IMPROVING RESOURCE UTILIZATION IN INFRASTRUCTURAL CLOUD

Abhinav Awasthi[1], Rohan Patil[2], Magzina Pinto[3], Vikram Sagadevan[4]

[1]*BE, Department of Computer Engineering, Imperial College of Engineering and Research, Maharashtra, India*
[2]*BE, Department of Computer Engineering, Imperial College of Engineering and Research, Maharashtra, India*
[3]*BE, Department of Computer Engineering, Imperial College of Engineering and Research, Maharashtra, India*
[4]*BE, Department of Computer Engineering, Imperial College of Engineering and Research, Maharashtra, India*

Abstract

In this paper, an introspective overview is made on the design aspects of (Software as Service) Cloud system by improving infrastructure utilization integrating different lease and scheduling techniques for user and resources to implement On-demand allocation of resources to the user. The primary aim of Cloud Computing is to provide mobility development of web-based application by means of early accessible tools and interfaces by using and manipulating infrastructure. Cloud-based services integrate global scattered resource, which offer its users different types of services without the difficulties and complications. In this paper main focus is on resource allocation to user, both Premium and Non-Premium with more priority to Premium user managing their effective utilization and providing security from data alteration and modification. In this paper a small protocol of cloud application is implemented adding security to it making the stored user data and information secure via the fraud detection system. Its main purpose is to improve utilization of infrastructure Cloud by providing On-demand availability of the resources to the users by reducing the expenses. Application are network based so that the business user free to use the services from anywhere that they choose using virtually any type of electronic device. Each application is pay-per-usage basis, allowing the business owner to predict their budget for the usage of number of application according to business need. This system offers a less expensive platform and infrastructure solution to improve the efficiency and elasticity of IT operations.

Keywords: *Cloud Computing, Encryption and Decryption, Reverse Circle Cipher and Upper Bound.*

----------***----------

1. INTRODUCTION

Assume that we are in the world where the users of today's internet world need not run, install or store their application or data on their personal computers, imagine the world where every piece of your information or data would be provided on the Cloud (Internet). Cloud computing comes into focus only when you think about what we always need: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends ICT's existing capabilities.

We are hosting our project on cloud. Cloud computing provides dynamically scalable and often virtualized resources are provided as a service over the internet. Cloud Computing is basically sharing of resources over the network. It aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles. Cloud computing provides the tools and technologies to compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

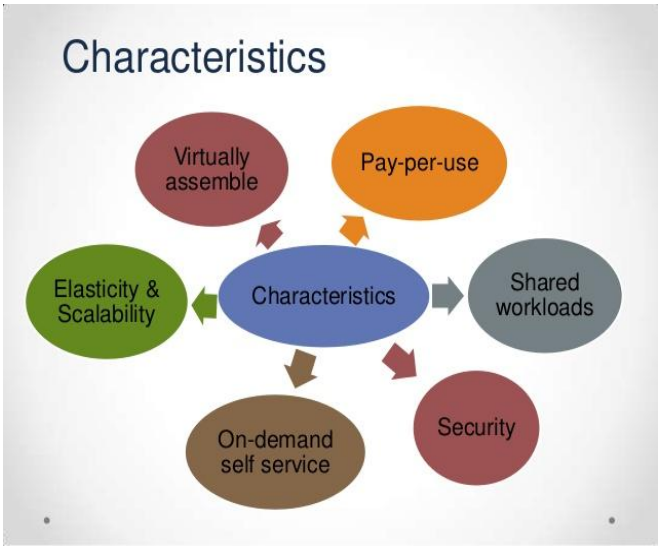

Fig -1: Cloud Computing Characteristics

2. LITERATURE REVIEW

In paper [1], Paul Marshall, Department of Computer Science University of Colorado at Boulder has proposed a cloud infrastructure that combines on-demand allocation of resources with opportunistic provisioning of cycles from idle cloud nodes to other processes by deploying backfill Virtual Machines (VMs).

In paper [2], Authors Amir Vahid Dastjerdi, Sayed Gholam Hassan Tabatabaei and Rajkumar Buyya proposed a system that contributes in the area of the encryption to make sure that the data does not fall in wrong hands at the cloud data centre.

In paper [3], Paul Marshall, Kate Keaheyand and Tim Freeman proposed a System architecture along with the issues involved with elastic provisioning such as security, privacy and various logistical considerations.

In paper [4], Dr. RaoMikkilineni and Vijay Sarathy Kawa proposed a System that utilizes dynamic provisioning of computing, network and storage resources made possible by virtualization technologies.

Thus the purpose of all above papers was to provide on demand provisioning that allows users to elastically expand and contract the resource base available to them based on an immediate need – a pattern that enables a quick turnaround time when dealing with emergencies, working towards deadlines or growing an institutional resource base.

But due to space limitations the performance data of SAGA-Map Reduce with different data-set sizes and varying workers numbers became complex. Also they failed to monitor the allocation of services and handle the memory requirement.

3. APPROACH

This system focuses on Cloud System by improving infrastructure utilization integrating different lease and scheduling techniques for user and resources to implement on-demand allocation of resources to the Premium user who is having highest priority and opportunistic allocation of resources to the Non-Premium user who is having lowest priority. This system also tries to provide security to the data with the help of fraud detection service.

The Infrastructure utilization is (SAAS) Cloud consist of multiple levels such as Software resources, resource allocation, system, and user type. In this system there are two lease On-Demand for Premium user and Opportunistic for Non-Premium user. System checks whether the user is Premium or Non-Premium and then depending on the type of user it allocates the resources. The Premium user has highest priority and Non-Premium have no priority .When user ask for resources then system first check for type of user and if user have high priority then it checks for availability of resources if the resources is available then it is allocated if not then system allocates from system backup. In this system there is limited number of user can access the service if the there is no place for new user and all places are occupied by High priority user then the new high priority user also directed to the queue.

The system monitors the allocation of service and decides whether to allocate the service to the user. The memory requirement and monitoring is assumed for this system and the main focus is on allocation of resources.

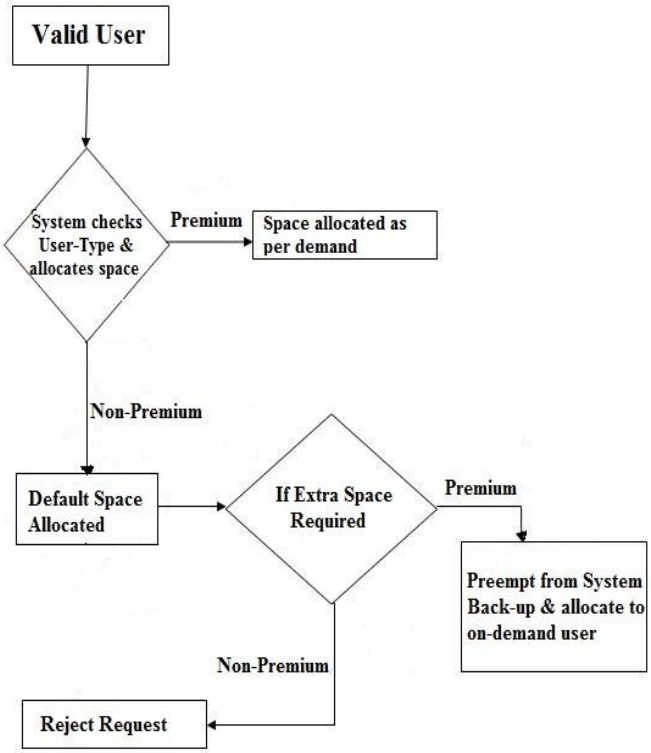

Fig -2: Block Diagram of proposed system

A compute infrastructure cloud operates by allowing a user to make leases against a number of resources that means it makes resources available to the user based on set of lease terms defining the availability, capacity and general conditions of leases:

3.1 Premium User

Premium user is having the higher priority as compared to the Non-Premium user. On-demand, non-pre-emptible and flexible leases give a user access to a resource within interactive time of making the request and make the resource available for an agreed-upon period of time.

3.2 Non-Premium User

Non-Premium user is the normal / free user having the lowest priority. Opportunistic, pre-emptible and pre-set leases give a user access to a resource at an indeterminate time and make the resource available to the user for an in determinate amount of time. Then, this resource is reset for the user by the cloud server, that means the user cannot provide his own VM.

3.3 Fraud Detection service

The main purpose of this service is to provide security to the user data. Certain rights like Read Only, Read/Write, Read/Share and Read/Write/Share are allocated to every user according to the type of user. Supposed a user is allocated Read Only right and he tries to Write/Modify the file then a message ‘Access Denied’ will occur.

4. IMPLEMENTATION

Nowadays Cloud Computing is becoming more and more popular and receiving high demands. Many of the corporate IT people started moving on cloud. Many corporate people term cloud computing as 'The End of Corporate IT'.

Cloud (SAAS) can offer users to use Software as a Service according to his need when the customer does not want to buy the software. System allocates different services depending on the type of user and provide the access rights. In additional to this, system also checks the type of user whether the user is Premium or Non-Premium and depending on that On-demand access is given to service.

The Cloud (Infrastructure Utilization Cloud) is (SAAS) cloud which provides the software as service like any other cloud service provider in the market. If a user asks for service the system allocates that software to that particular user. In case of Premium user if there is no space available then that Particular service is preempted from system backup and given to the user as he is having the higher priority. So there is no such request rejection and service interruption while accessing the resources because of On-demand availability service which satisfy customer needs and will provide ease in maintain Cloud.

We are hosting our project on cloud. Front end of this system is JAVA, JSP and HTML. Back end that is Database is MySQL. Tomcat 7.0 is the Application Server used to host the cloud. Apache Tomcat is an open source servlet container developed by the Apache Software Foundation (ASF). Tomcat implements the Java Servlet and the Java Server Pages (JSP) specifications from Oracle Corporation, and provides a "pure Java" HTTP web server environment for Java code to run.

Initially we need to activate the Tomcat server that will host our cloud. Like any social networking site you need to register yourself and create your account. Registration form will require your personal details and type of account you want to create, either Premium or Non-Premium. In case of Premium user, one has to pay as per the charges for the amount of space the user demands. Non-Premium is a normal user wherein specific amount of space is allocated by default free of charge. Here Premium user will have higher priority as compared to Non-Premium user. After registration the user can login to his account.

After getting into your account the user will be provided with Upload Files, Download Files and Share Files options. Both the users are allowed to download and upload as many files as they desire. As we know all services cannot be provided free of cost and to distinguish between Premium and Non Premium user the Share Files option is activated only for Premium user. The Non-Premium user cannot share the files as compared to Premium user. For sharing the files, the Non-Premium has to convert into Premium user. While sharing of files, the Premium user can share it to any number of users assigning certain rights like Read Only, Read/Write, Read/Share and Read/Write/Share. If any user tries to access the data when access rights are not meant to then the Fraud Detection Service will warn that particular user ACCESS DENIED. A specific size will be set for uploading the files to both Premium and Non-Premium user, if exceed that is the DOS attack a warning will be given to the users. All the history about updated files, downloaded files and shared files will be stored in the MySQL database. While sharing of files a secret key will be generated that will be common to both sender and receiver. If the receiver modifies and sends that particular data to third party a new secret key will be generated replacing the old one between the previous sender , receiver and the thirty party thus maintaining confidentially and avoiding unauthorized access.

Thus Sharing of resources takes place over the network by improving Resource utilization by Reverse Cipher Algorithm as well as providing security to secured data with help of Upper bound algorithm.

5. ALGORITHM

5.1 Encryption and Decryption

Information security is provided on computers and over the Internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on removable storage media like portable flash memory drives or external hard drives. But the most popular forms of security all rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it. Encryption is the process of encoding messages or information in such a way of authorized user can read it. This message is called plaintext and encrypted message is called ciphertext. Decryption is the process of decoding data that has been encrypted back into plaintext. This process requires a secret key or a password. Basically Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable.

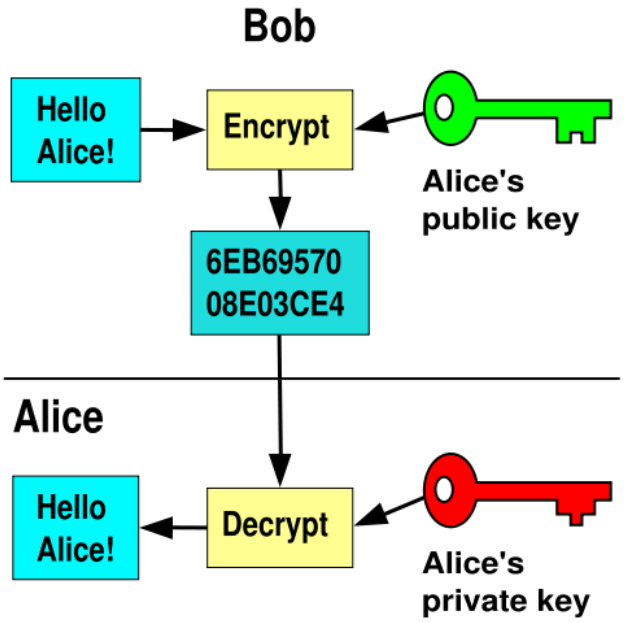

Fig -3: Encryption and Decryption Process

5.2 Reverse Circle Cipher

The Reverse Circle Cipher uses Circular Substitution and Reversal Transposition to exploit the benefits of both confusion and diffusion. It has a variable key length which is almost equal to the plaintext. This method can be best utilized for stand-alone systems providing personal data security.

The Reverse Circle Cipher does not work in the bit level, neither it manipulates the orientation of bytes, rather it manipulates directly onto the ASCII/UTF values of the text. The circular substitution implements confusion and it refers to the use of a string as the key and adding or passing to a function the ASCII/UTF equivalent of a character in the string with that of a character in the plaintext at the corresponding position with respect to the index of that character within the string. When index position of the key string reaches the end, the position restarts to the start index just like the Vernam cipher. This is called the circular key. This process carries on as the plaintext-ciphertext moves on till the end.

Reversal transposition implements diffusion and is simply buffering a certain length of characters of the plaintext and writing the reverse of the buffer on to the ciphertext file. This length is known as the reversal length Continue this operation till all of the plaintext is converted to ciphertext.

Each position of the buffer is then manipulated along with the corresponding position for the circular key with the function :

$$Ci = f\,(Pi\ ,\ k\ (0\ +len(k)\ i))$$

where +len(k) is the modular addition. The suffix I corresponds to the position under operation. The result is stored in the corresponding position within the ciphertext buffer. The contents of the ciphertext buffer is reversed and then appended into the ciphertext. This is repeated till the entire plaintext is processed into ciphertext.

The decryption process is fairly the converse of the encryption process. The ciphertext buffer is first loaded with the contents from the ciphertext file and the contents are reversed. The function $f\ -1$, the converse of f from encryption is used.

$$Pi = f\text{-}1(Ci\ ,\ k\ (0\ +len(k)\ i))$$

In which the input as the ciphertext buffer and the circular key and the output is fed in to the corresponding position i of the plaintext buffer which is directly appended on to the plaintext. The function f can be as complex as a permutation mixing of bit-level representation of the key and plaintext characters or even as primitive as ASCII/UTF level addition. The algorithm mmay even be fabricated within a processor. The algorithm in the form of pseudo code is as shown below:

5.2.1 Algorithm for Reverse Circle Cipher

P : Plaintext Buffer
C : Ciphertext Buffer
R : Reversal Length, hence the buffer size
Pi : Character at position i of plaintext buffer
Ci : Character at position i of ciphertext buffer
ki : Character at position i of the key
+len(k) : Modular addition with respect to key length taken as number of characters.

Encryption:

1. Start
2. Clear all buffers;
3. Open plaintext input file;
4. Open ciphertext output file;
5. Obtain key;
6. while(!eof(plaintext))
7. {
8. Load P from plaintext file;
9. For(i=0; i<R; i++)
10. Ci = f(Pi , k(0+len(k)i)
11. Reverse the contents of C;
12. Append C to ciphertext file;
13. Clear C and P
14. }
15. Close all files;
16. End

Decryption:

1. Start
2. Clear all buffers;
3. Open ciphertext input file;
4. Open plaintext output file;
5. Obtain key;
6. while(!eof(ciphertext))
7. {
8. Load C from ciphertext file;

9. Reverse the contents of C;
10. For(i=0; i<R; i++)
11. Pi = f^{-1}(Ci , k(0+len(k)i)
12. Append P to plaintext file;
13. Clear C and P
14. }
15. Close all files;
16. End

5.2.2 Architecture of the Cryptosystem

The following is the simple representation of Reverse Circle Cipher Algorithm. As it is a symmetric cipher, the same key is used for both Encryption and Decryption process.

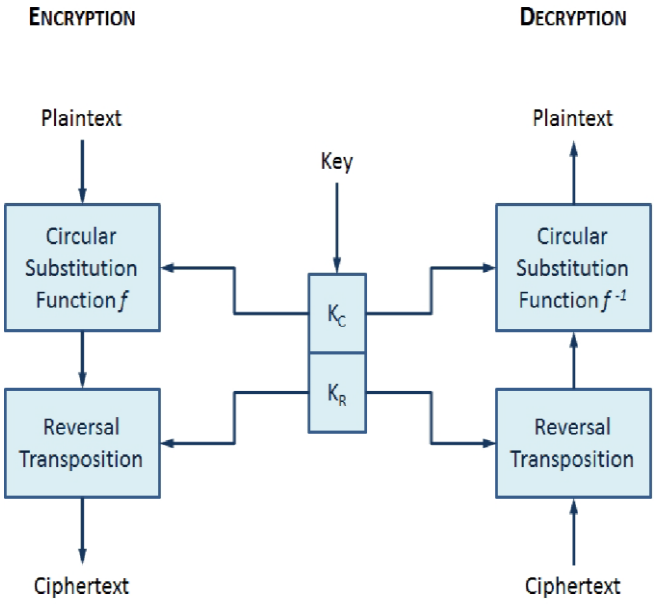

Fig -4: Simple Representation for Reverse Circle Cipher

From the above diagram we observe that the input key is a tuple of the circular character key KC and Reversal length integer key KR. During the process of Encryption, the circular substitution initially takes place with the plaintext taking the circular key as input. The output generated by this operation goes through reversal transposition along with the reversal length. We know that the Decryption process is the reverse of the Encryption process. The reversal algorithm is the same while the circular substitution function is the arithmetic converse of the function used for the Encryption process. Thus through successful operation, the plaintext obtained after the Decryption and before the Encryption will be the same.

5.3 Upper Bound

This technique allows us to preserve the privacy of intermediate datasets while transmission from one server to the other. It helps to identify which intermediate data sets need to be encrypted and which should be avoided, so that the cost of privacy-preserving can be reduced while the privacy requirements of data holders can still be satisfied.

6. FUTURE SCOPE

Over the year Cloud computing has been seen as a perfect alternative for physical storage. It provides sharing of resources over the network and tries to achieve coherence and to be economical to the utility over the network.

This paper proposes a system which combines Premium (on-demand) resource allocation with Non-Premium (opportunistic) provisioning of cycle using High Throughput Computing.

The system will provide On-demand Resource allocation to Premium users which allows them to dynamically expand or contract its allocated resource based on present need. Such type of pattern will provide a quick turnaround time when dealing with emergencies, to work within deadline, efficient utilization of resource, or growing infrastructural resource base. This pattern will prove useful for seamless transition in private cloud.

System proposes a distributed architecture which improves infrastructural utilization of Cloud. Unlike conventional (SAAS) cloud this system provides On-demand resource allocation to Premium users.

This paper proposes to improve infrastructure utilization of Cloud without sacrificing the ability of Cloud by providing On-demand availability of resource to the user by reducing expenses and providing ease of use and access to user and installation to host of the Cloud.

7. CONCLUSION

We propose a cloud infrastructure that combines on-demand allocation of resources with opportunistic provisioning of resources to the user. Because of this, two lease hosting of cloud will become easy and can be used by many cloud providers. This system will solve the request rejection problem and resources will be available as per customer requirements. Customers pay to the cloud providers without knowing the performance of cloud and there is no longer on-demand but because of this system the user need of on-demand allocation of resources will be get fulfilled.

ACKNOWLEDGEMENTS

We would like to take this opportunity to thank a few who were closely involved in the completion of this endeavor. Through this acknowledgement, we express our sincere gratitude to all those people who have been associated with this paper and have helped us with it. We sincerely thank Dr. Sachin Admane, Principal of Imperial College of Engineering and Research, Prof. Satish Todmal, Head of Computer Department, Prof. Vinod Wadne, Guide who have cooperated with us at different stages during the preparation of the paper.

REFERENCES

[1]. Improving Resource Utilization of Infrastructure Clouds by Paul Marshall, Department of Computer Science University of Colorado at Boulder.
[2]. Amir Vahid Dastjerdi, Sayed Gholam Hassan Tabatabaei and Rajkumar Buyya.”An Effective Architecture for Automated Appliance Management System Applying Ontology-Based Cloud Discovery”
[3]. Paul Marshall Kate Keaheyand and Tim Freeman: Using Cloud to Elastically Extend Site Resources.
[4]. Dr. Rao Mikkilineni and Vijay Sarathy Kawa Objects Inc: Cloud Computing and the Lessions from the Past.
[5]. Programming Abstractions for Data Intensive Computing on Clouds and Grids by Chris Miceli, Michael Miceli, ShantenuJha, Hartmut Kaiser and Andre Merzky.
[6]. Reverse Circle Cipher for Personal and Network Security by Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi, Jeppiaar Engineering College, Chennai, Tamil Nadu, India.
[7]. A Privacy Leakage Upper Bound Constraint-Based Approach for Cost-Effective Privacy Preserving of Intermediate Data Sets in Cloud Xuyun Zhang, Chang Liu, Surya Nepal, Suraj Pandey, and Jinjun Chen.
[8]. Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L and Zagorodnov D. Eucalyptus opensource cloud – computing system. In CCA08 : Cloud Computing and its Applications, 2008.

BIOGRAPHIES

Abhinav Awasthi, Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at JSPM’s Imperial College of Engineering and Research, Pune.

Rohan Patil, Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at JSPM’s Imperial College of Engineering and Research, Pune.

Magzina Pinto, is a Final Year Graduate Student, pursuing her Bachelor of Engineering Degree in Computer Science at JSPM’s Imperial College of Engineering and Research, Pune.

Vikram Sagadevan, is a Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at JSPM’s Imperial College of Engineering and Research, Pune.