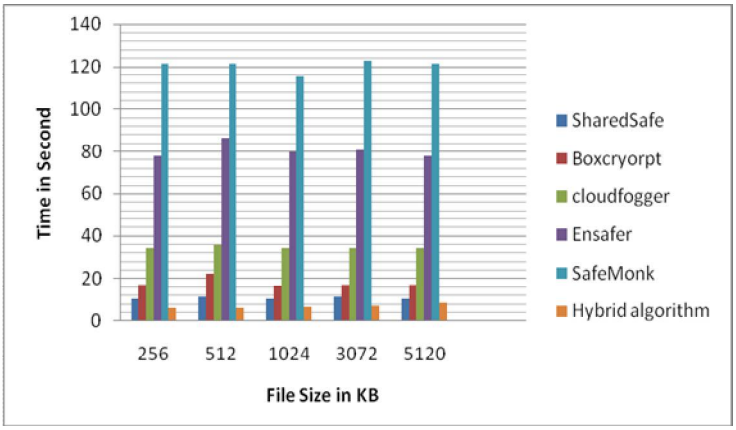
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Table 2. Average comparisons of all tools

Tools name	Average Data Size	Average Upload Time in second
1. SharedSafe	1996.8 KB	52.324
2.Boxcryptor		55.602
3.cloudfogger		51.354
4.Ensafer		53.312
5.SafeMonk		52.34
6. Hybrid		34.488



Graph 5: Average comparisons of all tools

As shown in above Graph 5, we can analyze that, the resultant performance of our system for encryption and uploading of files is better as compare with other encryption tools which are available in market.

VI. CONCLUSION & FUTURE WORK

During this work, we identified different issues related with mobile cloud computing and designed this system that provides the solution for encrypted security with less computation overhead on lightweight devices [9]. The system also supports sharing of encrypted data with large number of users and also gives easy way to upload and download encrypted data stored in the cloud system with attribute based data storage scheme. From analysis, we can conclude that using our Middleware system users can get more efficient and secure cloud computing environment for light weight mobile devices with low computation overhead on mobile. Hence our system is able to provide an effective and efficient mechanism for user to verify their data security, data integrity over more secure network by reliving much burden from mobile devices.

In future we will try to avoid linearly growing ciphertext size with constant cipher text size. And also try to improve further performance by precomputing and caching some mostly used access policy trees from ESP. Also using Hybrid algorithm we will provide more security to users keys and data with more speed of data transactions.

REFERENCES

[1] Bethencourt, A. Sahai, and B. Waters "Ciphertext-policy attribute- based encryption.", IEEE Symposium on Security and Privacy, 321-334, Washington, DC, USA, 2007. IEEE Computer Society.
[2] G. Ateniese, R. Burns and R. Curtmola, "Provable Data Possession at Untrusted Stores," Proceedings of ACM Conf. Computer and Communication and Security, (2007), pp. 598-609.
[3] Zhibin Zhou and Dijiang Huang "Efficient and Secure Data Storage Operations for Mobile Cloud Computing," IEEE TRANSACTIONS ON COMPUTERS, Oct. 2012, pp. 37-45

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

[4] Bo Tang and Ravi Sandhu, "Tenant Trust Models in Cloud Computing," IEEE Transactions on IRI 2013, vol. 99, 2011.August 14-16, 2013, San Francisco, California, 978-1-4799-1050-2/2013 IEEE
[5] Peng Xiao 1and Yanping Zhang, "CS-Mobile: A Cloud based Distributed Storage Middleware for Mobile Devices" international Journal of Smart Home Vol. 7, No. 1, January, 2013.
[6] Ahmed DheyaaBasha, IrfanNaufal Umar, and Merza Abbas, "A Mobile Applications as Cloud Computing: Implementation and Challenge," International Journal of Information and Electronics Engineering, Vol. 4, No. 1, January 2014.
[7] Subrata Kumar Das, Md. Alam Hossain, Md. Arifuzzaman Sardar, Ramen Kumar Biswas, "Performance Analysis of Client Side Encryption Tools," International Journal of Advanced Computer Research (ISSN (print): 2249-7277,Volume-4 Number-3 Issue-16 September-2014.
[8] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms," website: http://www.cse.wustl.edu.
[9] Akanksha R. Patil, Prof. Sandeep G. Sutar, "Attribute based secured storage Middleware for mobile cloud computing", IJATES, March 2016.