© 2017 IJSRSET | Volume 3 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Improving the Security in Cloud Computing using Diffie-Hellman Algorithm

Ankur Gupta
Assistant Professor, Computer Science, R. S. D. College, Ferozepur City, Punjab, India

ABSTRACT

Cloud security is the main issue over the wide area network. Cloud computing provide various types of services like software, platform and application as a service. These services are accessed through internet. Cloud provide services on demand, user can pay according to access. That's why today organizations prefer cloud services. Cloud computing provide various services but security is the main issue in cloud. In this paper security enhanced on user end by image pattern and further enhance security on data using diffie-hellman algorithm. This approach prevents threats and enhance the security.

Keywords: Cloud Computing, Pattern Based Security, Diffie-Hellman Algorithm.

I. INTRODUCTION

Cloud computing is a new emerging technology. Cloud is a broad solution that delivers information technology as a service. [1] Cloud computing ropes the data and applications that are used on the remote servers. It allows the users to access the personal files with the help of internet. Cloud computing support services like: SAAS, IAAS, PAAS. To offer these services, the service providers are used. The provider helps to deliver the storage and computing services by the use of internet access. To store the data in cloud computing, it makes ubiquitous data access possible. They can execute their applications using cloud computing platforms with software deployed in the cloud which reduces the upheaval task regarding full software installation and continual up gradation on their local devices.

Components of Cloud Computing:

Cloud computing consists of three main components. Each component in cloud computing plays a role that is specifically assigned to it.

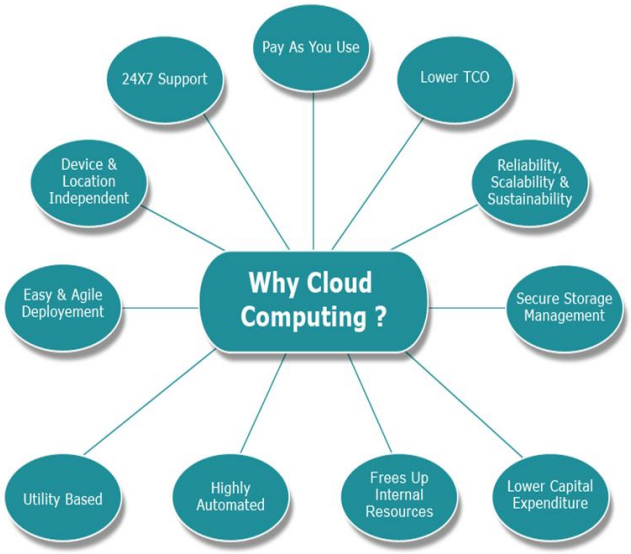

Figure 1: Cloud Computing

Clients: The first component is clients or we can say users. In the cloud computing, the information is managed by end users. They interact with the clients to manage information related to clouds. The clients are further classify into three categories [2]:

a. Mobile Client: The clients can be mobile in nature. It includes windows mobile smart phone, like a Blackberry or I Phone.
b. Thin: These clients do not do computation work. They only used to display information. These clients don't have the internal memory; the servers do all the work for the clients.
c. Thick: These clients use different browsers to connect the internet cloud. These browsers includes internet explorer, Mozilla Firefox or Google Chrome to connect to the Internet cloud.

Datacenter: The second component is datacenter. It is a collection of servers. These servers host the various applications. End users interact with datacenter to access various applications.

Now days, the concept called virtualization is used to install a software that allow multiple users to use applications virtually.

Distributed Servers: Distributed servers are one of the important components of cloud computing. These servers are present throughout the Internet. These server hosts the various applications.

Aspects of cloud management systems:

The cloud management system is a combination of software and technologies, these technologies are designed to manage many cloud environments. The cloud management system is able to manage a pool of heterogeneous compute resources. It provides the access to end users and it also helps to monitor security and manage resource allocation. The cloud management system covers frameworks for workflow structure mapping and management. The cloud management system has characteristics like, it has the ability to manage multiple platforms from a single point of reference. [3] It is able to deal with system failures automatically with abilities such as self tracking and monitoring, an explicit notification mechanism.

Introduction of Diffie-Hellman algorithm:

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. We can define the discrete logarithm in the following way. First, we define a primitive root of a prime number p as one whose powers modulo p generate all the integers from 1 to p 1. That is, if a is a primitive root of the prime number p, then the numbers are distinct and consist of the integers from 1 through p 1 in some permutation.

$a \bmod p,\ a^2 \bmod p, \ldots,\ a^{p1} \bmod p$

For any integer b and a primitive root a of prime number p, we can find a unique exponent I such that

$$b \equiv a^i \pmod{p} \text{ where } 0 \leq i \leq (p\ 1)$$

The exponent i is referred to as the discrete logarithm of b for the base a, mod p.

II. LITERATURE SURVEY

Sumit Goyal,(2013): In which author discuss about cloud computing types. These types are public cloud, private cloud, hybrid cloud and community cloud. Cloud computing is a distributed and virtualized system; it provides a large range of users with distributed access to scalable and virtualized infrastructure over the internet. Cloud computing provides various types of services like hardware services and software services over the internet.

Cong Wang, et.al, (2010): In this paper, author discuss about the security in cloud computing. Cloud Computing consists the architecture of IT enterprise. The cloud computing has the many advantages in the information technology field: on demand self service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. [4] Cloud computing brings the new and challenging security threats towards users outsourced data. For this purpose, cloud service providers are used. These are the separate administrative entities. The data correctness is the big issue in cloud computing. For the cloud computing, third party auditor is used. It

uses the two main requirements as: the third party auditor should be able to efficiently audit the cloud data storage without demanding the local copy of data and the auditing process should bring in no new vulnerabilities towards user data privacy. Here author describes the public key based homomorphism authenticator. For this the random masking is used. It helps to achieve the privacy preserving public cloud data auditing system, which meets all requirements.

Sonal Guleria, Dr. Sonia Vatta, (2013): describes that the Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. Cloud computing provides a computer user access to Information Technology (IT) services which contains applications, servers, data storage, without requiring an understanding of the technology. An analogy to an electricity computing grid is to be useful for cloud computing. To enabling convenient and on-demand network access to a shared pool of configurable computing resources are used for as a model of cloud computing.[5] Cloud computing can be expressed as a combination of Software-as-a-Service which refers to a service delivery model to enabling used for business services of software interface and can be combined creating new business services delivered via flexible networks and Platform as a Service in which Cloud systems offering an additional abstraction level which supplying a virtualized infrastructure that can provide the software platform where systems should be run on and Infrastructure as a Service which Providers manage a large set of computing resources which is used for storing and processing capacity. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing. This paper has been written to focus on the problem of data security. To ensure the security of users' data in the cloud, we propose an effective and flexible scheme with two different algorithms .A user can access cloud services as a utility service and begin to use them almost instantly. These features that make cloud computing so flexible with the fact that services are accessible anywhere any time lead to several potential risks. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication.

Shuai Han, et.al, (2011): In this paper, author uses a third party auditor scheme. Cloud computing technology acts as next generation architecture of IT solution. It enables the users to move their data and application software to the network which is different from traditional solutions. [6] Cloud computing provides the various IT services, due to which it contains many security challenges. The data storage security is the big issue in cloud computing. In this paper, author purpose a new scheme called third party auditor. It helps in providing the trustful authentication to user.

Tejinder Sharma, et.al, (2013): in this paper author discuss about the cloud computing. As, the computer networks are still in their infancy, but they grow up and become sophisticated. Cloud computing is emerging as a new paradigm of large scale distributed computing. It has moved computing and data away from desktop and portable PCs, into large data centers. It has the capability to harness the power of Internet and wide area network to use resources that are available remotely.[7] There are many security issues in the cloud computing. In this paper, author discuss about the various scheduling problems. One of the challenging scheduling problems in Cloud datacenters is to take the allocation and migration of reconfigurable virtual machines into consideration as well as the integrated features of hosting physical machines. In order to select the virtual nodes for executing the task, Load balancing is a methodology to distribute workload across multiple computers. The main objective of this paper to propose efficient and enhanced scheduling algorithm that can maintain the load balancing and provides better improved strategies through efficient job scheduling and modified resource allocation techniques.

Pradeep Bhosale et.al, (2012): discuss that today's world relies on cloud computing to store their public

as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects. In this paper author discuss about the enhancement of data security. Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing that make him a super power.[8] To enhance the data security in cloud computing used the 3 dimensional framework and digital signature with RSA Encryption algorithm. In 3 Dimensional frameworks, at client side user select the parameters reactively between CIA (Confidentiality, Integrity & Availability) and before actual storing the data in cloud a digital signature is created using MD 5 Algorithm and then RSA Encryption algorithm is applied then it stored on cloud.

Jasmin James, et.al, (2012): discuss about the security in cloud computing. Cloud computing is fast growing area in computing research. With the advancement of the Cloud, many new possibilities are coming into picture, like how applications can be built and how different services can be offered to the end user through Virtualization. There are the cloud services providers who provide large scaled computing infrastructure defined on usage, and provide the infrastructure services in a very flexible manner. The virtualization forms the foundation of cloud technology where [9] Virtualization is an emerging IT paradigm that separates computing functions and technology implementations from physical hardware. By using virtualization, users can access servers without knowing specific server details. The virtualization layer will execute user request for computing resources by accessing appropriate resources. In this paper, author firstly analyses the different Virtual Machine (VM) load balancing algorithms. Secondly, a new VM load balancing algorithm has been proposed and implemented for an IaaS framework in simulated cloud computing environment.

Jen-Sheng Wang, et.al,(2011): in this paper, author about the various methods and techniques which helps in managing the security of cloud computing. The information security is critical issue in the age of Internet. [10] The information is valuable and important. The cloud computing has made information security managing a most significant and critical issue. The information security in cloud computing requires many factors. In this paper, the Key Success Factors are used. These factors include many aspects as: external dimension, internal dimension, technology dimension, and execution dimension. These factors are used to purpose a new scheme, which is used to overcome the various problems in cloud computing that are related to the security.

III. PURPOSED WORK

Diffie-Hellman algorithm is used with the AES. The AES is very complexity and its size is very large. To reduce the system complexity we use Diffie-Hellman algorithm. It helps to make the cloud computer more efficient than the existing one. The Diffie-Hellman algorithm is used to provide the security to the system and it also helps in the management of the information.

All we know that security is a major issue in cloud computing because data is stored of some far location from user so number of attacks is possible on cloud computing like:

- Denial of Service (DoS) attacks
- Cloud Malware Injection Attack
- Authentication Attacks
- Man In The Middle Cryptographic Attacks

So here to prevent these attacks we are going to propose a new schema which is based on diffie Hellman. It works like in initial stage it will shows us a simple authentication with user name and password.

After that Diffie-Hellman is used to encrypt data. All the proposed architecture is shown as following:

Figure 2 : User Authentication

Here user enters user name and password and click on login

Diffie Hellman Algorithm

- Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$.
- Alice chooses a secret integer $a = 6$, then sends Bob

  $A = g^a \bmod p$

  $A = 5^6 \bmod 23$

  $A = 15{,}625 \bmod 23$

  $A = 8$
- Bob chooses a secret integer $b = 15$, then sends Alice

  $B = g^b \bmod p$

  $B = 5^{15} \bmod 23$

  $B = 30{,}517{,}578{,}125 \bmod 23$

  $B = 19$
- Alice computes $s = B^a \bmod p$

  $s = 19^6 \bmod 23$

  $s = 47{,}045{,}881 \bmod 23$

  $s = 2$
- Bob computes $s = A^b \bmod p$

  $s = 8^{15} \bmod 23$

  $s = 35{,}184{,}372{,}088{,}832 \bmod 23$

  $s = 2$

IV. RESULTS AND DISCUSSIONS

The new technology to enhance security is based on the Diffie-Hellman algorithm. As we know that the data is stored on far location in the cloud computing so we need high security and processing speed to make it confidential. Here the graph shows the performance of our proposed scenario. Bars in the graph are representing time taken by algorithm to do encryption. Different experimental results are shown in the graph which are done on the basis of different experiments.

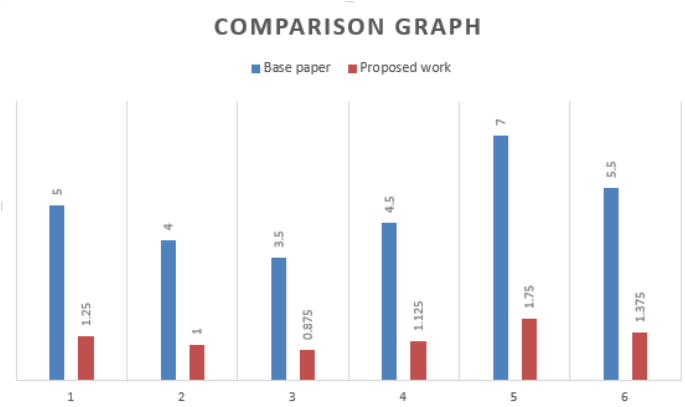

Figure 3 : Comparison evaluation

Now this graph contains the response time graph for previous scenario. At its y axes there are number of characters and the bars are showing time taken for encryption.

Table 1: results comparison

Number of characters	Time taken by Proposed scenario	Time taken by previous scenario
5	1.25 sec	5 sec
4	1 sec	4 sec
7	1.75 sec	7 sec
3	0.67 sec	3 sec
6	1.5 sec	6 sec

In our proposed schema the complexity of algorithm is not too much so it can provides much security in very less time as compare to base paper but the algorithms used in base paper are highly complex so they takes lots of steps and also time for encryption.

V. CONCLUSION AND FUTURE SCOPE

Conclusion

The schema is proposed to enhancement of security and performance of cloud computing during network

attacks. Cloud needs a high performance as well as security because the data on cloud is stored at some far place. A new come up is built by the integration of authentication and Diffie-Hellman algorithm. Experiment is done in NetBeans using cloud-sim simulator and results are shown in above section.

Future Work

As the security is growing day by day attackers are also being more cognizant. Each security schema has some weak points i.e. if attacker knew them then he can bypass security. So to make system more secure we can work on the weakness of algorithm and can further enhance the security.

VI. REFERENCES

[1]. Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.

[2]. Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing A Practical Approach, TATA McGRAW-HILL Edition 2010.

[3]. http://www.howstuffworks.com/cloud-computing/cloud-computing1.htm

[4]. Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013

[5]. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 978-1-4244-5837-0/10/$26.00 ©2010 IEEE

[6]. Shuai Han, Jianchuan Xing, ensuring data storage security through a novel third party auditor scheme in cloud computing, roceedings of IEEE CCIS2011

[7]. Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013

[8]. Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012

[9]. Jasmin James, Dr. Bhupendra Verma, efficient VM load balancing algorithm for a cloud computing environment, Jasmin James et al. International Journal on Computer Science and Engineering (IJCSE)

[10]. Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing