

Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA

Poonam Yadav¹ and Sujata²

¹ Software Engineering Department, ITMU gurgaon, Haryana (INDIA)
yadavpoonam96@gmail.com

² Assistant Professor CS/IT Department, ITMU gurgaon, Haryana (INDIA)
sujata@itmindia.edu

ABSTRACT

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. I 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.

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 .

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. This paper introduces a new CAPTCHA method called Two-Tier CAPTCHA. In this method CLAD node need to generate two things, first a alphanumeric CAPTCHA code with image. Second Query related to that CAPTCHA code. E.g. enter only Digit's .We can increase the rate of its difficulty in order to improve its resistance against the attacks by adding more and more query and combination in database. The algorithm of this method makes it hard for bot programs which mean that it is more secure. This project has been implemented by ASP.NET and PHP Language.

KEYWORDS

Cloud computing, Security Issues, Distributed Denial of Service, Defense against D DOS Graphical Turing Test, CAPTCHA

1. INTRODUCTION

Cloud Computing is set of computing resources and services offered through the Internet. Recently it becomes the hottest word in IT world. Many well known IT companies like yahoo,

International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013

Google, IBM, develop cloud computing system and related products for customer. There are still some difficulties for customer to adopt cloud computing because customer has to trust on third party for its sensitive (private) data. Every one poses, Is their information secure? [3] This study aims to identify the most vulnerable security threats in cloud computing. We discuss security requirements and related issues in cloud computing.

The rest of this paper is organized as follows: section 1 Introduces cloud computing overview. Section 2 Discusses security issues present in cloud computing and threats of availability DDOS. Section 3 Explain Graphical Turing test and study of CAPTCHA. Section 4 Introducing Two-Tier CAPTCHA. Section 5 gives the Conclusion and possible future work.

1. Definition 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. How the end users of cloud computing know that their required services and data is not having any availability and security issues? [3]

2. Delivery models

Cloud services are generally offered three Delivery models;

Table 1: Cloud services and provider.

	Services	Provider
SaaS	Application are accessible from various client device via web browser No need to control Infrastructure including OS, network, server etc	Google Docs Mobile Me Salesforce.com
PaaS	User has control over the Deployed application and application hosting environment configuration	Microsoft Azure Force.com Google AppEngine
IaaS	User has control over storage , OS , Deployed application and limited control of select networking component	Amazon S3 Sun's cloud Google compute Engine

2.1 Software-as-a-service (SaaS), where the cloud provider owns the application, server, storage operating system (OS) and infrastructure and you use the application remotely. Through a thin client interface such as Web browser [1]. In summary: "Just run it for me!"
It provides service in two distinct modes:

2.1.1 Simple multi-tenancy: each customer has its own resources that are segregated from other resources

2.1.2 Fine grain multi-tenancy: all resources are shared but customer data and access capabilities are segregated within the application. Examples include document sharing services, such as customer relationship management (CRM) applications, Salesforce.

2.2 Platform-as-a-service (PaaS), where the provider owns the OS and infrastructure, and you own the application. In this user does not control the cloud infrastructure including server, storage, OS, network etc but has control over the deployed application and application hosting environment configuration [1]. It can be summarised as: “Give me a nice API and you take care of the rest”.

2.3 Infrastructure-as-a-service (IaaS), where the provider owns just the infrastructure and you own both the OS and the application. Provide the user with the capability of processing, storage, network and other computing resources and allow the user to deploy and run software [1]. e.g. Amazon’s EC2 . In short: “Why buy machines when you can rent cycles?”

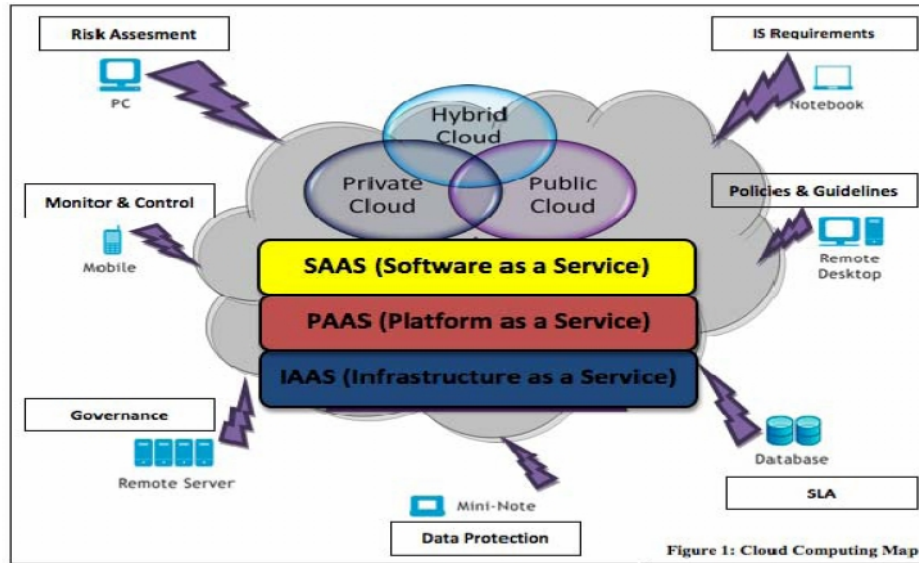


Figure 1: Cloud computing Architecture

3. Deployment Models

Four deployment models have been identified for cloud architecture:

3.1 Private cloud. The cloud infrastructure is operated for a private organization. It may be managed by the third party or a organization, and may exist on premise or off premise. In private cloud we get additional security benefits as the company has the server at its end.

3.2 Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has common mission, security requirements, policy, and compliance considerations. It may exist on premise or off premise. It may be managed by the organizations itself or a third party.

3.4 Public cloud. The cloud infrastructure is available for general public or a large industry group and is owned by an organization selling cloud services [1].

3.5 Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities. The hybrid cloud provides the local data benefits of the private with scalability, economies and on-demand access of the public cloud [2].

4. Challenges for Cloud Computing

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

1. Requirement of security

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 end users of cloud computing usually not aware about;

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

We are showing failover record from cloud service provider system. It create real problem when time is money and we depend on cloud [6].

Table 2: Attach perform on sits, 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, 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 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 attacking U.S. banking institutions and so on.

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

International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013
Traditionally, it contains three goals to achieve adequate security Confidentiality, Data integrity, Availability.

A. Confidentiality. It means keeping user data secret in the cloud systems. It ensures that user data which reside in cloud cannot be accessed by unauthorized person. There are two basic approaches to achieve such confidentiality, physical isolation and cryptography. Confidentiality can be achieved through proper encryption technique: symmetric and asymmetric algorithms.

B. Data integrity. Keeping data integrity is a fundamental task. It means in cloud system is to preserve information integrity. Data could be encrypted to provide confidentiality but it will not guarantee that data reside on cloud has not been altered. There are two approaches which provide integrity Digital Signature and Message Authentication Code.

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

Two strategies called Hardening and Redundancy are mainly used to enhance the availability.

Threats targeting availability can be either CSP availability or network based attack such as Distributed Denial of Service.

Many well known website which provide computing services via cloud e.g. Google, Amazon S3 suffered from DDOS attack.

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 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 [1].

2. 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 [9].

2.1 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 [5].

2.1.1 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.

2.1.2 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 [5].

2.1.3 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 usage [5].

Symptoms

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

2.2 Elements of DDOS

- **Victim (Target)** receives the brunt of the attack.
- **Attack Daemon Agents (Zombie)** Agent programs that actually carry out the attack on target victim. Attackers gain access and actually conduct the attack on victim. Daemons affect both the target and the host computers
- **Master Program/Agent** Coordinates the attack through the attack daemons, also known as handler.
- **Attacker/Attacking Hosts** Mastermind behind the attack using the master, which stays behind the scenes during real attack, which makes it difficult 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].

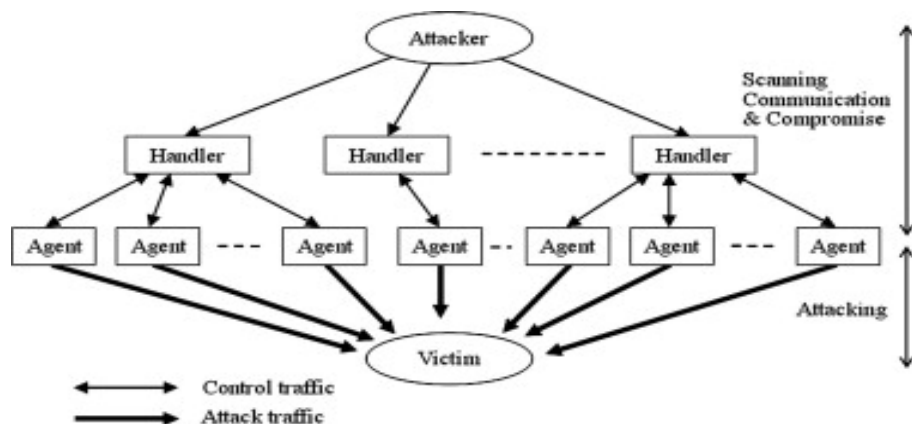


Figure 2: Components of Distributed Denial of service attack and steps take place during the attack.

1. The real attacker sends an execute command to master program.
2. The control master program receives the “execute” message and propagates the command to the attack daemons under its control.
3. Upon receiving the attack command, the attack daemons begin the attack on the victim.
4. Then the victim site goes down and not available to give services to its intended user.

2.3. Method of D DOS Attack

These are the method which is used for denial of service attack.

2.3.1 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.

2.3.2 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. The server being unable to process because of incoming connection queue gets overloaded [9].

2.3.3 UDP Flood attack is based on UDP echo and character generator services provided by most computers on a network. The 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 Teardrop attack, Land attack, Flood attack, Fraggle attack, Ping of death attack, Buffer overflow attack used by attacker to launch DDOS attack.

2.4 Technique used by attacker

Distributed denial of service methods employed by an attacker. These techniques help an attacker coordinate and execute the attack. The techniques are listed in chronological order. It can be observed that as time has passed, the distributed techniques (Trinoo, TFN, Stacheldraht, Shaft, and TFN2K) have become technically more advanced and more difficult to detect [9].

2.5. Defences against D DOS Attacks

Many observers have stated that there are currently no successful defences against a distributed denial of service attack, but there are numerous safety measures that a host or network can perform to increase the security of network and neighbouring networks. Two features that hinder the advancement of defence technique.

First, the source of DDOS attacks are very difficult to find in distributed environment. It's difficult to find out the real attacker because he/she can use the multiple layer of control master program.

Second, it's very hard to distinguish between normal traffic and DDOS attack traffic. Attacker generate same request as legitimate user and we don't have effective differentiation mechanism.

There are some distributed defence frameworks that provide defence against DDOS attack:

2.5.1 Filtering Routers: Filtering all packets entering and leaving the network protects the network from attacks conducted from neighbouring networks. Many people assume that routers, which use access control lists (ACLs) to filter out "undesirable" traffic, defend against DDOS attacks. ACLs can protect against simple and known DDOS attacks, such as ping attacks, by filtering unwanted, unknown protocols and also prevents the network itself from being an unaware attacker. This measure requires installing ingress and egress packet filters on all routers.

2.5.2 Load Balancing: It is used to implement failover-the continuation of service after the failure of one and more components. These components work under controlled supervision, when become non responsive, the load balancer informed and stop sending traffic to it. Through the use of load balancer we can minimize the resource consumption, keep cost low and also enable scalability.

2.5.3 Disabling IP Broadcasts: By disabling IP broadcasts, the host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks. To defend against this attack, all neighbouring networks need to disable IP broadcasts [9].

2.5.4 Audit: It means to watch what happened in cloud system. It could be added as an extra layer above the virtualized operating system to monitor what happen in the network. Main attribute should be audited:

Logs: Information about run time environment and user application

Events: The change of state and other factor that affect system/services availability.

Monitoring: It must be restricted to what the cloud providers reasonably need in order to run their facility [7].

2.5.5 Applying Security Patches: To guard against denial of service attacks, host computers must be updated with latest security patches and techniques. For example, in the case of the SYN Flood attack, there are three steps that the host computers can take to guard themselves from attacks: increase the size of the connection queue, decrease the time-out waiting for the three-way handshake, and employ vendor software patches to detect and circumvent the problem.

2.5.6 Disabling Unused Services: If UDP echo services are not required, disabling them will help to defend against the attack. If one computer opens 50 ports, the attacker can use these ports to launch different DDOS attack. If only two ports are opened the attack type will be restricted [13]. The services should be disabled to prevent attacks if network services are unneeded or unused.

2.5.7 Performing Intrusion Detection: By performing intrusion detection, a host computer and network are guarded against being a source for an attack, as while as being a victim of an attack. It is a device or software application that monitors network or system activities. If they found malicious activities or policy violations, the produces reports to a management station. Network monitoring is a very good pre-emptive way of guarding against denial of service attacks. By monitoring traffic patterns, a network can determine when it is under attack, and can take the required steps to defend itself [9].

3. GRAPHICAL TURING TEST

The authentication is 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). The authentication is performed by graphical Turing tests which are widely adopted to distinguish human users from robots through their reaction. A client who has failed graphical tests after a given number trials will be blocked, suspected as attacker and his/her HTTP requests will be dropped. We can also add overly-aggressive clients to a blacklist and avoid there request. On the other hand, a client who passes the graphical Turing tests will be allow proceeding and assigned a valid HTTP session key [15].

Graphical Turing Test we use a cloud attack defence system, named CLAD, which a network service is running on cloud infrastructures. The whole cloud infrastructure appears as a “super

International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013
 computer” so that any network-layer attacks to a single CLAD node, which is an application or a virtual machine can be defeated by the whole cloud infrastructure.

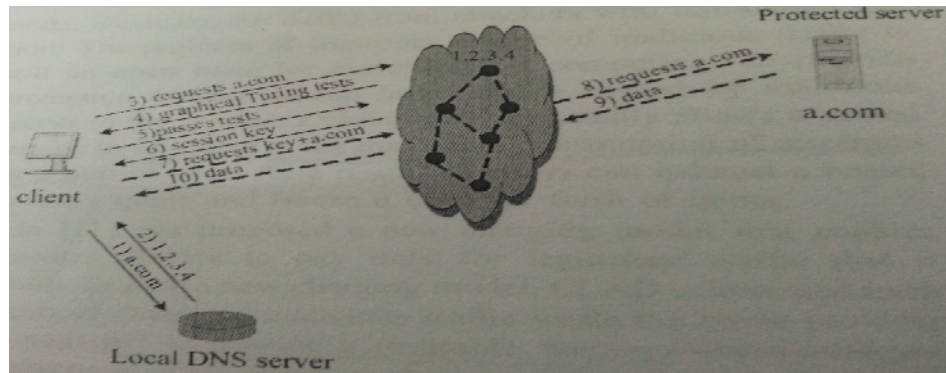


Figure 3: Shows the basic protocol of CLAD,

Figure 3 shows Full lines represent the connection setup processes. Dashed lines represent the data transfer processes.

The execution environment of each CLAD node should be independent of the operating system, hardware and physical location of the cloud infrastructure. If a user passes the Graphical Turing Test then only he/she can be able to establish the connection to cloud infrastructure.

Some detail like architecture of CLAD is omitted because they are not the scope of this paper

The CLAD system works as follows;

- **Steps 1-2:** To make connection to the protected server a.com, the client first need to sends a request to the local DNS server to query the server’s IP address. Then DNS server returns the IP address of CLAD node.
- **Steps 3-6:** When the client requests a.com to the CLAD node 1.2.3.4, the CLAD node performs **graphical Turing tests** for authentication. If the client can pass the tests, the CLAD node allows her to request to the protected server and assign her a session key.
- **Steps 7-10:** The client can access a.com with the session key through 1.2.3.4. After the CLAD node has validated the session key, then the communication start between a.com and client, it relays the request to a.com, and then relays the responded data from a.com to the client [15].

For Graphic Turing Test we use CAPTCHA

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 bot 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, Pessimial 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.

Table 3: List of CAPTCHA used by well known Origination.

	CAPTCHA Image	Origination
1		Google
2		Hotmail
3		eBay
4		Yahoo
5		Rediffmail
6		Frendester
7		Jeans
8		Pcl news

4. PROPOSED APPROACH

There are two major issues 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 solve. Second, the way puzzles and responses are processed must be 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 users have to provide a data after solving the query associated with CAPTCHA. The query must be very difficult for computers to solve and relatively easy for humans.

4.1 Algorithm of Advance TWO-TIER CAPTCHA

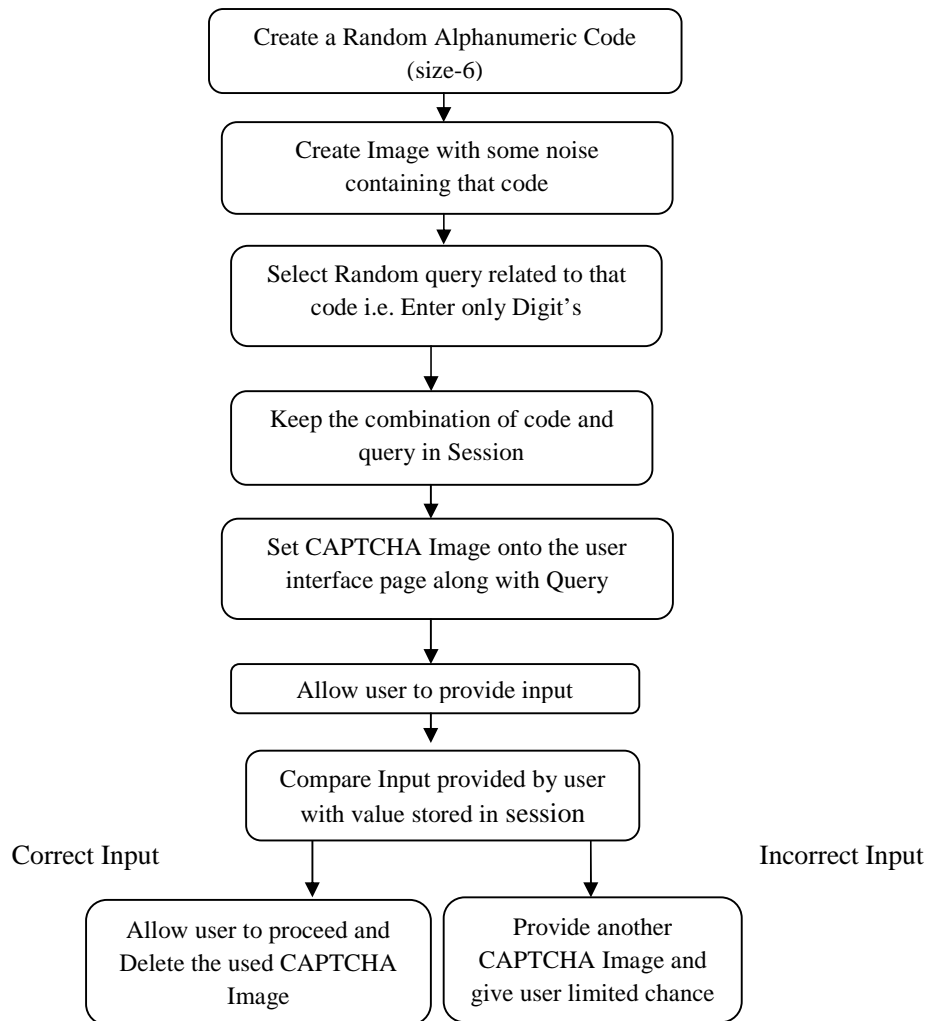


Figure 4: Work Flow of Advance Two Tier CAPTCHA

International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3, June 2013
The programming steps of the Two-Tier CAPTCHA algorithm are given with pseudo code and runtime output screenshots as in follows;

1. Create Web Application in Asp.Net, start the session.
2. Create custom class to generate/create random image
3. Generate random 6 bit alphanumeric code (included "0-9, A-Z, a-z") for CAPTCHA and keep it in session.
4. Define combinations (query related to CAPTCHA e.g Enter only digit) 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 generated. 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 or session), the form post is successful and processing can continue. If applicable, the previously generated CAPTCHA image is deleted.

Please provide only first and third character of image



[Go To Basic Captcha](#)

Dig. The valid input for this CAPTCHA is "7q" first and third character of image. 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 Two-Tier CAPTCHA because in this method CLAD node need to generate two things, first a alphanumeric CAPTCHA code with image. Second Query related to that CAPTCHA code. In this method human can provide input according to query that is not easy for software bots. The advantage of using Two-Tier CAPTCHA is it can recognizable by human users and difficult to read by bots. Our Two-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 input box. Thus it is easy to learn and use by any user. The algorithm of this method makes it hard for bot programs which mean that it is more secure. We can increase the rate of its difficulty in order to improve its resistance against the attacks through adding more queries, changing pattern of Query and combination in 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 human user too. Answering these queries is difficult for the computer program because a bot program required some ability to provide correct input for Two-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 query 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, which is required because the query generated randomly, there is no specific pattern between queries and in some query we use another field of the 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 attack needs to make their program much smart so the program will be able to get values from previous field.

5. CONCLUSION

In this paper, we explain Cloud Computing its Models (delivery, deployment) security issues and threats, detail of distributed denial of service and its solution via Two-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 proposed 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 associated 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 Two-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, so not easy to identify the pattern

Also Resistance to many attack;

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

Work Done and Future Direction

Implemented Advance Two-Tier CAPTCHA in ASP.NET and also implement this CAPTCHA on ITM University's Upcoming Alumni Website in PHP.

I will work to make application much secure, Identify Techniques to optimize resources along with better performance. To reduce the drawback of cloud computing and work to provide quality services to the cloud user in cost effective manner.

References

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

Authors

Poonam Yadav is a final year student in ITMU gurgaon, department of Computer Science and Information Technology. Her Research interest includes Cloud Computing and Network Security. She received her B.Tech in Information Technology from Y.M.C.A Faridabad. She also qualify NET exam. She is a student member of the Tech Target. Her research interests lie in cloud computing software engineering, Network Security and artificial intelligence.



Sujata is a assistant professor in ITMU gurgaon Department of Computer Science and Information Technology. Her Research interest Includes Software Engg. and Software Testing.