International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-2 Issue-5, November 2013

Secure Data Storage in Cloud Service using RC5 Algorithm

Sachindra K. Chavan, Manoj L. Bangare

***Abstract*: Enterprises always used organizational internal storage system for storing data. Mainly in a Customer Relational Management i.e. CRM system, the internal storage will be used for storing all the data of the customer. On the other hand, the main drawbacks in the data storage is there may be intruder's in the administrator side and they may acquire all the information about a customer. Above threats can happen in same service provider in a cloud computing environment. To overcome with this kind of challenges in cloud computing, there is need of an innovative algorithmic approach for data security in cloud computing.**

A CRM (Customer Relational Management) system services is represented in this paper using RC5 algorithm. In the proposed system the party that uses cloud storage services must encrypt data before sending it to cloud while the service provider who is responsible for encryption/decryption of the user's data and then must delete data once encryption/decryption process is completed. In this paper the use of CRM services which demonstrates how the parties involved in secure storage and retrieval when data is saved to the cloud.

***Index Terms*: Cloud Computing, CRM Service, Data Retrieval and Storage, Encryption/Decryption, RC5 algorithm, Secure Storage.**

I. INTRODUCTION

The term "Cloud" comes from the telecommunication world when providers began using the virtual private network (VPN) services for data communication. Cloud computing associated with the computation, software, data access and storage services, that may not be needed knowledge of end users of the physical location and the system configuration that is delivering the services. The basic concept of cloud computing is that the computing is "in the cloud". It is related to accessing end user applications and storing data in the "cloud" which is representation of the Internet or a network and using associated services. In IT enterprises, the cloud are recent trends, i.e. it is ability to moves computing and data away from desktop and portable PCs into large data centers.

The definition of cloud computing provided by National Institute of Standards and Technology (NIST) [2] says that: "Cloud computing is a model for enabling 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."

With the help of large scale enterprise the internet grows rapidly around the world, applications can now be delivered as services over the internet. As a result this overall cost is reduced.

The main objective of cloud computing is to make a better use of distributed resources, combine them to achieve higher throughput and be able to remove large scale computation problem. Cloud computing deals with scalability, interoperability, virtualization, quality of service and cloud delivery model, namely private, public and hybrid.

Cloud computing is an emerging technology. Recently in IT enterprises many big players are existing, such as Google, IBM, and Microsoft comes with the cloud solutions that enable people and organizations gain access to enormous computational and other resources in pay per use fashion. According to Weiss [3], cloud computing is a related to many existing technologies. They include utility computing in the service oriented fashion [4], grid computing [5], and large data centers that are used to store enormous amounts of data of cloud users. Before cloud computing came into existence, organizations used to store data in their internal storage media and security is provided by various means to prevent attacks from internal and external users. As organizations require more and more resources they may operate to use cloud services. In such case, the cloud server maintained by the service provider when their data are stored directly. The data securities play an important role when storing data on cloud servers. A cloud service provider takes care of the security of their user's data. However, from user aspect, the cloud is not secure. This is because the administrators of cloud storage servers are privileged to have unauthorized access to data about clients. The data have to be prevented. This is research work takes from this motivation. This paper proposed the methods to prevent it.

Commonly service providers provide convincing security and service policies which are to be accepted by the client or users. Every application which requires people involvement has some sort of agreement with clients or users. For example Yahoo! Web mail requires user agree to its term and conditions. In a cloud computing environment also the users might have different storage requirement at different times. These requirements and server's rule and regulation and any other issue are clearly mentioned in the agreement, often they are known as Service Level Agreements (SLAs) [6]. The logging on SLAs indicate that user have accepted to the terms and conditions and both service provider and client. Commonly storage security is provided by using encryption and decryption concept.

Revised Manuscript Received on 30 November 2013.
* Correspondence Author
Sachindra K. Chavan, P.G. Scholar, IT Department, SKNCOE, Pune, India.
Manoj L. Bangare, Professor, IT Department, SKNCOE, Pune, India.

A system administrator is capable to access to the private data of users in cloud computing. If in this case, users' data may not be secure. This paper concentrates on this security threat.

In this paper propose a new method where the storage and encryption/decryption are separated into two different cloud servers. In one cloud server storage of data takes place securely while another server only takes care of encryption and decryption process to see that data of the user remain secure and data integrity and implements the One Time Password Authentication including email updates and application system. This paper uses the core concept of CRM to describe the new proposed method.

II. RELATED WORK

Internet technology has been introduced in the 1990's era for the facilities of ubiquitous computing and growing rapidly in distributed computing. Evaluation of cloud computing has started the journey from parallel computing to distributed computing to grid computing. Cloud computing can be known as the computing environment where the need of the computing by one party can be outsource the other party and as per the need of computing power or resources like database or email can be accessed via internet. The cloud computing is an emerging technology that makes it possible for individuals and organization to gain to enormous state-of-the-art resources through Internet in pay-per-use fashion without any capital investment. This concept may be help for peoples in making use of resources through the Internet and pay-per-use. The resource usages can be arranged based on the customer requirements [8]. The cloud computing has many services such as IaaS (Infrastructure as a Service), SaaS (Software as a Service), and Paas (Platform as a Service) [9]. The IaaS take care of infrastructure such as data centers, storage and secure server etc cloud users. The SaaS take care of software to cloud client as a service. The PaaS takes care of development platform that enables programmers to write applications that interact with the cloud. A General mechanism for protecting user data include encryption prior to storage, user authentication procedures major for storage or retrieval, and establishes secure channels for data transmission. These protection mechanisms normally require cryptography algorithm and digital signature techniques, are explained below. Usually data encryption mechanism includes symmetric and asymmetric cryptography algorithm. Symmetric cryptography is used in U.S. Federal Information Processing Standard's (FIPS), 46-3 TDEA (Triple Data Encryption Algorithm), AES (Advanced Encryption Standards), Blowfish, RC5 and others. In this case RC5 symmetric algorithm is most effective and efficiently algorithm from rest of the other symmetric algorithms. This type of encryption and decryption process uses a secret key. Asymmetric cryptography, in this case, uses two different keys, for the process of encryption uses a "public key" and for the process of decryption uses a "private key". For example RSA cryptography [10] and Elliptic Curve Cryptography (ECC) [11]. In most cases, symmetric cryptography is more efficient and suitable for encrypting huge amount of data. Asymmetric cryptography needs more computation time and is used for the decryption keys needed for symmetric cryptography.

The comparatively result in cryptography algorithm as shown in Table. I.

TABLE I. COMPARISION OF VARIOUS CRYPTOGRAPHIC ALGORITHM[12]

Cryptographic Algorithmic Matric	DES	3DES	RC5	RSA
Key Length in Bits	56	112	64	1024
Attach Time in Year	1.37 x 10^{11}	1.25 x 10^{28}	3.61 x 10^{13}	2.40 x 10^{17}
Attack Steps	2^{56}	2^{112}	2^{64}	Factoring
Rounds	16	48	Variable 0,1 to 255	Not applicable
Algorithmic Strength	CS	CS	CCS	CCS

*CS- Computationally Secure.

*CCS- Conditionally Computationally Secure.

The use of passwords as an authentication process is more familiar to users, but the data sent by the user can be hacked easily. In more advance the authentication system , the system side will generate a random number to send the user a dispute message, requesting the user to send encrypted message in reply to the challenge message, thus authenticating that the user has the correct encryption key. Without the key, the client will not be permitted to access. In the process of challenges and response the user's encrypted key uses the user's password to convert a derived value. In this case, each communication between the user and server is unique, and a hacker using an old message would fail to access the system. In additional, the One-Time-Password (OTP) authentication system differ from most people's conception of password. Most clients understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP, however is the single-use nature of the password. In this case, after receiving authentication form the user side, then the must need to create a secure transmission channel between the system and user's for the use to sharing information between system and user. The Secure Sockets Layer (SSL) is a common method of building secure channels, primarily using RSA encryption to transmit the secret keys needed for the both sides to encrypt and decrypt data transmitted between them.

III. PROPOSED METHODOLOGY

A. *Core Concept*

This study proposed business model for cloud computing based on separate Independent Secure Cloud as a Service. The concept based on separating the storage and encryption/decryption of user data. This process is as visualized in Fig. 1. Secure Storage Cloud as a Service is provided by one cloud service provider and Independent Secure Cloud as a Service provided by another service provider. Independent Secure Cloud as a Service and Secure Storage Cloud as a Service are not provided by a single operator. In addition, the secure storage cloud as a service provider may not store unencrypted user data and once the provider of independent secure cloud as a service has finished encrypting the user data handed it off to an application (e.g. CRM system), the independent secure cloud service system must delete all encrypted and decrypted user data.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

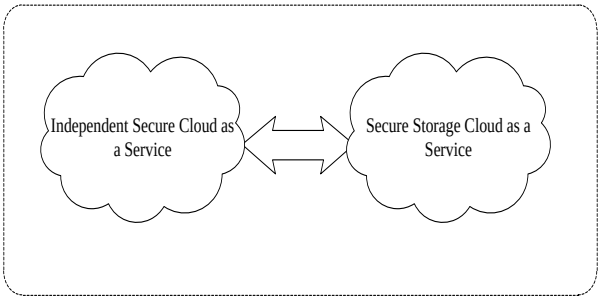

Fig. 1. Independent Secure Cloud as a Service

To demonstrate the concept of our proposed business model, as can be seen in Fig. 2 present an example in which the user uses separate cloud service for CRM, Secure Storage and Independent Secure Cloud Service. According the user requirements in this model, the user interact with CRM, Cloud service. In this case, the CRM service interaction both secure storage cloud service and also independent secure cloud service. The interaction with each other they are bidirectional. The secure storage cloud service, independent secure cloud service and CRM cloud service are having bidirectional communicate to each other. The CRM cloud service could be exchanged for other function-specific application service (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operation Cloud Services).

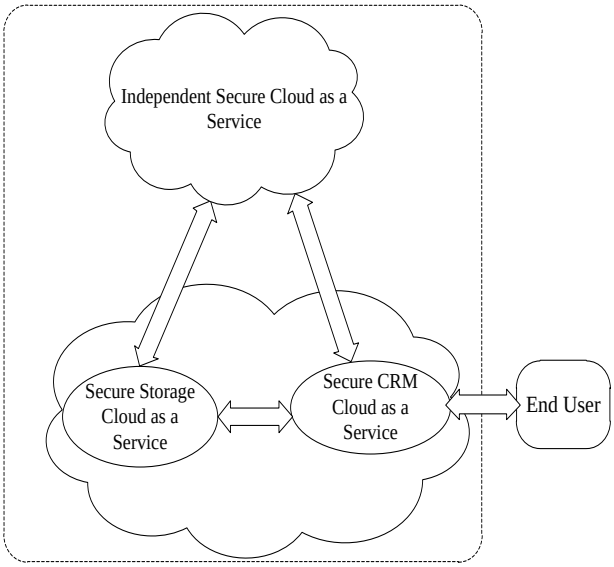

Fig. 2 Proposed Business Model for Stores User's Data in Cloud

B. Data Retrieval Program

In this section, focus on how users will do interaction with the CRM to encrypt and decrypt the user data. For that purpose, after the user login into the secure CRM cloud service system, CRM system requires any client information, it will execute a data retrieval program. The data retrieval program is illustrated in Fig. 3 and is explain below.

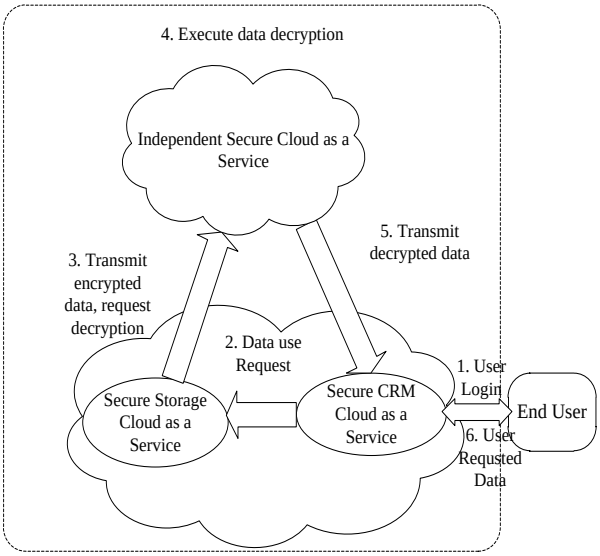

Fig. 3 Data Retrieval Program of Cloud Computing

When a user needs to access the secure CRM cloud service, he/she will do first execute the Login Program in step 1. In this step, can be use current e-commerce or other service which has already securely verified the user registration. In such case, symmetric key-based challenge and reply login verification or through a One-Time-Password (OTP).

After the user login has been successfully verified, if the secure CRM cloud service system get the client information from the user, then after it can send a request for information to the secure storage service system, as can be visualized in step 2. In this process, the CRM service system transmits the user ID to the secure storage cloud service system. The user ID can be used to search for the client's encrypted data. So, once found, then after a request must be sent to the independent secure cloud service system along with the user ID. Step 3 can perform the execution of transmit of encrypted client data and user ID from secure storage cloud service system and independent secure cloud service system.

Since, the independent secure cloud service system can serve a number of the user i.e. multiuser and each encrypting/decrypting user data may require a different key. Therefore each user's having a unique ID and keys are stored together. Therefore in this step 4, the independent secure cloud service system uses the received user ID to index the user's data decryption key, which then after using for decrypt the received data. The decryption key for the use to decrypted data to restoring the data to its original format.

In step 5, transmit decrypted client data to the CRM cloud service system. And then after in step 6, the decrypted data can show the user, complete the data retrieval program. The independent secure cloud service system and the CRM service system can be established a secure data transmission channel to securely transmit the decrypted client data. After that sent the decrypted client data, independent secure cloud system is not permitted to hold the decrypted data and any unencrypted data must be deleted to protect the encrypted data and the decryption key from a store in the same system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. Data Storage System

In this section, after the user login into the secure CRM cloud service system, CRM system requires any client information; it will execute a data storage program. The data storage program is demonstrated in Fig. 4 and is explain below.

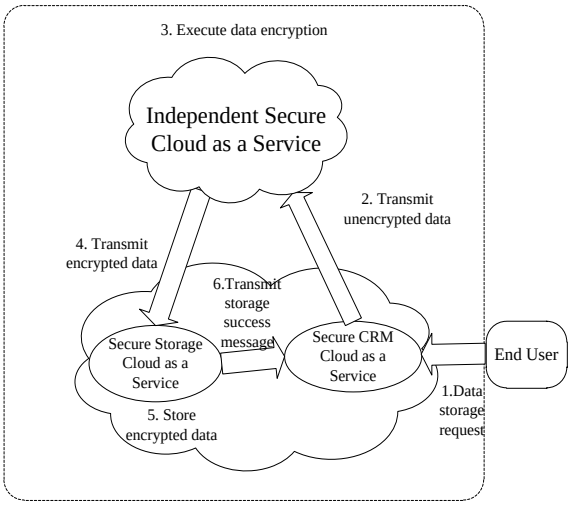

Fig. 4 Data Storage Program of Cloud Computing

In step 1, as per Fig. 4 , the client sending a data storage request to the CRM service system which then invokes the data storage program, requesting encryption of data from the independent secure cloud service system as shown in step 2. In step 2, establishing secure data transmission channel between the secure storage cloud service system and independent secure cloud service system for transmitting the user ID and the data requiring from the CRM service system to the independent secure cloud service system.

The different user requires different keys for the data encryption in step 3, the independent secure cloud service system invokes encryption of data, which including user the received user ID to index the user encryption key and then after used to encrypt the received data.

After completion of the encrypted client data with the help of encryption algorithm in the independent secure cloud service system must be transferred to secure storage cloud service system where the user ID and encrypted data are stored together. In step 4 perform, it must transmit the encrypt client data and user ID to the secure storage cloud service system. In step 5 execute in the secure storage cloud service system receiving the user ID together with the data for storage. In this business model, the completion of step 4 at the independent secure cloud service system, all unencrypted and decrypted user's data must be deleted.

At the final step, i.e. step 6 is the data storage program, transfer a completion message of data storage from the secure storage cloud service to the CRM service system. At this stage the CRM service system may confirm that the Client data has been stored. Otherwise, if it doesn't receive the completion message of data storage, it can be re-invoke the data storage program or after a while a period of time, proceed with exceptional situation handling.

D. RC5 Algorithm

RC5 is a symmetric encryption algorithm developed by Ron Rivest in 1994. RC stands for "Ron's Code" or "Rivest Cipher". It is suitable for hardware and software implementation.

The RC5 encryption algorithm is a w is word block cipher that converts plaintext data blocks of 16, 32 and 64 bits into the cipher text blocks of the same length. RC5 uses a key selectable length b (0, 1, 2, ...,, 255) byte. The algorithm is organized as a set of iteration called rounds r that takes values in the range (0, 1, 2,...,, 255) as demonstrate in Fig. 5.

The operation performed on the blocks include bitwise X-OR of words, data-dependent rotations by means of circular left and right rotations and Two's complement addition/subtraction of words, which is modulo- 2^w addition/subtraction. RC5 is a fully parameterized family of encryption algorithm; it is more accurately specified as RC5-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r and b denotes the length of the encryption key in bytes. The original suggested choice of parameter were w=32bits, r=12 and b=16 bytes. For all variants, RC5-w/r/b operates on two w-bit words using the following operations.

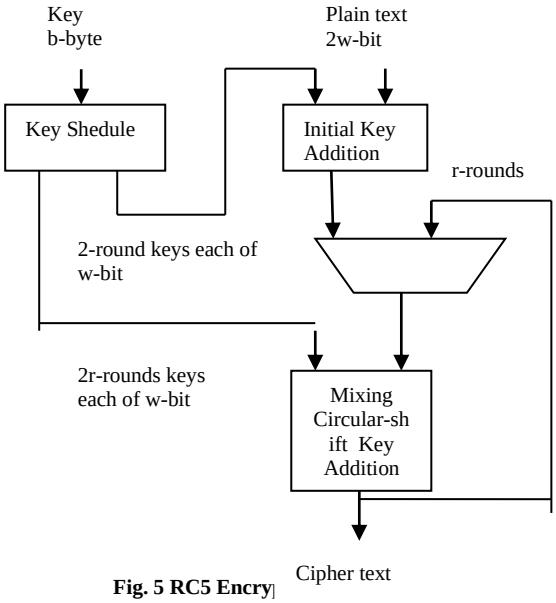

Fig. 5 RC5 Encry

The basic operation in RC5 is defined as follows:

- A+B integer addition modulo-2^w
- A+B integer subtraction modulo-2^w
- A⊕B bitwise exclusive-or of w-bit words
- A<<<B rotation of the w-bit word A to the left by the amount given by the least significant lg w bits of B
- A>>>B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B

There are three routines in RC5: key expansion, encryption and decryption. In this section discuss, the key - expansion algorithm is used to generate the round sub keys that will be used in both encryption and decryption algorithm. RC5 has a different algorithm for encryption and decryption, in the encryption it uses integer addition modulo-2^w but in decryption it uses integer subtraction modulo-2^w. RC5 is a symmetric key encryption so encryption and decryption algorithm uses the same key [13].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Key-Expansion Algorithm

The user gives a key b bytes, copy the secret key K [0.... b-1] into an array L [0..... c-1] of the c= ceil (b/u), where u=w/8 in Little-Endian order. Means, fill up L using u consecutive key bytes of k. Any unfilled byte positions in L=0. In the case that b=c=0, set c=1 and L [0] =0. The number of w-bit words that will be generated for additive round keys is 2 (r+1) and these are stored in the array S [0, ... , 2r+1].

Magic Constant Pw and Qw are defined for arbitrary w as follows:

Pw = Odd ((e-1) 2^w) .....(1)

Qw = Odd ((v-1) 2^w) .....(2)

Where

e is the base of the natural logarithms (e = 2.178282828459) and

v is the golden ratio (v = 1.618033988749)

Odd (x) is the odd integer nearest to x [2].

Key-Expansion with RC5-w/r/b

Input: b byte key that is preloaded into c word array L [0,1,…, c-1], r denotes the no of rounds.

Output: 2r+2 w-bit round keys S [0, 1, …, 2r, 2r+1].

Procedure:

S[0] = Pw,

For i= 1 to 2r+1 do

{

S[i] = S[i – 1] + Qw

}

X = Y = a = b = 0

Iteration =3 * max (c, 2r+2)

For i = 1 to Iteration do

{

X = S[a] = (S[a] + X + Y) <<< 3

Y =L[b] = (L[b] +X + Y) <<< (X + Y)

i = (a + 1) mod (2r + 2)

j = (b + 1) mod c

}

Encryption Algorithm

In Fig. 6 discuss about the encryption procedure of RC5; the decryption procedure is just reversed of the structure by converting the addition operation to subtraction operations.

RC5 works with two w-bit registers A and B which contains the initial input plain text as well as the output text as the end of encryption. The first bytes of plain text or cipher text is placed in the least-significant byte of A, the last byte of the plain text or cipher text is placed into the most-significant byte of B. Pseudo code of encryption is given below; at first load a plain text into register A and B then apply these to encrypt the plain text.

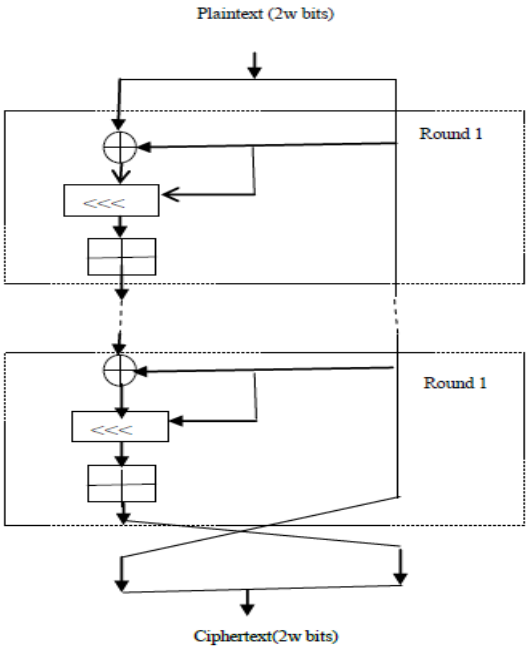

Fig. 6 RC5 Block Cipher[13]

Encryption with RC5-w/r/b:

Input: plain text stored in two w-bit input register A and B. R denotes the number of rounds and 2r+2 w-bit round keys S [0, ..., 2r+1]

Output: Ciphertext will be stored in A and B.

Procedure:

A = A + S [0]

B = B + S [1]

For i = 1 to r do

{

A = ((A ⊕ B) <<< B) + S[2i]

B = ((B ⊕ A) <<< A) + S[2i+ 1]

}

After this encryption operation on register A and B plain text converted into the cipher text and store it in any file.

Decryption Algorithm

Decryption pseudocode is given below; for decryption of cipher text load cipher text register A and B then apply these operations to convert cipher into plain text.

Decryption with RC5-w/r/b

Input : cipher text stored in two w-bit input register A and B. Denotes the number of rounds and 2r+2 w-bit round keys S [0,...., 2r+1]

Output: plaintext will be stored in A and B

Procedure:

for i = r to 1 do

{

B = ((B – S [2i + 1]) >>> A) ⊕ A

A = ((A – S [2i + 1]) >>> B) ⊕ B

}

B = B – S [1]

A = A – S [0]

Decryption algorithm uses integer subtraction modulo-2^w and right rotation on register for getting plain text; it exactly reverses operation on the register.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. COMPARISON AND ANALYSIS

A comparative analysis of RC5 and Blowfish are performed to provide some measurement on the encryption and decryption. Effects of several parameter such as number of rounds, block size and length of secret key on the performance evalution criteria are investigated.

These two encryption algorithm were implemented in Java in Eclipse IDE. Performance was measured on 1.67GHz Intel Centrino with 1GB RAM running Windows7.

A. Performance Comparison

In addition, to improve the accuracy of our timing measurement program was executed 10 times for each input file and we report the average of times there by obtained. In this observation key size is 32-bits, 64-bits and 128-bits for RC5 and Blowfish. Number of rounds (r) was fixed 12 for RC5 and 16 for Blowfish.

On the basis of execution time, we compare the execution time of each algorithm on text file type for this purpose we mainly used in 5 files and recorded their execution (encryption and decryption) times in millisecond for their two algorithm.

List of input file and their size are given in table 2.

TABLE II. COMPARISION ON THE BASIS OF EXECUTION TIME

Sr. No.	File Size in(KB)	RC5-32	RC5-64	RC5-128	Blowfish-32	Blowfish-64	Blow fish-128
1.	752	2886	2482	2450	5291	4789	4758
2.	1034	3869	3433	3386	5949	5437	5412
3.	1410	5179	4665	4619	6883	6320	6298
4.	1691	6038	5570	5540	7572	7189	6979
5.	2232	7691	7348	7287	9218	8311	8307

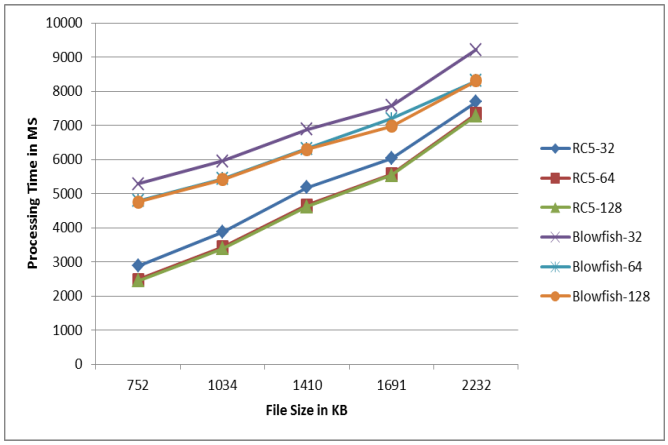

Fig. 7 Execution Time of RC5 and Blowfish

V. CONCLUSION

In this paper study of RC5 algorithm, its effectively and efficiently recognized security laws in the secure CRM application. This paper has put infront of world a new security idea to protect the data of cloud users. It proposes of separation of secure storage and independent secure services into different cloud service providers. Storage of the data is take place at one cloud server and security service has taken another server. When a user sends unencrypted data from secure cloud service provider to independent secure cloud service system, then after independent secure cloud service encrypted data and then after sending it to secure storage cloud system. For the data decryption in the cloud is exactly reverse process of encryption system. In this system, the independent secure cloud service uses RC5 symmetric encryption/decryption algorithm.

This system will be beneficial for the end user and enhancing data security in cloud computing.

REFERENCES

1. Jing-Jang Hwang, Hung-kaiChung, Yi-Chang Hsu, Chien-Hsing Wu, *"A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service"* , IEEE 2011.
2. National Institute of Standards and Technology - Computer Security Resource Center - www.csrc.nist.gov
3. A. Weiss, *"Computing in the clouds"*, networker, vol. 11, no. 4, pp. 16-25, December 2007.
4. C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya, *"Autonomic metered pricing for a utility computing service"*, Future Generation Computer Systems, vol. 26, issue 8, pp. 1368-1380, October 2010.
5. M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," International Journal of Software:Practice and Experience, vol.32, pp. 1437-1466, 2002.
6. B. R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues,"in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.
7. R. Sterritt, "Autonomic computing," Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.
8. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.
9. L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.
10. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.
11. V. Miller, "Uses of elliptic curves in cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.
12. Norman D. Jorstad, Landgrave T. Smith, Jr., *"CRYPTOGRAPHIC ALGORITHM METRICS"* Institute for Defense Analyses Science and Technology Division, Jan 1997.
13. Harsh Kumar Verma, Ravindra Kumar Singh, *"Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms"* , in International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012.

AUTHOR PROFILE

Sachindra K. Chavan pursuing Master of Engineering in Information Technology from Smt. Kashibai Navale College of Engineering, Wadgoan Bk., Pune-41, Maharashtra- India. His interested area is Cloud Computing and Cryptography. He has author of one International paper and two national papers.

Prof. Manoj L. Bangare pursuing Ph.D . He has received a Master of Technology in Computer Engineering from College of Engineering, Pune. Maharashtra- India. He has 8 years experience in teaching and recently working in Smt. Kashibai Navale College of Engineering, Wadgoan Bk, Pune-41, Maharashtra-India. His current research interests area in Cloud Computing and information security. He has authored of two technical papers published in various prestigious international conferences.