INTERNATIONAL JOURNAL OF SCIENCE

ISSN: 2455-0108 | WWW.IJOSCIENCE.COM

VOLUME II ISSUE III JUNE 2016

A Hybrid Algorithm for Cloud Data Security Using MD5 and ABE

Umesh Joshi
M. Tech CSE Scholar RITS, Bhopal
&
Prof. Anurag Jain
Professor Dept. of CSE RITS, Bhopal

Abstract

The evolution of IT technology Cloud computing shows the strength in past year. It takes controls in all three services Saas, Paas and Iaas. But with gradual increment of technology the quality of services also main issues. Services should be accurate up to date and secure. The level of approval for any computing model is calculated by its strength quality and weakness. The current note is focusing on the security of data in Cloud network, it calculate the current scenario and proposed the Hybrid Secure solution. The paper provides the idea implementation to secure the data in cloud. It provides the hybrid secure solution which combine attribute based cryptography with hashing function MD5. It implements the idea on Cloudsim and provides the improved result in tested environment.

Keywords: *Cloudsim, Encryption of cloud data, ABE, MD5, AES.*

I. INTRODUCTION

In the IT jargon, the cloud computing was recently introduced. With the consumer oriented services, the cloud give best example. It gives all control to the end user of services. It allows the IT companies to leasing their services whether they are infrastructural, platform dependent or software oriented [1].

Due to the effective on demand services the cloud computing emerged rapidly over the IT infrastructure. The massive use of resources in cloud network, it is quite complicated in security.

II. SECURITY ISSUES

The confidentiality, integrity and availability of resources are three major issues in this cloud computing security [2,7]. IT infrastructure developers are eager to deal with gradually increasing secure algorithms in cloud networks. Still the area of cloud is open for data security in cloud network and seeking for more reliable, secure and less complex model.

The security in the field of cloud being more improved when the attribute based encryption [3]implemented in cloud data. Where the encryption of data with the key and that key is encrypted with adopted attribute, the whole combination of cipher text, key and attribute combine to become master key.

The cloud maintains the flexible data storage thus the correctness and on demand data availability required in distributed cloud environment. In 2012 the AME (AES Modern Encryption) technique comes in light where it is better in security provision in encryption while deal with Amazon EC2, and DES is suitable for time complexity (2). The Triple Encryption scheme was popular for the purpose for the security in Hadoop supported Cloud data storage; they combine the HDFS file encryption with RSA and DEA technique (4).

III. PROPOSED WORK

A. *Idea Algorithm*

The idea for the algorithm comes with the basis on the novel approach [4,6] where the encryption and decryption strategy is based on the three steps, 1. Encrypt the private key, 2. Encrypted key transmitted to cloud server, 3. Cloud server receives the data and stores it in date center. The based algorithm is quit efficient to work with cloud with little time complex. Here we deal with the encryption technique where the client generate the hash value of its private key and send it to cloud, on the other end cloud generate the hash value and match it, cloud compute the hash value and generate the secrete key. The XOR combination of these two key is use as an encryption key in encryption zone.

Hash function. In the field of cryptography, the importance of hash function is very much since few decades. The function takes the arbitrary length of inputs called message and generates the short fixed size of output called as message digest. This hash message is the fingerprint of that message and is unique for every message. We follow the Message Digest 5 hash algorithm for achieving the data integrity.

AES Algorithm. The Advanced Encryption Standard is symmetric key block cipher technique, which takes 128 bit block length message and key of 128, 192 and 256 bits length. It contains the rounds of substitution, row wise permutation and column wise mixing round. It takes 128 bit block of plaintext and converts it into cipher text. Here we include the AES algorithm in our proposed method which takes 128 bits key length.

Attribute Based Encryption. The encryption is based on the properties of file or message [3]. The attribute may be file size, file type etc. in the proposed work we are using the file size which combine with the hash value and make 128 bit key.

B. *Proposed Method*

Section presents proposed security scheme which provides a complete outsourcing solution of data– not only the data confidentiality but also its authentication. Proposed security scheme consists of four stages (AuthUser, KeyGen, EncryData, and DecryData). AuthUser is a stage to authenticate the user for secure outsourcing of data at the cloud end. KeyGen is a module that is run by cloud server to generate a secure key that is to be used in next stage of this scheme. EncryData is a stage where data is encrypted using proposed algorithm and store it at cloud database. DecryData is stage that is used at retrieval time of data; this module decrypts the data using proposed algorithm.

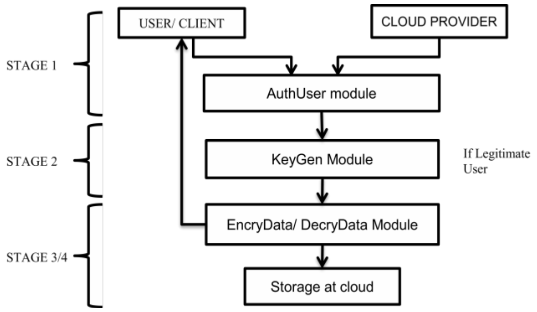

Figure 1 Stages of Encryption

C. *Notations and Preliminaries*

The following are the notation which is used for describing the proposed method.

- F- Data file that is to be outsourced. 'Len' determines the length of data file i.e. Len=Length(F).
- U_N- User name set by the client that is used as an attribute.
- H, h- cryptographic hash function.
- G- Key Generator which generates a key value using random set of variables, V. V is a set of variables i.e. Vi∈ V, {i=1,2,3,….n,}.
- S_K –Secret key generated by cloud server for each user. S_K= GenerateKey(G, V).
- M_K- Master key is generated in KeyGen stage of proposed scheme and termed as M_K,
- i.e.M_K= KeyGen(S_K, H).This key is used in EncryData & DecryData stage for respective encryption and decryption of data files.
- CE_F- Encrypt(F, Len)
- E_F- Output generated after EncryData stage,
  i.e. Encrypt($CE_{F,}$$M_K$)
  D_F- Output generated after DecryData stage,
  i.e. Decrypt(M_K,E_F)
- CD_F- Decrypt($D_{F,}$Len), such that CD_F==F.

D. *Module description*

Stage 1: AuthUser Module. Authentication of user, who wants to access services of cloud, is checked. Password, P, is shared between end user and the cloud server. The hash value of password is generated using MD5 at both end (user end and cloud end) and matched at cloud end. If hash value generated at both end is matched then user is legitimate. Later after authentication secure key generation process is performed in second stage i.e. KeyGen module.

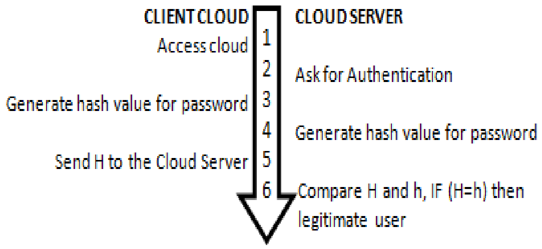
CLIENT CLOUD
CLOUD SERVER
Access cloud
1
2
Ask for Authentication
Generate hash value for password
3
4
Generate hash value for password
Send H to the Cloud Server
5
6
Compare H and h, IF (H=h) then legitimate user

Figure 2 Auth User

Module Stage 2: KeyGen Module

In KeyGen module a Master Key, M, is generated. Master Key is generated by performing XOR operation between cryptographic hash values generated, i.e. H and secret key, SK. As a result of this key generation technique, an encrypted key of size 256-bit (MK= KeyGen(SK, H)) is generated which reduces the threat of key exposure to intruders, undoubtedly.

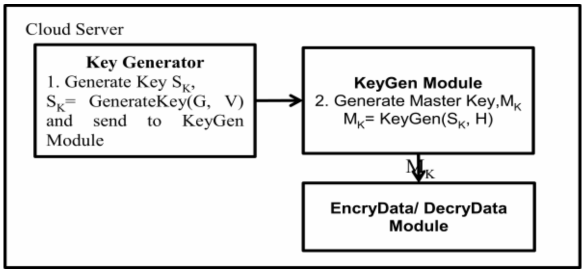
Cloud Server
Key Generator
1. Generate Key S_K,
S_K= GenerateKey(G, V) and send to KeyGen Module
KeyGen Module
2. Generate Master Key,M_K
M_K= KeyGen(S_K, H)
M_K
EncryData/ DecryData Module

Figure 3 KeyGen

Module Stage 3: EncryData Module

In the third stage, proposed work deals with new designed encryption algorithm which is based on the concept of Ceaser cipher and AES cryptographic algorithm (stream based and block based respectively). In this stage the Ceaser cipher performs variable shift on the plaintext. The shift that is performed is equal to the size of plaintext. After ceasered text is generated then it is encrypted using AES algorithm which uses 256-bit block size for the encryption purpose and this 256-bits block size is encrypted with the help of the encrypted key which size is also 256-bits. Lastly, user has to set user name which is used for authentication purpose at retrieval time. So in this way through the new designed encryption algorithm provides the double level of data security.

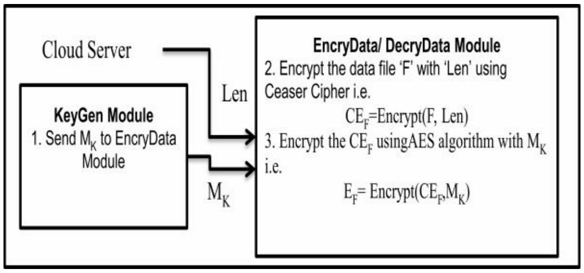
Cloud Server
Len
KeyGen Module
1. Send M_K to EncryData Module
M_K
EncryData/ DecryData Module
2. Encrypt the data file 'F' with 'Len' using Ceaser Cipher i.e.
CE_F=Encrypt(F, Len)
3. Encrypt the CE_F usingAES algorithm with M_K i.e.
E_F= Encrypt(CE_F,M_K)

Figure 4 EncryData

module Stage 4: DecryData Module

At the time of retrieval, DecryData module is used. For authentication purpose at data retrieval time, user has to give Len, UNand password P. If all the three values match then only user has authority to access the data that is stored at the cloud end. After matching the attributes, DecryData module retrieve the original data file using AES algorithm and Ceaser Cipher and send it to the user.

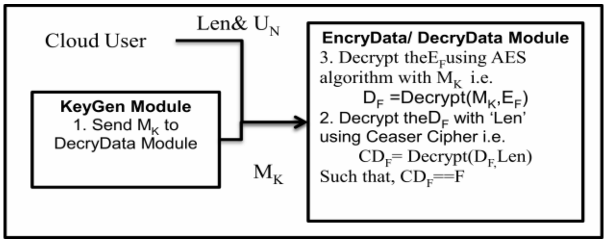
Cloud User
Len& U_N
KeyGen Module
1. Send M_K to DecryData Module
M_K
EncryData/ DecryData Module
3. Decrypt the$E_F$using AES algorithm with M_K i.e.
D_F =Decrypt(M_K,E_F)
2. Decrypt theD_F with 'Len' using Ceaser Cipher i.e.
CD_F= Decrypt(D_F,Len)
Such that, CD_F==F

Figure 3 DecryData Madule

E. Storing Process

Authentication of cloud user is verified using password or secret key. If the user is authentic then only cloud provider give the authority to access the cloud database. To check authentication of the user, hash value of the password is generated by the user and cloud provider, the hash values is compared. If match is found then the user is authentic. After that, user sends the data and set a user name. Then, cloud provider generates a secret key of 256-bit, which generates a master key. Master key and file size thus generated are used by encryption/decryption module. After encryption process, encrypted data is saved at cloud data center. With encrypted data, user name and file size is also saved at cloud data center.

F. *Retrieving Process*

At the time of data retrieval time, authentication of cloud user is again verified using password or secret key. If the user is authentic then only cloud provider give the authority to access the cloud database. User is asked for password, user name and file size. If and only if, all the three values are matched then only user is given authority to retrieve data. Master key and file size are used by encryption/decryption module. After decryption process, decrypted data is send to the user.

IV. PERFORMANCE EVOLUTION AND SECURITY ANALYSIS

A. *Experimental Scenario*

To perceive the experiment we have worked on the program that implement in the region of java programming. The tentative idea performed on the conventional computing devices.

B. *Analysis Parameter*

The performance of the proposed algorithm is analyzed on the *Avalanche, Key Size, Authentication Scenario, confidentiality, time complexity.*

C. *Result Analysis*

The methode output result is based on the time of encryption and decription. The algorithm [4] is impleneted on Handoop thus we also implemeted it in cloud simulation environment and retrieve the result. We try the different input stream with different combination for the proposed algorithm and analys the output. Some of the input output analysis are given in the table 2.

D. *Security Analysis*

The security in a cloud is based ont the level of encryption. The size of keys and confidentialiyt. The general comparision of security is analysed in table 1.

Parameters	**Existing Work** (5)	**Proposed**
Key	64 bit key is used.	256 bit key is used.
Authentication	No	MD5 is used for authentication
Confidentiality	Data is encrypted by DES.	Data is encrypted by Hybrid Encryption based on Ceaser Cipher & AES.
Avalanche effect	Average	Good

As we know the avalanche is one of the key factor of security. In the avalanche change in plain text give significant change in cipher text. A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts. There for it improve the security level as well. We analys the avalanche in both the existing [4] and proposed algorithm in fig 7.

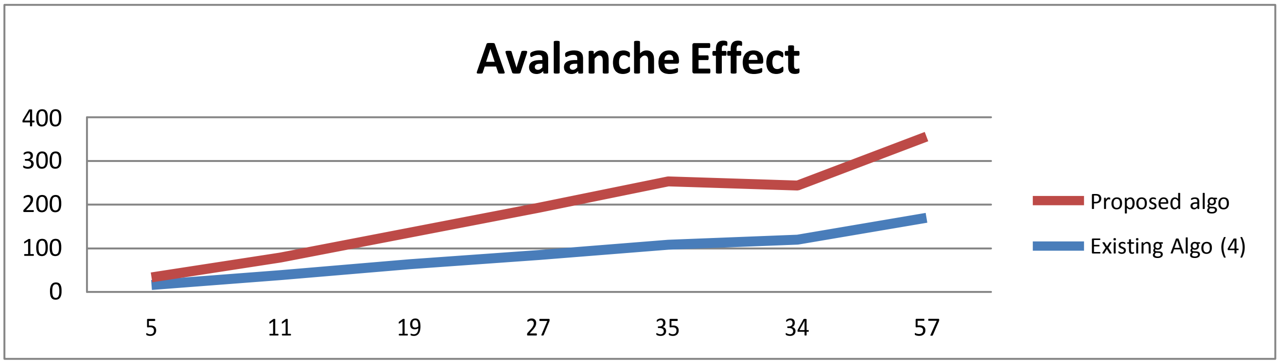

Figure 7. the Analysis of Avalanche

Input Data	Length of Input	Observation (Time Required for Encryption)		Observation (Time Required for Decryption)		Observation (Time Difference)	
		Base [4]	Proposed	Base [4]	Proposed	In Encryption	In Decryption
A	1	3824531380	211119449	5147792510	1010898	3613411931	5146781612
AA	2	2441770953	158789659	6357795866	1250366	2282981294	6356545500
AAA	3	968131058	167674785	6690175175	1215729	800456273	6688959446
AAAA	4	1737291401	167992508	5971075661	2117155	1569298893	5968958506
AAAAA	5	626231177	148491671	7851119194	1257208	477739506	7849861986
AAAAAA	6	810808996	165884333	6678380083	2003409	644924663	6676376674
AB	2	2955392204	148267170	7664662831	1268753	2807125034	7663394078
ABC	3	1401183657	179208173	6421345170	1252932	1221975484	6420092238
ABCD	4	1054190801	173305281	8926828350	1263623	880885520	8925564727
ABCDE	5	1332336975	181407004	7782066397	1254215	1150929971	7780812182
ABCDEF	6	2082445911	166157156	14553873719	1480854	1916288755	14552392865
1	1	3549338789	259615610	7325005399	1010470	3289723179	7323994929
11	2	2313093138	161031253	6673953769	1273030	2152061885	6672680739
111	3	1529903236	158958143	9335251249	1491973	1370945093	9333759276
1111	4	3768797712	146120081	29481172781	1310661	3622677631	29479862120
11111	5	2759562210	163533268	19381209814	1419276	2596028942	19379790538
111111	6	1263370247	162191390	6144107530	1299971	1101178857	6142807559
1A	2	1446446745	180615476	59179696520	1271748	1265831269	59178424772
1AB	3	2366968487	171561867	9529619291	1258064	2195406620	9528361227
1AB#	4	1113489726	183555376	2112535119	1255070	929934350	2111280049
#	1	1113489726	158029348	24530611818	1239676	955460378	24529372142
@@	2	1643129971	171813309	6874947188	1404310	1471316662	6873542878
$$	2	1786508820	163099231	6281069807	1268326	1623409589	6279801481
#$	2	820024666	163722704	19320007988	2132122	656301962	19317875866
#$%^	4	2161049333	173154331	12891552875	1268754	1987895002	12890284121
XYZ	3	1191777466	169453264	9231815080	1519340	1022324202	9230295740
XYZ ABC	7	1933442550	170408999	43524925208	1362830	1763033551	43523562378

X1Z 2B3	7	3614613107	169818880	29438278178	1333325	3444794227	29436944853
1AB# 1AB#	9	4312540304	169002978	6869356367	1277734	4143537326	6868078633

Table 2. the time analysis of proposed Algorithm.

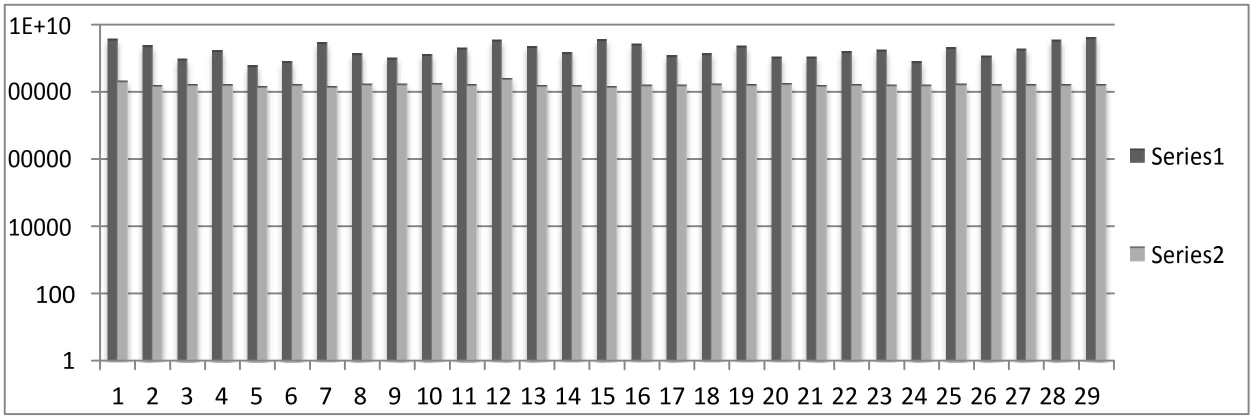

Figure 8 Encryption time Analysis

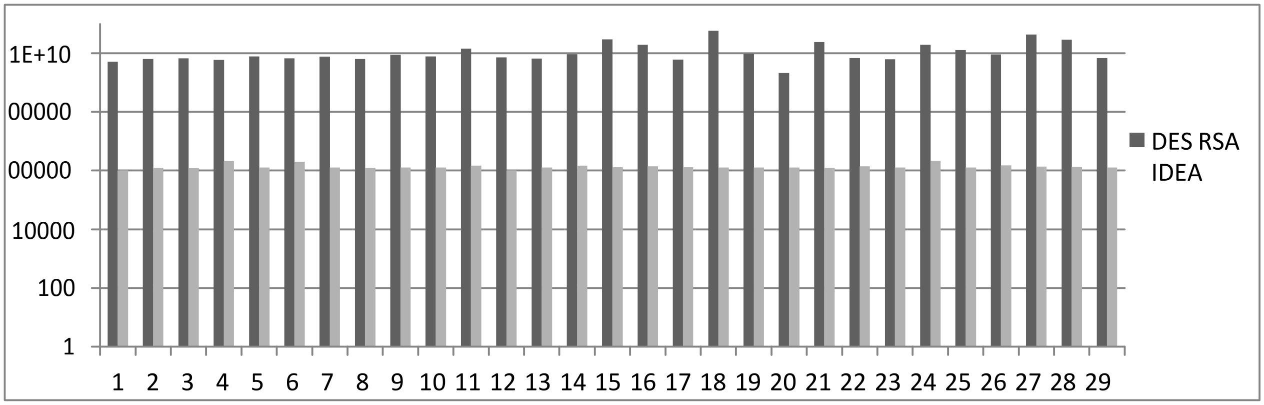

Figure 8 Decryption time Analysis

V. CONCLUSION

Though Cloud computing can be seen as new evolving phenomenon, there are yet numerous practical difficulties which have to be answered. Among such problems, one of the most concern areas is of storage security. Cloud computing is very essential to have highly secured cloud, if the cloud has a common security methodology then, it will be a high value asset target for hackers because of the fact that hacking the security system will make the entire cloud vulnerable to attack. The datacenters also have to maintain the security of processing of data, which can be achieved by integrity and preventing the loss of data in the cloud. As per above discussions it is concluded that, data protection, [6] integrity check and authentication are major security parameters that are preserved by applying cryptographic algorithms and such security algorithms are currently used in a cloud computing environment. The work contains one of the secure hybrid algorithms to overcome the turmoil condition of cloud data security. In future there may be more combination which finds the optimal way for the same problems.

REFERENCES

[1] *Cloud Computing*. **Buyya, Rajkumar and Sukumar, Karthik.** 1, s.l. : CSI Communication, 2011, Vol. 35. 0970647X.

[2] *Modern Encryption Techniques for Cloud Computing*. **El-etriby, Sherif, Eman M., Mohamed and Abdul-kader, Hatem S.** s.l. : ICCIT, 2012.

[3] *Based on the attribute encrypted cloud storage*. **ZHU, LI-YE.** s.l. : IEEE, 2003. CPS (Conferencing Publishing Services).

[5] *A Novel Triple Encryption Scheme for Hadoop- based Cloud Data Security*. **YANG, Chao, LIN, Weiwei and LIU, Mingqi.** s.l. : CPS, 2013. Fourth International Conference on Emerging Intelligent Data and Web Technologies. pp. 437-442.

[5] *Survey On Security Of Information At Cloud Storage In Cloud Environment*. **Priya, Aayushi and Rana, Y. K.** 10, Bhopal : IJARCSSE, 2014, Vol. 4.

[6] *Security Design for Instant Messaging System Based*. **Guo, Wenping, et al.** 2009, IEEE.

[7] *An analysis of security issues for cloud computing.* **Hashizume, Keiko, et al.** s.l. : Springer, 2013.