Introducing Three-Tier Captcha to Prevent DDOS Attack in Cloud Computing

Bharat Yadav
Computer Science & Engineering Department ,WCTM
Gurgaon, Haryana (INDIA)
bharatyadav55@gmail.com

Roopal Satija
Assistant Professor CS/IT Department, WCTM
Gurgaon, Haryana (INDIA)
roopalsatija@gmail.com

***Abstract*—** cloud computing refers to a computing hardware machine or group of computing hardware machines commonly referred as a server or servers connected through a communication network such as the Internet, an intranet, a local area network (LAN) or wide area network (WAN). Any individual user who has permission to access the server can use the server's processing power to run an application, save data, or perform any other computational task. Therefore, instead of using a personal computer every time to run a single native application, the individual can be now run the application from anywhere in the entire world, as the server provides the processing power to the application and the server is also connected to a network via the Internet or other connection platforms to be accessed from Remotely. It will become possible due to increased computer processing power available to humankind with decreased cost as stated in Moore's law.
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 unauthorised 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. The term was coined in 2000 by Manuel Blum, Luis von An, Nicholas J. Hopper of Carnegie Mellon University and John Langford of IBM[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. The most common type of CAPTCHA was first invented by Mark D. Lilli bridge , Martin Abdi, Krishna Bharat and Andrei Z. Brooder. 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 D DOS, CAPTCHA*

*****

I. OVERVIEW OF CLOUD COMPUTING

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.
The research paper is summarized in following: section 1 Brief of cloud computing. Section 2 Prevent Security Issues in cloud computing and threats of availability DDOS and study of CAPTCHA. Section 3 Introducing Three-Tier Captcha. Section 4 gives the Conclusion and possible future work.

1. Brief of cloud computing

A cloud computing gives high productivity and low cost at the same time. Less of security lock is the biggest hurdle in adoption of cloud computing. It has many issues like examining the utilization resources and provide services to its authorized user. The wide area of usage raised security risks along with the uncountable benefits. How the user's of cloud computing know that their required services and data is not having security issues and availability?

2. Support of Delivery models

It is generally proposed in three delivery models that are summarized below.

- **Saas(Software-as-a-service)**
- **PaaS(Platform-as-a-service)**
- **IaaS(Infrastructure-as-a-service)**

	Services	**Provider**
SaaS	Service of application are accessible from various remote device via web browserNo need to worry about Infrastructure including, server ,OS, network etc	Mobile Me Google Docs
PaaS	The end user had fully control over the application & its hosting environment	Force.com Google AppEngine
IaaS	The service user had fully control over infrastructure Service & environment including Server,OS etc	Amazon S3,Sun's cloud Google compute Engine

2.1 *Software-as-a-service :*

In this model cloud Service provider has own infrastructure environment & user have to use it remotely. SaaS is closely

related to Application Service Provider and on demand computing software delivery models Benefits of the SaaS model include:

- Easier administration
- Fully Automatic updates and patches management
- To Enhance compatibility All users will have the same version of software that.

.

2.1.1 *Simple multi-tenancy:*

Each remote user have its own access of resources that is separated from other resources.

2.1.2 *Fine grain multi-tenancy:*

All Cloud resources are shared but customer data and access capabilities are segregated within the application.

2.2 *Platform-as-a-service* **:**

The cloud service provider has its own infrastructure environment including OS , storage & network devices. The user only work on the application interface and use the all service provide by the Cloud service provider through single API. The all access of application is under the service provider but all user controls are provided through the application program.

2.3 *Infrastructure-as-a-service :*

Where the cloud service provider has own his infrastructure and OS with application are residing at the user side. It allow user to deploy & run the software .the user can access & maintain the small portion of his application & storage. This type of environment is used in large scale it companies that provide their product online like Amazon's EC2 .

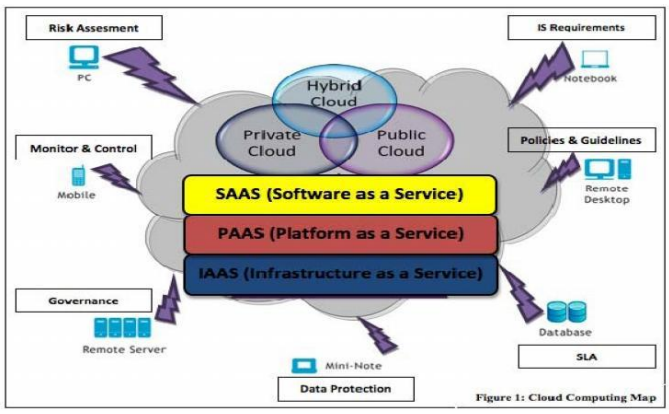

Figure 1: Cloud computing Architecture

3.. Short comings in Cloud Computing

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

4. Security Issues:

Cloud security isn't a black and white question. You can't say "no, I won't use cloud because it isn't secure"; neither can you say "yes, cloud services are the solution to everything."

The users of cloud computing usually not aware about;

- Whether the service provider been tested by a reputable third party?
- When effectively your data segregated from other users?
- Whether your data encrypted with good algorithm? Who holds the keys?
- Where is your data located? Which country? What about data protection legislation?
- Where is the backup?
- How data transmitted and encrypted? How are users authenticated?

We are showing few fail over record from cloud service provider history . It was created real problem when time is money and we depend on cloud [6].

Table 2: Attach performance on sites, its date and duration

Service and Outage	Duration	Date
Gmail and Google Apps Engine	2.5 hours	Feb 24, 2009
Gmail : Site unavailable	1.5 hours	Aug 11, 2008
Google AppEngine : Programming Error	5 hours	June 17 , 2008
S3 outage: overload leading to unavailability	2 hours	Feb 15, 2008
FlaxiScale: core Network Failure	18 hours	Oct 31, 2008
Indiegogo	5-6 hours	Apr 3,2013
Reddit	2-3 hours	Apr 20,2013
Mt.Gox	4-5 hours	Apr 21, 2013

On three consecutive days, from Oct. 16 to Oct. 18, **HSBC Holdings many**, **BB&T Corp.** and **Capital One** were attacked with DDoS attacks.

On March 2013, DDoS experts who track and monitor online activity say, three online role-
playing game sites were hit by **Bot**.

On April 21, 2013, the world's largest Bitcoin information exchange Mt. Gox has been hit by a distributed denial of service (DDoS) attack.

On April 23, Cyber Fighters Izz ad-Din al-Qassam, which claims it's attacked U.S. banking institutions and so on.

Every year thousand of website struggle with unexpected down-time, and hundreds of network break down/failure. So, our motive is to minimize such kind of failure to provide the reliable service and security.

Basically , it is following three goals to achieve adequate security **Confidentiality**, **Data integrity**, **Availability**.

A. Confidentiality. It means keeping user data secret in the cloud Service systems. It ensures that user data which reside in cloud cannot be accessed by unauthorized person.

B. Data integrity. Keeping data integrity is a fundamental & critical task. It means in cloud system is to preserve informational integrity. Data could be encrypted to provide confidentiality but it will not guarantee that data reside on

cloud has not been altered.

C. Availability. Data should be available when it is requested via legal user. It ensure that user can be able to use the service any time from any place.

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

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

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 pillar of this level is: Access control, Application security, Data security, Cloud management control security, Virtual cloud protection, Communication security.

In Virtual level Cloud 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 [1].

5. 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 of resources. An unauthorized/attacker may attempt to: "flood" a network and thus reduce a legitimate user's having bandwidth, disrupt service to a specific system and a user prevent access to a service [9].

5.1 *Impact of DDOS*

The attacker sends a huge amount of nonsense request to one target victim or certain level service. The impact of such a flooding attack is expected to be amplified very drastically. Now we discussed different kinds of impact [5].

Symptoms

- Unusually slow Network Performance
- Inability to access any Website
- Dramatic Increase in the No. of Spam E-mail

5.2 *Elements of DDOS*

- **Victim (Target)** receives the brunt of the attack.
- **Attack Daemon Agents (Zombie)** Agent programs that actually carry out the attack on particular victim. Attackers gain access and actually conduct the attack on Targeted victim. Daemons affect both the target and the host computers
- **Master Program/Agent** Coordinates the attack through the attacker daemons (critical)**,** also known as handler.
- **Attacker/Attacking Hosts** Mastermind behind the attack using the master program, which stays behind the scenes during attack that is real , which makes it tuff task to trace. To do all this attacker has to work hard on it he/she need to study the network topology and bottleneck that can be exploited during the attack [9].

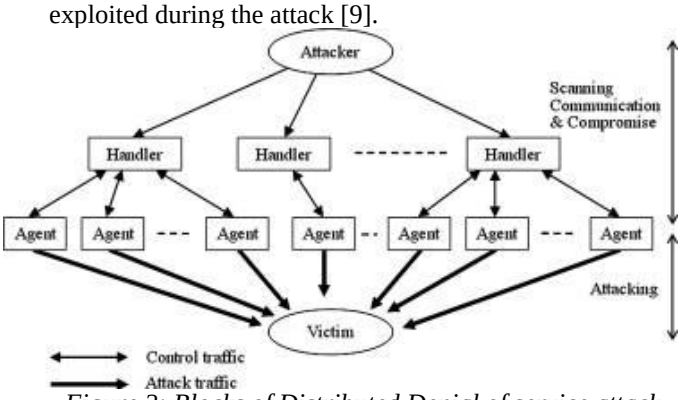

Figure 2: Blocks of Distributed Denial of service attack and steps take place during the attack.

5.3. *Methods of D DOS Attack*

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

5.3.1. *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.

5.3.2 *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 [9].

5.3.3.*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.

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

6.1 *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.
- Step 6. Allow user to provide input.
- Step7. Examine Input provided by user with value stored in session.
- Step8 If Input is correct: Allow user to proceed and Delete the used CAPTCHA Image.
- Step9 If Input is Incorrect Generate another CAPTCHA Image and give user limited chance

Show: Steps of implementing Three-Tier Captcha

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 Exceuting. If applicable, the previously generated CAPTCHA image is deleted.

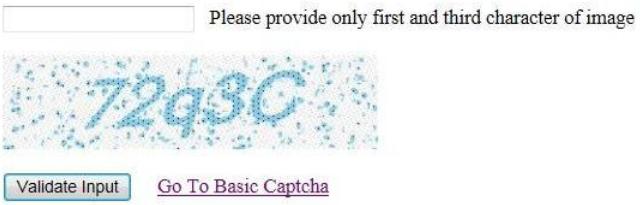

Fig. The valid input for this CAPTCHA is "7q" first and third character of image or sequence. User no needs to fill complete code.

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 two 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. 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 an text box. Thus it is easy to learn and run by any user. The algorithm of this method makes it hard for bot 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.
- 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 bot 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.

5. CONCLUSION

In this research paper, we explain Cloud Computing its Models (delivery, deployment) security issues and threats, 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 because it is not like a IQ test of user like in Question-Based CAPTCHA performed.

Advantage of Advance THREE-TIER CAPTCHA

- Enhanced Security
- Easy to use because user need to provide input like OCR-

based CAPTCHA.
- Prevent automated attacks
- Random combination will be generated, its not easy to identify the pattern

Also Resistance to many attack;

- Resistance to Pre-Processing
- Resistance to Vertical Segmentation
- Resistance to Color pattern-Filling Segmentation
- Resistance to Pixel-Count Attack
- Resistance to Universal Character Recognition by using OCR
- Resistance to Dictionary Attack

Work Done and Future Direction

I will work to make application much secure & reliable, Identify Techniques to optimize resources along with best performance. To reduce the drawback of cloud computing and work to provide quality services to the cloud user in cost effective manner.in upcoming time I will try to implement captcha on my new website based on cloud computing issues.

REFERENCES

[1] Bhaskar Parsad Rimal, Eunmi Choi, Ian Lumb "A taxonomy and survey of cloud computing system" Fifth International joint Conference on INC, 2009.
[2] Sameera Abdulrahman Almulla, chan Yeob Yeun, "Cloud computing security management", IEEE, 2010.
[3] Glenn Carl , Richard R. Brooks, Suresh Rai "Denial of service attack detection technique" IEEE computer society, Feb,2006.
[4] Felix Lau, Stuart H. Rubin, Michael H.Smith "Distributed Denial of service attacks" IEEE, 2000
[5] Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues", University of the Aegean, Syros 84100, Greece –IEEE Dec 22, 2010.
[6] Palivela Hemant, Nitin.P. Chawande, Avinash, Hemant Wani "Development of server in cloud computing to solve issues related to security and backup" – IEEE CCIS,2011.
[7] Farhan Bashir Shaikh, Sajjad Haider, "Security threats in cloud computing" 6th International Conference on Internet Technology, Abu Dhabi, Dec 11-14, 2011.
[8] http://searchsecurity.techtarget.com/ezine/Information-Security-magazine/Setting-up-for-BYOD-success-with-enterprise-mobile-management-andmobile applicationsecurity/Security-as-a-Service-Benefits-and-risks-of-cloud-based-security
[9] Meiko Jensen, Jorg Schwenk, Nil Gruschka "On technical issues in cloud computing", IEEE International Conference on cloud computing, 2009.
[10] Bhaskar Parsad Rimal, Eunmi Choi, Ian Lumb "A taxonomy and survey of cloud computing system" Fifth International joint Conference on INC, 2009.
[11] Minqi Zhou, Rong Zhang, Wei Xie "Security and Privacy in Cloud computing: A Survey" sixth International Conference on Semantics, 2010.
[12] Sameera Abdulrahman Almulla, chan Yeob Yeun, "Cloud computing security management", IEEE, 2010.
[13] Felix Lau, Stuart H. Rubin, Michael H.Smith "Distributed Denial of service attacks" IEEE, 2000.
[14] Yonghua You, Mohammad Zulkerine, Anwar Haque, " A distributed Defense framework for flooding-based DDOS attack" Third International conference on Availability and security, 2008.
[15] Glenn Carl , Richard R. Brooks, Suresh Rai "Denial of service attack detection technique" IEEE computer society, Feb,2006.
[16] David R. Raymaon, Scott F. Midkiff "Denial-of –service in wireless sensor Networks: attack and defenses" IEEE CS, 2008.
[17] Lin Jingna " An analysis on DOS attack and defense technology" seventh International Conference on Computer Science, Melbourne, Australia, July 14-17, 2012.
[18] Simon Liu " Surviving Distributed Denial of service attacks" IEEE CS, 2009.
[19] Ping Du, Akihiro Nakao, "DDOS defense as a Network service" IEEE, 2010.
[20] Jeff Yen, Ahmad Salah, " CAPTCHA security-Case Study", IEEE CS, 2009.
[21] Mohammad Shirali-Shahreza, Sajad Shirali-Shahreza, " Question Based CAPTCHA", IEEE International Conference on Computational Intelligence, 2007.
[22] Ahmad EL Ahmad, Jeff Yan, "CAPTCHA design color, usability and security", IEEE CS 2012.
[23] http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/whitepaper_13513031862.pdf white per from computer weekly.
[24] http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/whitepaper_68713275917.pdf white paper from computer weekly.
[25] http://pandodaily.com/2013/04/03/indiegogo-was-hacked/
[26] http://zeenews.india.com/news/net-news/reddit-suffers-massive-online-attack_843434.html
[27] http://thenextweb.com/insider/2013/04/21/here-we-go-again-top-bitcoin-exchange-mt-gox-taken-down-for-hours-by-another-strong-ddos-attack/#comments
[28] http://www.bankinfosecurity.com/bank-attacks-7-steps-to-respond-a-5221
[29] http://www.bankinfosecurity.com/new-ddos-attacks-hit-game-sites-a-5622

The Authors

Bharat Yadav is a final year student in WCTM Gurgaon, department of Computer Science and Information Technology. His Research interest includes Cloud Computing and Network Security. He received her B.Tech in Information Technology from G.I.T.M. He also certified in .NET from Microsoft. He is currently working as a Senior Executive at DCM Ltd.

Roopal Satija is a assistant professor in WCTM Gurgaon Department of Computer Science and Information Technology.