International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-3 Issue-5 September-2012

Java Based Resource Sharing with Secure Transaction in User Cloud Environment

Sanjay Kumar Brahman[1], Brijesh Patel[2]
PG scholar in Department of CTA, SRIT Jabalpur[1]
HOD, Computer Science, SRIT Jabalpur[2]

Abstract

The increased degree of connectivity and the increasing amount of data has led many providers and in particular data centers to employ larger infrastructures with dynamic load and access balancing. This lead to the demand of cloud computing. But there are some security concerns when we handle and share data in the cloud computing environment. In this paper we proposed a trusted cloud environment. In this environment we upload the data after applying private-key cryptography. In this a secret key may be held by one person or exchanged between the sender and the receiver of a message. The cloud admin can read the data after applying the same key for decryption. If the Admin want to update the data then again a decryption key is needed but it is different from the reading key. We also provide sharing of data which is based on the deployment model of the cloud architecture.

Keywords

Private key cryptography, deployment model, cloud, secret key

1. Introduction

In today's era the main problem is to process large amount of data. Cloud Architecture supports that processing in very efficient manner. In conventional approach if we need about several large scale computing machines it is difficult , but now a days it is possible by cloud computing. There are other difficulties like it is difficult to get the machines when one needs them. It is difficult to distribute and coordinate a large-scale job on different machines, run processes on them, and provision another machine to recover if one machine fails. It is difficult to auto scale up and down based on dynamic workloads. It is difficult to get rid of all those machines when the job is done. Cloud architecture provides several different services and solves the problem with different segmentation.

Cloud computing has emerged as one of the most promising and challenging technologies of our time. This new paradigm utilizes two separate technological development utility computing and service oriented architecture to provide the users (individuals, SMEs and enterprises) with highly scalable, pay-per-use, everything as a-service model for IT delivery. Some of the properties that characterize the cloud computing service delivery model are scalability/elasticity, on-demand service provisioning, shared resource pooling, multi-tenancy hosting, utility pay-as-you-use pricing and abstraction of lower layers. These characteristics give rise to several business drivers that make cloud computing an attractive service delivery model from a customer's point of view. They include capital expenditure reduction, increased IT agility, faster return on investment, resilient infrastructure leading up to better business continuity.

As with any technology, though, cloud computing raises many concerns including security, management and control, disaster recovery and business continuity, supplier management, regulations and legislations, and the lack of standards and guidelines. In order to minimize the impact of these concerns, risk mitigation is imperative if organizations want to take advantage of the many benefits of cloud computing while protecting and safeguarding systems and data.

Management is under pressure to ensure adequate mitigation of risks to reduce the impact on business. Risk mitigation strategies and the implementation of controls are further complicated since standards and guidelines dealing with cloud computing security do not exist [1][2][3].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 services offer by cloud become popular on the Internet, users are more and more resorting to service 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 [4], [5], [6],[7],[8].

We provide here an overview of cloud computing. The rest of this paper is arranged as follows: Section 2 describes about recent scenario; Section 3 shows the problem domain; Section 4 shows the proposed approach. Section 5 describes Conclusion and outlook.

2. Recent Scenario

In 2010, Saira Begum et al. [9] 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. [10] 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. [11] 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. [12] 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. Problem Domain

Zhidong Shen et al. [13] observe that the cloud computing developed from the grid computing technology and paid attention to provide distributed service to different users. A typical cloud model described by Frank Gillett [14] is shown in Figure 1 , that model does not seem to address end-to-end management. Ultimately, the cloud service infrastructure [14] must provide end-to-end service assurance to meet both service creation and service delivery platform user requirements. The service creators must be able to develop services rapidly using reusable and collaborating service components available globally. The infrastructure must also accommodate billions of users globally who will contribute to wildly fluctuating workloads.

Web Based Service	**Software as a Service**
Application Component as a Service	
Software Platform as a Service	
Virtual Infrastructure as a Service	
Physical Infrastructure as a Service	

Figure 1: Cloud Computing Model

The above model shows the aspect of client server interaction in the network. It also focuses on the requirement of the security which is following [13]:

Confidentiality: The information belongs to different owners in the cloud computing resources should be open to the trusted objects.
Dynamic of the services: The cloud computing system should also be able to provide services to users dynamically. This dynamic mechanism gives the user convenience to use the services and

resources in the cloud computing environment. The trust among the participant. As described above, the participants, including users, local organizes and distributed resources, should build trust relationships among the entities that will have mutual operation to each other. The trusted relation is based on the authentication.

Dynamically building trust domains: In the cloud computing system, participants need to organize dynamically to solve different problems. Instead of the above things ashutosh dubey et al. [15] focuses on different security prospectus for a trusted cloud computing. Which includes malicious insiders, data sharing security, data loss and security of API and Interfaces in cloud computing.

4. Proposed Approach

Our trusted computing system model is categorized in two parts. First part describes the working procedure of cloud user and the other part describes the working procedure of the cloud admin.

If the user of the cloud want to upload the data in the cloud environment then the cloud user first encrypt the data using private-key cryptography .A secret key may be held by one person or exchanged between the sender and the receiver of a message. For example, if you encrypt data for storage on a hard drive, you remember the key and usually do not give it to another person. But if you want to send secure messages to a business partner using symmetric cryptography, you need to make sure your partner knows the key that will decrypt the messages The secret (or private) key in a public-key cryptographic system is never transmitted or shared. For example, when using this method for client-side authentication, the server sends some data to your client program. The client uses your private key to encrypt that data. Using your public key, the server will attempt to decrypt the returned data, and, if successful, know that it has established communication with you.

If private -key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone, you have never met; you will need to figure out a way to exchange keys in a secure way. One method is to send it via another secure channel. Means the admin of the cloud use the same key for decryption of the data for read. A different encryption\decryption key is needed for the updating of data from the cloud environment. The above phenomena are shown in Figure 2.

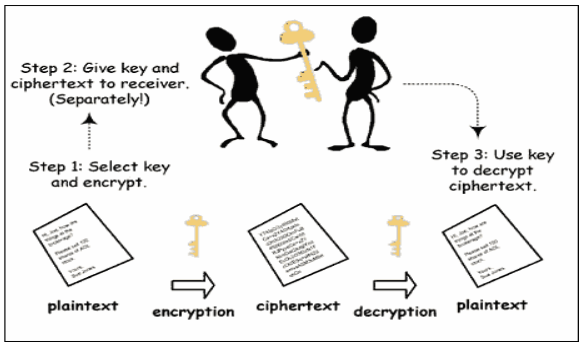

Figure 2: Encryption\Decryption

The private key or symmetric algorithm is the quickest and simplest encryption algorithm in widespread use today. The term symmetric refers to the fact that the same key is used for encryption and decryption (using a encryption notation this means that K = K-1), hence only one key is required in order to encrypt and decrypt data. We use the following terms when talking about encryption -Plaintext - the initial unencrypted data or the encrypted data after it has been decrypted.

Cipher text - the plaintext after is has been encrypted and is no longer readable.
Key - the value applied to the plaintext and encryption algorithm in order to achieve encryption. Conversely the value applied to the cipher text and decryption algorithm in order to achieve decryption.
Encryption - the process of converting the plaintext to cipher text.
Decryption - the process of converting the cipher text back to plaintext. The different algorithms in use have various means of achieving the encryption and decryption but they all have the same general goals.
Secure Encryption - It should not be practical to decipher the cipher text without the key.
Key secrecy - It should not be feasible to deduce the key from the cipher text.
The key point here is the word “practical” in practice it is almost always mathematically possible to decipher the cipher text without a key. The aim is to make it so difficult (usually in terms of required computing power) that it is not practical to achieve this decryption - within a week, year, decade or whatever timescale is required. This is typically

achieved by varying the key size, longer keys take longer to break, but require more computing power to encrypt and decrypt with in the first place.

Algorithm: RC 4
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
Random byte St

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.

If we use 4 bytes state, and 2 bits key for example.
Iteration 1:
i=0, f=0, g=0
S[ ]=[S0, S1, S2, S3] = [0, 1, 2, 3]
K[ ]=[K0, K1] = [2, 5]
Because f=(f + S0+ K0)mod 4=2, then swap S0with S2
New array S[ ]=[S0, S1, S2, S3] = [2, 1, 0, 3]
i = i +1 = 1
g =(g+1)mod 2 = 1
Iteration 2:
i=1, f=2, g=1S[ ]=[S0, S1, S2, S3] = [2, 1, 0, 3]
K[ ]=[K0, K1] = [2, 5]Because f=(f + S1+ K1)mod 4=0, then swap S1with S0
New array S[ ]=[S0, S1, S2, S3] = [1, 2, 0, 3]
i = i +1 = 2
g =(g+1)mod 2 = 0
Iteration 3:
i=2, f=0, g=0 S[ ]=[S0, S1, S2, S3] = [1, 2, 0, 3]
K[ ]=[K0, K1] = [2, 5]Because f=(f + S2+ K0)mod 4=2, then swap S2with S2
New array S[ ]=[S0, S1, S2, S3] = [1, 2, 0, 3]
i = i +1 = 3
g =(g+1)mod 2 = 1
Iteration 4:
i=3, f=2, g=1 S[ ]=[S0, S1, S2, S3] = [1, 2, 0, 3]
K[ ]=[K0, K1] = [2, 5]
Because f=(f + S3+ K1)mod 4=2, then swap S3with S2
New array S[ ]=[S0, S1, S2, S3] = [1, 2, 3, 0]

For this example we use plaintext “HI”
“H” :
i=0, f=0
S[ ]=[S0 , S1, S2, S3] = [1, 2, 3, 0]
Because i = (i + 1)mod 4 = 1
f =(f + S1)mod 4 = 2, then swap S1with S2
New array S[ ]=[S0, S1, S2, S3] = [1, 3, 2, 0]

t = (S1+ S2)mod 4 = 1
S1= 3 (0000 0011)
H
0100 1000
XOR 0000 0011
0100 1011

“I” :
i=1, f=2 S[ ]=[S0, S1, S2, S3] = [1, 3, 2, 0]
Because i = (i + 1)mod 4 = 2
f =(f + S2)mod 4 = 0, then swap S2 with S0
New array S[ ]=[S0, S1, S2, S3] = [2, 3, 1, 0]

t = (S2+ S0)mod 4 = 3
S3= 0 (0000 0000)
I
0100 1001
XOR 0000 0000
0100 1001
Result Plaintext: 0100 1000 0100 1001
Cipher: 0100 1011 0100 1001

This algorithm produces a stream of pseudo-random values. The input stream is XORed with these values, bit by bit. The encryption and decryption process is the same as the data stream is simply XORed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version. The RC4 encryption algorithm is shown in Figure 3.

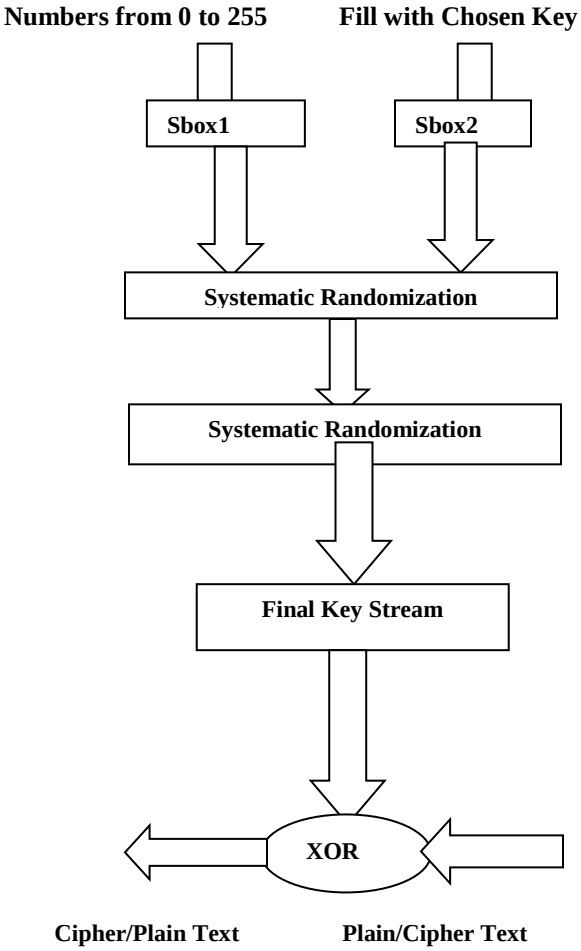

Figure 3: RC 4 Encryption Algorithms

Our algorithm provides a secure way of data transaction through multi cloud environment.

5. Conclusion and future Work

In this paper we provide a secure environment in the cloud environment so that we can securely perform the transaction through the cloud environment which is pay per basis. Our framework also suggests security with the data sharing with multiple cloud environments.

References

[1] I. Berger "Keeping Cloud Computing's Prospects Safe and Sunny", May 2010.

[2] K. McCabe and R. Nachbar. ,"Survey by IEEE and Cloud Security Alliance Details Importance and Urgency of Cloud Computing Security Standards", October 2010.

[3] Centre for the Protection of National Infrastructure (CPNI),"Information Security Briefing", 2010.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Yang Zhang, Jun-Liang Chen. A delegation solution for universal identity management. IEEE Transactions on Services Computing, 2011.3, pp. 70-81, 2011.

[9] Saira Begum and Muhammad Khalid Khan , "Potential of Cloud Computing Architecture" , 2010 IEEE.

[10] Sang-Ho Na, Jun-Young Park, Eui-Nam Huh , "Personal Cloud Computing Threats", 2010 IEEE Asia-Pacific Services Computing Conference.

[11] SiyuanXin, Yong Zhao, Yu Li," Property-Based Remote Attestation Oriented to Cloud Computing" , 2011 Seventh International Conference on Computational Intelligence and Security.

[12] 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.

[13] Zhidong Shen, Li Li, Fei Yan, Xiaoping Wu , "Cloud Computing System Based on Trusted Computing Platform", 2010 International Conference on Intelligent Computation Technology and Automation, IEEE.

[14] Frank E. Gillett, "Future View: The new technology ecosystems of cloud, cloud services and cloud computing" Forrester Report, August 2008.

[15] 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.