International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-12 September-2013

Data sharing and Management based on RC4 in User Cloud Environment

Sanjay Kumar Brahman[1], Brijesh Patel[2]

Abstract

There is vast demand of cloud computing are increases in the today's era because of the on demand service of cloud computing. Our paper main direction is to make data communication better in the cloud environment. It means secure communication will be provided for preventing unauthorized access. We proposed an efficient approach by using RC4 mechanism to support encrypted data transmission in cloud environment. We also test our results based on the software measures like F-Measure (FM), Odd Ratio OR and Power (PO) which emphasize on the effectiveness of our approach.

Keywords

Cloud computing, data sharing, rc4, Encryption

1. Introduction

In today's discretion the cloud platform is to engagement substantial amount of data. Dim Make-thither supports ramble processing in very efficient manner[1]. In capitalistic go if we attend not far from combine wide edge computing machines it is formidable , but adapt an era it is possible by cloud computing. Fro are revision accountability appearance it is wearisome to achieve the machines unhesitatingly one needs them. It is vigorous to gain wholly of all over those machines when the job is done [2][3][4][5]. Cloud invention provides connect additional assistance and solves the problem with different segmentation [6].

Management is under pressure to ensure adequate mitigation of risks to reduce the impact on business. The strategy for risk finding are not fully developed so this direction is also vacant for researchers. [7][8][9].The focus of this paper is to provide recommendations for the mitigation of cloud computing security risks as a fundamental step towards the development of guidelines and standards

for secure cloud computing environments from both aspect of client and server. The ritual afford by dreary evolve into distinguished on the Internet, users are nearly and close by resorting to grant-in-aid providers for publishing resources shared with others.

Service providers are requested to realize data and service outsourcing architecture on a wide scale. Their basic assumption that service providers have complete access to the stored resources is not applicable for all actual scenarios such as outsourcing sensitive data. We come with the encryption techniques instead of the legal protection offered by contracts when enforcing access control, i.e., the data owner encrypts data, sends cipher texts to the service providers for storage, and distributes the corresponding key to authorized users [10], [11], [12],[13],[14].

Cloud computing has emerged as a handful of the outdo fluorescent and disobedient technologies of our time [15][16][17][18][19]. This progressive first-rate utilizes pair cool technological development utility computing and assist oriented architecture—to house the users (individuals, SMEs and enterprises) with a highly scalable, pay-per-use, everything as a-promote chisel for IT superintendence. Differing of the bestowal depart variety the stupid computing promote delivery model are scalability/elasticity, on-demand service stock, base resource pooling, multi-tenancy hosting, utility pay-as-you-use pricing and abstraction of lower layers. These colophons around push to unite matter drivers depart beg numbing computing an attractive service delivery model from a customer's point of view. They regard benefit payment reduction, increased IT agility [20].

The rest of this paper is arranged as follows: Section 2 describes about recent scenario; Section 3 shows the shows the proposed approach. Section 4 shows the result analysis. Section 5 describes Conclusion.

2. Literature Review

In 2010, Saira Begum et al. [21] analyses that Cloud computing is a massively central advancement in the technique that businesses and users devour and work on computing. It's a elementary modify to an prepared model in which applications don't subsist out their lives on a specific section of hardware and in which possessions are more supplely deployed than was the historical standard. It's a primary shift to expansion and utilization model that replaces hard-wired, proprietary associations surrounded by software components and the clients of those components with unimportant Web services and Web-based software admittance.

In 2010, Sang-Ho Na, et al. [22] proposed analyze security threats and requirements for previous researches and propose service model and security framework which include related technology for implementation and are possible to provide resource mobility.

In 2011, Siyuan Xin et al. [23] proposed about the property-based remote attestation mechanism in Trusted Computing is imported into clouding computing, and a property-based remote attestation method oriented to cloud computing is designed based on the characteristics of cloud computing. In this method, through the attestation proxy, the remote attestation of the computing platform's security property is realized without disclosing the platform's configuration, and users can validate the security property of the actual computing platform in the virtual cloud computing environment.

In 2012, Hiroaki YUZE et al. [24] studied a safety confirmation system for the students in the University of Shizuoka, Japan, since 1999 in order to consider with Tokai Great Disaster. However, our safety confirmation system has been enlarged by additional functions such as not only for earthquakes but also pandemic information by new types of influenza virus. Thus, the functions and managements of the system have been reconsidered from the experience of the disaster, and the renewal system is constructed with the cloud computing type architecture. They report how their safety confirmation system used under the Great East Japan Earthquake by the analysis of the registrations' logs. Then, the selection of the system's functions by the conditions of the earthquake is reported.

3. Proposed Approach

In this paper we present an efficient way of data communication on cloud environment. The flowchart of figure 1 shows the effectiveness of our approach. Our approach is mainly divided on three parts:

1) RC4 Encryption
2) Chi-Square Test
3) F-Measure (FM), Odd Ratio OR and Power (PO).

The unsympathetic principal or well-balanced algorithm is the quickest and simplest encryption algorithm in widespread use today. We take the concept of encryption from [25].
The terms are following which are used in our approach.
Cipher text – Encrypted Plain text.
Key – The key is applied for achieving in its original form.
Encryption – Plain text to Cipher text conversion.
Decryption – Cipher Text to plain text conversion.

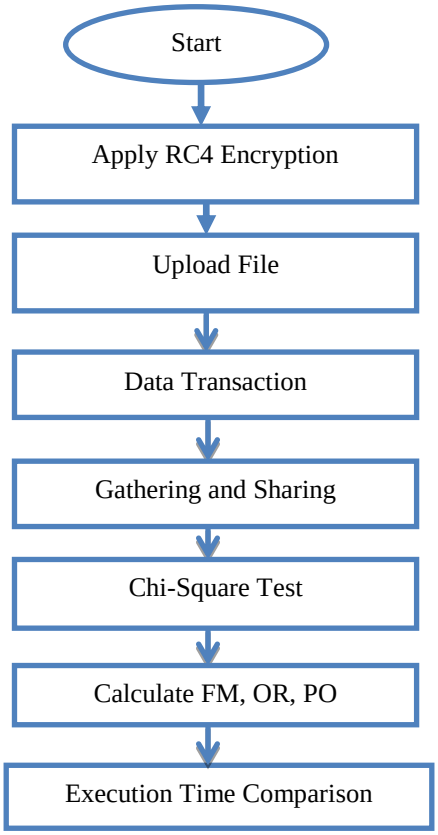

Figure 1: Flowchart for the proposed approach

The vital want alongside is the pronouncement "sensible" in deal it is surrounding ever after mathematically calling-card to interpret the ciphertext without a root. The goal is to feel sorry it consequently back-breaking (usually in order of likely computing power) range it is pule practical to do this decryption - basically a week, year, decade or whatever timescale is required. This is usually achieved by authoritarian the key space, longer keys around longer to ruin, but enquire after alongside computing power to encrypt and decrypt with in the first place.

Algorithm: RC 4[16]
Stream cipher symmetric key
Use two arrays, state and key
1. 256-byte state table.
State [256]=[0 .. 255]
2. It has the capability of using keys between 1 and 2048 bits.
Key [1..2048] = […….]

Two phases
‰ Key Setup
1. f = (f + Si+ Kg) mod 4

2. Swapping Siwith Sf
‰
Ciphering (XOR)
1. i = (i + 1) mod 4 , and f = (f + Si) mod 4
2. Swaping Si with Sf
3. t = (Si+ Sf) mod 4

The steps for RC4 encryption algorithm is as follows:
1- Get the data to be encrypted and the selected key.
2- Create two string arrays.
3- Initiate one array with numbers from 0 to 255.
4- Fill the other array with the selected key.
5- Randomize the first array depending on the array of the key.
6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text.

4. Result Analysis

We can test our hypothesis by Chi-Square test which is shown in Figure 3. We will always have a null hypothesis which states that the observed distribution is not significantly different from the expected distribution and of course use words relevant to that particular problem [20].

The decision rule for this test will always be $\chi^2 < \chi_c^2$ where the critical value has to be read from the χ^2 distribution table. The only two numbers needed to look up this critical value are the level of significance α and the number of degrees of freedom. The degrees of freedom for this test will be defined as the number of categories minus 1[19].

The test statistic is $\chi^2 = \sum \frac{(E-O)^2}{E}$ where E and O are the expected and observed frequencies per category. The chi-square test will be used to test for the "goodness to fit" between observed and expected data [20].

Then we apply three parameters for finding the best among them. The parameters are F-Measure(FM), Odd Ratio OR and Power(PO).
A measure that combines precision and recall is the harmonic mean of precision and recall, the traditional F-measure or balanced F-score:
FM= (2* Precision *Recall)/(Precision + Recall)
The odds ratio is a measure of effect size, describing the strength of association or non-independence between two binary data values.
OR=2* Recall (1-Precision) /(1-Recall*Precision)
Power (PO) is defined as:
PO= ((1-Precision)k-(1-Recall)k)

Table 1: FM Ratio

		FM			
Sno	**filename**	**class**	**object**	**inheritance**	**dma**
1	ConvolveFilter.java	0.43	0.24	0.43	0.24
2	frequent.java	0.43	40.56	0.43	40.56
3	GaussianFilter.java	0.24	0.03	0.43	0.03
4	NewJFrame.java	0.43	0.43	0.43	0.43
5	pass5.java	0.43	25.63	0.43	25.63
6	pass6.java	0.43	25.63	0.43	25.63
7	pat_Option2.java	0.43	2.67	0.43	2.67
8	pat_report.java	0.43	16.67	0.43	16.67
9	PixelUtils.java	0.43	0.11	0.67	0.11
10	pur_result.java	0.43	18.03	0.43	18.03
11	result_ass.java	0.43	18.03	0.43	18.03
12	roger_method.java	0.43	44.83	0.43	44.83
13	Second.java	0.43	47.04	0.43	47.04
14	show_disease.java	0.43	19.44	0.43	19.44
15	show_min.java	0.43	6	0.43	6
16	Update_data.java	0.43	32.67	0.43	32.67

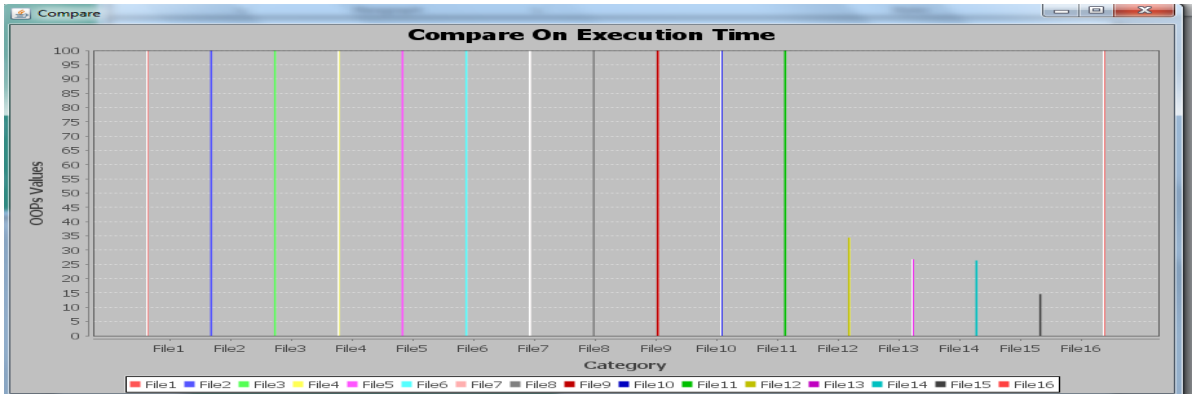

Figure 2: Compare Based on Execution Time

Table 2: OR Ratio

OR					
Sno	**filename**	**class**	**object**	**inheritance**	**dma**
1	ConvolveFilter.java	0.14	0.12	0.14	0.12
2	frequent.java	0.14	0.98	0.14	0.98
3	GaussianFilter.java	0.12	0.02	0.14	0.02
4	NewJFrame.java	0.14	0.14	0.14	0.14
5	pass5.java	0.14	0.98	0.14	0.98
6	pass6.java	0.14	0.98	0.14	0.98
7	pat_Option2.java	0.14	0.86	0.14	0.86
8	pat_report.java	0.14	0.96	0.14	0.96
9	PixelUtils.java	0.14	0.07	0	0.07
10	pur_result.java	0.14	0.97	0.14	0.97
11	result_ass.java	0.14	0.97	0.14	0.97
12	roger_method.java	0.14	0.99	0.14	0.99
13	Second.java	0.14	0.99	0.14	0.99
14	show_disease.java	0.14	0.97	0.14	0.97
15	show_min.java	0.14	0.91	0.14	0.91
16	Update_data.java	0.14	0.98	0.14	0.98

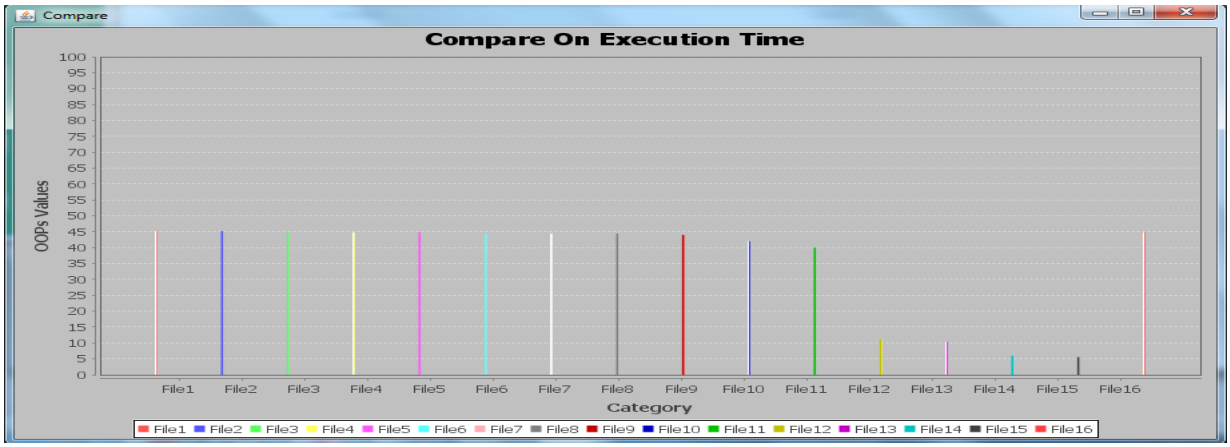

Figure 3: Compare Based on Execution Time

Table 3: PO Ratio

PO					
Sno	**filename**	**class**	**object**	**inheritance**	**dma**
1	ConvolveFilter.java	-0.33	-0.26	-0.33	-0.26
2	frequent.java	-0.33	2715.29	-0.33	2715.29
3	GaussianFilter.java	-0.26	-0.04	-0.33	-0.04
4	NewJFrame.java	-0.33	-0.33	-0.33	-0.33
5	pass5.java	-0.33	1069.79	-0.33	1069.79
6	pass6.java	-0.33	1069.79	-0.33	1069.79
7	pat_Option2.java	-0.33	8	-0.33	8
8	pat_report.java	-0.33	443.75	-0.33	443.75
9	PixelUtils.java	-0.33	-0.14	-0.25	-0.14
10	pur_result.java	-0.33	521.33	-0.33	521.33
11	result_ass.java	-0.33	521.33	-0.33	521.33
12	roger_method.java	-0.33	3323.67	-0.33	3323.67
13	Second.java	-0.33	3663.48	-0.33	3663.48
14	show_disease.java	-0.33	608.57	-0.33	608.57
15	show_min.java	-0.33	51.75	-0.33	51.75
16	Update_data.java	-0.33	1751.75	-0.33	1751.75

Figure 4: Compare Based on Execution Time

5. Conclusion

In this paper we present an efficient approach where we upload the data using RC4 encryption standard. Then for testing we apply chi square test to find the optimal points which are authentic for registration in the cloud. That is validated by software measurements like FM, PO and OR. Finally by analysis the results show the effectiveness of our approach.

References

[1] Mr. Ajey Singh,Dr. Maneesh Shrivastava "Overview of Security issues in Cloud Computing",International Journal of Advanced Computer Research (IJACR) Volume 2,Number 1,March 2012.

[2] Igor Ruiz-Agundez, Yoseba K. Penya and Pablo G. Bringas, "Cloud Computing Services Accounting",International Journal of Advanced Computer Research (IJACR) ,Volume 2, Number 2, June 2012.

[3] Hai Zhong, Kun Tao, Xuejie Zhang , "An Approach to Optimized Resource Scheduling Algorithm for Open-source Cloud Systems", The Fifth Annual China Grid Conference, 2010.
[4] Mrs. Shital Patil ,Prof. R. A. Kulkarni, "Improving Performance Guarantees in Cloud Computing through Efficient and Dynamic Task Scheduling", International Journal of Advanced Computer Research (IJACR),Volume-2 Number-4 Issue-6 December-2012.
[5] Bharat Prajapat and Dr.Manish Shrivastava, "Mobile Cloud Computing through J2ME application: Cloud Enabled Web Services", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4 Issue-6 December-2012.
[6] M.Malathi, "Cloud Computing Issues-A Survey",International Journal of Advanced Computer Research (IJACR) Volume 2 Number 2 June 2012.
[7] I. Berger "Keeping Cloud Computing's Prospects Safe and Sunny", May 2010.
[8] K. McCabe and R. Nachbar. ,"Survey by IEEE and Cloud Security Alliance Details Importance and Urgency of Cloud Computing Security Standards", October 2010.
[9] Centre for the Protection of National Infrastructure (CPNI),"Information Security Briefing", 2010.
[10] A. Ceselli, E. Damiani, S. De Capitani di Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati. Modeling and assessing inference exposure in encrypted databases. ACM Trans. on Information and System Security 8, 1, pp. 119-152, 2005.
[11] H. Hacigumus, B. Iyer, and S. Mehrotra. Providing database as a service. In Proc. of ICDE'02. IEEE Computer Society, Washington, pp. 29-39, 2002.
[12] H. Hacigumus, B. Iyer, and S. Mehrotra, and C. Li . Executing SQL over encrypted data in the database-service-provider model. In Proc. of ACM SIGMOD'02. ACM, New York, pp. 216-227, 2002.
[13] S. De Capitani di Vimercati, S. Foresti, S. Jajodia. Preserving Confidentiality of Security Policies in Data Outsourcing. Proceedings of the 7th ACM workshop on Privacy in the electronic society, pp. 75-84, 2008.
[14] Yang Zhang,Jun-Liang Chen. A delegation solution for universal identity management. IEEE Transactions on Services Computing, 2011.3, pp. 70-81, 2011.
[15] Astha Pareek, Dr.Manish Gupta, "Review of Data Mining Techniques in Cloud Computing Database", International Journal of Advanced Computer Research (IJACR) Volume 2 Number 2 June 2012.
[16] Mr. Sanjay Kumar Brahman,Prof. Brijesh Patel," Java Based Resource Sharing with Secure Transaction in User Cloud Environment", International Journal of Advanced Computer Research (IJACR) Volume-2 Number-3 Issue-5 September-2012.
[17] Deepak Mishra, Dr. Manish Shrivastava, "Economic Price Estimation for cloud business",International Journal of Advanced Computer Research (IJACR), Volume-2,Number-4,Issue-6 December-2012.
[18] Zhengxiong Hou, Xingshe Zhou, Jianhua Gu,Yunlan Wang, Tianhai Zhao, "ASAAS: Application Software as a Service for High Performance Cloud Computing", 2010 12th IEEE International Conference on High Performance Computing and Communications.
[19] Abdur Rahim Choudhary," Baseline Requirements and Architecture for Cloud Computing Services", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4 Issue-7 December-2012.
[20] Sampada Kembhavi , Ravindra Gupta , Gajendra Singh," An Efficient Algorithm for Auto Upload and Chi-Square Test on Application Software", nternational Journal of Advanced Computer Research (IJACR), Volume-3 Number-2 Issue-10 June-2013.
[21] Saira Begum and Muhammad Khalid Khan, "Potential of Cloud Computing Architecture" , 2010 IEEE.
[22] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, "Personal Cloud Computing Threats", 2010 IEEE Asia-Pacific Services Computing Conference.
[23] SiyuanXin, Yong Zhao, Yu Li," Property-Based Remote Attestation Oriented to Cloud Computing" , 2011 Seventh International Conference on Computational Intelligence and Security.
[24] Hiroaki YUZE and Naoyoshi SUZUKI, "Development of Cloud Based Safety Confirmation System for Great Disaster", 2012 26th International Conference on Advanced Information Networking and Applications Workshops.
[25] Ashutosh Kumar Dubey,Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava," Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG 2012.

I completed my B.Sc. (PCM) from RDVV University Jabalpur in 2005. Then I completed my MCA from RKDF Instiute of science & technology-MCA, (RGPV Bhopal) in 2008. Currently I am pursuing my M.Tech from Shriram Instiute technology, Jabalpur, M.P in Computer Science branch.