International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-10)

Research Article | **October 2016**

RCT: A New Data Security Service for Cloud Computing Environment

[1]V. Poongodi, [2]Dr. K. Thangadurai

[1] Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India

[2] Head, PG & Research Dept. of Computer Science, Government Arts College, Karur, Tamilnadu, India

Abstract:

Many organizations are now migrating to the cloud computing technology. This technology has solved many problems of the traditional computing, such as handling peak loads (storage), installing software updates, high availability of services and maintenance for cloud customers at reasonable cost. Due to the fact that the services and information of many organizations are stored in the huge data centers which are reside in the third party control. Due to this lot of data security issues were exist. The data security issues are overcome by implementing cryptographic techniques but still the many research works are carried out to improve the cloud data security. In this paper a new data security algorithm is proposed to improve the data security in the cloud environment.

Keywords: Cloud Computing, Deployment Models, Data Security issues, cryptographic cloud storage, RCT.

I. INTRODUCTION

Cloud computing is an emerging technique to provide the software and hardware resources according to the customers' needs. In this technique everything is an internet based service where the user can easily use storage, services without knowing how it is actually working internally. Cloud computing is a collection of virtual machines in which user only uses the services provided by the virtual machines they don't have a control on virtual machines[1].

II. CLOUD DEPLOYMENT MODELS

The cloud computing technique offers three different deployment model namely, Public Cloud, Private Cloud and Hybrid Cloud [2].

- ***A. Public Cloud*** - In this the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services. Public cloud services may be free or offered on a pay per usage model. Owned and maintained by the cloud provider.
- ***B. Private Cloud*** - The cloud infrastructure is operated solely for an organization. The main advantage of using a private cloud is the security, compliance and QoS. Sometime it is risky to put sensitive data outside the organization and premises on a public cloud. Owned and operated by user organization.
- ***C. Hybrid Cloud*** - The cloud infrastructure is a combination of two or more clouds. It is used when a certain organization is not willing to put its data on public cloud but want to use the financial benefits of cloud data storage private cloud within public cloud. Owned and maintained by a cloud provider.

III. CLOUD SERVICES

In this technique it offers three different services such as Software as Service, Platform as a Service and Infrastructure as a Service[3].

- ***A. Software as a service (SaaS):***SaaS refers to the software available on the internet. It includes youtube, facebook, google applications.
- ***B. Platform as a service (PaaS):*** an operating system, hardware, and network are provided, and the customer installs or develops its own software applications. It include Amazon DB/S3, Google AppEngine.
- ***C. Infrastructure as a service (IaaS):*** provides just the hardware and network; the customer installs or develops its own operating systems, software and applications. Examples of IaaS providers include Amazon EC2, GoGrid, FlexiScale.

IV. CHARACTERISTICS OF CLOUD COMPUTING

Location Independence: it means location of device is not necessary for the user where it is located; the user only uses the services through internet. They don't need to know what kind of device is used by user or cloud; they only know how to use it [4].

- ***A. Multitenancy:*** it means a single piece of resource is used by multiple users. A single user is known as the tenant. So cloud provides a facility to use a single instance of resource across a large pool of users uses multiple redundant (copied) sites which make it well suitable for business and disaster recovery.
- ***B. Reliability:*** Measured service: it means cloud automatically measures about services, resources used by users and providing transparency from users.

- ***C. Scalability:*** modification of services quickly according to user's requirement without any problem in existing services.
- ***D. Security:*** due to centralization of data security is the main characteristics of data. It provides better security but need to increase the security level.
- ***E. On demand self-service:*** in which user can use the services according to their need without interference of the service provider.

V. DATA SECURITY ISSUES

Security of data in cloud is one of the key challenges which acts as an obstacle in the implementation of cloud computing. The data stored in the cloud get increased every day and hence there is a need to develop a new mechanisms to ensure that our data are stored in secured manner without any unauthorized access. Security for the data stored in the cloud environment [5] is a wanted one. The primary solution to deal with this difficult situation is to use the cryptographic methods in cloud environment.

VI. CRYPTOGRAPHIC CLOUD STORAGE

The data may get disclosed or modified by any unauthorized access. It is essential that a special care must be taken to protect our sensitive data. A secure storage [6] must be achieved in cloud computing. So we adopt cryptographic techniques for the secure storage. The data is encrypted by the data owner before the data is uploaded to the cloud. The major feature of a cryptographic storage is that the security properties that are described below are accomplished.

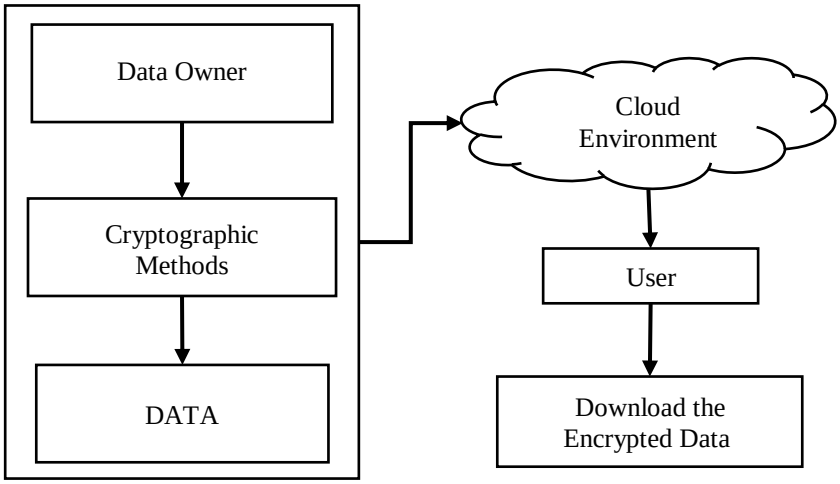

Fig 1. Cloud Strategy

The above fig1 represents cryptographic cloud storage. The owner of the data applies cryptographic methods to the sensitive data to protect the information from unauthorized access. The data owner uploads the encrypted data to the cloud environment. The authorized user can decrypt the data and download the required file.

VII. STRENGTH OF CRYPTOGRAPHIC CLOUD STORAGE

- ***A. Confidentiality:*** It provides confidentiality as the main characteristics. The information were encrypted with the advanced cryptographic techniques and thus the secrecy is maintained.
- ***B. Integrity:*** Cloud Storage provides Integrity to the data and thus it prevents any unauthorized people to modify the data.

VIII. MICROSOFT WINDOWS AZURE

Azure is Microsoft's Cloud computing offering to build and deploy applications on a Pay-per-use basis. Azure is a comprehensive set of storage, computing, and networking infrastructure services that reside in Microsoft's network of datacenters. Which provides a scalable infrastructure for consumer to run and host web based applications. To support cloud applications and data, Windows Azure has five components, as shown in fig 2.

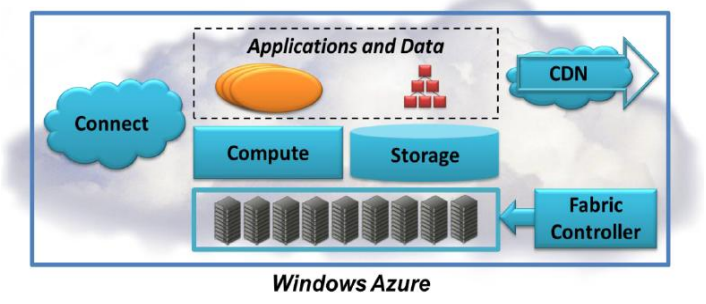

Fig 2: Windows Azure has five main parts: Compute, Storage, the Fabric Controller, the CDN, and Connect.

The AzureTM Services Platform (Azure) is an Internet-scale cloud computing and services platform hosted in datacenters created by Microsoft Corp., which provides an operating system and a set of developer services that can be used individually or together. The flexible and interoperable Azure platform can be used to build new applications to run from the cloud or enhance existing applications with cloud-based capabilities. Its open architecture gives developers the choice to build Web applications, applications running on connected devices, PCs, servers or hybrid solutions offering the best of both worlds(online and on-premise).

Compute: runs applications in the cloud. Those applications largely see a Windows Server environment, although the Windows Azure programming model isn't exactly the same as the on-premises Windows Server model.

Storage: Windows Azure provides multiple storage services that are highly durable, scalable as well as constantly available. Azure offers three types of storage services, BLOB, Table and Queues, which cater to unstructured, structured as well as transient data requirements.

Fabric Controller: deploys, manages, and monitors applications. The fabric controller also handles updates to system software throughout the platform.

Content Delivery Network (CDN): speeds up global access to binary data in Windows Azure storage by maintaining cached copies of that data around the world.

Connect: allows creating IP-level connections between on-premises computers and Windows Azure applications.

IX. PROPOSED WORK

Symmetric Algorithms

1.RC6 Algorithm

In cryptography, RC6 (Rivest Cipher 6) is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES)competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits, but, like RC5, it may be parameterized to support a wide variety of word-lengths, key sizes, and number of rounds. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations.

Encryption Algorithm

```
B = B + S[0]
D = D + S[1]
for i = 1 to r do
{
        t = (B*(2B + 1)) <<<lg w
        u = (D*(2D + 1)) <<<lg w
        A = ((A ⊕ t) <<< u) + S[2i]
        C = ((C ⊕ u) <<< t) + S[2i + 1]
                        (A, B, C, D)  =  (B, C, D, A)
}
A = A + S[2r + 2]
C = C + S[2r + 3]
```

Decryption Algorithm

```
C = C - S[2r + 3]
A = A - S[2r + 2]
for i = r downto 1 do
{
        (A, B, C, D) = (D, A, B, C)
        u = (D*(2D + 1)) <<<lg w
        t = (B*(2B + 1)) <<<lg w
        C = ((C - S[2i + 1]) >>> t) ⊕ u
        A = ((A - S[2i]) >>> u) ⊕ t
}
D = D - S[1]
B = B - S[0]
```

2.TORDES Algorithm

TORDES is a block cipher algorithm. It is a unique and independent approach which uses several computational steps along with string of randomized operators and delimiter selections by using some suitable mathematical logic with transformation and mirror image operation. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message in its class. It also safeguard against various attacks like Brute-force because it is not fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys. The following information invariably used inTORDES for encryption techniques.

1) 32 bit key.
2) Code sequence string generated from a particular process (Multithread).

3) Transformation of String.
4) Mirror image of String.
5) Lookup Table
6) Randomized delimiter string

RCT

In the proposed TOR security algorithm we used symmetric and asymmetric key cryptographic techniques. In this algorithm the computational speed is little complex and the size of the cipher text is also high to reduce the computational complexity and the size of the cipher text we used two symmetric key algorithm techniques in a hybrid form. The proposed RCT algorithm is used to enhance the data storage in the cloud environment. The proposed algorithm is integrated with two symmetric cryptographic techniques namely, RC6 and TORDES.

The working process of the proposed RCT algorithm is clearly explained in the following steps to know how the cloud users' data are stored in a highly secured way over the cloud storage environment.

STEP 1: *Researcher proposed security service algorithms using different hybrid cryptographic techniques.*
STEP 2: *The Proposed **RCT** algorithm is deployed in the cloud environment as security services.*
STEP 3: *The cloud users want to store their data in the cloud storage environment. For this user request any one of the cloud security services in the cloud environment.*
STEP 4: *The requested cloud security service is offered to the cloud user to encrypt or to decrypt their data.*
STEP 5: *Finally, the cloud users encrypt / decrypt or their data to store or to reterieve form the cloud storage environment.*

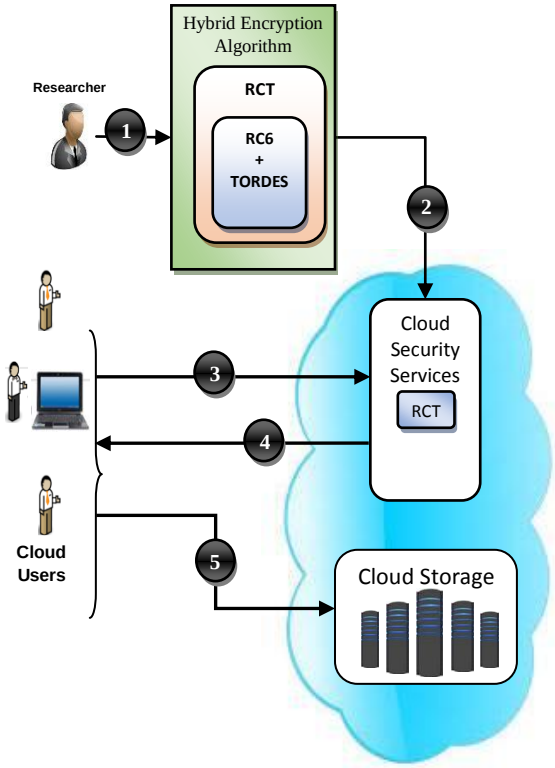

Fig 3. RCT Hybrid Security Service Algorithm

X. SIMULATION RESULT

The proposed algorithm is implemented using .NET. The simulation analysis is performed in the cloud environment (Microsoft Azure) with different data input. The time taken to Encrypt and Decrypt the given input data is calculated for the proposed RCT and Existing RSA, AES and BlowFish Algorithms. The results are compared and tabulated in table 1 and it is graphically represented in fig 4.

Table 1.Comparative Analysis based on Encryption Time

Size	**Algorithms**			
	RSA	**AES**	**Blowfish**	**RCT**
	Encryption Time(Minutes)			
1 MB	14.6754	13.9436	10.8872	8.9769
5 MB	19.7381	17.8764	13.7968	10.8976

10 MB	24.6786	21.7548	17.9647	15.7963
15 MB	27.8654	24.6979	21.6548	19.6875

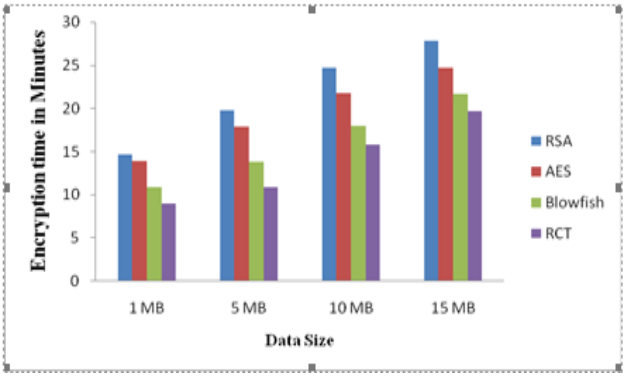

Fig 4. Comparative Analysis based on Encryption Time

Table 2 presents the performance comparison of decryption with existing techniques. The time taken by the existing and proposed decryption algorithms is calculated for different sizes of data.

Table 2.Comparative Analysis based on Decryption Time

Size	**Algorithms**			
	RSA	**AES**	**Blowfish**	**RCT**
	Decryption Time(Minutes)			
1 MB	11.9738	9.7382	7.6347	5.8945
5 MB	15.7357	13.8172	10.8796	9.7654
10 MB	20.6937	18.9073	15.9363	13.8673
15 MB	24.8392	20.6382	17.9826	15.6759

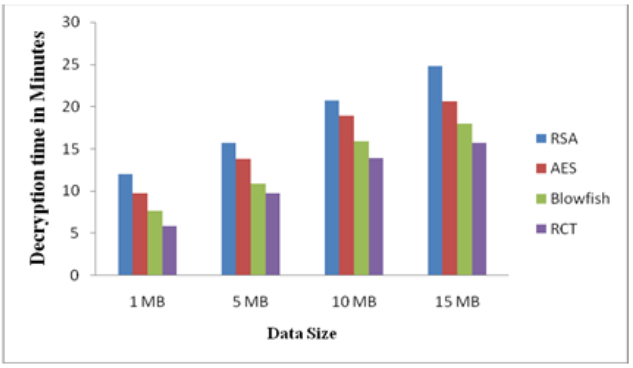

Fig 5. Comparative Analysis based on Decryption Time

Fig 5 presents the performance of existing and proposed algorithms based on the time taken for decryption process. The result shows that compared to the existing algorithms, the proposed RCT hybrid security algorithm has taken minimum time duration for decryption of different sizes of data

Table 3 and Fig 6 represent the comparison of security levels. The result shows that compared to the existing algorithms, RCT hybrid Security algorithm produces maximum security for cloud data. Security level of RCT is 85%, RSA is 82%, AES is 79% and Blowfish is 74%. RCT shows maximum security level when compared with existing encryption techniques.

Table 3. Comparison of Security Levels of Existing and Proposed Algorithms

Algorithms	**Security Level(%)**
BlowFish	74
AES	79
RSA	82
RCT	85

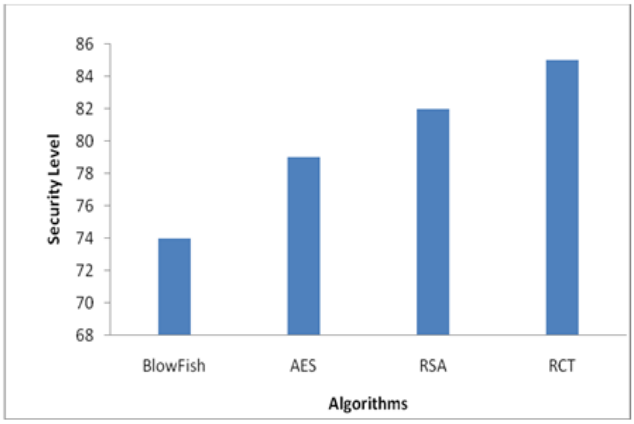

Fig 6. Comparison of Security Levels of Existing and Proposed Algorithms

XI. CONCLUSION

It is indeed that cloud computing can prove to be a boon in today's work environment hence this paper deals with data security issues related to cloud computing. This issue is overcome by proposing new data security algorithm using hybrid cryptographic technique is used. The proposed algorithm is converted into cloud security service. The proposed RCT cloud service is compared with the existing services and the result shows that the proposed algorithm improve the data security.

REFERENCES

[1] Security and privacy in cloud computing by Zhifeng Xiao and Yang Xiao in IEEE Communications Surveys and tutorials, 15.

[2] Data security in the world of cloud computing by Lori M. Kaufman John Harauz in IEEE Computer and Reliability society.

[3] Enhanced data security in cloud computing with third party auditor by Indrajit Rajput in International Journal of Advanced Research in Computer Science and Software Engineering, 3.

[4] Robust Data Security for Cloud while using Third Party Auditor by Abhishek Mohta,Ravi Kant Sahu and LK Awasthi, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol No. 2, Issue 2,Feb 2012.

[5] Cloud Data Security using Authentication and Encryption Technique by SanjoliSingla and Jasmeet Singh in IJARCET Vol 2, Issue 7, July 2013.

[6] Survey on triple system security in cloud computing by ParulMukhi and Bhawna Chauhan in IJCSMC, Vol. 3, Issue. 4, April 2014.

[7] Enhancing security in cloud computing structure by hybrid encryption by Aparjita Sidhu and Rajiv Mahajan in International Journal of Recent Scientific Research Vol. 5, Issue, 1, pp.128-132, January, 2014.

[8] Data Security in Cloud Computing by K. S. Wagh, SwapnilChaudhari, Anita Deshmukh and PrajaktaKhandave in International Journal of Current Engineering and Technology.

[9] A proficient model for high end security in cloud computing by R. BalaChandar, M. S. Kavitha and K. Seenivasan in ICTACT journal on soft computing ,january 2014, volume: 04, issue: 02.

[10] Enhancing Data Storage Security in Cloud Computing Through Steganography by MrinalKanti Sarkar and Trijit Chatterjee in ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014.

[11] Enhancing Security in Cloud computing using Public Key Cryptography with Matrices by BirendraGoswami and Dr.S.N.Singh in Vol. 2, Issue 4, July-August 2012, pp.339-344.

[12] Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment by VarshaYadav and Preeti Aggarwal in IJCSMC, Vol. 3, Issue. 5, May 2014.

