A technique to MAGCIPHER for applying a data protection strategy in hybrid cloud

D. I. George Amalarethinam¹ and J. Madhu Priya²*

Abstract
Cloud computing is sweeping the globe, and because of its many benefits, the need to secure data stored in the cloud is unavoidable. To hold the data, are using cloud deployment models such as public cloud, private cloud, hybrid cloud, and community cloud. To protect user data from ever being compromised in a cloud environment, data protection must be fully enforced. There are many techniques for preserving a customer’s information. Encryption and digital water marking methods are among them. Cryptographic policies often include the task of encrypting the data in order to convert into unintelligible form. The original data will be retrieved once the decryption process is finished. Before the data is shared to the public cloud, it runs through an encryption process. - specifically, data at rest encryption is done.

Keywords
Cloud Computing, Data Security, Cryptography, water marking, Encryption, Hybrid Cloud.

1. Introduction
According to NIST “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. The key characteristics that make up the cloud are lower computing costs, improved performance, instant software updates, unlimited storage capacity, device independence, Increased data reliability.

There are three Service models and four Deployment models in cloud computing. Service models are SaaS -Software As a service, PaaS - Platform As a service and IaaS - Infrastructure As a service. Saas provides end user applications rendered as a service rather than on-premises software. PaaS- gives application platform or middleware as a service on which developers can build and deploy personalized applications. IaaS yields compute, storage or other IT framework as a service instead of a dedicated capability. The deployment models of cloud computing are Public cloud where cloud infrastructure is given for open use by the general public. The Public cloud exists on the premise of the cloud provider. The second deployment model is the private cloud where cloud infrastructure is given for dedicated use by a single organization consisting of multiple business units.

It can exist on or off premise. The Hybrid cloud offers distinct advantages over the public and private clouds reason being that data and applications can be distributed between public and private clouds and provides business with enhanced flexibility. The community cloud provides cloud infrastructure for exclusive access for a specific group of consumers from organizations that have common concerns. [2]

The MAG Cipher paper is already published with its algorithm. This paper discusses the implementation of MAG
A technique to MAGCIPHER for applying a data protection strategy in hybrid cloud — 671/674

Cipher to enhance the data protection of Public cloud part of a hybrid cloud.

1.1 Cloud Security
Data security, privacy and trust become crucial issues that affect the success of cloud computing. Storing data at cloud increases the risk of unauthorized access. Cloud data centers are becoming the targets of attacks. Data management operations, such as data storage, backup, migration, deletion, query and access in the cloud may not be fully trusted by its owners. Data process and computation in the cloud could be compromised. [3]

Data protection in the cloud storage is the core security problem. Data protection is primarily concerned with data confidentiality. Other parameters include integrity, authentication and availability. Data confidentiality means the data stored in the cloud is safe. Proper mechanisms must be built to prevent data misuse. The privacy and secrecy of the data can be checked either by the client directly or through a third party auditor (TPA). The TPA manages data according to service level agreements (SLA) saved onto the cloud by the owner. [4]

Data integrity refers to information that has not been modified or remains untouched. Authentication verifies whether the user is an authorized person or not. Data availability means the ability to guarantee to use data in time when needed and also ensures the availability of cloud service provider on-demand [5]. Considering all concerns of users for security of their data, it is highly essential to enforce robust security measures to protect user’s data from unauthorized accesses and data disclosures. Cryptography is accepted method of ensuring data security. It is a process of converting data into a non-readable form.

There are two cryptographic algorithms namely symmetric encryption and Asymmetric encryption. The symmetric encryption uses only one key for encryption and decryption. The asymmetric encryption uses two keys, one for encryption called the public key and other key for decryption called the private key [6].

Jinan Shen et al present a scheme for a multi-security-level cloud storage system that uses AES symmetric encryption and an improved identity-based proxy re-encryption (PRE) algorithm. [9]

Fenghua Zhanget et al presented a hybrid encryption algorithm based on AES and RSA. This algorithm combines the characteristics of AES encryption algorithm and RSA algorithm to ensure the security of medical data in cloud database. [10]

Shafi’i Muhammad Abdulhamid et al proposed a Symmetric Block Cipher called blowfish encryption scheme for secure data storage in public and commercial cloud computing environments. This paper developed an application for protection of third party data using infrastructure as a service cloud [11].

Dr. R. Sugumar et al proposed technique to improve the classical encryption techniques by integrating substitution cipher and transposition cipher. In the proposed algorithm, the plain text is converted into corresponding ASCII code (Hexa) value of each alphabet. The Key value ranges between 1 to 256. This algorithm is used in order to encrypt the data of the user in the cloud [12].

Manikandasaran S. S. et al proposed a hybrid security service algorithm, EOcipher to protect the data in the cloud storage. It uses encryption and obfuscation techniques to secure the data. Keys used for encryption and obfuscation are generated in the cloud. They are retained by the user for performing tasks like decryption and de-obfuscation [13].

S. Balamurugan et al discussed an Enhanced Security Service Algorithm, ESSAO using data obfuscation techniques. The proposed algorithm is provided as a service to user from the cloud. and it obfuscates only the numerical data in the original data. It uses different mathematical methods [14].

M Sulochana et al proposed multi cloud architecture, where the application logic layer and the data persistence layer are separated into two distinct public clouds. The admin resides in another private cloud. It allows only the authenticated users to access the data storage. To provide security to the user data, the administrator performs encryption using RSA of the uploaded data [15].

Dr. L. Arockiam et al proposed a technique where the converted ASCII values are stored in a square matrix and written in three different matrices namely upper, lower and diagonal matrices. Each matrix uses three different keys [16].

2. Related works
R. Manoj et al proposed the security and privacy of access to medical records using hybrid cloud in a Secure and Scalable Electronic Health Record Sharing (HSS-EHRS) system. For this, the system is divided into two security domains namely Public Domains (PUD) and Personal Domains (PSD) based on the data access requirements of recipients. In both domains, Attribute Based Encryption (ABE) scheme was used [7].

Prasanna Balaji et al discussed a DNA based key for user authentication to get entry or data access permission in the network/cloud applications. A new proposed encryption method is used based on random number generation for creating a DNA pattern. The entire algorithm comprises of three stages such as key generation, random key generation and encryption-decryption [8].

3. Problem definition
One of the top most strategies in today’s world is Cloud Computing. Many organizations use various Deployment models for their varied business needs. The choice of adapting Saas, PaaS, or IaaS yields further to the world of exploring cloud computing benefits. To enforce stronger security for data protection in cloud, data can be stored in a Hybrid Cloud. The hybrid cloud uses two different clouds one being the public cloud where data is accessible to the general public and other one is a private cloud where sensitive data’s are stored. It is responsible for cloud service providers to maintain the security
of the data in cloud. But in public cloud environment, there is a possibility that service provider can access the data without the knowledge of data owner. Hence proper security measures must be ensured to safe guard the data in public clouds which may be vulnerable.

4. MAG CIPHER Algorithm

The cryptographic algorithms are broadly classified into Symmetric or Asymmetric encryption techniques. The MAG CIPHER Algorithm uses symmetric key and it performs data-at-rest encryption.

4.1 Features of MAG CIPHER

The entire process of encryption involves series of operations which include key insertion, one’s complement computation, finding XOR, splitting, joining and merging. The necessity for these operations is relevant to the fact that the process of finding the key to decrypt the encrypted text becomes extremely difficult.

4.2 Pseudo code for MAG CIPHER algorithm

Algorithm:- magcipher(OT)

Inputs:- Users’ data 1. start
2. S ← sizeof (OT) // find the length of the plain text
3. for i ← 1 to S
   asc ← ascii(OT) // convert into ASCII
   bits - binary(asc) // convert into 8bits binary
   buffer ← append(bits) // Buffer variable for combine all the binaries next i
4. N ← sizeof(buffer) // count the number of 0’s and 1’s
5. NB = N/128 // calculate total no. of 128 bits blocks
6. pt = 0
7. While (pt<=NB)
   bk[pt] ← split(buffer, 128) // split the binaries into 128 bits block
   pt++
   loop 8. Generate a key K1 from cloud service
   // Alternative insert the key K1 into each blocks of binary using f() function
9. for i ← 0 to NB
   b1k[i] < f(bk[i], K1)
   // Find 1’s complements on each blocks using c() function
   oneblk[i] ← c(b1k[i])
   // Use the same key K1 to find XOR with each 128 bits blocks using x0 function
   xorblk[i] ← x(oneblk[i], K1)
10. next i
11. w = v = q = 0
12. for i ← 0 to NB
   1 ← m = 0
   //Split each 128 bits block into 64 bits block by using wave transformation
   for j ← 1 to sizeof(NB)
   oB[w] < xorblk[1]
   eB[v] ← x orblk[m]
   1 ← 1 + 1
   m ← m + 2
   next j
   //Find the 1’s complement on each 64 bits block using c() function
   ooB[w] ← c(oB[w])
   oeB[v] ← c(eB[v])
   //Join the two 64 bits block into one 128 bits block
   sblk[q] ← merge (ooB[w], oeB[v])
   //Find the reverse of each block using r() function
   revsblk[q] ← reverse(sblk[q])
   w++, v++, q++
13. next
14. for i← 1 to NB
   NeBits ← sizeof(revsblk[i])/8 // to find the no. of 8bits blocks
   1 ← 1
   m ← 1
   while (1 < NeBits)
   eBlks[i] ← split(revsblk[j], 8) //split the binaries into 8bits block
   1++
   i ← j + 8
   loop
   i. for k ← 1 to eBits
   dec[k] ← ascii(eBlks[k]) // convert the 8 bits into decimal
   ctbuff ← append (ascii (dec[k]))
   next k
   mbuff ← append(ctbuff)
15. next i
16. CT← mbuff
17. End

4.3 Sample experiment with MAG CIPHER algorithm

User data are considered as the original text

OT- > The Hybrid Cloud
The key chosen is, K1 = ABCD458461,$ + q@5

CT :

```
1 | 4 | A | EOT | ; | v | µ | X | ? | / | # | EM | Ă | CA | N | É | + | q
C | É | U | ? | D | STX | ‘ | − | i | 1 | 4 | SP | # | ó | $
```

Decryption is the reverse process of encryption. The cipher text is considered as the input. It is converted into original text. The decryption process uses the same key. After the decryption process is complete, the original text is produced.
A technique to MAGCIPHER for applying a data protection strategy in hybrid cloud — 673/674

CT:

\[
\begin{align*}
1 / 4 & \quad \Delta \quad \text{EOT} ; \quad \nu \quad \mu \quad \chi \quad ? / \quad \# \quad \text{EM} \quad \hat{A} \quad \text{CA} \quad \hat{N} \quad \hat{E} \quad + \quad \nu \\
C \quad \hat{E} \quad U \quad ?' \quad D \quad \text{STX} \quad \_ \quad \_ \quad 1 / 4 \quad \text{SP} \quad \# \quad \delta \quad \$ \\
\end{align*}
\]

OT ← The Hybrid Cloud

5. Comparison of Encryption and Decryption Time

The proposed encryption techniques is tested with different size of data and compared with existing algorithms like IDEA, Blow fish. Table below shows the time taken for encryption by the proposed and existing techniques.

Table 1. Comparison of Proposed and Existing Techniques with respect to Encryption Time

| Size     | Encryption Techniques | IDEA | Blowfish | MAG cipher |
|----------|-----------------------|------|----------|------------|
|          |                       | Milliseconds |          |            |
| 5 MB     | 2012                  | 1540 | 1003     |
| 10 MB    | 4987                  | 2890 | 2110     |
| 15 MB    | 6002                  | 4454 | 3089     |
| 20 MB    | 8104                  | 5789 | 4289     |
| 25 MB    | 10028                 | 6032 | 5438     |

Figure 1 given below represents the encryption time comparison of proposed and existing encryption techniques. Figure 1 shows that, the proposed MAGcipher takes minimum time duration for encrypting the data than existing techniques.

6. Analysis of MAGCIPHER

The Hack man tool measures the security level of each existing and proposed algorithms by hacking the data generated by the corresponding algorithms. Table 3 and Figure 3 describe the assessment of security levels for the encryption algorithm. The outcome demonstrates that proposed MAG cipher produces the highest security level. Based on calculation described above percentage of security is calculated and compared as shown below in table and graph.

7. Conclusion

Using MAG CIPHER, it is shown that security is enhanced greatly in public cloud. The MAG CIPHER algorithm uses randomly generated keys from the cloud. It applies operations such as XOR, complement, to make the relationship between

Table 2. Comparison of Proposed and Existing Techniques with respect to Decryption Time

| Size     | Decryption Techniques |
|----------|-----------------------|
|          | IDEA | Blowfish | MAG cipher |
|          | Milliseconds |          |
| 5 MB     | 1998 | 1498     | 943        |
| 10 MB    | 4901 | 2787     | 2001       |
| 15 MB    | 5989 | 4399     | 2991       |
| 20 MB    | 8006 | 5688     | 4178       |
| 25 MB    | 9993 | 5978     | 5339       |

Figure 2

Table 3. Security Level of Proposed and Existing Encryption Techniques

| Security Algorithms | Security Level (%) |
|---------------------|--------------------|
| Blowfish            | 83                  |
| IDEA                | 74                  |
| MAGcipher           | 92                  |
A technique to MAGCIPHER for applying a data protection strategy in hybrid cloud — 674/674

Figure 3. Security Levels of Proposed and Existing Encryption Techniques

the plain text and the key complex, so that output is getting changed even for a small input change. As the key is chosen from cloud key management as a service, it is not possible for the attacker to predict the keys and attack the data.

References

[1] Khalid et al makkaoui, abdellah ezzati,” Data Confidentiality In The World Of Cloud”. Journal of Theoretical and Applied Information Technology. 84(3)(2016). ISSN: 1992-8645, E-ISSN: 1817-3195
[2] Sankar Somepalle article on “3 Service and 4 Deployment Models of Cloud Computing” in Linked in.
[3] Zheng Yan et al”Cryptography and Data Security in Cloud Computing” Elsevier Information Sciences, 387(2017), 53-55.
[4] Ashalatha R et al “Data StorageSecurity Algorithms for Multi Cloud Environment”, International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB 16) 978-1-4673-9745-2 ©2016 IEEE 695
[5] Dr.L.Arockiam et al “Efficient Cloud Storage Confidentiality to EnsureDataSecurity”, 2014 International Conference on Computer Communication and Informatics (ICCCI -2014).
[6] Manisha Malhotra et al “hybrid two-tier security framework for improved security in cloud Environment”, International Conference on Computing for Sustainable Global Development, (INDIACom) 978-9-3805-4421-2/16, 2016.
[7] R. Manoj et al “Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud” 978-1-5090-6325-3/17, IEEE, 2017.
[8] Prasanna Balaji et al “DNA Cryptography Based User Level Security for Cloud Computing and Applications”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, Blue Eyes Intelligence Engineering & Sciences Publication Retrieval Number: B2845078219 /2020©BEIESLPJanuary 2020
[9] Shen et al” Multi-security-level cloud storage system based on improved proxy re-encryption”, EUROSPI JOURNAL on wireless communication and Networking, Springer Open, 277(2019).

[10] Fenghua Zhang et al” Hybrid encryption algorithms for medical data storage security in cloud database”. International Journal of Database Management Systems, (IJDMS) 11(1)(2019).
[11] Shafi’i Muhammad Abdulhamid et al.,”Development of Blowfish Encryption Scheme for Secure Data Storage in Public and Commercial Cloud Computing Environment”, International Conference on Information and Communication Technology and its Applications, (ICTA 2018) Federal University of Technology, Minna, Nigeria, 2018.
[12] Dr. R. Sugumar et al “DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm”, International Journal of Engineering Research & Technology, (IJERT) ISSN: 2278-0181 6(10)(2017).
[13] Manikandasaran S. S. et al”EOCIPHER: A hybrid approach to enhance security Of outsourced data in public cloud storage”, 4th International Conference on Artificial Intelligence and Computer Science (AICS2016), MALAYSIA, e-ISBN 978-967-0792-11-8. 2016.
[14] S. Balamurugan et al” ESSAO: Enhanced Security Service Algorithm using Data ObfuscationTechnique to Protect Data in Public Cloud Storage”, Indian Journal of Science and Technology, 9(17), ISSN (Print) : 0974-6846 ISSN (Online) : 0974-5645, May 2016.
[15] M Sulochana et al” Preserving Data Confidentiality using Multi-Cloud Architecture”, 2nd International Symposium on Big Data and Cloud Computing, (IS-BCC’15)ELSEVIER, Science Direct, Procedia Computer Science 50 (2015) 357-362.
[16] Dr. L. Arockiam et al”Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering, 2(8)(2013), ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021.