ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

PREVENTION OF DDOS ATTACK USING THREE TIER CAPTCHA

Prof. Sonika A. Chorey[*1], Prof. Pritika V. Mamankar[2] and Prof. Rachana S. Sawade[3]
[*1,2,3]Assistant Professor, Department of IT P.R.M.I.T.R, Badnera, India

ABSTRACT

At virtual level DDOS (Distributed Denial of Service Attack) is biggest threat of availability in cloud computing Service. In Denial of service attack an attacker prevent legitimate users of service from using the desired resources by flood a network or by consuming bandwidth .So authentication is need to distinguish legitimated clients from unauthorized clients, which can be performed through strong cryptographic verification (for a private server) or graphical Turing tests. The attacker traced the ip address of that server & remove all the control access over that application make that user unreachable, where the authentication & security is performed by Graphical Turing Tests for public server, which is widely used to distinguish human users from robots through their reaction. A CAPTCHA is a type of challenge-response test used in computing to determine whether or not the Client is human. This form of CAPTCHA requires that the user type the letters of a given distorted or puzzled image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. The basic reason behind this captcha to explore security in cloud computing network. The user can easily use an application or service without any interruption. Because the test is administered by a computer system, in contrast to the standard Turing test that is controlled by a human, a CAPTCHA is sometimes described as a reverse or Graphical Turing test. This term is ambiguous because it could also mean a Turing test in which the participants are both attempting to prove they are the computer.

Keywords- *Cloud computing, Security Issues, Distributed Denial of Service, Prevention of DDOS, CAPTCHA.*

I. INTRODUCTION

Cloud Computing is a group of resources which are published through Internet. It is well known word in top IT companies like Google, yahoo develop cloud computing system and related products for customer. There are some obstacles for user to adopt cloud computing network because customer has to faith on third party for its private data. This study aims to identify the most hot security threats in cloud computing service. We will discuss security requirements and related issues in cloud computing.

1. Brief of cloud computing

It offer high productivity and low cost at the same time. Lack of security is the biggest hurdle in wide adoption of cloud computing. Cloud computing has many issues like securing data, and examining the utilization resources and provide services to its authorized user. The wide acceptance raised security risks along with the uncountable benefits. [1]

Cloud computing offers 3 different kinds of services:

i) Software as a Service

These services are applications over Internet. Normally the user can run these applications using a web-browser. User abstract totally about the hardware and software that is using and simply access to an interface with a web browser and from there he have access to some information and functionalities. It's dedicated to current users; an example to this kind of services may be Google Docs.

ii) Platform as a Service

These services are focused on the deployment of applications or services online letting to the developer manage the hardware or software necessary, including also a solution stack. This service includes all the life-cycle of the deployment of application/ service such as design, implementation, testing, deployment, integrity with databases, etc.

There are three characteristic points in this service:

- Services for deployment, testing and maintenance of applications

ISSN 2348 – 8034
Impact Factor- 3.155

- Multi-user architecture, in other words scalability.
- Collaborative tools.

An example of these services is Google App engine.

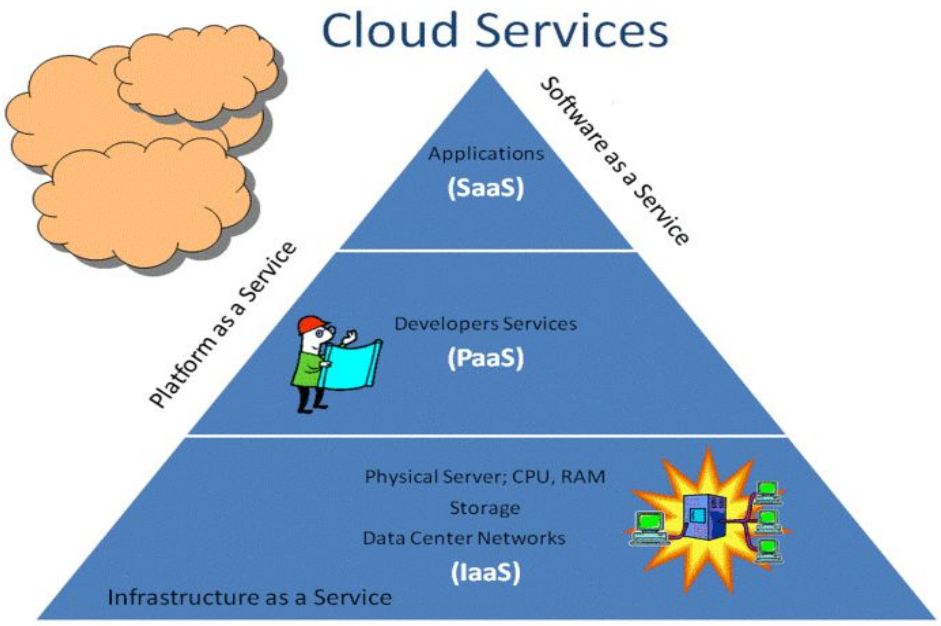

Figure 1: Architecture of Cloud Computing

iii) Infrastructure as a Service

These services are focused to offer a computer infrastructure. All the servers, connections, software and other resources are offered by the providers. And the users see it like an entire infrastructure hosted in the same organization.

Cloud computing is simply a metaphor for the internet. User does not required knowledge, control, and ownership in the computer infrastructure. User simply access or rent the software and paying only for what they use. Advantage of cloud computing is huge like Broad network access, Cost effectiveness, Rapid elasticity, Measured services, On-Demand service, Resource pooling, Location independence, Reliability, Energy saving and so on. But its global phenomenon that everything in this world has advantage as well as disadvantage, cloud computing also suffering from some drawback like security & privacy, Internet Dependency, Availability, And Current Enterprise Applications Can't Be Migrated Easily. Conclude that security is biggest hurdle in wide acceptance of cloud computing. User of cloud services are in fear of data loss, security and availability issues. [2]

II. CHALLENGES OF CLOUD COMPUTING

Security
Data Location & Privacy
Internet Dependency, Performance & Latency
Availability & Service Levels
Not easy to migrate Current Enterprise Applications

User-specific security requirements we can divide into three major Levels.

a. Application Level
b. Virtual Level
c. Physical Level

ISSN 2348 – 8034
Impact Factor- 3.155

Virtual Level: At this level user get service as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and the users are Developer–moderator applies to a person or organization that deploys software on a cloud infrastructure The Security requirement of this level is: Access control, Application security, Data security, Cloud management control security, Virtual cloud protection, Communication security. In Virtual level Security Threats are: Session hijacking, Software modification, Software interruption (deletion), Impersonation, Traffic flow analysis, Exposure in network, Defacement, Connection flooding, **DDOS,** Impersonation, Disrupting communications, Programming flaw.[2]

III. DISTRIBUTED DENIAL OF SERVICE ATTACK

A denial of service is characterized by an explicit attempt by an attacker to prevent authenticate users from using computing resources. An attacker may attempt to: "flood" a network and thus reduce a legitimate user's bandwidth, disrupt service to a specific system and a user prevent access to a service.

a. Impact of DDOS

The attacker sends a huge amount of nonsense request to one target victim or certain service. The impact of such a flooding attack is expected to be amplified drastically. Now we discussed different kinds of impact.

b. Direct Denial of Service

When the Cloud Computing operating system notices the high workload on the particular service; it will start to give more computational power like virtual machines, service instances etc to cope with the additional workload. Cloud protection systems try to work against the attacker.

c. Indirect Denial of Service

It Depending on the Computational power in control of the attacker, side effect of the direct flooding attack on a Cloud service potentially consists in that other services provided on the same hardware servers may suffer from the workload caused by the flooding. Thus, if a service happens to run on the same server with another, flooded service instance, this can affect its own availability as well. [2]

d. Accounting Cloud computing

Service is charging the customers according to their actual usage of resources, another major effect of a flooding attack on a Cloud service is raising the bills for Cloud usage drastically. The problem is there are no "upper limits" to computational power.

At virtual level DDOS (Distributed Denial of Service Attack) is biggest threat of availability in cloud computing. In Denial of service attack an attacker prevent legitimate users of service from using the desired resources by flood a network or by consuming bandwidth .So authentication is need to distinguish legitimated clients from malicious clients, which can be performed through strong cryptographic verification (for a private server) or graphical Turing tests (for a public server). Where the authentication is performed by Graphical Turing Tests, which is widely used to distinguish human users from robots through their reaction.

IV. METHODS OF DDOS ATTACK

The methods which are used for denial of service attack are described below.

1. *Smurf-attack* involves an attacker sending a large amount of Internet Control Message Protocol (ICMP) echo traffic to a set of Internet Protocol (IP) broadcast addresses.

2. *SYN Flood attack* is also known as the Transmission Control Protocol (TCP) SYN attack, and is based on exploiting the standard TCP Three-way handshake process. The server being unable to process because of incoming connection queue gets overloaded [3].

3. UDP Flood attack is based on UDP echo and character generator services provided by most computers on a network. The spy/attacker uses UDP packets to make connection to the echo service on one machine to the character generator service on another machine. There is another method like Ping of death attack Flood attack, Fraggle attack, buffer overflow attack used by attacker to launch DDOS attack.

On the other hand, CAPTCHA (Completely Automated Public Turing Tests to Tell Computers and Humans Apart) is used for Graphical Turing Test. There are many OCR or Non-OCR based CAPTCHA's are used widely

but they are vulnerable to many attacks like Pixel-Count Attack, Recognition by using OCR, Dictionary Attack, and Vertical Segmentation .[4]

V. CAPTCHAs AND THE TURING TEST

CAPTCHA technology has its foundation in an experiment called the **Turing Test**. Alan Turing, sometimes called the father of modern computing, proposed the test as a way to examine whether or not machines can think -- or appear to think -- like humans. The classic test is a game of imitation. In this game, an interrogator asks two participants a series of questions. One of the participants is a machine and the other is a human. The interrogator can't see or hear the participants and has no way of knowing which is which. If the interrogator is unable to figure out which participant is a machine based on the responses, the machine passes the Turing Test. Of course, with a CAPTCHA, the goal is to create a test that humans can pass easily but machines can't. It's also important that the CAPTCHA application is able to present different CAPTCHAs to different users. If a visual CAPTCHA presented a static image that was the same for every user, it wouldn't take long before a spammer spotted the form, deciphered the letters, and programmed an application to type in the correct answer automatically. [1][2]

3.1. Completely Automated Public Turing Tests to Tell Computers and Humans

Apart
(CAPTCHAs) are now almost standard security mechanisms for defending against Undesirable and malicious boot programs on the Internet. CAPTCHAs generate and grade tests that most humans can pass but current computer programs can't. It is also known as Human Interaction Proofs (HIPs).
A good CAPTCHA must not only be human friendly but also robust enough to resist computer programs that attackers write to automatically pass CAPTCHA tests. However, designing CAPTCHAs that exhibit both good robustness and usability is much harder than it seem.

Advantage
· Distinguishes between a machine and a human
· Makes online polls more legitimate
· Reduces spam and viruses
· Makes online Shopping safer
· Reduce abuse of free email account services

3.2 Groups of CAPTCHA

The CAPTCHA methods can be divided into two categories. OCR-based and non-OCR-based methods as follows:

3.2.1 OCR-based method:

The distorted image of a word is shown to the user. Then the user is asked to type that word. This method is based on the drawback of the OCR software because this software has difficulty reading text from distorted image, i.e. Gimpy method, Pessimal Print method, Persian/Arabic Baffletext CAPTCHA, Examples of these methods are used by Google, Hotmail, Yahoo and eBay. In this paper, a new kind of OCR-based method is proposed.

3.2.2 Non-OCR-based method:

Instead of show the distorted image of a word and ask user to type it. This method based on the features of multimedia systems like pictures, sound, and videos. Examples of these methods are Collage CAPTCHA, Text-to-Speech CAPTCHA, Drawing CAPTCHA and Implicit CAPTCHA.

VI. PROPOSED APPROACH

There are basically two major steps involved in building a strong CAPTCHA solution. First, the basis for the puzzle or challenge must be something that is truly difficult for computers to simplify. Second, the way puzzles and responses are processed must easy for human users. The proposed method has been developed to distinguish human users and computer programs from each other by the same fact that human user have to provide a data after solving

ISSN 2348 – 8034
Impact Factor- 3.155

the query associated with CAPTCHA implementation . The query must be very difficult for computers to solve and relatively easy for humans.

Algorithm of Advance Three-Tier Captcha

Step1. Create a Random Alphanumeric Code (Size of 6)
Step2. Create Image with few noise containing that code
Step3. Select Random query related to code i.e. Enter only Digit's.
Step4. Put the combination of code and query in Session.
Step5. Put CAPTCHA Image onto the user interface page along with Query.
Step6.Create image based CAPTCHA Icon image is placed on background image
Step7.Click on icon image which is placed on background image
Step8. Allow user to provide input.
Step9. Examine Input provided by user with value stored in session.
Step10. If Input is correct: Allow user to proceed and Delete the used CAPTCHA Image.
Step11. If Input is Incorrect Generate another CAPTCHA Image and give user limited chance

The programming steps of the THREE-TIER CAPTCHA algorithm are given with pseudo code Executing output screenshots as in follows:

1. Create Web Application in Asp.Net software, start the session.
2. Create custom class to generate/create random image
3. Generate random 6 bit alphanumeric code for CAPTCHA and keep it in session.

4. Define combinations (query related to CAPTCHA e.g Enter only Numeric) in the system and keep current combination in the hidden field or session.

5. Now create random image of the generated code
6. Validate input provided by the user with the CAPTCHA code and combination

7. If the value is empty or incorrect new CAPTCHA is shown. Users should never get a second chance at answering the same CAPTCHA

8. If the answer supplied by the user is correct (same as combination store in hidden field cum session), the form post is successful and processing can executing. If applicable, the previously generated CAPTCHA image is deleted.

We propose a new generation of the CAPTCHA method that uses Query associated with CAPTCHA instead of simple CAPTCHA. We called it THREE-TIER CAPTCHA because in this method CLAD node need to execute three things, first a alphanumeric CAPTCHA code related with image. Second Query related to that CAPTCHA code. In this process human can provide input according to query that is not easy for software bots. Third Image Based captcha icon image is placed on background image, first user has to click on the image in the nested images (image on image) then user will clear the captcha test. In this way we are proposing three way strong security. The advantage of using THREE-TIER CAPTCHA is it can recognizable by human users and difficult to read by bots. Our THREE-TIER CAPTCHA methods use a same input method as used by many well known web sites and services where users type some keywords or characters into a text box. Thus it is easy to learn and run by any user. The algorithm of this method makes it hard for boot programs which mean that it is highly secure. We can increase the rate of its difficulty in order to improve its resistance against the attacks through adding many queries, changing pattern of Query and combination in application database. Like-

· Please provide only Digit's shown in image.

· Please provide only Character shown in image.

· Please provide only Alphabet shown in image.

ISSN 2348 – 8034
Impact Factor- 3.155

· Please provide only first digit and last alphabet shown in image.

· Please provide the value as you provide in User Name (or specify any field name and program accordingly) shown in image.

· Please provide the counting number of character shown in image and so on.

These are some sample of Query, which we can provide with CAPTCHA image to resist it to attack but we also need to take care of the complexity of queries because this will make to solve CAPTCHA more difficult to end user too. Answering these queries is difficult for the computer program because a boot program required some ability to provide correct input for THREE-TIER CAPTCHA.

1. Computer program must recognize alphanumeric code shown in image through OCR- based software.
2. After recognition of alphanumeric code from CAPTCHA image computer should be able to understand the string related to that CAPTCHA.
3. At last and even if computer does all the above mentioned steps successfully it's very difficult to evaluate the correct input pattern, which is required because the query generated anonymously, there is no specific pattern between queries and in some query we use another field of the application web form, i.e. Please provide the value as you provide in User Name (or specify any field name and program accordingly) shown in image.

So that the attack needs to make their program much smart so the program will be able to get values from previous field.

VII. CONCLUSION

In this research paper, we explain Cloud Computing its Models (delivery, deployment) threats and security issues, detail of distributed denial of service and its solution via THREE-TIER CAPTCHA.As we specified earlier, a good CAPTCHA must not only to resist computer programs that attacker use to pass graphical Turing Test but it should be human friendly also. Our newly method is also very easy for human user to answer these questions and the only thing they must do is to provide the input according to query fix with it, little time is required to answer but they can provide input easily and accurately without much difficulty.

REFERENCES

[1] Farhan Bashir Shaikh, Sajjad Haider, "Security threats in cloud computing" 6th International Conference on Internet Technology, Abu Dhabi, Dec 11-14, 2011.
[2] N. Soradge, K. Thakare, "A Novel Anti Phishing Framework On Cloud Based On Visual Cryptography", proceeding of 12th IRF International Conference, 29th June-2014, Pune, India, ISBN: 978-93-84209-31-5.
[3] Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.
[4] Poonam and Sujata, "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA", proceeding of International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013
[5] Varun Ambrose Thomas, Karanvir Kaur "Cursor CAPTCHA – Implementing CAPTCHA Using Mouse Cursor" IEEE Conference 978-1-4673-5999-3/13-2013 IEEE
[6] Charles C. Palmer, David Naccache, Peter Gutmann et.al, "CAPTCHAs: Humans vs. Bots" Aleksey Kolupaev and Juriy Ogijenko OCR Research Team. Published by the IEEE Computer Society, 2008 IEEE, pp 1-2.
[7] Poonam and Sujata, "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA", proceeding of International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013
[8] Felix Lau, Stuart H. Rubin, Michael H.Smith "Distributed Denial of service attacks" IEEE, 2000.