INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SECURITY FOR MULTI-CLOUD USING RC5 ALGORITHM

J. Jayashri[1], V. Priyadharshini[2], S. Mahima[3], N. Kohila[4]

[1](M.Phil) Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Namakkal, jayashrimbs@outlook.com
[2](M.Phil) Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Namakkal, priyaadharshini@hotmail.com
[3]Assistant Professor, Vivekanandha College of Arts and Sciences for Women, Namakkal, blessie_john@yahoo.com.
[4]Assistant Professor, Vivekanandha College of Arts and Sciences for Women, Namakkal, padmeeshraj@gmail.com.

Abstract

Cloud Computing is technology for next generation Information and Software enabled work that is capable of changing the software working environment. It is interconnecting the large-scale computing resources to effectively integrate, and to computing resources as a service to users. Cloud computing allows users to use applications without installation any application and access their personal files and application at any computer with internet or intranet access. Cloud computing effectively the actual separation of physical and virtual services, a variety of business services reduced costs, improved utilization of network resources. However, users have security concerns as they outsource their valuable business data to cloud and treat the cloud as "untrusted". With a single cloud service provider there might be the risk of service availability, failure possibility and insider theft of data. Moving towards multiple clouds or inter-clouds or clouds-of-clouds can address security problems. This paper aims of investigating how multi-cloud deployments can reduce security risk by using security algorithm.

Keywords: Cloud Computing, Multi-cloud infrastructure, Storage, Security, Encryption.

1. Introduction

Cloud computing becomes the boom invention of today internet world .It is being used by many organizations and the benefits are realized by general public in many ways. The services include Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS). These services can be used by cloud users in pay per use fashion without investment. Cloud service providers such as IBM, Microsoft, Amazon, and Oracle and so on are providing various kinds of cloud services. Through this technology users can consume services at any time by their particular needs. Before cloud computing, users have to buy individual or costly software, hardware resources but now it become easy to access the services on demand over the network. It facilitates the user to access shared

resources, common infrastructure or database resources, for as long as they need, without thinking about the cost and maintenance of resources.

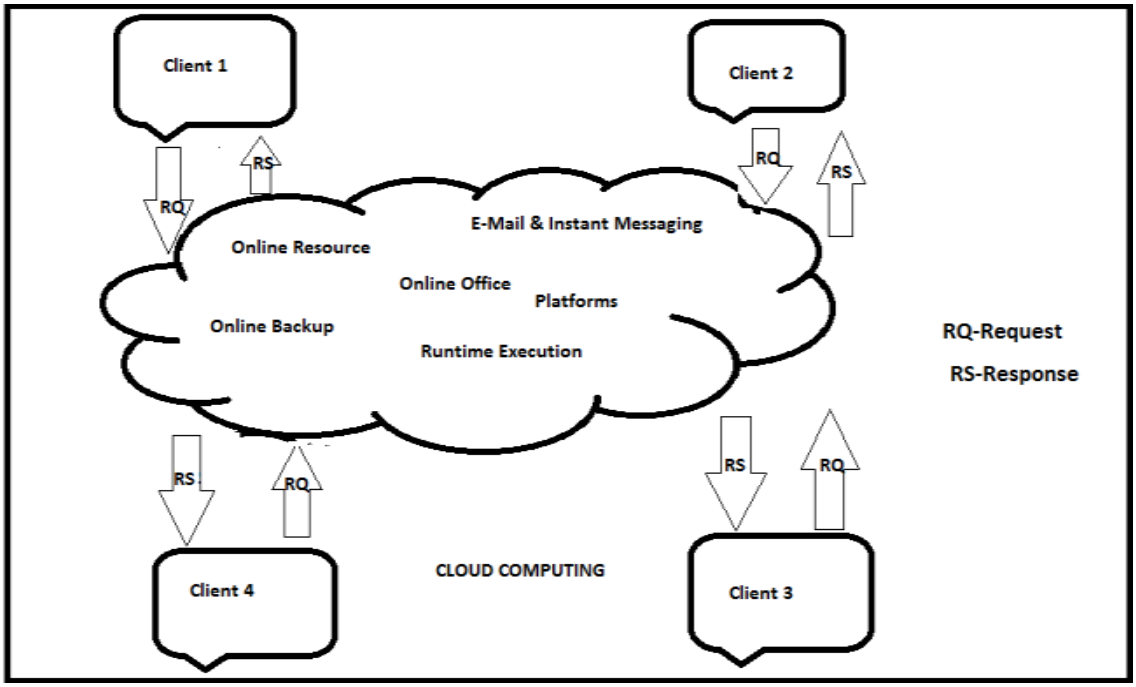

Figure 1: Cloud Computing Architecture

Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multiclouds", "intercloud" or "cloud-of-clouds".

2. Multi-cloud Architecture

The term "multi-clouds" is similar to the terms "interclouds" or "clouds-of-clouds". The cloud computing should not end with single cloud. A cloudy sky incorporates different colors and shapes of clouds which lead to different implementation and administrative domains.
There are two layers in a multi-cloud environment:

- Inner-cloud
- Inter-cloud

Multi cloud infrastructure can be exposed to the public has utility computing. The use of multiple clouds enables the following advantages:

1. Import and export data from various clouds.
2. Enables "choice" ability to move clouds easily based on price and Service Level Agreement.
3. Stops vendor lock-in;

4. Automated synchronization of different clouds;
5. Fault tolerance with primary back and high availability of data;
6. Infrastructure cost reduction.

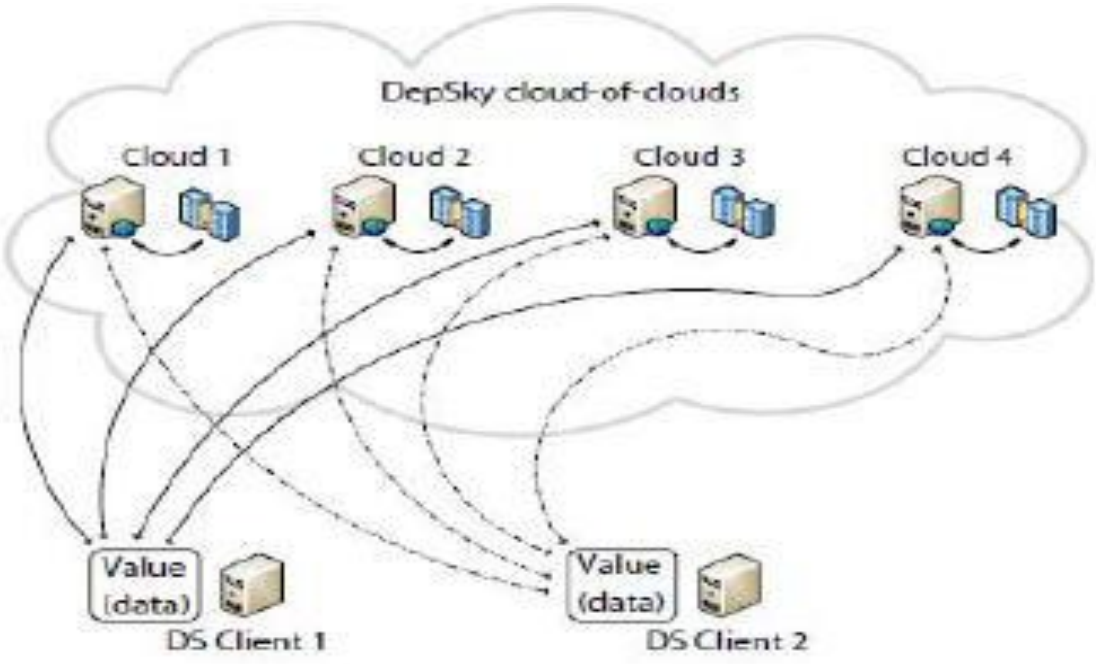

Figure 2: Multi-cloud Architecture

As can be seen in fig. 2, it is evident that the architecture has provision for multiple clouds. The data outsourced by clients can store in any cloud. It does mean that the multiple clouds work together. This will automatically improve service availability and reduce the risk of losing data as well. With regard to internal theft strict measures are to be used by cloud service providers.

2.1 Security Issues

In the multi-cloud architecture we have meet some security problems depends on the service providers. There are multiple security issues for cloud computing and it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

There is a critical need to securely store, manage, share and analyze massive amounts of data and to improve the quality of services. Because of the critical nature of the applications, it is important that clouds to be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. There are different Security Issues shown in figure 3. To overcome the above security problems we encounter some Security Algorithm.

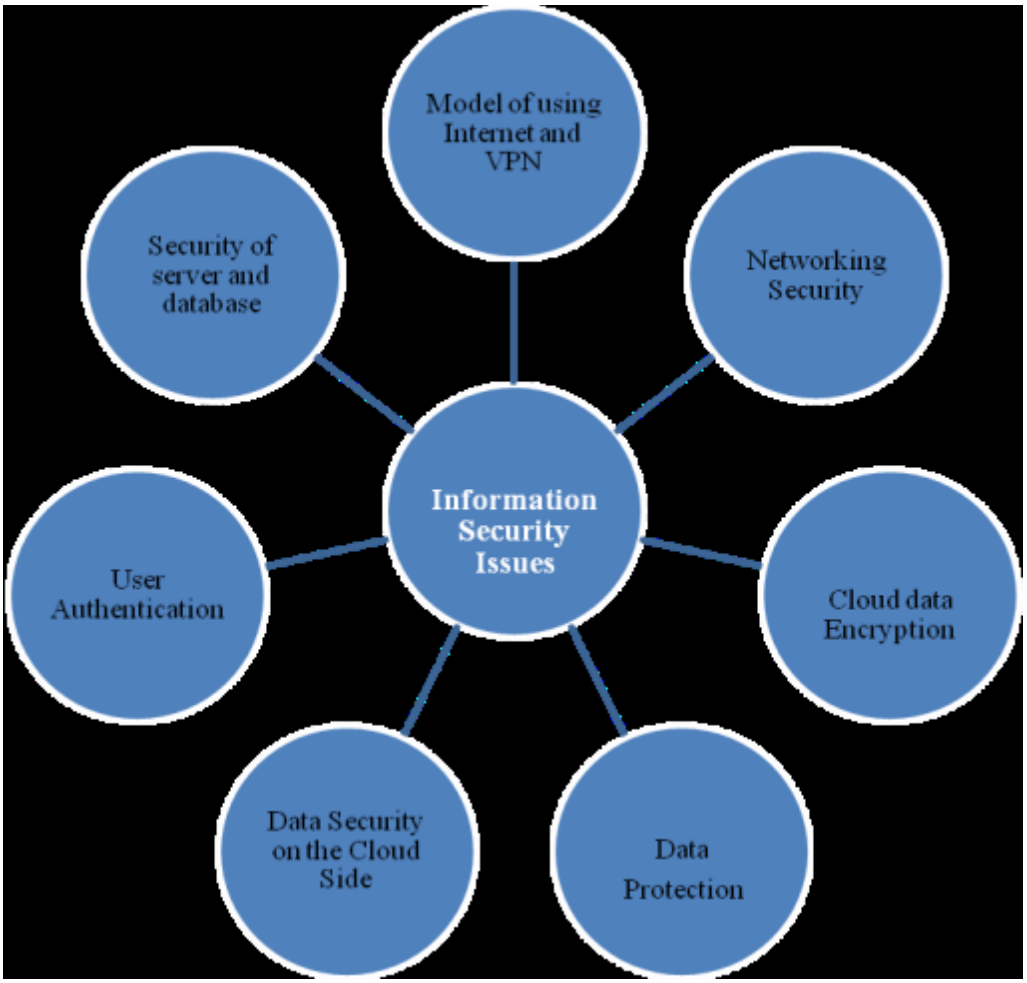

Figure 3: Security issues on multi-cloud

3. Related Work

Multi-cloud technique is the use of two or more cloud services to minimize the risk of large amount of data loss or temporary fault in the computers due to a localized component failure in a cloud computing environment. In multi-cloud environment a lot security problems arises, so some security algorithms are used to provide security for data such as secret-sharing algorithm, RSA algorithm etc.

In this paper, we use RC5 algorithm for encryption, multi-cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key cannot be restored. Only the user knows the key, the multi-clouds do not know the key. Also, because the properties of encryption, the multi-cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage.

4. RC5 Algorithm

RC5 is a fast symmetric block cipher suitable for hardware or software implementations. A novel feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable word size, a variable number of rounds, and a

variable-length secret key. RC5 is exactly designated as RC5-w/r/b, where w denotes word size in bits, the standard value is 16,32 and 64 bits; r denotes number of rounds and allowable value ranges from 0 to 255; b denotes length of user's secret key in bytes and the allowable value ranges from 0 to 255.

The RC5 Algorithm consists of three components of:

- Key expansion algorithm
- Encryption algorithm
- Decryption algorithm

a. Key-Expansion Algorithm

The user supplies a key of b bytes, copy the secret key K[0...b-1] into an array L[0..c-1] of c = ceil(b/u), where u = w/8 in little-endian order. In other words, we fill up L using u consecutive key bytes of K. Any unfilled byte positions in L are zeroed. 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 Constants Pw and Qw are defined for arbitrary w as follows:
Pw = Odd ((e -1) 2w) … (1)
Qw = Odd ((v - 1) 2w) … (2)
Where
e is the base of natural logarithms (e = 2.718281828459) and
v is the golden ratio (v =1.618033988749)
Odd (x) is the odd integer nearest to x [2].

b. Encryption

We assume that the input block is given in two w-bit registers A and B. We also assume that key-expansion has already been performed, so that the array s[0…t-1] has been computed. Here is the encryption algorithm is pseudo-code:

```
A=A+S[0];

B=B+s[1];

for i=1 to r do

A = ((A Xor B) <<< B) + S[ 2 * i ];
B = ((B Xor A) <<< A) + S[ 2 * i + 1];
```

The output is in the registers A and B. We note the exceptional simplicity of this 5-line algorithm. We also note that each RC5 round updates both registers A and B, whereas a "round" in DES updates only half of its registers. An RC5 "half-round" (one of the assignment statements updating A or B in the body of the loop above) is thus perhaps more analogous to a DES round.

c. Decryption

The decryption routine is easily derived from the encryption routine.

```
for i = r down to 1 do
B = ((B -S[2 * i + 1] >>> A) Xor A;
A = ((A -S[2 * i] >>> B) Xor B;
B = B -S[1];
A = A -S[0];
```

Data dependent rotations – amount of rotation is not pre-determined. The behavior of each round is different as the rotation amount is different. Each round ends by adding expanded key from S
It was experimentally determined that after eight rounds in RC5-32, each message bit affected some rotation amount.

5. Conclusion

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We support the migration to multi-clouds due
to its ability to decrease security risks that affect the cloud computing user. Security problems must be the first priority and thus switching of connection between the clouds must be with immediate. Through RC5 algorithm we provide security for data which are stored in multi-cloud.

REFERENCES

1. Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences,2012.
2. Shaik.Aafreen Naaz, Pothireddygari.Ramya, P.Vishunu Vardhan Reddy. "Cloud Computing: Use of Multi-Clouds".
3. Vinod Kumar Paidi, P.Varaprasada Rao."Multi-Cloud Architecture to Reduce Security Risks in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering**, Volume** 3, Issue 8, August 2013.
4. E.Sathiyamoorthy, S.S.Manivannan "An Efficient and Light weight Secure Framework for Applications of Cloud Environment using Identity Encryption Method" , International Journal of Engineering and Technology (IJET).
5. Jay Singh, Brajesh Kumar, Asha Khatri."Securing Storage Data in Cloud Using RC5 Algorithm", "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds", International Journal of Advanced Computer Research, December-2012.
6. Rivest, R. L. (1994). "The RC5 Encryption Algorithm" (pdf). *Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994e. pp. 86–96.* http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf
7. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloudcomputing", Journal of Network and ComputerApplications, 34(1), 2011, pp 1-11.
8. M.M.Boroujerdi, S.Nazem, "Cloud Computing: Changing Cogitation about Computing", World Academy of Science, Engineering and Technology, December 2009, p.58.
9. C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuringdata storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication andComputing, 2010, pp. 1-9.