



Improved Secure Data Storage with Integrity Verification in Mobile Cloud Computing

Shakkeera L*

Assistant Professor (Senior Grade)

Department of Information Technology

B. S. Abdur Rahman Crescent Institute of Science and Technology

Chennai, Tamilnadu 600048, India

lshakeera@crescent.education

Sharmasth Vali Y

Assistant Professor

Department of Computer Science and Engineering,

Dhanalakshmi College of Engineering

Chennai, Tamilnadu 601301, India

vali566@gmail.com

ABSTRACT

Mobile cloud computing (MCC) provides cloud storage as a service to the mobile users for hosting their data in the public clouds. Data access control is the well-organized method to provide data security in cloud. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is commonly considered for data access control in cloud storage. CP-ABE requires heavy computations for encrypting and decrypting the data, where wireless mobile devices especially lightweight devices such as cell phones and sensors, cannot perform those computations with limited resources. Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) is proposed to overcome the heavy computation by outsourcing the heavy encryption and decryption computation without exposing the responsive data contents or keys to the service providers. An Attribute Based Data Storage (ABDS) system is used for the data storage with less communication overheads. The uploading of new file and updating existing file in cloud data center resources are much easier with respect to the proposed scheme where the data is splitted into various blocks. Hash Based Message Authentication Code (H-MAC) scheme is used to guarantee the integrity of the data stored in the cloud storage. An ABDS system minimizes the cost charged by the service providers with efficient management of data storage in the cloud resources with high security and availability. The proposed system minimizes the communication overhead, delay, energy consumption on the mobile devices by considering cloud storage space and ensures the integrity of the data stored in mobile cloud. To make the system work more efficiently, it can be accessed by multiple mobile users to update and access the files simultaneously.

Keywords—*data storage; data encryption; data decryption; data integrity; H-MAC; mobile devices; mobile cloud computing;*

INTRODUCTION

Cloud computing (Ardagna et al., 2014, Sahu et al., 2012) is a model for enabling ever-present, on-demand network access to a shared collection of configurable computing resources (e.g., networks, servers, storage, input/output devices and applications) that can be rapidly utilized and released with service provider interaction. In cloud computing, the user's data are not stored internal storage, but is stored in the data center resources. The main technology for cloud computing is virtualization. It is used for abstraction of the computing resources. The business companies which provide cloud computing services could control and maintain the operations of these data center resources. The consumers can access the stored data from cloud at any time by using interfaces provided by cloud service providers through any system connected with the internet connectivity. The hardware and software services are also available to the public and business markets.

Smartphone and its application have rapid development due to its popularity and usage. The computing capability and application of smartphone may surpass laptop and PCs. Mobile cloud computing (Rehman et al., 2013, Gupta and Gupta, 2012, Huang et al., 2010, Atre et al., 2016) aim to dispute computing capabilities of mobile devices, conserve local resources especially battery, extend storage capacity and enhance data security to enrich the computing experience of mobile users. Mobile devices effectively make best use advantage of cloud computing to improve and extend their functions. To overcome the disadvantages of limited resources and computing capability in mobile devices in order to access cloud computing with efficiency like traditional PCs and servers.

The security and privacy (Rajarajeswari and Somasundaram, 2016) protection services are achieved with the help of secure cloud application services (Bhisikar and Sahu, 2013). In addition to security and privacy, the secure cloud application services provide the data encryption and decryption, integrity verification, processing speed to mobile users. There is a need for a secure communication model between mobile devices and cloud resources. In this scenario, secure routing protocols can be used to protect the communication overhead, achieve the integrity of data and check the

confidentiality between the mobile devices and the cloud. A data security framework for mobile cloud computing (Patel et al., 2015) paper addresses the concept of secure cloud storage services on resource limited mobile devices. Before uploading the data into the cloud storage servers, the confidentiality of data and information must be ensured. In cloud storage, huge volumes of complex security operations are offloaded remotely. The existing security frameworks focus on reducing the complexity of cryptographic algorithms or methods to offer confidentiality and security. In this framework the cryptographic methods as well as algorithms are used for encryption and decryption of mobile user data. It ensures the additional security and confidentiality for user's sensitive or significant data. This security framework is for the purpose to secure and provide privacy and integrity of user's confidential data in mobile cloud environment.

A secure mobile cloud computing platform (Hao et al., 2015) discusses about the mobile devices and devices are used by the mobile users in the modern world. The mobile-cloud platform allows users to execute the entire mobile device operating system and subjective applications on virtual machines. It has two design requirements. First, the applications can freely migrate between the user's mobile device and cloud server. So, the users can run the applications either in cloud resources for high security or they can run the applications on mobile devices itself for improved user experience. Secondly, in order to protect the user's data on the mobile devices, use hardware virtualization, which isolates the data from the mobile device OS.

The survey paper on mobile cloud computing: issues, security, advantages, trends (Tayade, 2014) discusses that a market of smartphones is growing at a very high speed. Together with a growth of the mobile applications and cloud computing concepts, mobile cloud computing has been introduced for mobile service applications. MCC integrates the cloud computing into the mobile environment and overcome impediments related to the performance (battery life, storage, and bandwidth), environment (heterogeneity, scalability, and availability), and security (integrity and privacy). This work discusses the information about the mobile cloud computing applications, security issues and their solutions.

The data security and integrity of cloud storage in cloud computing concept (Gunjal and Jeny, 2013) addresses that a mobile user stores the mobile data in cloud data storage through a service provider into data center servers, which occurring at the same time and running in collaborating manner. Redundant data removal or server crashes when a user's data grows in maximum size are two main problems in cloud storage. The traditional integrity techniques are not supporting unexpected and rapidly changing data in short duration. It requires new solutions to solve the problems. Therefore, for strong and secure cloud storage system will be needed for data storage correctness (Batra et al., 2013). This paper work is highly efficient and resilient against complex failures. The proposed technique is not adequate for mobile cloud computing scenarios where the mobile devices are less weight to process the compute-intensive mobile applications.

An effective data storage security scheme for cloud computing (Kalpana and Meena, 2015) paper discusses a cloud data storage system, in that user's stores their data on cloud resources and guarantee that correctness and availability of data. Unauthorized data modification and corruption are effectively needed to be detected. In this work, the files are divided into a number of blocks and dissolved across a set of distributed cloud servers. In all the servers, the data is stored in encrypted form and the dynamic database operations like insert, update and delete can be performed on the different data blocks. When retrieving the data from data blocks, the respective files are merged and return it back to the user. To check the accuracy of the files, tokens are generated and send it to the cloud storage. The communication and computation overhead and cost is reduced by storing blocks of data files. This system is not suitable for mobile cloud computing, where the mobile devices are less weight to process the mobile applications like gaming, image processing etc.,

PROBLEM STATEMENT

In mobile cloud computing, the light weight devices have limited resources which cannot perform the heavy computation like encryption and decryption processes in CP-ABE. It is very complicated process to share encrypted data with a large number of users, in which the data sharing group can be changed frequently. The CP-ABE scheme is used for key management and cryptographic access control in an efficient way. The unique features of CP-ABE solutions in cloud storage system require an efficient data access control. The CP-ABE does not provide effective solution to mobile cloud computing where the mobile devices are light weight with limited resources. Hence, heavy computations such as encryption and decryption involved in the CP-ABE cannot be performed by light weight mobile devices.

IMPROVED SECURE DATA STORAGE WITH INTEGRITY VERIFICATION IN MOBILE CLOUD COMPUTING

The proposed framework is to secure the storage system in public and private clouds without exposing the data to the service providers. The improved secure data storage with integrity verification framework is shown in Figure 1. Privacy Preserving Cipher Policy Attribute Based Encryption (PP-CP-ABE) and Attribute Based Data Storage (ABDS) techniques are proposed for lightweight mobile devices, it can securely outsource the encryption and decryption operations to cloud service providers without exposing the data and secret keys. Data access control policies are implied in ABDS system. In ABDS, the user's attributes are managed in hierarchy so the cost for membership revocation can be reduced. ABDS system is also suitable for mobile cloud to balance the communication and storage overhead and thus reduces the cost of data management operations. There are three independent cloud service providers are mentioned namely Storage Service Provider (SSP), Encryption Service Provider (ESP), Decryption Service Provider (DSP). Even if SSP, DSP and ESP are colluded each, the data content and other sensitive information of the cloud user is secured because part of the secret information of the process is retained by the data owner. This concept is used to minimize computation, storage, and communication overheads and highly protected to store and retrieve data in public cloud with minimal management cost.

Energy Consumption: It is the overall time taken to complete the processing of the start and end uploading of mobile applications. It can be calculated using Equation 1.

$$\Delta E_{\text{Total}} = \Delta E_{\text{start}} + \Delta E_{\text{end}} \quad (1)$$

Here, ΔE_{start} is the execution of data uploaded at start of energy and ΔE_{end} is the execution of data uploaded at end of energy.

Computational Overhead: Computational overhead is the total time taken to complete the processing of compute-intensive mobile applications. The overall computational overhead between different mobile applications is calculated using the Equation 2.

$$C = (CE - UE) / TE * 100 \quad (2)$$

Where,

TE-Total Energy

UE-Utilized Energy

CE-Current Energy

Average Delay: Average delay is the differentiation between the current time and the time at which applications are entered into the queue initially. The average delay is calculated using the Equation 3.

$$L = \sum (t_c - t_q) / n \quad (3)$$

Where t_c is the current time while t_q is the time at which an application entered the queue. n is the total number of applications.

Processing Speed: The amount of processing speed consider for transferring the storage elements to the cloud storage.

The proposed system is divided into five important phases, namely:

- Data Owner (DO) Registration
- PP-CP-ABE Encryption phase
- ABDS Data Storage in SSP
- PP-CP-ABE Decryption Phase
- Integrity Verification

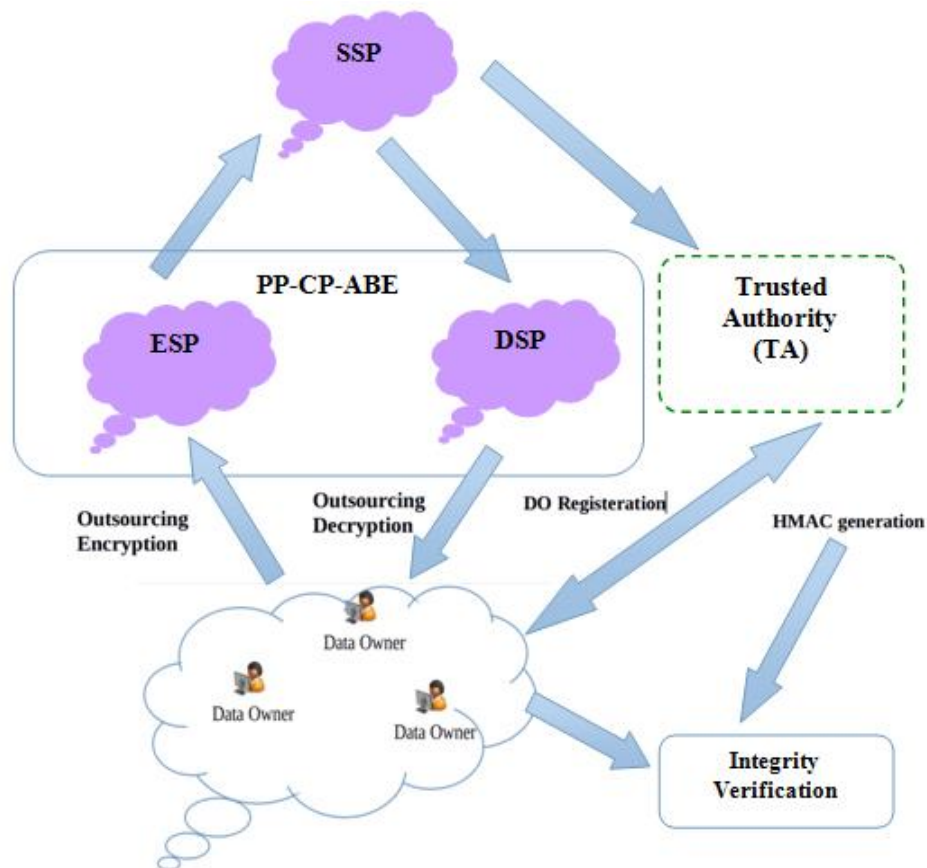


Fig. 1. Improved secure data storage with integrity verification in mobile cloud computing

A. Data owner registration

The data owner must be registered with Trusted Authority (TA) in order to get the secure data storage services from cloud. The data owner sends their credentials such as username, password and other attribute details to the TA, then TA store the data owner details in database and generate the unique private key for data owner. The secret key is send to the DO through secure channel. The data owner registration process is shown in Figure 2.

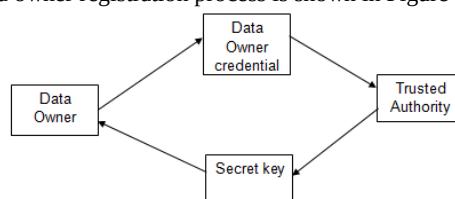


Fig. 2. Data owner registration

B. PP-CP-ABE encryption phase

Before the data owner is use the encryption service from cloud, DO is get authenticated by the TA. The data owner is splitting the data into multiple blocks. The DO send the data access to the ESP and same time DO does the part of the encryption in order the keep the data content secure from the ESP. After encrypting each block local H-MAC code will be generated for each and this hash code is stored locally for future integrity verification of the data. Then ESP does the encryption process and sends the ciphertext to the storage service provider. The encryption method of PP-CP-ABE is shown in Figure 3.

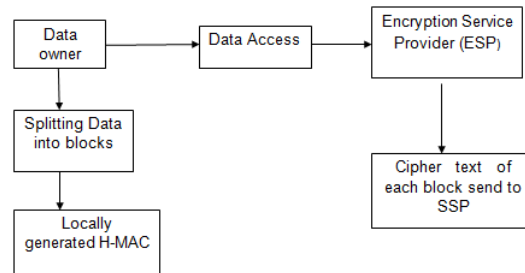


Fig. 3. PP-CP-ABE encryption

C. ABDS data storage in SSP

ESP sends the encrypted ciphertext to the storage service provider. Then SSP stores the ciphertext based on block wise method (ABDS) in cloud servers. The data storage processing in SSP using ABDS method is shown Figure 4.

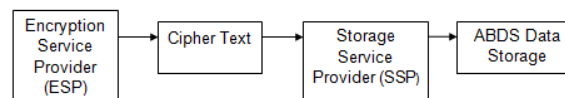


Fig. 4. ABDS data storage in SSP

D. PP-CP-ABE decryption phase

The data owner is requesting the data contents from the cloud servers or want to update the accessible block of data in the cloud. Then storage service provider send the stored cipher text to the decryption service provider as well as invoking the DO request to the TA for Hash based Message Authentication Code. The decryption service provider(DSP) decrypts the cipher text received from SSP using DO secret key. This private key blinded by the data owner(DO), hence even if the DSP decrypts the data content which does not revealed to the DSP, because final part of the decryption process is done by the DO. The decryption process of PP-CP-ABE is shown in Figure 5.

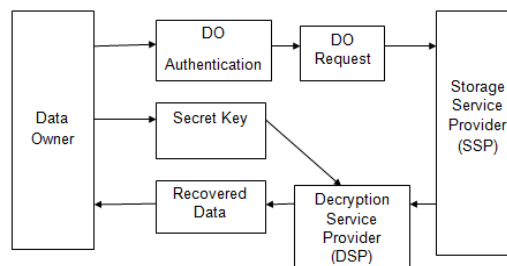


Fig. 5. PP-CP-ABE decryption

E. Integrity verification

After decryption of the data, H-MAC code will be received from trusted authority. If the H-MAC code received from the TA and locally generated H-MAC code is matched, then the integrity of the data is verified successfully. The process of integrity verification using H-MAC technique is shown in Figure 6.

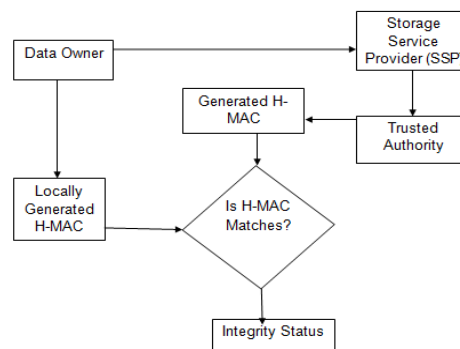


Fig. 6. Integrity verification

Algorithm 1 - Privacy Preserving Cipher Policy Attribute-Based Encryption and Decryption (PP-CP-ABE)

```

(1) Begin
(2) Register (DO credentials)
(3) Return  $Pri_K$  from TA
    Encrypt_Data ( DO data)
(4) Begin
(5) Generate(Access_Policy)
(6) Split(data)
(7) For (i=1; i<data block;i++)
(8)     Encrypt(i) at ESP
(9)     Generate_HMAC
(10) End
    Store (Data)
(11) Begin
(12) Send ciphertext (CT) from ESP to SSP
(13) At SSP use ABDS
(14) End
    Decrypt_Data (CT)
(15) Begin
(16) Send_data_request from DO to SSP
(17) At SSP invoke TA
(18) Forward CT to DSP
(19) At DSP Decrypt (CT,  $Pri_K$ )
(20) Return decrypted data
(21) End
    Integrity
(22) Begin
(23) At DO
(24) Generate_HMAC()
(25) Get_HMAC from TA
(26) Status=Compare(generated HMAC, received HMAC)
(27) If(status==true)
(28)     Integrity ensured
(29) Else
(30)     Integrity not ensured
(31) End
(32) End

```

OPERATIONAL WORKFLOW

Figure 7 shows the operational workflow of proposed system. First create a mobile cloud environment for mobile users to execute heavy application from mobile devices. The H-MAC algorithm is executed and integrity is verified. The operational method is as follows:

1. Data Owner (DO) is register with Trusted Authority (TA).
2. TA provides the private key through the secure channel.
3. Data is splitted and DO generates Secret key for the blocks.
4. Encryption process outsource into Encryption Service Provider (ESP).
5. Attribute Based Data Storage(ABDS) at SSP
6. DO request to Decryption Service Provider (DSP) for data access.
7. DSP will request to SSP.
8. SSP sends the Cipher text to the DSP.
9. SSP will invoke the Cipher text to the TA.
10. DSP send the recovered text using secret key to DO

11. TA regenerates the Hash Based Message Authentication Code (H-MAC).
12. TA sends the regenerated H-MAC to DO
13. DO compare locally generated Hash Based Message Authentication Code (H - MAC) and regenerated HMAC to ensure the data integrity.

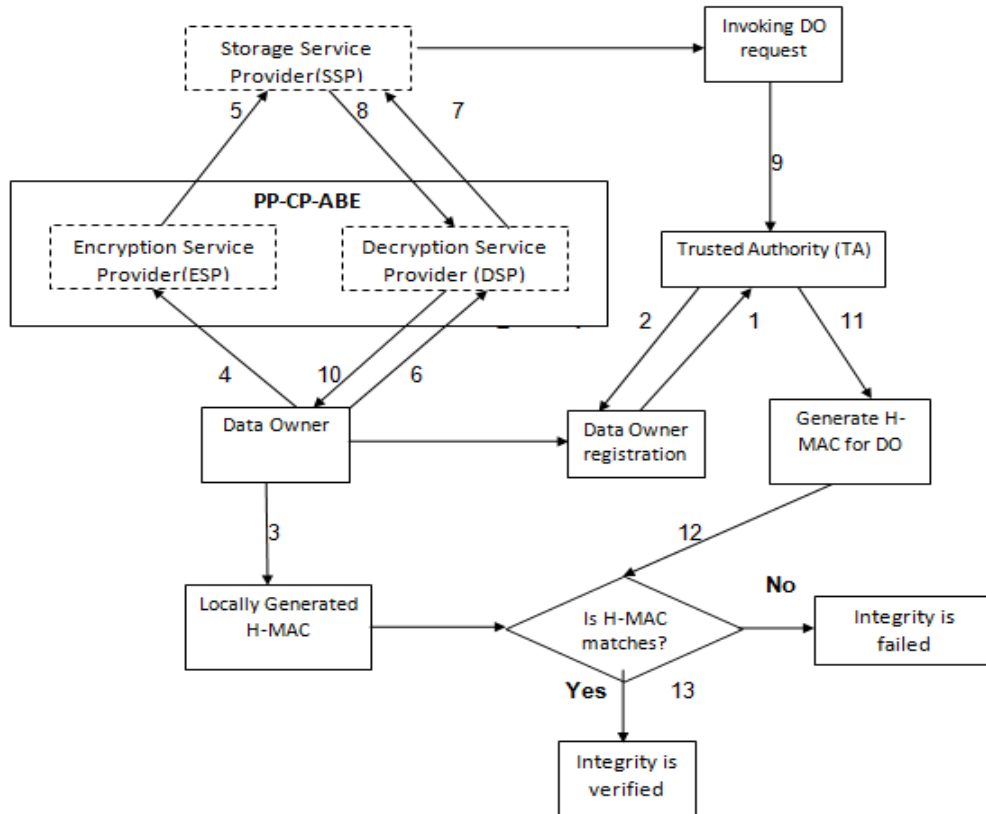


Fig. 7. Operational Workflow

A. Experimental setup

To simulate a private cloud environment, NetBeans IDE with JDK, MySQL is used. Private cloud is set up by creating datacenter with hosts, mobile users (clients) and mobile service providers. Virtual machines are created and provide cloud services to the clients. The existing algorithm is compared with the PP-CP-ABE algorithm. The performance metrics such as energy consumption, computational overhead, delay, storage space and processing speed are calculated for different mobile applications (offloaded) in both existing and proposed algorithms. All these experiments are performed for a maximum of 50 applications (offloaded) from mobile users. Experiment 1 discuss about the energy consumption. Experiment 2 calculates the average delay. Experiment 3 calculates the processing speed. Experiment 4 discusses about the storage space and Experiment 5 analyze about computational overhead.

B. Energy consumption

Figure 8 shows the energy consumption of both CP-ABE, PP-CP-ABE algorithms. The energy consumption is calculated using Eq.(1). It is evident from the comparison that PP-CP-ABE has better energy consumption of about 80% than CP-ABE. This is because data uploading prevents wastage of energy in servers. Hence the energy consumption happens due to the key generation of each data.

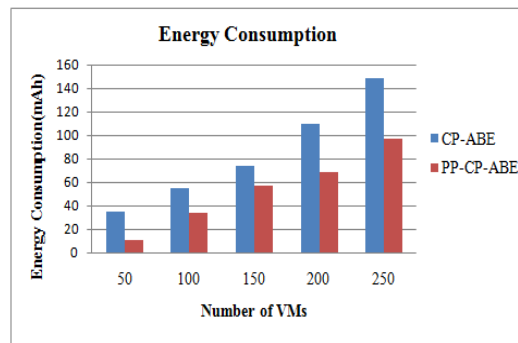


Fig. 8. Energy Consumption

C. Average delay

Average delay is the difference between the current time and the time at which application entered into the queue initially. The average delay is calculated by using the Eq. (3). The PP-CP-ABE algorithm reduces the average delay around 50% when compare to CP-ABE algorithm. This is because the compute-intensive and resource-intensive mobile applications are executed in mobile cloud environment instead of mobile devices itself. Figure 9 shows the average delay of both CP-ABE, PP-CP-ABE algorithms.

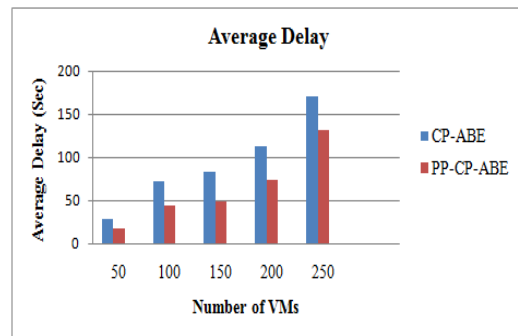


Fig. 9. Average Delay

D. Processing speed

Figure 10 shows the processing speed mobile devices both in CP-ABE, PP-CP-ABE algorithms. The experimental result shows that our proposed PP-CP-ABE algorithm increases the overall processing speed by 70% when compared that of CP-ABE algorithm. This is because of data are splitted in to block wise and store into cloud storage using ABDS approach.

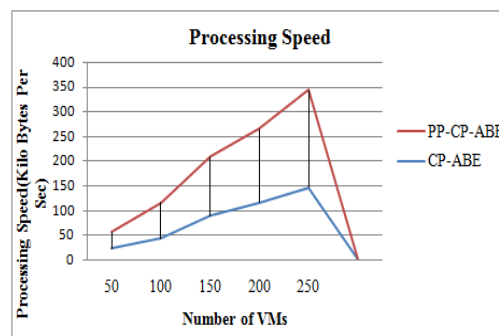


Fig. 10. Processing Speed

E. Computational overhead

Figure 11 shows the computational overhead of the CP-ABE, PP-CP-ABE algorithms. The computation overhead is calculated using Eq. (2). It shows that our proposed PP-CP-ABE algorithm reduces the overall computational overhead (based on energy consumption) by 60% when compared to that of CP-ABE. This is because of data storage space is increases.

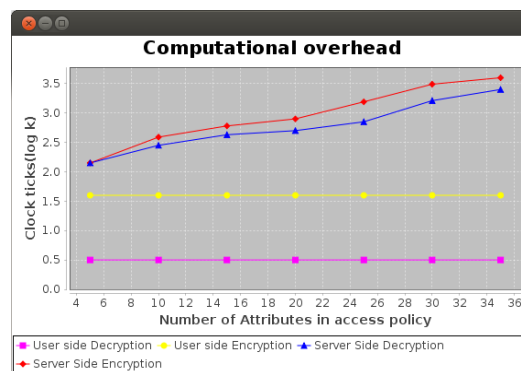


Fig. 11. Computational Overhead

F. Storage space

Table 1 shows the storage space in mobile devices and cloud storage space. When compared to CP-ABE, the storage spaces for mobile applications are decreased using PP-CP-ABE algorithm in cloud environment. This is because storage service provider in cloud environment stores the processed ciphertext based on ABDS scheme in block wise scheme. The scheme effectively uses the cloud storage space.

TABLE I. COMPARISON OF STORAGE SPACE IN CP-ABE AND PP-CP-ABE

Mobile Applications	CP-ABE		PP-CP-ABE	
	Mobile devices	Cloud	Mobile devices	Cloud
Gaming	5MB	200MB	6KB	530KB
Image Processing	3MB	250MB	200KB	450KB
Video Streaming	5MB	300MB	150KB	700KB
Adobe Reader	100KB	300KB	200KB	500KB
Notepad	1MB	100MB	250MB	400MB

G. Integrity verification

Figure 12 shows the integrity of application data between CP-ABE and PP-CP-ABE algorithms. The algorithm is used to check the modification data in cloud storage space. It shows that the proposed PP-CP-ABE algorithm check the integrity verification of the data by 80% when compared to that of CP-ABE using H-MAC.

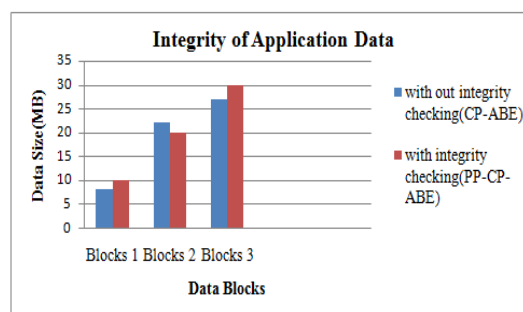


Fig. 12. Integrity of Application Data

CONCLUSION

The proposed security framework discusses the cloud data storage services to secure the data management in private/public clouds. Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) provides the encryption and decryption services in order to minimize the heavy computations at the mobile devices. The scheme Attribute Based Data Storage (ABDS) provides the efficient data management and storage based on the attributes with minimal cost. An integrity verification mechanism also applied to the system using Hash Based Message Authentication Code (H-MAC). Hence the data owner can check the integrity of data stored in the cloud. The proposed mechanism is implemented with low cost, less communication and computation overheads with high security strength. This project

work discuss about improved secure data storage operations with integrity verification for mobile cloud computing. Most approaches concentrate on light weight devices. In the future, to make the system work more efficiently, the system can be accessed by multiple mobile users to update and access the files simultaneously.

REFERENCES

- [1] D. Ardagna, G. Casale, M. Ciavotta, J.F. Pérez, W. Wang, “Quality-of-service in cloud computing: modeling techniques and their applications”, Springer Transaction on International Journal of Internet Services and Applications, Vol. 5, No. 11, pp. 1-17, 2014.
- [2] H. Atre, Karan Razdan, Raj Kumar Sagar, “Offloading Computation for Efficient Mobile Cloud Computing”, Indian Journal of Science and Technology, Vol. 9, No. 22, pp. 1-6, 2016.
- [3] K. Batra, Ch. Sunitha, Sushil Kumar, “An Effective Data Storage Security Scheme for Cloud Computing”, International Journal of Innovative Research Computer And Communication Engineering, Vol. 1, No. 4, 2013.
- [4] P. Bhisikar, A. Sahu, “Security in Data Storage and Transmission in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 3, 2013.
- [5] Y. Gunjal, and R. Jeny, “Data Security and Integrity of Cloud Storage in Cloud Computing”, International Journal Of Innovative Research in Science, Engineering And Technology, Vol. 2, No. 4, 2013.
- [6] P. Gupta, S. Gupta, “Mobile Cloud Computing: The Future of Cloud”, International Journal in Computer Communication Engineering, Vol. 1, No. 3, 2012.
- [7] Zijiang Hao, Yutao Tang, Yifan Zhang, Ed Novak, Nancy Carter, Qun Li, “SMOC: A Secure Mobile Cloud Computing Platform”, IEEE Conference on computer communications-INFOCOM, 2015.
- [8] D. Huang, et al., “Mobile Cloud: A Secure Mobile Cloud Framework For Pervasive Mobile Computing And Communication”, 2010.
- [9] V. Kalpana and V. Meena, “Study on Data Storage Correctness Methods in Mobile Cloud Computing”, Indian Journal of Science and Technology, Vol. , No. 6, pp. 495–500, 2015.
- [10] Chandni Patel, Sameer Singh Chauhan, Bhavesh Patel, “A Data Security Framework for Mobile Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, No. 2, 2015.
- [11] S. Rajarajeswari and K. Somasundaram, “Data Confidentiality and Privacy in Cloud Computing”, Indian Journal of Science and Technology, Vol. 9, No. 4, 2016.
- [12] Atta ur Rehman Khan, Mazliza Othman, Sajjad Ahmad Madani, Samee Ullah Kahn, “A Survey of Mobile Cloud Computing Application Models. IEEE Communications Surveys and Tutorials, Vol. 16, No. 11, pp. 393-413, 2013.
- [13] Deepti Sahu, Shipra Sharma, Vandana Dubey, Alpika Tripathi, “Cloud Computing in Mobile Application”, International Journal of Scientific and Research Publications, Vol. 2, No. 8, 2012.
- [14] D. Tayade, “Mobile Cloud Computing: Issues, Security, Advantages, Trends” International Journal of Computer Science and Information Technologies, 2014.
- [15] R. Joseph Manoj, M.D. Anto Praveena, K. Vijayakumar, “An ACO-ANN based feature selection algorithm for big data”, Cluster Computing The Journal of Networks, Software Tools and Applications, ISSN: 1386-7857 (Print), 1573-7543 (Online) DOI: 10.1007/s10586-018-2550-z, 2018.
- [16] G. Indrajith and K. Vijayakumar, “Automatic Mathematical and Chronological Prediction in Smartphone Keyboard” International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 5 Issue 5 May 2016, Page No. 16714-16718.
- [17] K. Vijayakumar and C. Arun, “A Survey on Assessment of Risks in Cloud Migration”, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.66 May 2015.
- [18] K. Vijayakumar, C. Arun, Automated risk identification using NLP in cloud based development environments, J Ambient Intell Human Computing, DOI 10.1007/s12652-017-0503-7, Springer May 2017.

AUTHORS BIBLIOGRAPHY



Shakkeera is working as Assistant Professor (Senior Grade) at B. S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India since 2006. She has received B.Tech. in Information Technology from Crescent Engineering College affiliated to Anna University, Tamilnadu, India in 2005, M.E in Computer Science and Engineering from B. S. Abdur Rahman Crescent Engineering College affiliated to Anna University, Tamilnadu, India in 2010. She has a teaching experience of 13 years. She has published more than 25 research publications in refereed International/National Journals and International/National Conferences. Her areas of specializations are Cloud Computing, Mobile Cloud Computing, Internet of Things, Network Security, Mobile Ad-Hoc Networks and Web Services.



Sharmasth Vali is working as Assistant Professor at Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India since 2013. He has received his B.Tech. in Computer Science and Engineering from Shadan College of Engineering and Technology, JNTU Hyderabad in 2007, M.E. in Computer Science and Engineering from B.S.Abdur Rahman Crescent Engineering College, Anna University in 2009. He is presently doing Ph.D in Information Technology from B. S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, Tamil Nadu, India. He has a teaching experience of 9 years. He has published more than 10 research publications in refereed International/National Journals and International/National Conferences. His areas of specializations are Network Security, Intrusion Detection and Prevention Systems, cloud computing and Mobile Ad-Hoc Networks.

