International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 7 – APRIL 2017 (SPECIAL ISSUE)

A Collective Attitude to Certify Data Security in Cloud Computing

B GOWRI[#1] and M PENASIR PHUTO[*2]

[#]*ME, Dept. of Computer Science Engineering, Idhaya Engineering College for Women, Chinnsalem-606201, Tamilnadu, India*

[*] *Assistant Professor, Dept. of Computer Science Engineering, Idhaya Engineering College for Women, Chinnsalem-606201, Tamilnadu, India*

***Abstract*— Cloud computing is a forthcoming revolution in information technology (IT) industry because of its performance, Convenience, low cost and many other amenities. It is an approach to maximize the capacity or step up capabilities dynamically without investing in new infrastructure, nurturing new personnel or licensing new software. It provides enormous storage for data and faster computing to customers over the internet. It essentially shifts the database and application software to the large data centers, which are cloud, where management of data and services may not be completely trustworthy. That is why companies are unenthusiastic to deploy their business in the cloud even cloud computing offers a wide range of luxuries. Security of data in cloud is one of the major issues which acts as an obstacle in the implementation of cloud computing. In this paper, a frame work comprising of different techniques and specialized procedures is proposed that can efficiently protect the data from the beginning to the end, that is from the owner to the cloud and then to the user. The strategy followed to protect the data utilizes various measures such as the SSL (Secure Socket Layer) 128-bit encryption and can also be raised to 256-bit encryption if needed, MAC (Message Authentication Code) is used for integrity check of data, searchable encryption and division of data into three sections in cloud for storage. The division of data into three sections renders supplementary protection and simple access to the data. The user who wishes to access the data is required to provide the owner login identity and password, before admittance is given to the encrypted.**

***Index Terms*— Cloud computing, Security, Distributed System, Encryption, Data Packets**

I. INTRODUCTION

Now a day's people are downloading files from any website in internet. They are making use of internet to download any data, updating the application and launching new application on their device. All the users want to download their files in a quicker and efficient manner without the loss of data. Many protocols have been used so far to transfer the files from source to the target. Generally, the file transfer protocol is used for years to achieve efficient transfer. The proposed technique aims at using message broker instead of protocols to transfer files between the data centers. It helps in eliminating the extra amount of time that is required to download a file from a source server and also promises reliable file transfer. Cloud became the phenomenon thing for all kinds of users in internet. It provides marvelous storage facilities and security mechanisms for the user and the corporate offices. Anybody can own a cloud space and they can use it for storing and manipulating the data and information. The best known example of cloud is our email system. Every day are making use of email like Gmail or Yahoo. The software of that email system does not exist on the user's computer. It is actually present on the server side. Just making use of internet to access the email. This scenario depicts what cloud is actually doing. Message brokers are used to transfer the messages between the source and the target server. They aim at moving the messages from one place to another more quickly and precisely. The main advantage of this message broker is that message transfer will consume fewer amounts of time and overhead while are comparing with file transfer protocol. Although, file transfer can be done by any communication protocol, it will not guarantee reliability when they are trying to transfer the files between the data centers which are too far from each other.

Cloud computing is the distributed model for provide convenient, on demand network access to a distributed environment of computing resources like services, applications, storages and servers and so on. Securely store and retrieve the data as like using cloud computing. But when transmit the data over a public area network is not much secure, there are various attacks like Byzantine server failures, malicious data modification attack. So propose an effective and flexible distributed scheme with two algorithms AES and MD5. Use of this algorithm we transmit a data securely in public area network.

A. Mobile cloud computing

Mobile cloud computing is the combine of cloud computing features and mobile web, which is the most popular tool for mobile users to access services and applications on the Internet. It provides users storage services and data processing in clouds. Mobile cloud applications move the data storage and computing power away from mobile phones and into the cloud. The cloud computing features provided in the mobile phone, which allows users an online access to unlimited computing power and storage space. Many applications based on Mobile Cloud Computing, such as Google's gmail, Voice Search, Maps and Navigation systems

for mobile, and some applications on an Android platform, LiveMesh from Microsoft, MobileMe from Apple and Motoblur from Motorola, have been developed and served to users [2]. The combination of cloud computing, mobile Web, portable computing devices, wireless communication infrastructure, location-based services etc., has base the foundation for a computing model, called mobile cloud computing.

B. Android Based Application

Android platform is a smart mobile phone platform released by Google. Android is open and free, providing an easy-to use development kit and runs on the Linux Kernel. Android provides the support of location service and mobile map, which is probably a concern of large numbers of developers. Android depend on Linux for core system services such as security, process management, network stack, memory management, and driver model.

Android consists of the user interface, operating system, and middleware, application software [10]. The Android SDK provides tools and APIs to develop applications using Java language codes on the Android platform. Android supports GPS, compass, Video Camera, and 3d-accelerometer. It enables replacement and reuse of components and an efficient database. Users can easily access, control and process the free Google map.

Various techniques were introduced for efficient storage and file transfer. At present, cloud has become the vital storage solution for all the users. Cloud environment has more problems than others so it requires a better design for achieving less time for download and good load balancing. Starting from File Transfer Protocol (FTP), the traditional file transfer protocol for downloading a file is not much preferable. It is created only for a single connection but not for more than one connection and parallelism requires more amount of coordination. This method is not suitable for a generic infrastructure. Precisely, cloud has several different features like the resources are dispatched across many places and they are connected through a heterogeneous infrastructures. As a whole, this method will not improve the performance because of single con¬nection for download. The next approach designed for file transfer is Dynamic Adaptive Data Transfer Model2 (DADTM). This aims at providing better load balancing than traditional file transfer protocol by using replication servers. They are making use of Lightweight Directory Access Protocol (LDAP) to identify replicas location and the client will provide the file to be downloaded.

II. LITERATURE REVIEW

The cloud is a terminology with a long history in telephony, which has in the past decade, been adopted as a metaphor for internet based services, with a common depiction in network diagrams as a cloud outline. The underlying concept dates back to 1960 when John McCarthy opinion that ‘‘Computation may someday be organized as a public utility’’, indeed it shares characteristics with service bureaus which date back to the 1960s. The term cloud had already come into commercial use in the early 1990s to refer to large Asynchronous Transfer Mode (ATM) networks. By the turn of the 21st century, the term ‘‘cloud computing’’ had started to appear, although major focus at this time was on Software as a Service (SaaS). In 1999, salesforce.com was established by Marc Benioff, Parker Harris. They applied many technologies of consumer web sites like Google and Yahoo! to business applications. They also provided the concept of ‘‘On demand’’ and ‘‘SaaS’’ with their real business and successful customers. IBM extended these concepts in 2001, as detailed in the Autonomic Computing Manifesto, which describes advanced automation techniques such as self-monitoring, self-healing, self-configuring and self-optimizing in the management of complex IT systems with heterogeneous storage, servers, applications, networks, security mechanisms and other system elements that can be virtualized across an enterprise. Amazon.com played a key role in the development of cloud computing by modernizing their data centers. It found that the new cloud architecture resulted in significant internal efficiency improvements and providing access to their systems by way of Amazon Web Services in 2005 on a utility computing basis.

The projected shift to cloud computing will result in dramatic growth in IT products in some areas and in significant reductions in other areas. Despite all the hope of gaining maximum advantage from this cloud computing, it seems to have born with security and management concerns, which time to time hinders its growth. For this, lot of research work has been done to secure the data in cloud computing (primary concern) from every perspective, but everything seems to face a new challenge as soon as it is employed. However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the pre-processing steps that the user conducts before outsourcing the data file. Any change to the contents of data file, even a few bits, must propagate through the error-correcting code, thus, establishing significant computation and communication complexity. A homomorphism distributed verification scheme using Pseudorandom Data to verify the storage correctness of user data in cloud. This scheme achieves the guaranty of data availability, reliability and integrity. However, this scheme was also not providing complete protection to user data in cloud computing, since pseudorandom data would not cover the entire information. In this technique provides a new way to authenticate in 3-dimensional approaches. It provides availability of data by surmounting many existing problem like denial of services and data leakage etc. Additionally, it also provides more flexibility and capability to meet the rising demand of today’s complex and diverse network. But in this model, the data stored is not in encrypted form and once the username and password is lost, the data can easily be retrieved by any unauthorized user. One more solution provided to maintain the data securely on clouds through token generation algorithm for secure cloud storage service. In this scheme data stores in cloud encrypted block data from and perform token checking algorithm on this encrypted blocks and verify the data in case of modifications of files before storing to cloud. This approach provided two way verification of file blocks which result ensure that data will not be modified.

III. PROPOSED METHODOLOGY

Proposed framework has been structured to provide complete security to the data throughout the entire process of cloud computing, be it in cloud or in transit. Thus, multiple mechanisms and available techniques are applied to shield the critical information from unauthorized parties. The proposed frame work is divided into two phases. First phase deals with process of transmitting and storing data securely into the cloud. Second phase deals with the retrieval of data from cloud and showing the generation of requests for data access, double authentication verification of digital signature and integrity, thereby providing authorized user with data on passing all security mechanisms. This phase deals with mechanisms and methods to store and secure the data from beginning and transmitting it securely to the cloud in encrypted form. It is further divided into sub-sections (Classification, Index Building and encryption, Message Authentication Code (MAC) which provide stepwise details of action on the data).

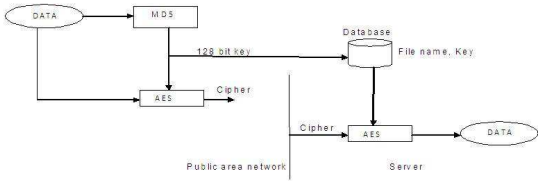


Figure1: Upload File

1. Firstly data are goes to MD5 and AES algorithms; MD5algorithm generates 128 bit keys.
2. That keys are going to AES algorithm and database
3. AES generate a cipher text use of MD5 key.
4. Now data are upload in cloud database, in this database contains file name and key
5. In server side AES use of cipher text and MD5 key, that key contain in database and decrypt the data.
6. Same processes are repeated in reverse order when download the data.

IV. CLASSIFICATION

The data in the cloud is intended to be stored, an approach is introduced for storing the data in different sections in the cloud(public, private, limited access) basis of three cryptographic parameters viz: Confidentiality, Availability and Integrity. These values will be listed by the client himself and sensitivity rating (SR) will be calculated using the proposed algorithm shown ahead. The value of C (confidentiality) is based on the level of privacy needed at each step of data processing, value of I (integrity) is based on how much accuracy of data, reliability of information and protection from unauthorized modification is required, and value of A (availability)is based on how frequently data is accessed and should available immediately when requested.

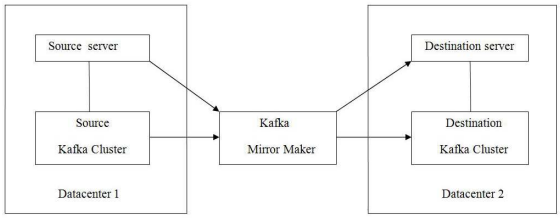


Figure 2: Block diagram

Although Enhanced Kafka provides reliability, can add some security features to make it more efficient. The file is encrypted using one of the best encryption mechanisms called Advanced Encryption Standard (AES) in order to avoid unauthorized access to the file by the external users. The purpose of encryption is to ensure that only somebody who is authorized to access data will be able to read it, using the decryption key. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information. Once the file is encrypted it will be mirrored to the destination Kafka cluster. On the other hand, it will be decrypted to get the original file.

A. *AESAlgorithm*

1. Input: Data, protection section, D [] array of n integer size.
   Where D[ ] array consisting of C, I, A, SR, R of n integer size.
2. Output: Categorized data for corresponding section.
3. For i=1 to n
   - 3.1 C [i]=Value of Confidentiality.
   - 3.2 I [i]=Value of Integrity.
   - 3.3 A [i] =Value of Availability.
   - 3.4 Calculate *SR* [i]=(C[i]+(1/A[i])*10+I[i])/2

4. For j=1 to 10
   - For i=1 to n
   - IF SR [i]== 1||2||3 then
   - S[i]=3
   - IF SR[i]== 4||5||6 then
   - S[i] =2
   - IF SR [i]== 8||9||10 then
   - S[i] =1

Categorize the data on the basis of cryptographic parameters viz: C, I and A. Here D [ ] represents the data and the user has to give values of C, I and A. After applying the proposed formula as shown above, the value of Sensitivity Rating (SR) is calculated. This ‘‘SR’’ value is used to allocate the data to one of the three sections in cloud, i.e., S3 [Public], S2 [Private] or S1. Cloud storage solve the issue of small storage of mobile device i.e. user can store data on cloud. Our main goal is provide security during data transmission in public are a network. Security on cloud during data transmission through the public area network is not secure, so used two securities Advanced Encryption Standard (AES) algorithm and message digest 5 algorithms when data are transmit. Thus the following computational and properties are requiringfulfilling in proposed solution using below figure.1. User firstly initiated connectivity request from cloud server, then authentication server initiated by cloud storage. Server asks a password which is one of the information which is submitted during the registration process in random manner. If users enter valid user id and password then authentication server give permission to access the cloudstorage.2. Therefore when a user making a service request to the cloud storage the user, mobile pre-estimate the file size and file

type. In response of that authentication server are encrypted data uses of Advanced Encryption Standard (AES) algorithm and message digest 5 algorithms.

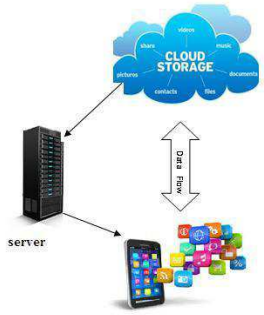
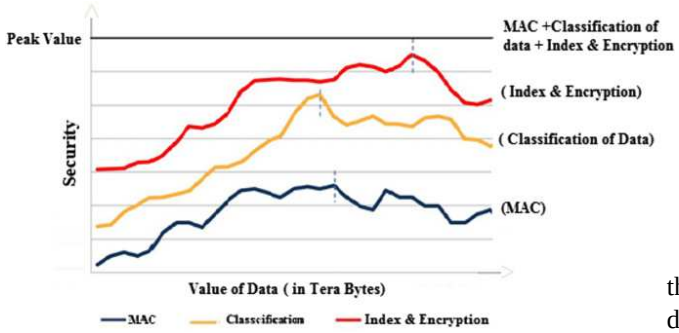


Figure 1 proposed system

Our main aim is provided security during data transmission when data transmit two secure devices so proposed concept is use of two cartographic algorithms AES and MD5 when data are transmit.

V. Experimental Result and Discussions

The experimental evaluation and the system performance are computed and parameters are obtained and listed with their obtained observations.



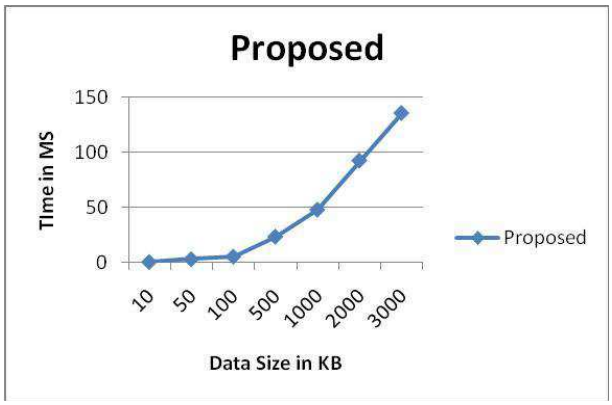
The comparison of proposed model shows that it covers most of the possible security concerns by providing functions and techniques that are good enough to deal with the security issues of cloud computing. The following points are also used to keep the security of data.

1. Background screening of any employee or contractor who has responsibility for back-up or restore of data, if something is found, must be prosecuted.
2. Right to pursue permissible legal action against any supplier employee or contractor's wrong doing if found by the cloud supplier or audit team.
3. Notification, within the context of applicable law (state/federal), of legal department for any confirmed breach into owner'sdata (query or removal).
4. Cloud computing supplier maintains security monitoring logs of all access to owner's data and documents access as routine ,random audit, or suspicious leveraging their prescribed scripts and operational procedures as the basis for all audit, for notless than seven years.
5. Off-site back-up for disaster recovery and business continuity must be encrypted and all vendors must subscribe to all security measures above, without exception, including the audit.

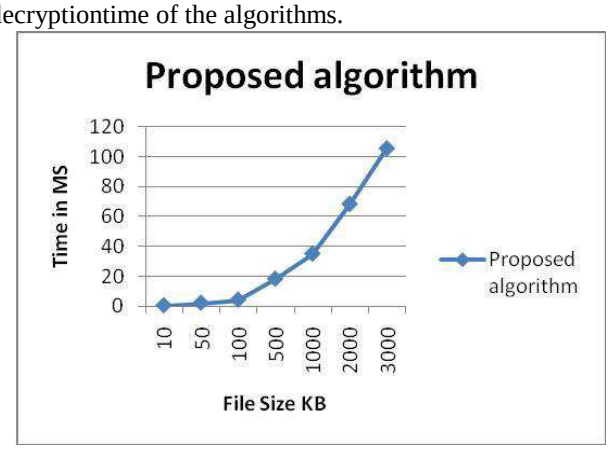
The proposed technique is analyzed with respect to implementation. This model is tested on cloud computing simulator named Hadoop. Shows that the status of security after implementation of security parameters namely MAC, Classification of data and Index and Encryption technique. MAC providesless security than classification of data and classification of dataprovide lesser security than the implementation of index and encryption technique. Overall, the security of data related to owner is very good if combination of all three security parameters viz: MAC, Classification of data and Index and Encryption in taken into account. It results in very good security of the proposed model, which is represented as a peak value.

The experimental evaluation and the system performance are computed and parameters are obtained and listed with their obtained observations.

Encryption time- The amount of time required to perform encryption using the selected algorithm is termed as the encryption of the cryptosystem.



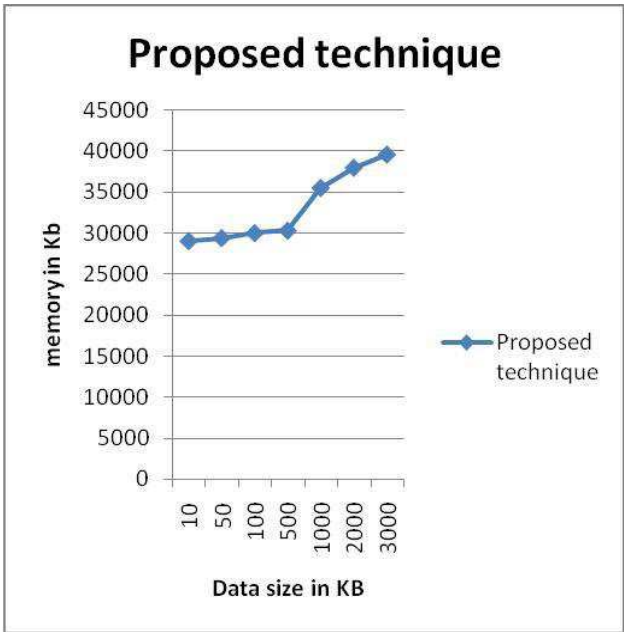
Decryption time-The amount of time required to recover theoriginal data from the cipher text is known as the decryptiontime of the algorithms.



Encryption memory- The amount of main memory requiredto execute the algorithm with the input amount of data isknown as the encryption memory.

Decryption memory The amount of main memory requiredto recover the original file from the cipher text is known asthe decryption memory consumption.

.



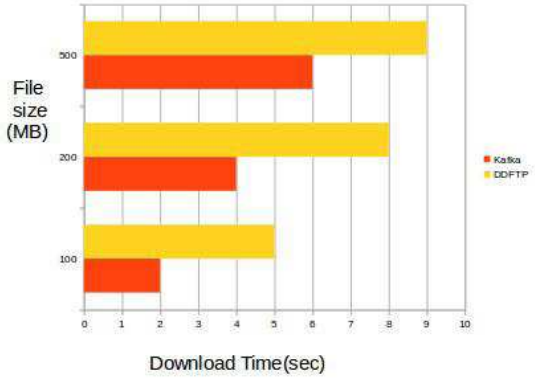


Fig 3.Performance analysis

Experiments have been conducted for various file sizes that includes 100, 200, 300 and up to 500 MB and the resultant time taken for file download is recorded. The main objective of the proposed model is to depict how well the file transfer between the data centers can be done. It also aims at reducing the time it takes to transfer the file and download it in the client side. The use of message broker helps the file transfer more secure and faster.After many color images are done experimentally, the existing and proposed comparison table is generated. This table is shown in Table I. The corresponding comparison chart is given in the figure 6 and 7 for sample image 1. The chart presents the existing methods take long processing time with less threshold values. Whenever increasing the threshold value, the proposed method reduces the processing time and gives better quality image.

VI. CONCLUSION

The proposed technique provides a way to protect the data, check the integrity and authentication by following the best possible industry mechanisms. It introduces the division of data into different sections, Index builder, 128-bit SSL encryption, Message authenticate code and a double authentication of user one by owner and other by cloud and verification of digital signature of the owner. It provides availability of data by surpassing many issues like data leakage, tampering of data and unauthorized access even from the cloud service provider. Proposed method achieves the availability, reliability and integrity of data traversing through owner to cloud and cloud to user. In addition to this, it also provides more flexibility and capability to meet the new demand of today's complex and diverse network and also enable the user to retrieve files from cloud by searching over an encrypted data. Proposed a scheme of secure data and file sharing for public area network use of two algorithms Advanced Encryption Standard (AES) algorithm and message digest 5 algorithms when data are transmit. This security system is implementation on android mobile device. Use of this design securely transfer the data and easily store and retrieve data on both cloud and mobile device. In future, this method can be enhanced to transfer files in the open virtual private network to ensure the authorized access and this can be used by the enterprises to transfer their log files more securely10 and they can save time for copying in more than one cluster at the same time. It also provides the partitions of the log file to track the transfer at any instance to make it more efficient.

REFERENCES

[1] Alowolodu, O, D & Ogundele, O,S.. Elliptic Curve Cryptography for securing Cloud Computing Applications. International Journal of Computer Applications, Vol. 6,pp: 1-7, 2013.

[2] Al-Sakib Khan Pathan et al., "Security in Wireless Sensor Networks: Issues and Challenges" ISBN 89-5519-129-4, Feb. 20-22, 2006 ICACT2006

[3] Bharill, S, Hamsapriya, T & Lalwani, P. A Secure Key for Cloud using Threshold Cryptography in Kerberos. International Journal of Computer Applications, Volume 79, 7: pp:1-11, 2012.

[4] Dinesha, H & Agrawal, V, K..Framework Design of Secure Cloud Transmission Protocol. International Journal of Computer Science Issues. Vol 10, pp: 1-10, 2013.

[5] Dua, I..Data Security in Cloud Oriented Application using SSL/TLS Protocol. International Journal of Application or Innovation in Engineering & Management, Vol.11, pp:1-6, 2012.

[6] Eludiora, S, Olatunde, A, Ayodeji, O, Adeniran, O, Onime, C & Kehinde, L. A User Identity Management Protocol for Cloud Computing Paradigm. International Journal of Communications, Network and System Sciences, Vol 5, pp: 1-7, 2012.

[7] Suhas Holla et al., "ANDROID BASED MOBILE APPLICATION DEVELOPMENT and its SECURITY" International Journal of Computer Trends and Technology- volume3Issue3- 2012.

[8] Pragya Gupta et al., "Mobile Cloud Computing: The Future of Cloud" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012.

[9] P.Srinivas et al.,"Secure Data transfer in Cloud Storage Systems using Dynamic Tokens" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 2, Issue 1, January ,2013.

[10] Yong Wang et al., "A Survey of Security Issues In Wireless Sensor Networks" IEEE Communications Surveys & Tutorials • 2nd Quarter 2006.