Society for Science and Education United Kingdom

TNC Transactions on Networks and Communications

Volume 2, Issue 6
ISSN: 2054 - 7420

Multilevel Cryptography with Metadata and Lock Approach for Storing Data in Cloud

[1]Dinesha H A and [2]Vinod Kumar Agrawal
PES Institute of Technology, Visvesvaraya Technological Univeristy, Belgaum, India;
[1]sridini@gmail.com; [2]vk.agrawal@pes.edu;

ABSTRACT

Cryptography is a technique for secure communication. Cryptography main objectives are confidentiality, integrity, non-repudiation, availability and authentication. Cryptography is a well defined and used technique to secure sensitive data. It has been using in cloud computing technology by various cloud service provider. Customers across the world are looking for storage infrastructure to store huge amount of data securely. Hence they are opting on demand, ready available, internet based and maintenance free infrastructure known as cloud data storage as a service. Many potential vendors like Microsoft and Amazon providing this service to customer across the globe. But major challenge is customer trust on vendor. Vendor has to prove customer that their data is safe via cryptography, security breach penalty, policies and security agreement so on. However, it is difficult to gain customer confident on vendor security. Hence we are proposing customer end algorithm called multilevel cryptography for secure cloud data storage where customer performs multiple cryptography operations on their data before storing into a cloud. In this paper we present the multilevel cryptography algorithm for secure cloud data storage with design and analysis.

Keywords: Cloud service provider, Data storage as a Service, Multilevel Cryptography, Secure Cloud Data, and Secure Communication.

1 Introduction

Today data security are achieving through cryptography. Many encryption and decryption techniques are in place and ready to use in cloud computing technology. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque [1] have proposed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm used to encrypt the data to provide security so that only the authorized user can access it. It consists of Public-Key and Private-Key. Public-Key is known to all, whereas Private-Key is known only to the user who is authenticated. Once the data is encrypted with the Public-Key, it is possible to decrypt with the corresponding Private-Key only. Eman M.Mohamed, Hatem S. Abdelkader [2] explain the data security system implemented into cloud computing using RC4, RC6, MARS, AES, DES, 3DES, Two-Fish and Blowfish algorithm. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. Kan Yang, Xiaohua Jia [3] describes the multilevel encryption for Ensuring Public Cloud. This technique applies multiple encryption algorithms for given plaintext. Follow the same level of decryption to convert back from cipher text. Cong wang, Qian wang, and Kui ren, Wenjing Lou describes how to ensure the data storage security in cloud computing [4]. In Cryptography and Network Security Principles and Practices [5],

DOI: 10.14738/tnc.26.591
Publication Date: 07th December 2014
URL: http://dx.doi.org/10.14738/tnc.26.591

mentioned many encryption technique and cryptography principles which can be adopted in cloud computing technology [5]. The following are amongst the most well known: i) DES: This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system. Ii) RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman. Iii) HASH: A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'. iv) MD5: MD5 is a 128 bit message digest function. It was developed by Ron Rivest. AES

This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST. V) SHA-1: SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes). Vi) HMAC: HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1 [5].

Many authentications also exist to ensure the cloud customer authentication while using cloud service they are i) Simple text password ii) Third party authentication iii) Graphical password iv) Biometric and v) 3D password object and etc are explained in [6][7][8][9]. We have presented multilevel authentication technique for accessing cloud services in [10].Some of the existing cloud authentication methods and techniques are described in [11] - [17].

The main challenge is though there are many techniques , method are available in cryptography and literature, what is the method to make sure customer that their data is keeping confidentially at cloud service provider end? What are the ways to gain customer faith on service vendor cryptography? As a solution, can vendors announce one service plan that customer is responsible for data confidentiality and vendor only responsibility is providing storage area with data disaster recovery. We are getting the motivation of the paper including shortcoming of the work carried out by various authors. In this paper, we present such service plan in details. We proposed a plan to customer to have a dedicated setup of software known as multilevel cloud cryptographer with customized option. It performs cryptography on sensitive data in multiple levels and in multiple ways before migrating customer data to service vendor infrastructure. Detailed information presented in remaining section of this paper. This paper is organized as following manner. Section II, presents the multilevel cryptography algorithms. Section III, describes the system design details of proposed algorithms Section IV presents the detailed analysis. Section V, concludes the paper along with future enhancement.

2 Multilevel Cryptography for Secure Cloud Data Storage

In this section we describe the proposed multilevel cryptography algorithm. This algorithm applied in customer side against their sensitive data. Before migrating to cloud vendor storage infrastructure customer performs data cryptography in multiple levels and in multiple ways. The levels and ways are decided by customer based on their data confidentiality and organizational structure. In this section we proposed three levels and three different ways on customer behalf. Proposed three levels are Chief Data officer, Cryptography Officer and Data Designers and its corresponding three ways are Data lock, Data encryption and Metadata respectively. Customer can customize levels and ways of cryptography. Customer is free to apply any techniques/methods available in literature as multiple levels way without knowing to service vendor or anybody. But first level and last level are recommended as important to have in their customized setup. Because its added different features in proposed cloud cryptography than encryptions alone. In algorithm1, we consider customer sensitive data as plaintext message m and migrated data as cipher text c.

Algorithm1: multilevel cryptography algorithm for migrating

```
Step 1:  plaintext message m processed in metadata to get jumbled message ‘mo’
  mo: jd (m)
Whereas ‘j’ refers to jumbled process, ‘d’ is data about the  jumbled  process
Step 2:  Data encryption for processed metadata and pack in file/folder f.
c=e (mo)
f= c1, c2, …cn
$f=\sum_{i=1}^{n} c$
Step 3 :Locking the data file/folder/package and send to cloud storage s
s: lock(f)
Therefore for migration formula is => lock ( f+ (e(jd (m))) obtained.
Algorithm2: multilevel cryptography algorithm for accessing the migrated data
Step 1: Unlocking the retrieved data file/folder/package from cloud storage
f: unlock(s)
Step 2:  Extract Folder/file and perform decryption to get back mo.
For i=1 to n
   c=Split (f)
mo =d (c)
Step 3:  processed in metadata to get plaintext message m from jumbled message ‘mo’
  m: j-d (mo)
Therefore for accession formula is => j-d(d (split - (unlock (s)))) obtained
Example
Let us take example and apply this algorithm for set of sensitive data i.e customer pin set
{2345, 4567, 5645}.
i) Below are the migration steps to get migrated data output
1. mo= jd jumbled with even first and odd next,  left to right i.e change data position to
2413 order
i.e = {3524, 5746,6554} d has order info i.e 2413 .
2. Apply any encryption algorithm we used simple substitution i.e add +2 to mo
 c= {5746, 7968, 8776}
3. Pack all, lock and place in file
lock (f= {574679688776 }) hence migrated data is locked 574679688776
ii) Below are the accession steps to get plain text from migrated data.
Split (Unlock (574679688776)) with size of 4
{5746, 7968, 8776}
Decrypt with -2  for spitted data {5746, 7968, 8776}
{3524, 5746,6554}
Reorder with jumbled inverse function i.e 2413-1
j-d({3524, 5746,6554})
=>{2345, 4567, 5645}
```

Proposed three levels and corresponding ways are in described in table 1 and corresponding architecture are represented in figure 1.

Table 1: Proposed multilevel cryptography

Level No	Level Name	Ways of Cryptography	Description
1.	Chief Data Officer	Data lock	Locks the data with one suitable authentication (password, biometric, Multi Level Authentication and etc)
2	Cryptography Officer	Data encryption	Responsible for data encryption with private. He is free to choose available encryption technique like RSA, DES, AES and etc.
3	Data Designer	Metadata	Responsible for data storage order/structure/pattern designs. Keep the data pattern of sensitive data.

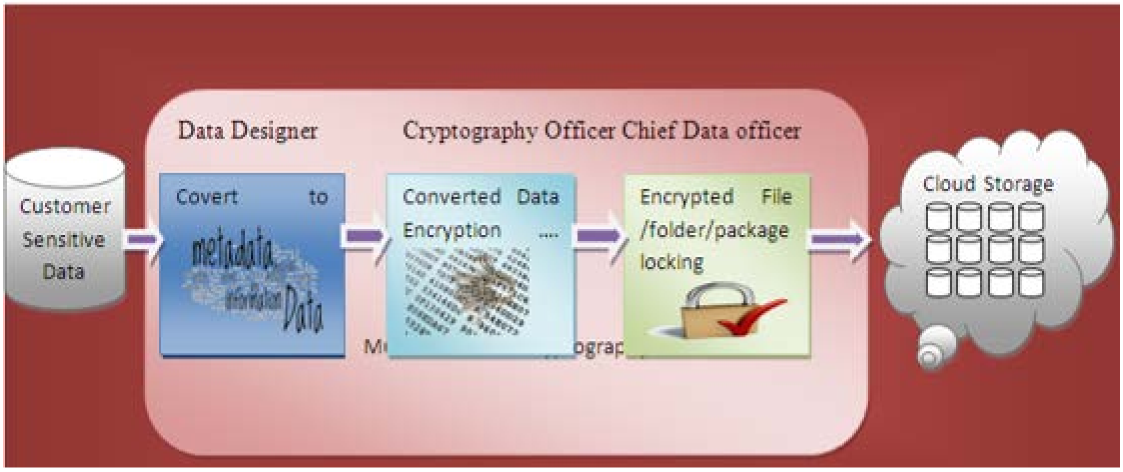

Customer
Sensitive
Data
Data Designer
Cryptography Officer Chief Data officer
Covert to
Converted Data Encryption ....
Encrypted File /folder/package locking
Cloud Storage

Figure 1: Proposed multi-level cryptography architecture (before migration)

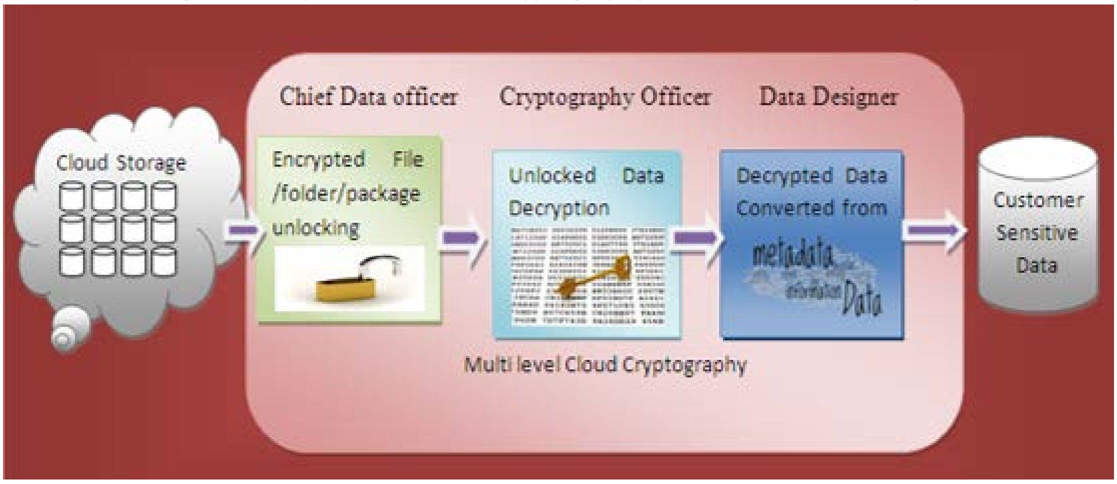


Figure 2: Proposed multi-level cryptography architecture (during accession)

Proposed architecture presents, sensitive data first converts into metadata by data designer. In second level converted data get processed with data encryption by Cryptography officer. This encryption algorithm can be multiple or single; it depends on customer and their confidentiality. Final step encrypted data file/folder/package locking done by chief data officer. Customer has to follow these multilevel steps before migrating data. Now, as a description for accessing the same data, customer has to follow the reverse steps as below figure 2. First, Chief Data officer has to unlock received data from cloud vendor. Cloud vendor may use cryptography technique or it just provides data storage with data disaster recovery. After unlocking, cryptography officer decrypt the unlocked files/folder/package. Finally data designed use metadata to take back original order/structure/pattern. Finally it reaches actual data base. Here, all the levels people are equally responsible and required in this process.

3 System Design

In this section we present the designs of the proposed multilevel cryptography using petri net theory. The system modeling is done using Petri nets, which are vividly portrayed in figure 6. Petri nets are a special form of bipartite directed graph represented by < P, T, In, Out> , in which Place (denoted as p) and Transitions (denoted as t) are disjoint sets of nodes, and In and Out are sets of edges. We carry out formal modeling for our system to precisely discover how user can migrate to cloud using multilevel cloud cryptography. How user can access the sensitive data back from migrated cloud. The model is explained as follows. Figure 3shown Petri net model before migrating into cloud storage. The places p1, p2, p3, p4, p5 and p10 represent the steps to convert from sensitive data to multilevel cryptography based migrated data. The transitions t1, t2, t3, t4 and t5 present the corresponding actions in it. The condition places p6, p7, p8, p9 and p11 has to be satisfied for successful migration.

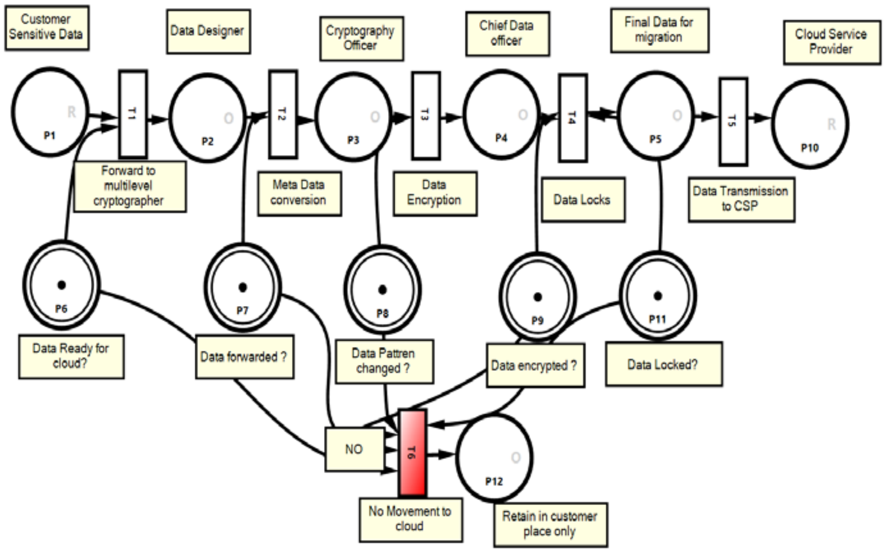


Figure 3: Petri net model before migrating into cloud storage

Figure 4 presents Petri net model for accessing the migrated data from cloud. The places p1, p2, p3, p4, p5 and p6 represents the steps need to follow before accessing the migrated data. The transition t1, t2, t3, t4 and t5 present the corresponding actions to achieve the same. The condition p7 and p8 has to satisfy for successful data reception.

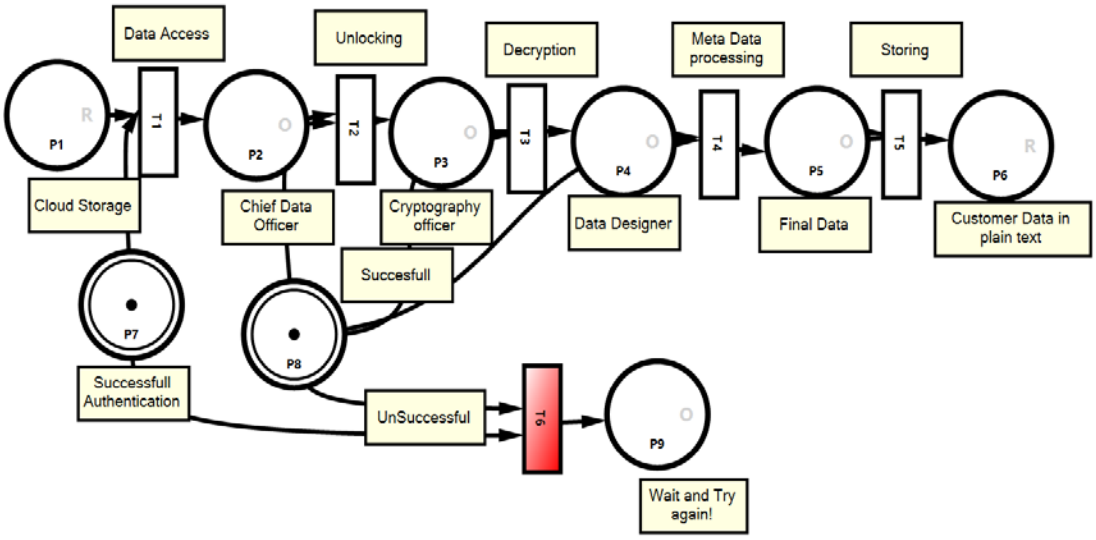


Figure 4: Petri net model for accessing the migrated data from cloud

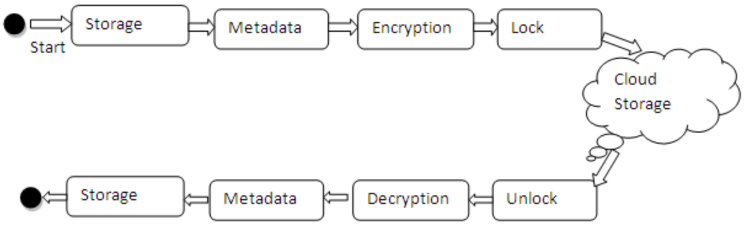


Figure 5: State Chart Diagram of migration and accession

Figure 5 shows the different states of the data to be stored in cloud before migrating and accessing the data from the cloud after migration. This can also be applying to save the local Virtual Machines related files. In cloud IaaS, VMs playing major rule. Private IaaS cloud setup having its own set of VMs that they use in regular business application. Backup of this VMs and its corresponding template files like .vmx, .vmdk and so on can be stored in cloud using this technique. A new optimized ranking algorithm.

4 System Analyze

In this section we analyze the proposed multilevel cryptography algorithm.

(a) Let's take the above derived migration process formula Cloud encryption Ce is => lock (f+ (e(jd (m))) and accession formula for Cloud decryption process Cd is M=> j-d(d (split - (unlock (s)))). Let us consider the number of levels is 3, hence to migrate and access levels L1, L2 and L3 and t L3, L2 and L1 has to be follow respectively.

Let us try to analyze probability of breaking this security from untrustworthy vendor or hacker H. If H breaks the confidentially then he should be success in L1(unlock key) , L2(decryption key & algorithm) and L3 (metadata details) levels. As shown in figure 6 , to breach confidentiality H should Success as SSS probability if we take sample space for 3 leves with Success S and Failure F outcomes.

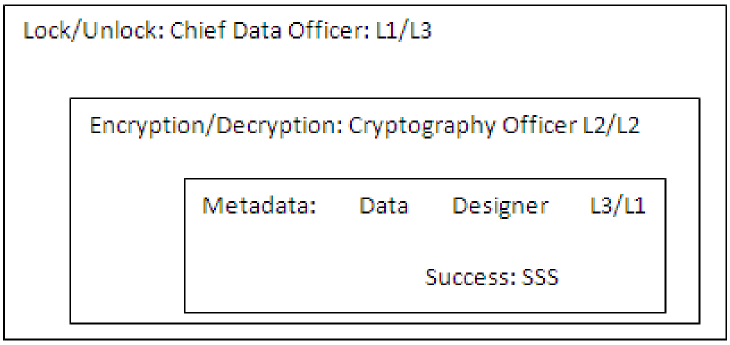

Lock/Unlock: Chief Data Officer: L1/L3
Encryption/Decryption: Cryptography Officer L2/L2
Metadata: Data Designer L3/L1
Success: SSS

Figure 6: Multilevel Cryptography Security Model

Probability of Hacking Event E is P(E)=P(SSS)= 1/8. Therefore (probability Theorem) for Inverse of Event P(E~)=1-P(E)= 1-1/8 =>7/8.

Consider the attack of n times and what is the probability of getting exactly three success SSS. Applying Probability Theorem 3.6 Given n Bernoulli trials with probability p of success on each experiment, the probability of exactly j successes is can be derived as

$$b(n, p, j) \quad = \binom{n}{j} p^j q^{n-j}$$

Where n=number of times attacks, j = number of success, p = probability of success in each try = 1/2=0.5 q=1-p.

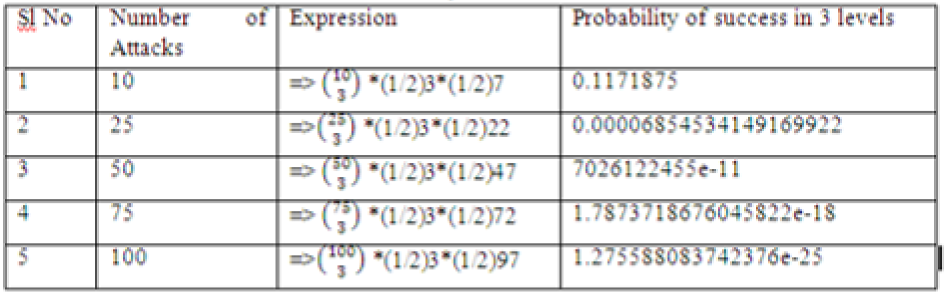
Case 1: If hacker attacks 10, 100 and 1000 times, what is the probability of success in all three levels?

b (10, 0.5,3)= $\binom{10}{3}$ *(1/2)3*(1/2)7 = 120*(1/8)*(1/128)

=120/1024 =15/128

=>120*0.125*0.0078125 =>15/128=>0.1171875

Table 2: Probability of success in 3 level



Sl No	Number of Attacks	Expression	Probability of success in 3 levels
1	10	=> $\binom{10}{3}$ *(1/2)3*(1/2)7	0.1171875
2	25	=>$\binom{25}{3}$ *(1/2)3*(1/2)22	0.00006854534149169922
3	50	=> $\binom{50}{3}$ *(1/2)3*(1/2)47	7026122455e-11
4	75	=> $\binom{75}{3}$ *(1/2)3*(1/2)72	1.7873718676045822e-18
5	100	=>$\binom{100}{3}$ *(1/2)3*(1/2)97	1.275588083742376e-25

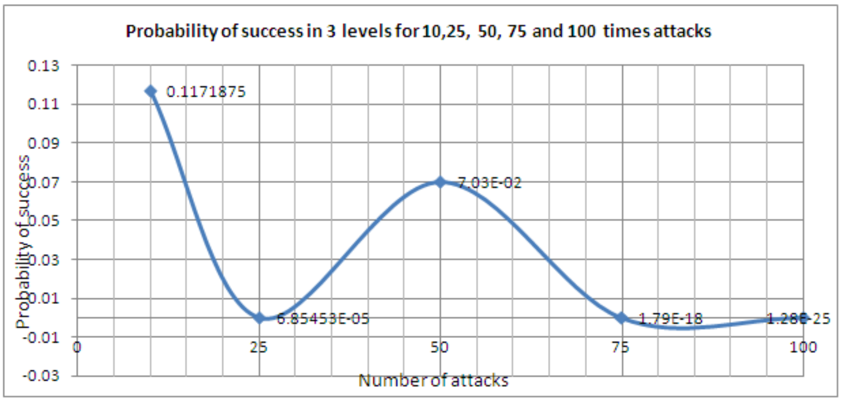
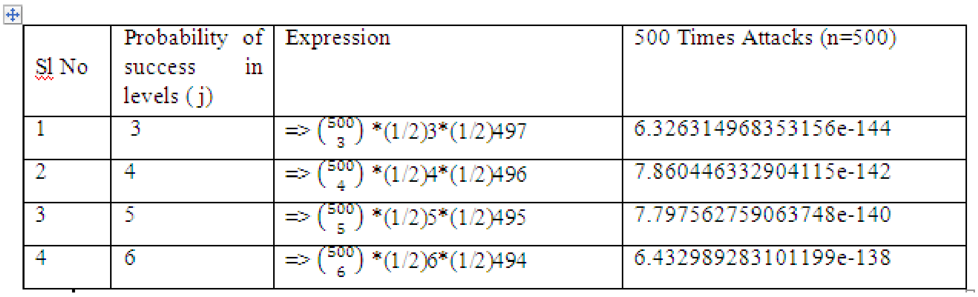


Figure 7: Graphical Representation: Security distribution for attacks n= {10, 25, 50, 75, 100} for 3 levels.

Table 3: Probability of success for 500 attacks in different levels of security



Sl No	Probability of success in levels (j)	Expression	500 Times Attacks (n=500)
1	3	=> $\binom{500}{3}$ *(1/2)3*(1/2)497	6.326314968353156e-144
2	4	=> $\binom{500}{4}$ *(1/2)4*(1/2)496	7.860446332904115e-142
3	5	=> $\binom{500}{5}$ *(1/2)5*(1/2)495	7.797562759063748e-140
4	6	=> $\binom{500}{6}$ *(1/2)6*(1/2)494	6.432989283101199e-138

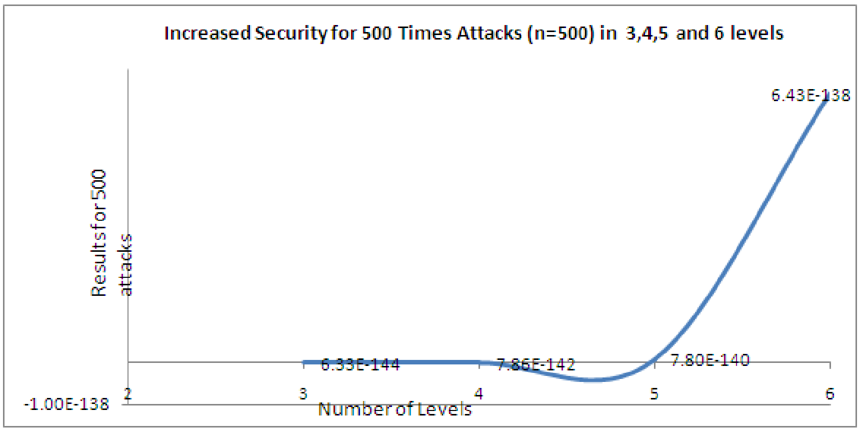


Figure 8: Graphical Representation Security Distribution for j= {3, 4, 5, 6} for 500 times attack

Different ways of attack could be man in the middle attack, phishing attack, multi tenancy attack, brute force attach, dictionary attack and so on. By providing multilevel security with multi way and multi man operation we can provide better security to cloud storage. As shown in above graph1, though the any number of attacks increases the security continues to be stable and security gets increases when the levels are increased. Though there are multilevel and each individual in the level have no burden of remembering many passwords and techniques. Hence it is not complex too.

5 Conclusion and Future Enhancement

Cryptography is a best technology to store customer data in cloud. Many algorithms and methods are exists to place the customer data in encryption format. However, it is difficult to gain customer confidence amount the service provider. We presents on method which helps customer to process their data in multiple levels and ways before migrating to cloud. Hence the customer no need worry about the service provider cryptography way. Both migration and accession steps are discussed in detail. Further we would like to implement this algorithm and make this as a customer side migration package known as multilevel cloud cryptographer software package.

ACKNOWLEDGMENT

Our sincere thanks to Prof. K N B Murthy, Principal and Prof. Shylaja S S, HOD, Department of Information Science and Engineering, PES University, Bangalore, for their constant encouragement.

REFERENCES

[1]. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012, 181-185.

[2]. Eman M.Mohamed, Hatem S. Abdelkader, Enhanced Data Security Model for Cloud Computing, The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track, Faculty of Computers and Information - Cairo University, CC-12.

[3]. Kan Yang, Xiaohua Jia, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013, 1717-1726.

[4]. Cong wang, Qian wang, and Kui ren, Wenjing Lou,”Ensuring data storage security in cloud computing” at IEEE (8-1-4244-3876-1/09).

[5]. William, S., 2005. Cryptography and Network Security Principles and Practices. 4th Edn. PHI.

[6]. CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx

[7]. X. Suo, Y. Zhu, G. S. Owen, “Graphical passwords: A survey,” in Proc. 21st Annual Computer Security Application Conf. Dec. 5–9, 2005, pp. 463–472.

[8]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Proc. Human-Compute. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.

[9]. Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication," IEEE, http://ieeexplore.ieee.org., Last Updated – 6 Feb 2008.

[10]. [10]Dinesha H A, Dr.V.K. Agrawal, Multi-level Authentication Technique for Accessing Cloud Services, IEEE conference, Dindigul.

[11]. Mostafa Hajivali , Faraz Fatemi Moghaddam , Maen T. Alrashdan , Abdualeem Z. M. Alothmani , Applying an Agent-Based User Authentication and Access Control Model for Cloud Servers, ICTC 2013, 978-1-4799-0698-7/13, 807-902,2013.

[12]. Laurent Hubert, Renaud Sirdey, Authentication and secured execution for the Infrastructure-as-a-Service layer of the Cloud Computing model, 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 978-0-7695-5094-7, 291-296, 2013.

[13]. Ming-Huang Guo, Horng-Twu Liaw, Li-Lin Hsiao, Chih-Ta Yen, Authentication Using Graphical Password in Cloud, 177-181, 2013.

[14]. H. B. Tang*, Z. J. Zhu, Z. W. Gao, Y. Li, A SECURE BIOMETRIC-BASED AUTHENTICATION SCHEME USING SMART CARD,IEEE, 39-43,2013.

[15]. A. K. Das. "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards", IET Information Security, 5 (3), pp. 145-151, 2011.

[16]. Wei Xie1, Lei Xie2, Chen Zhang1, Quan Zhang1, Chaojing Tang1, Cloud-based RFID Authentication, 2013 IEEE International Conference on RFID, 978-1-4673-5750-0/13,168-175, 2013.

[17]. Bernd Zwattendorfer, Arne Tauber, SECURE CLOUD AUTHENTICATION USING EIDS, Proceedings of IEEE CCIS2012, 978-1-4673-1857-0/12/, 397-401, 2012.