Ant Colony Model (AnCoMoDaS) for Data Security in Cloud

B. Rex Cyril[1], DR.S. Britto Ramesh Kumar[2]

[1]Research Scholar and Assistant Professor, Department Of Computer Science, St.Joseph's College(Autonomous), Trichy, Tamilnadu, India.

[2]Asst.Professor, Department of Computer Science, St.joseph's College(Autonomous) Trichy, Tamilnadu, India.

---***---

Abstract:*After the invention of Cloud Model, awareness of using common storage in increased. Considering investment for hardware to store mass data as well as to keep secures them cloud provides ease solutions. For the reason data storage in cloud is increased. The previous algorithms for securing the cloud data designed to encrypt the content without any knowledge about the type of data. But the proposed algorithm Ant Colony Model for Data Security in Cloud (AnCoMoDaS) encrypts the content depends the type of content available in the document. So it's proved that the size and time is reduced than any other previous algorithms.*

Key Words: ***Ant Colony, Encryption, Cryptography***

1. INTRODUCTION

Cloud is nothing but the group of servers and datacenters that are placed at different places and these severs and datacenters are responsible for providing on demand service to its users with help of internet. The service provided by cloud is not present on user's computer. User has to access these services with help of internet connection through subscribing them. The main advantage of Cloud computing is that it eliminates the need for user to be in same location where hardware software and storage space is physically present. Cloud makes it possible to store and access your data from anywhere anytime without worrying about maintenance of hardware software and storage space. All these services are provided to user at low cost. User has to pay according to storage space he is using. Due to this flexibility everyone is transferring his data on cloud.

Security becomes big issue when any one stores its important information to a platform which is not directly controlled by the user and which is far away [1]. While sending of data and during storage data is under threat because any unauthorized user can access it, modify it, so there is need to secure data. A data is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorized disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorized user. Availability refers to assurance that user has access to information anytime and to any network. In the cloud confidentiality is obtained by cryptography.

Cryptography is a technique of converting data into unreadable form during storage and transmission that it appears waste to intruder. The unreadable form of data is known as cipher text. When data is received by receiver it, will appear in its original form which is known as plain text. Conversion of plain text to cipher text is known as encryption and reverse of this (cipher text to plain) is known as decryption. Encryption takes place at sender's end whereas decryption takes place at receiver's end.

The rest of the paper is organized as follows. In Section II and III, we have defined the related work and background for the proposed security system respectively. Our proposed system security algorithms and performance analysis are explained in Section IV and V respectively. Finally we conclude in Section VI.

2. RELATED WORK

To ensure the data integrity of a file consisting of a finite ordered set of data blocks in cloud server several solutions are defined by Qian Wang et al, in [2]. The first and straight forward solution to ensure the data integrity is, the data owner pre-compute the MACs for the entire file with a set of secrete keys, before our sourcing data to cloud server. During auditing process, for each time the data owner reveals the secret key to the cloud server and ask for new MAC for verification. In this method the number of verification is restricted to the number of secrete keys. Once the keys are exhausted, the data owner has to retrieve the entire file from the cloud server to compute the new MACs for the remaining blocks. This method takes the huge number of communication overhead for verification of entire file, which effect the system efficiency.

Qian Wang et al, in [4] designed an efficient solution to support the public audit-ability without retrieving the data blocks from server. The design of dynamic data operations is a challenging task for cloud storage system. They proposed a RSA signature authenticator for verification with data dynamic support. To support the efficient handling for multiple auditing task, they extended the technique of bilinear aggregate signature and then they introduced a third party auditor to perform the multiple auditing task simultaneously. In the recent resource sharing paradigm in distributed system such as cloud computing, the most challenging task.

In DES algorithms block cipher is of 64 bits [5] and key used is of 56 bits out of 64 bits of key is used rest of 8 bits are padded. In block cipher we encrypt block of data which consist of plain text by combination of confusion and diffusion to make cipher block then this cipher block has to pass 16 rounds, before passing through these 16 rounds the 64 bits of data is divided into 32 bits. After dividing the data into 32 bits, F-function (Feistel function) is applied. F-function consists of substitution, permutation, key mixing. The output of function is combined with other half of the data using XOR gate alternate crossing of data is done; then crossing of data is done.

To increase the revenue and degree of connectivity from cloud computing model while accessing and updating data from data center to the cloud user, Dubey et al. in [7] devel-oped a system using RSA and MD5 algorithms for avoiding unauthorized users to access data from cloud server. The main drawback of this method is that the cloud service provider has also an equal control of data as the data owner and the computation load for cloud service provider is proportional to the degree of connectivity so that the performance of the system can degrade.

3. PROPOSED ALGORITHM

Fig .1 Shows the complete architecture of proposed algorithm.

As in the architectural diagram the content of given document is read and the Ant initialized is traveled throw all the characters and increase the promone for each characters depend its type. At final the size of the promone declares the encryption type. As per the size of the promone either Character based encryption or Value base encryption has been done.

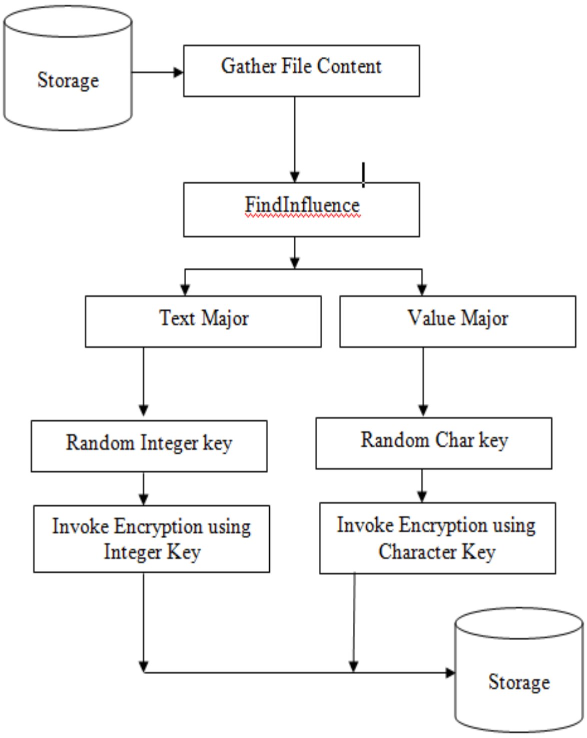
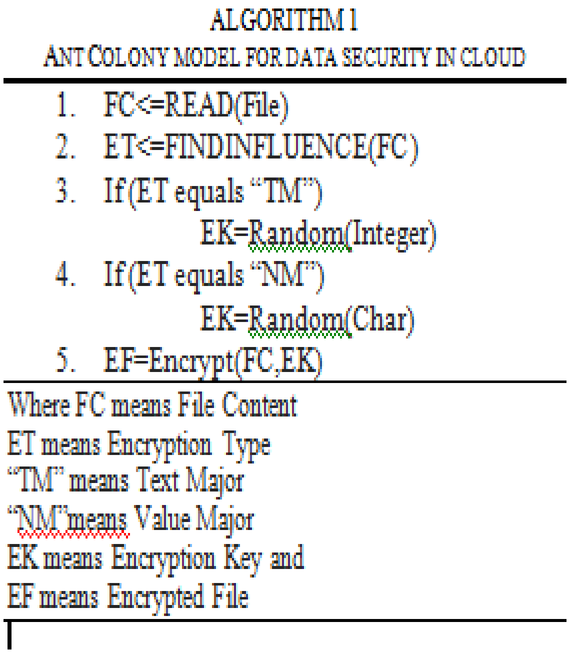


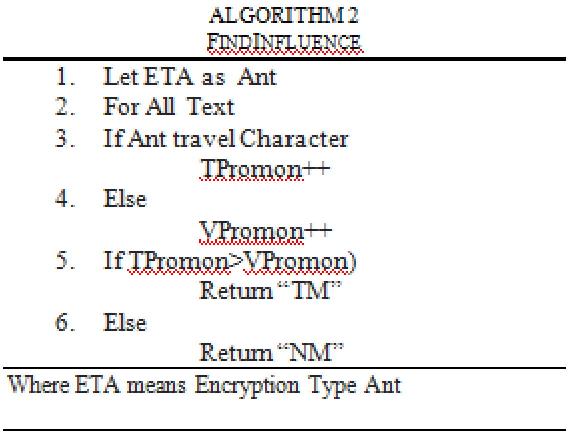
Fig -1: Architecture Diagram of proposed algorithm



ALGORITHM 1
ANT COLONY MODEL FOR DATA SECURITY IN CLOUD

```
1.  FC<=READ(File)
2.  ET<=FINDINFLUENCE(FC)
3.  If(ET equals "TM")
            EK=Random(Integer)
4.  If(ET equals "NM")
            EK=Random(Char)
5.  EF=Encrypt(FC,EK)
```

Where FC means File Content
ET means Encryption Type
"TM" means Text Major
"NM"means Value Major
EK means Encryption Key and
EF means Encrypted File



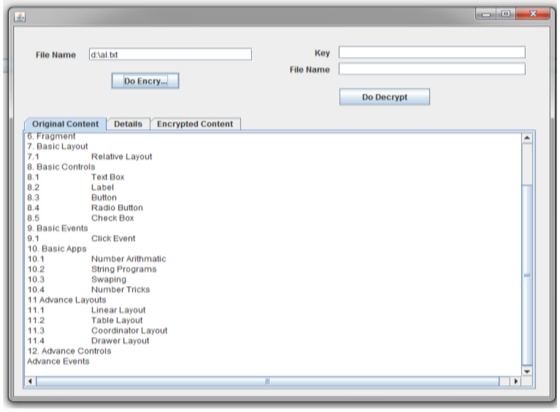
```
ALGORITHM 2
FINDINFLUENCE
1.  Let ETA as Ant
2.  For All Text
3.  If Ant travel Character
            TPromon++
4.  Else
            VPromon++
5.  If TPromon>VPromon)
            Return "TM"
6.  Else
            Return "NM"
Where ETA means Encryption Type Ant
```

The file line of the Algorithm 1 tells that the contents of the file will be buffered (FC) for further operations. After the contents were buffered the file is categorized whether it is TEXT Major File or Value Major File. To do so two ants are initialized and let them to travel through all the contents that are buffered. For every move any of the two ant will be increased depends the type of character. Finally the if Text majore file encrypted with text based encryption element and value majore file encrypted with Number based encryption. If both are equal in case there is both the encryption are invoked to give maximum security to the content.

The output earned using this algorithm shows that the size of the encrypted file is less compared to the traditional encrypted algorithms. A tool is developed to show the accuracy of the proposed algorithm.

4. EVALUATION AND RESULTS

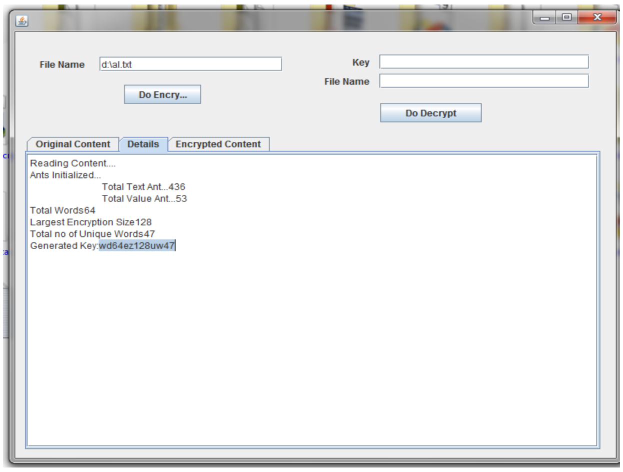
A file taken to check the functionality of proposed algorithm



File Name d:\al.txt
Key
File Name

```
6. Fragment
7. Basic Layout
7.1              Relative Layout
8. Basic Controls
8.1              Text Box
8.2              Label
8.3              Button
8.4              Radio Button
8.5              Check Box
9. Basic Events
9.1              Click Event
10. Basic Apps
10.1             Number Arithmatic
10.2             String Programs
10.3             Swaping
10.4             Number Tricks
11 Advance Layouts
11.1             Linear Layout
11.2             Table Layout
11.3             Coordinator Layout
11.4             Drawer Layout
12. Advance Controls
Advance Events
```

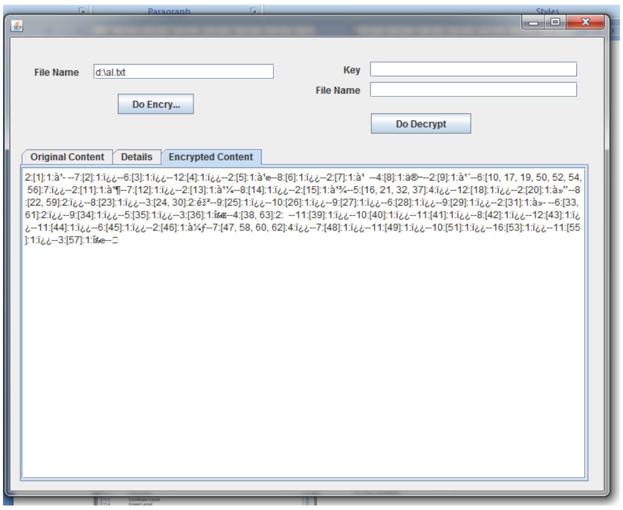
The below results are return by the tool



File Name d:\al.txt
Key
File Name

```
Reading Content....
Ants Initialized...
                    Total Text Ant...436
                    Total Value Ant...53
Total Words64
Largest Encryption Size128
Total no of Unique Words47
Generated Key:wd64ez128uw47
```

The key generated by the proposed algorithm is marked with gray in output screen for clear view.
The Encrypted content



File Name d:\al.txt
Key
File Name

```
2:[1]:1:à¹- --7:[2]:1:ï¿¿--6:[3]:1:ï¿¿--12:[4]:1:ï¿¿--2:[5]:1:à¹œ--8:[6]:1:ï¿¿--2:[7]:1:à¹ --4:[8]:1:ä®—-2:[9]:1:à¹´--6:[10, 17, 19, 50, 52, 54,
 56]:7:ï¿¿--2:[11]:1:à¹¶--7:[12]:1:ï¿¿--2:[13]:1:à¹¼--8:[14]:1:ï¿¿--2:[15]:1:à¹¾--5:[16, 21, 32, 37]:4:ï¿¿--12:[18]:1:ï¿¿--2:[20]:1:à»"--8
:[22, 59]:2:ï¿¿--8:[23]:1:ï¿¿--3:[24, 30]:2:é§²--9:[25]:1:ï¿¿--10:[26]:1:ï¿¿--9:[27]:1:ï¿¿--6:[28]:1:ï¿¿--9:[29]:1:ï¿¿--2:[31]:1:à»- --6:[33,
61]:2:ï¿¿--9:[34]:1:ï¿¿--5:[35]:1:ï¿¿--3:[36]:1:î‰Œ--4:[38, 63]:2:  --11:[39]:1:ï¿¿--10:[40]:1:ï¿¿--11:[41]:1:ï¿¿--8:[42]:1:ï¿¿--12:[43]:1:ï¿
¿--11:[44]:1:ï¿¿--6:[45]:1:ï¿¿--2:[46]:1:à¼ƒ--7:[47, 58, 60, 62]:4:ï¿¿--7:[48]:1:ï¿¿--11:[49]:1:ï¿¿--10:[51]:1:ï¿¿--16:[53]:1:ï¿¿--11:[55
]:1:ï¿¿--3:[57]:1:î‰œ--□
```

The detailed functionality of the tool developed will be presented in separate paper

5. CONCLUSION

In this paper, we discuss the problem of data security in cloud storage system. To control the outsourced data and provide the quality of the cloud storage service for the users, we propose an efficient data encryption using Ant Colony Model and cryptographic techniques. It is concluded that the proposed algorithm generate more secured encrypted content with reduced size and time taken is considerably low than the previous traditional algorithms.

REFERENCES:

[1] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. **(2011).**

[2] Cong Wang, Kui Ren, and Jia Wang, *Secure and Practical Outsourcing of Linear Programming in cloud computing*, In IEEE Internationa Conference on INFOCOM, pages 820-826, 2011.

[3] Q. Wang, C. Wang, J. Li, K. Ren,and W.Lou, *Enabling Public Verifi-ability and Data Dynamics for Storage Security in Cloud Computing*, In Proceeding of 14th European Symposium, Research in Computer-Security (ESORICS 09), pages 355-370, 2009.

[4] Neha Jain and Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security', VSRD International Journal of CS & IT. **(2012)**, Vol.2 Issue 4, pp. 316-321.

[5] Dubey A K, Dubey A K,Namdev M, Shrivastava S S, *Cloud-user Security based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment*, Software Engineering (CONSEG), CSI Sixth International Conference on, pages 18, September 2012

[6] M Armbrust, A Fox, R Grifth, A D Joseph, and R Katz, *Above the Clouds: A Berkeley View of Cloud Computing,* U C Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 2009.

[7] Cong Wang, Ning Cao, Jin Li, Kui Ren and W Lou, *Secure Ranked Keyword Search over Encrypted Cloud Data*, In IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pages 253-262, 2010.

[8] Kuyoro S O, Ibikunle F, Awodele O, *Cloud Computing Security Issues and Challenges*, In International Journal of Computer Networks, vol. 3, issue 5, 2011.

[9] Cong Wang, Kui Ren, W Lou, Jin Li, *Toward Publicly Auditable Secure Cloud Data Storage Services*, In IEEE Computer Networks, pages 19-24, 2010.

BIOGRAPHIES

Prof. B. Rex Cyril is working as Assistant Professor and pursuing doctor of philosophy in Department of Computer Science, St. Joseph's College,(Autonomous),Tiruchirappalli, Tamil Nadu, India. He received his M.Phil degree from Prist University. He received his MSc degree from St. Joseph's College, Tiruchirappalli. His area of interest is Cloud Security Services.

Dr. S.Britto Ramesh Kumar is working as Assistant Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India He has published many research articles in the National/International conferences and journals. His research interests include Cloud Computing, Data Mining, Web Web Mining, and Mobile Networks.