A Secure Data Storage over Cloud using ABE (Attribute based Encryption) Approach

Avinash Shukla
M. Tech
Dept. of CSE
UIT, RGPV
Bhopal, India

Sanjay Silakari, PhD
Professor
Dept. of CSE
UIT RGPV
Bhopal, India

Uday Chourasia
Assistant Professor
Dept. of CSE
UIT, RGPV
Bhopal, India

ABSTRACT
Cloud computing technology, its component and various storage strategies is emerging today. All Industries are moving towards cloud due to its fast and scalable in nature. Further a data sharing is possible in between the organization or in group of people. There is technique which uses encryption technique, data access control or verification of users data. Cloud computing technique emerges in its own technique to provide best effort and reliability to the user. Existing approaches used different key generation model for data storage. In this paper an enhance session creation technique is used which is providing the security assurance to the user. The experiment performed with both existing and proposed approach over user data upload. It is further observed that the proposed work outperform data access with less computation time and cost. It can further be used for real-time application without security compromise , as well as in mobile computing.

Keywords
Cloud security, data encryption,auditing approach, virtualization, and data access.

1. INTRODUCTION
Cloud computing (on-demand computing), it is a branch of computing which is based on Internet, In this cloud computing, computing resources, data and information can be shared between one system to another system on demand. Cloud computing is a computing model to be available anywhere. Cloud computing provides solution for storage to clients and different organization with various capability to save and process their data in third-party data centre[14,15]. It depends on sharing of resources to get consistency and economies of scale, same as the usefulness into a network. At the time of cloud computing creation, it is the large concept of converged infrastructure, resources with shared services.

To preserve integrity and privacy of data, encryption and decryption techniques are used. The plaintext is original form of data and the cipher text is the encrypted form of data. Encryption techniques[11,12] take plain text (original form of data) as an input and convert it into cipher text (encrypted form of data), based on algorithm using a key. A key is a component on the basis of which data is encrypted. A decryption technique takes the cipher text (encrypted form of data) and converts it into plain text (original form of data) based on algorithm using a key[13].

Cloud is defined by the two essential concepts:
1) Abstraction: Abstraction is one of the most important concepts of cloud computing. It store detail description of operation and execution perform by the user. User's application, location where data is store and outsource data is not defined.

2) Virtualization: In virtualization two resources are used, first is sharing of data and second is pooling of data. It is based on the centralized infrastructure, where central system or server share data according to requirement. Cost of sharing data is depending upon used data by the user.

Cryptography serves the following goals of security:-

- **Confidentiality:** Confidentiality means the information is known to the sender and the intended receiver only. It is unknown to the other persons. Only authorized person can access the information.
- **Authentication:** Authentication specifies identity of the sender of the information whether the sender is authorized or not.
- **Integrity:** Integrity means the message has not been modified before reaching to the intended receiver. The contents of message cannot be altered by another person.
- **Non Repudiation:** When the message is sent by the sender it cannot refute that message has not been sent. In a similar way, the message cannot be denied by the receiver that has not been received.
- **Access Control:** It specifies that what could be accessed by an authorized person.
- **Availability:** It specifies that the authorized parties will have availability of resources all the time.

A further paper organization is performed as section II. Described the related work and algorithms, while section III. Described the problem definition from the existing approach. Section IV defines the proposed methodology. Section V with experiment and VI with result analysis part. Further VII section is described with conclusion and future work.

2. RELATED WORK
Cloud computing contains various different technique of computing data process and providing security over network for users. In the recent research there are study is performed that how a security can be performed to make sure user data not get compromised. In the recent research various security algorithm [1] such as AES, DES, Blowfish, ECC [2] and many other approach is performed by different author. Thus there are various challenges being observed such computation time, computation cost.

Providing secure session and approach is again an issue while dealing with large amount of data and users. The existing

study works with key generation [3] approach over cloud computing environment and its data model technique.

3. PROBLEM DEFINITION

As per the literature survey is performed with different techniques and different results from the algorithms were monitored and other different technique for data processing, security approach over data store. The techniques for security over the cloud data is also performed by different services to make it more secure and accessible. Cryptographic technology for information integrity [4, 5] and availability which is based on the Hash functions and signature schemes will not working on outsourced data.

Upon verifying different scenario and the available technique different short comes with the Existing algorithm AES-SHA2 with file key generation which is taken as base for our research work.

The following are the monitored points which identified as problem and further analyzed and performed further with enhancements.

1. Previous technique such as file based scheduling doesn't over count all its data parts , or internal division which can further be duplicate over the large amount of data . thus an efficient monitoring is required which can further be monitor file distribution with data division.

2. AES algorithm [6] takes an advantage of asymmetric encryption technique which is used by base paper, but still when we talk about the multiple tenant, multiple ownership and multiple user over the data. Thus a security of key sharing is still a challenging issue which is faced by authors.

3. The Key length taken for the purpose of security in previous research is not considerable today . Today's scenario required an efficient and long length key for security purpose. Matrix based approach is also need more computation[7,11].

4. PROPOSED METHODOLOGY

As per our observation about the previous technique and their disadvantage in different terms and scenario's. Our work present a new approach which is highly secure and consumes low computational time and thus computational cost over the large number of structured available dataset.

Our work propose a new algorithm[8] , Enhanced lockbox algorithm with more secure algorithm AES is performed .

Our algorithm also checks for proper access control using more secure and reliable parameters.

The proposed algorithm is described below :

1. Listing and loading of all the parameter , component for the simulation purpose and configuration of all the required scenario framework.

2. Creating an object of all required component.

4.1 Cloud object creation:

VM – virtual machine creation requirement
DC- local Data server is configured with WAMP 2.35.

3. Perform communication in between UB-user base and data store using a secure algorithm.
4. Perform session key generation.
5. Perform encrypted data transmission over the DC and storage in the scenario.
6. Monitoring de-duplication redundancy verification over the data store and producing the output value of matching.
7. Finding the execution time as per formulae-

Execution time = final completion time- initial time;

8. Observing the execution time and thus it effect computational cost for the complete transmission.
9. Exit .

4.2 Algorithm Pseudo Code

Enhance Lockbox approach:
Input : File f, Datastore DS.
Output : Communication process, data security matching result MS, Computation time.
Steps :

```
While(true) do{
Datastore file listing{f1,f2….fN};
DataUploadRequest();
LoginLockbox();
Performing LockboxIDGen();
session Verificatoin :
If(session()==true)
{
Data creation();
Send Encrypted data to data store;
Set status=Active; generate datastats();
}else
{
Status=exit;
generating data for request;
}
Return Computation time;
}
End.
```

5. EXPERIMENTAL SETUP

In this section detail about the implementation and results is presented. Java language over NETBEANS IDE simulator is used to implement the proposed methods and a comparison of result with the existing technique is presented[10].

5.1 Performance Measures

Computation Time[9]

A training time of a dataset in Java is computed with the help of start and end time class variables defined in the tool.

6. RESULT ANALYSIS

In result analysis here is the system tolerance detail I have applied some file uploads and observed my best analysis result.

Thus a fast algorithm is again modified to make it more efficient with no security compromise.

The proposed and existing technique is performed with the above different data size file, where the data is processed and following output results were monitored:

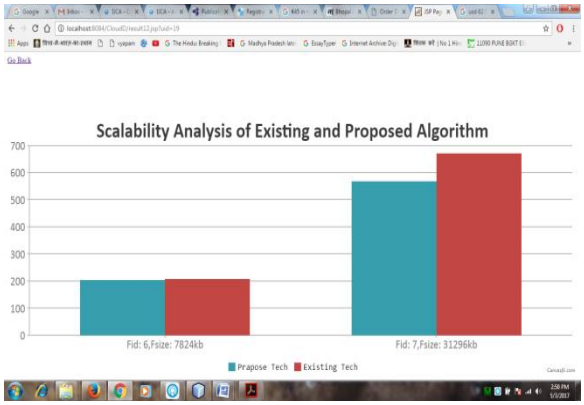

Fig 1: Statically analysis of obtained result

Table 1: Statically analysis of obtained result

Technique Approach File size / Computation time in ms	Existing technique (Computation time in msec)	Proposed Technique (Computation time in msec)
30 KB	328 ms	324 ms
80 KB	141 ms	136 ms

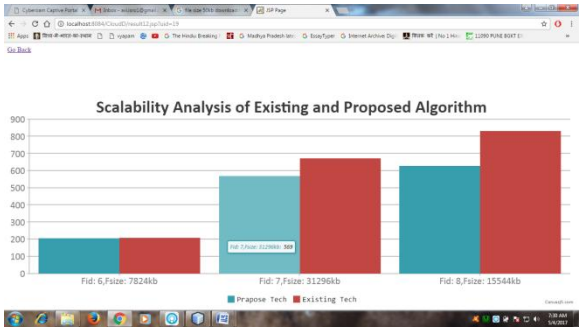

Fig 2: More File Comparison Line graph for technique analysis

Table 2: Statically analysis of more files obtained result

Technique Approach File size / Computation time in ms	Existing technique (Computation time in msec)	Proposed Technique (Computation time in msec)
30 KB	328 ms	324 ms
80 KB	141 ms	136 ms
300 KB	207 ms	191 ms
400 KB	240 ms	221 ms
1000 KB	386 ms	320 ms

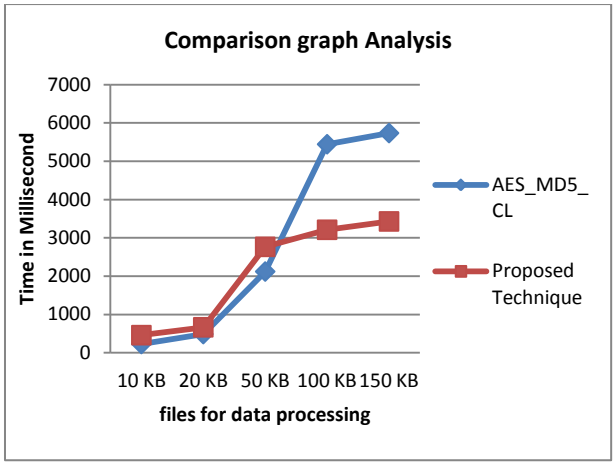

Fig 3: Comparison Line graph for Technique analysis

Working on text based graphical algorithm such as our proposed technique authentication will be efficient and easy to visualize and in order to make it easier for user to use, such outlier technique will be efficient to use.

7. CONCLUSION

Cloud computing is an emerging area of research, where most of the IT infrastructure is moving to make their service and delivery more efficient. Cloud computing make it more scalable, more reliable, secure and accessible with plenty of option to perform its best. In this paper our work approach leads behind the data ownership and security providing over the user session. The existing technique based on key generation for the user session and further the extension is performed on Enhanced lockbox session concept for file sharing and management. The concept behind the research is taken a secure and reliable algorithm, approach which can find the solution for security as well as de-duplication redundancy optimization over the data store.

The existing base paper discussed about the file level distribution where as to transmit and store the data AES (Asymmetric encryption system) algorithm is used to provide data security.

Thus to overcome these issues associated with traditional paper approach. Our optimization algorithm with more secure algorithm which is session based enhanced lockbox approach. Our algorithm also checks for proper access control using more secure and reliable parameters. As the work represent the cloud security , it is more intended to work towards the fully privacy preserving with mobile environment.

8. FUTURE WORK

A consistent proposed Enhance Lockbox algorithm provides an high level security alongside data distribution approach with data store. There are still further work can be done to prove our work in knowledge and for industry use. The following work is left for future work.

1. The real time implementation can be done, which can apply over the industry level cloud infrastructure and to find it more secure, reliable than the other alternate available over the web.
2. More study over the Hashing can be done, thus that an removal of that part can be done, which can make it more fast accessible.

9. REFERENCES

[1] Tiantian LIU, Tongkai JI, Qiang YUE, Zhenchu TANG "G-Cloud: A Highly Reliable and Secure IaaS Platform" IEEE, 2015.

[2] Kadam Prasad,Jadhav Poonam,Khupase Gauri, N. C. Thoutam "Data Sharing Security and Privacy Preservation in Cloud Computing" IEEE, 2015.

[3] N. Shanmugakani, R. Chinna "An Explicit Integrity Verification Scheme for cloud Distributed systems" ICSO, IEEE, 2015.

[4] Mehmet Sabir Kiraz, Isa Sertkaya, Osmanbey Uzunkol "an Efficient Id based Message Recoverable Privacy Preserving Auditing schme" PST, IEEE 2015.

[5] Nivedita Simbre, Priya Deshpandey "Enhancing Distributed Data Storage security for cloud computing using TPA and AES algorithm" IEEE, 2015.

[6] Naithik Shah, NisargDesai,ViralVashi," Efficient Cryptography for Data Security",2014 International Conference on Computing for Sustainable Global Development (INDIACom).

[7] M. Yamuna, S. Ravi Rohith, Pramodh Mazumdar, Avani Gupta "Text Encryption Using Matrices ", International Journal of Application or Innovation in Engineering & Management (IJAIEM)Volume 2, Issue 3, March 2013.

[8] Devendra Prasad,Govind Prasad Arya, Chirag Chaudhary, Vipin Kumar, "A Text Encryption and Decryption Technique Using Substitution-Transposition and Basic Arithmetic and Logic Operation ",International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014.

[9] Udepal Singh, UpasnaGarg," An ASCII value based text data encryption System", International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013 1 ISSN 2250-3153.

[10] Charru, Paramjeet Singh, Shaveta Rani "Efficient Text Data Encryption System to Optimize Execution Time and Data Security"International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume4,Issue7,July2014.

[11] J. Gitanjali, Dr. N. Jeyanthi, C. Ranichandra, M. Pounambal, "ASCII Based Cryptography Using Unique ID, Matrix Multiplication and Palindrome Number", The International symposium on Networks, Computers and Communications, IEEE, 2014.

[12] Cloud Security Alliance. (2009) Security guidance for critical areas of focus in cloud computing V2.1. http://www.cloudsecurityalliance.org/guidance/csaguide. v2.1.pdf

[13] M. Jensen. et. al. (2009) "On Technical Security Issues in Cloud Computing" IEEE International Conference in Cloud Conouting, pp.109-116, Sep 2009.

[14] M. McIntosh and P. Austel. "XML Signature Element Wrapping Attack and CounterMeasures" Workshop on Secure Web Service, pp.20-27, 2005.

[15] S. Subashini, ,Kavitha,V."A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. In Press, Corrected Proof.