



ISSN: 0975-766X  
CODEN: IJPTFI  
Research Article

Available Online through  
www.ijptonline.com

## DDOS DETECTION AND MITIGATION FOR MANAGED SECURITY OF CLOUD RESOURCES

Deepa Mani\*, Anand Mahendran<sup>#1</sup>

\* Assistant Professor (Senior), School of Information Technology and Engineering,  
VIT University, Vellore-632014, Tamilnadu, India.

<sup>#</sup> Associate Professor, School of Computer Science and Engineering,  
VIT University, Vellore-632014, Tamilnadu, India.

Email: mdeepa@vit.ac.in

Received on 25-07-2016

Accepted on 20-08-2016

### Abstract

Achievement of the distributed environment in cloud world view expected on its autonomous-interest, own administration, and its independent nature. As indicated by the worldview, impacts with the Denial of service (DoS) assaults include naive just the aspect of the enforcement, additionally the administration upkeep costs as far as asset preservation particularly, the greater the identification postponement is, the higher the expenses to be brought about. So, a specific consideration must be paid for stealthy DoS assaults. They go for lessening this perceivability, and in the meantime, they can be as hurtful as the animal power assaults. They are advanced assaults customized to influence the worst case execution of the objective framework through particular intermittent, beating, and less-rate movement designs. Here, we are proposing a procedure via coordinate undercover assault designs, whatever show gradually expanding power pattern intended to dispense the most extreme budgetary expense to the client using the cloud, while regarding assignment volume addition to that enforcement entry estimation forced away the recognition components. Here personally everyone depict the application of the asserted technique, those consequences for objective framework sent in the distributed environment of the cloud.

### Introduction

Cloud computing is all over the place. Get any tech magazine or visit any IT site or blog and we will be convinced to see a discussion on distributed environment of cloud. The prime affair is that not people relinquish to its own nature. When challenged about this to exclusives killed people about what distributed environment is, and we will get different answers. Sodistributed environment indeed, even rationalised amidst all the reinforces. A few individuals don't think so."The PC business is the main business that is more mold driven than ladies' style," he said to a gathering of Prophet Experts. So we should discuss what distributed computing is and take care of our definition and

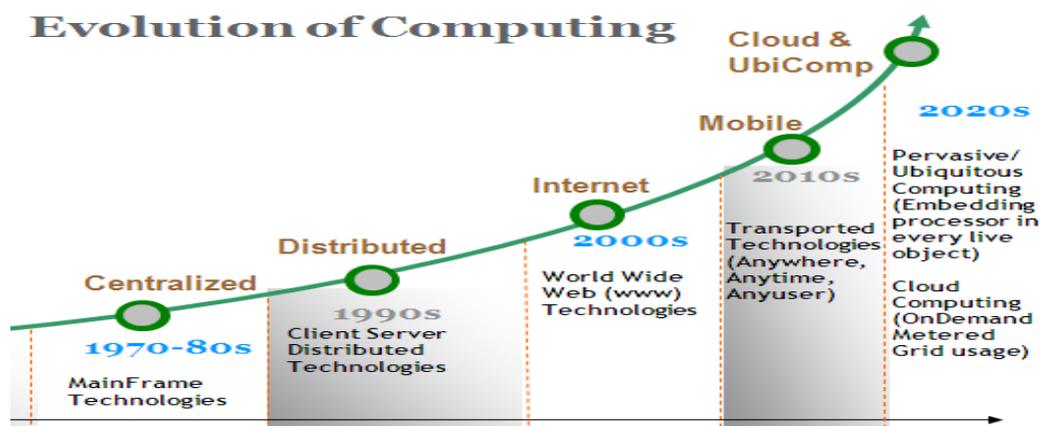
comprehension of this execution. In the maximum direct terms, distributed computing infers confinement, recovering data and undertakings over the internet as opposed to your system's hard disk. The distributed environment is ethically a purposeful anecdote for the internet. It performs an inversion to the seasons of flow sheets and propositions that will address the colossal server-farm base from internet as just a enlarged, distributed cloud, enduring affiliations and allocating away the information since it floats.

Whenever you are stocking your image svia internet as opposed to on your home system, or use electronic mail or a comprehensive interpersonal correspondence website page, you are using a "circulated figuring" organization. If you are an affiliation, and you have to use, for occasion, a web account organization rather than overhauling the in-house one you have been using for quite a while, that web invoicing organization is a "dispersed registering" organization. Dispersed registering insinuates the transport of preparing resources over the Web. As opposed to keeping data in solitude hard drive or overhauling applications for your necessities, you use an organization over the Web, at another region, to stock your information or use its applications. Doing all things considered may offer rising to certain surveillance recommendations. What distributed environment is nothing related to your hard disk. When you stock data on or execute code from the hard disk, that is called close-by limit and preparing. Now what wedemand is objectively related to you, whereas it suggests obtaining to the data is speedy and basic, for that one PC, or others on the close-by framework. losing off the hard disk is the methods through where the eratreated for an extensive time allotment; some would battle's despite everything it superior to anything distributed computing.

The distributed environment is additionally no more holding a committed system appended capacity equipment or server in home. Putting away information at house or at business area will not grant utilizing the distributed environment. Hence to be "distributed computing," weshould obtain the data or fewtasks over the internet, they have that type of dataintegrated with alternative details over the internet. In a major criteria, we may recognize totally to consider about for what is on the another oblique of the association. The concluding reaction is homogeneous: with a connected club, distributed computing should be available anywhere. We're discussing distributed computing since it properties singular shoppers—who stay at home and use the internet all the time. Here it is a totally diverse "cloud" with regards to outsourceful. Some organizations execute Software as-a service (SaaS), where the outsources prefers to the operation it utilizes to the internet. Similarly platform as-a service(PaaS), where a business can make its own particular custom applications for use by all in the organization. Also, keep in mind the powerful infrastructure as-a service (IaaS).

The channels in the neighbourhood processing with the distributed environment infrequently become extremely foggy. So on the grounds that the cloud is a piece of data in recent times. So without much of stretch have a close programming which utilizes the distributed environment to the scope of the process.

So, Microsoft additionally offers an arrangement of Web applications, now called Office On the web, that are online-just forms of Word, Exceed expectations, PowerPoint, and OneNote got to by means of the internet source beyond introducing all. Also means a form of distributed computing Organisations are interested in cloud computing because they can essentially lessen the expense and unpredictability of controlling and engaged with the systems. Cloud environments will regularly twisting and adherent to employ, and substitutes can offer proper environment regarding this arrangement of the periodic assessment.



**Characteristics of Cloud Computing**

The constitutions of distributed environment consolidate with its autonomous interest own enforcement, broader system design, credit blending, immense adaptability and consistent enforcement. Autonomous enforcement intends the customers who ask for and command for their self projects. The broader mechanism approaches enforcements which are advertised over the internet. Credit blending intends the customers to obtain the credit from integrated set of processes that are loaded in the main memory.

**Identity Access Management (IAM):**

Identity access management (IAM) is a structure for the outsourcing forms that supports the voltaic style enforcement. The organization consolidates the variation which is expected to strengthen the sense of enforcement. IAM deviation can be used to capture and monitor customer natures and their relevant approaches in a automated style. This ensures connection profits are handed over by elucidation of strategy reasonably accepted, endorsed and examined. Inadequately managing IAM conducting may allow immediate enforcement rebelliousness for the risk in the spirit getting abused.

## Service Models

The appropriated figuring organization models are programming as an administration (SaaS), Platform as an administration (PaaS) and Infrastructure as an administration (IaaS). In a product as an administration model, it is already done model, close by any required programming, working structure, hardware, and framework are given. In PaaS, a working structure, hardware, and framework are given, and the customer presents or develops their self specific coding and techniques. The IaaS model gives just the gear and framework; the customer presents or develops its own specific working structures, codings and techniques.

## Deployment Models of Cloud Services

Distributed environmental organizations were normally made open by method for a confidential cloud, group cloud, open cloud or mixture cloud. When in doubt, organizations gave by an open cloud are offered over the internet and are guaranteed and supervised by a cloud provider. A couple tests consolidate organizations has gone for the general populace, for instance, web photo stockpiling organizations, mailing organizations, or comprehensive relation between the correspondence destinations. Regardless, organizations for endeavour scan in like manner be offered in an open cloud. In a confidential cloud, the cloud objects are employed solely for a specific affiliation, and is directed by the affiliation or an outcast. In a group cloud, the organization is divided by a couple of affiliations and made open just to those social affairs. The establishment may be guaranteed and worked by the affiliations or by a cloud organization provider. A mixed cloud is a mix of different procedures for resource crediting.

## Challenges of Cloud Computing

### 1. Security & Privacy

Security is an extraordinary sympathy toward CIOs while moving their information to the cloud. In spite of the fact that security in the cloud is by and large dependable and capable, CIOs need to realize that the cloud supplier they worked with has a completely secure cloud environment. A settled distributed computing seller will guarantee they have the most recent modern security frameworks set up to guard against dangers

### 2. Service Quality

Service quality is a monotonous isolation between many huge volatile resources that organizations incur within the sole property of the system. Regularly organizations think according to a late review 43% of IT chiefs are wanting to put more into distributed computing this year. CIOs need affirmation that the organization's information will be secure and accessible, and the administration dependable at all times. Guaranteeing greatest upkeep of the administration is central for the productivity and maintainability of the business

### **3. Downtime & Accessibility**

Service quality doesn't need to be traded off when your information is in the cloud. Getting to your information when you require it is an essential necessity from numerous associations. The test with the cloud is that the information is gotten to by means of a web association as opposed to a neighbourhood association. So when the system or web association is down, it additionally implies that cloud administrations are likewise down; in this manner information can't be accessed. Performance of the cloud base can be influenced by the heap, environment and number of clients. Guaranteeing that your cloud framework is flexible to blackouts is fundamental. Whilst it is practically difficult to moderate all server blackouts, a respectable supplier will have hearty versatility measures set up to secure your information.

### **4. Access to Data**

Cloud-based servers don't generally have the best or fitting client administration emotionally supportive networks. CIOs regularly express their worries around information possession and losing control of their information when moving to the cloud, yet this shouldn't be an issue. Selecting where and how your information is put away is an essential component inside the basic leadership process. Combination is an issue for some associations. Guaranteeing that the greater part of the applications can consistently coordinate with each other is likewise a typical test.

### **5. Transition to the Cloud**

Numerous cloud appropriation difficulties are obscure because of the way that cloud innovation is still in its relative earliest stages. CIOs are tested settling on the most ideal approach to move to the cloud and finding a cloud arrangement that meets the points of the organizations, whilst enhancing efficiencies. Despite the fact that transitioning to the cloud is a perplexing and included procedure, there isn't one course to achievement. CIOs must guarantee that the proposed arrangement compliments their plan of action. There are different ways organizations can move to the cloud. Whether it's by means of private, open or cross breed advancements, distinguishing the right administration model for your business is a key step.

### **Design of the system**

#### **Intrusion detection system**

An intrusion detection system (IDS) is a sort of preservation encoding technique that is expected to subsequently prepared chiefs when a person or whoever is endeavouring to exchange off information structure via threatening activities or through surveillance approach encroachment. An IDS accumulates by checking system development via investigating suspectability in the structure, whereas uprightness with records in driving a examination of case in light

of certainly common assaults. moreover hence explains over the web to chase off any of the latest risks which will achieve a eventual attack.

An IDS should be used for recognizing perils and things being what they are is thrown away on the framework structure, inferring therefore it is not a certifiable persistent coherence path via the dealer and beneficiary of information. On the other hand perhaps, IDS game plans will routinely misuse to explore a copy of the inline development branch.

### **Analysis Engines of Intrusion Detection Systems**

There are 3types of analysis engines available commercially:

- Designation/Event -based Analysis
- Analytical Analysis
- Flexible Systems

### **Designation Orevent Based Analysis**

The occasion, or mark based, frameworks work much like the counter infection programming with which a great many people are well known. The merchant creates a rundown of examples whereas regards a characteristic in the assault; the intrusion system simply filters threats from this earth. system will next process via obtaining a client characterized activity, cautioning, or creating an extra chunk activity. This system is widely recognized sort in the interruption location framework.

### **Analytical Analysis**

Analytical analysis framework constructs factual models of the earth, for example,

A telnet period's actual radius, hereby searches for fluctuations with "typical". then more than a long time of research by the government, few items were simply starting for fusing with the innovation towards attractive items.

### **Flexible Systems**

The adaptive systems frameworks begin with summed up guidelines for the earth, then learn, or adjust to, neighbourhood conditions that would some way or another be strange. After the underlying learning period, the framework sees how individuals collaborate with the earth, and after that caution administrators about irregular exercises.

There is a lot of dynamic research here. You ought to remember the system will slip a few sorts with doubtful action and flag cautions. So hence associations should possess a solid manual methods which connects the system to assess

working ambience. system knowledge of many interruption location Frameworks were as yet developing, however momentum exploration is attempting to enhance this.

### **Network IDS**

The system IDS for the most part has two intelligent segments: first the examination and second the administration locality. The examining mounts on a system section, checking them for any cautious activity. here administration locality gets cautions against the examining area and alerts an administrator. They are normally devoted frameworks which already present just to screen the system. This holds a system model in indiscriminate channel, whereas it implies get system activity, only which is bound with its IP location, and it capture acquiring system activity for investigation.

### **Strengths**

The system interruption location frameworks can identify a portion of the assaults that utilization the system. They are useful for identifying access without power or a few sorts of entry in overabundance with power this system-based IDS need notcrave alteration in generation of manager. favourable position since creation servers regularly have close working resiliences for CPU, I/O, and circle limit; introducing extra programming may surpass the frameworks limits.

The IDS is not on a critical way for any creation administrations or procedures in light of the fact that a system based IDS does not go about as a switch or other basic gadget. Framework disappointment does not significantly affect the outsourcing.

An added advantage in prone with experience minimum contention beyond many individuals inside the association; the danger with preplanned basic procedures is less in this entity framework than with a host framework. these frameworks have a tendency to be more independent than host-based frameworks. They keep running on a devoted framework that is easy to introduce; simply unpack the gadget, do some therapeutic setup, and attachment it into your system in an area that licenses it to screen delicate activity.

### **Weakness**

A system based IDS, then again, just inspects system movement on the section to which it is straightforwardly associated, yet it can't recognize an assault that goes through a diverse system portion. This issue 'confined sight' especially regional in an exchanged local area network- locality.

The issue might need that any association buy numerous nodes keeping in mind the end goal to meet their system scope objectives. Since every sensor costs cash, expansive scope with system IDS sensors can turn out to be

restrictively costly. System interruption location frameworks tend to utilize signature examination with a specific end goal to meet execution prerequisites. This will identify basic modified assaults from outer sources, however it is deficient for identifying more unpredictable data dangers. This requires a more vigorous capacity to analyze nature.

### **System Based IDS**

This searches indications in interruption within nearby system framework. Those much of time utilize the system framework's review component in wellspring data investigation. These search uncommon movement which are bound within nearby system, for example, accessing, inappropriate document access, unapproved benefit heightening, or adjustments on framework benefits.

This IDS design for the most part uses guideline based motors for investigating movement; a sample of such a standard may be, "superuser benefit must be achieved through the su order." hence progressive access endeavors record may be declared as an assault.

### **Strengths**

This greatly capable apparatus for breaking down a conceivable assault. For case, it can some of the time tell precisely aggressor charges documents, framework, instead of only fairly unclear allegation a endeavoured perilous order. This normally gives significantly mostly point by point so applicable data within system ids Host frameworks have a tendency to have brought down. Then in light of those fact that scope of charges particular system is substantially engaged sorts in activity streaming over the system.

### **Weaknesses**

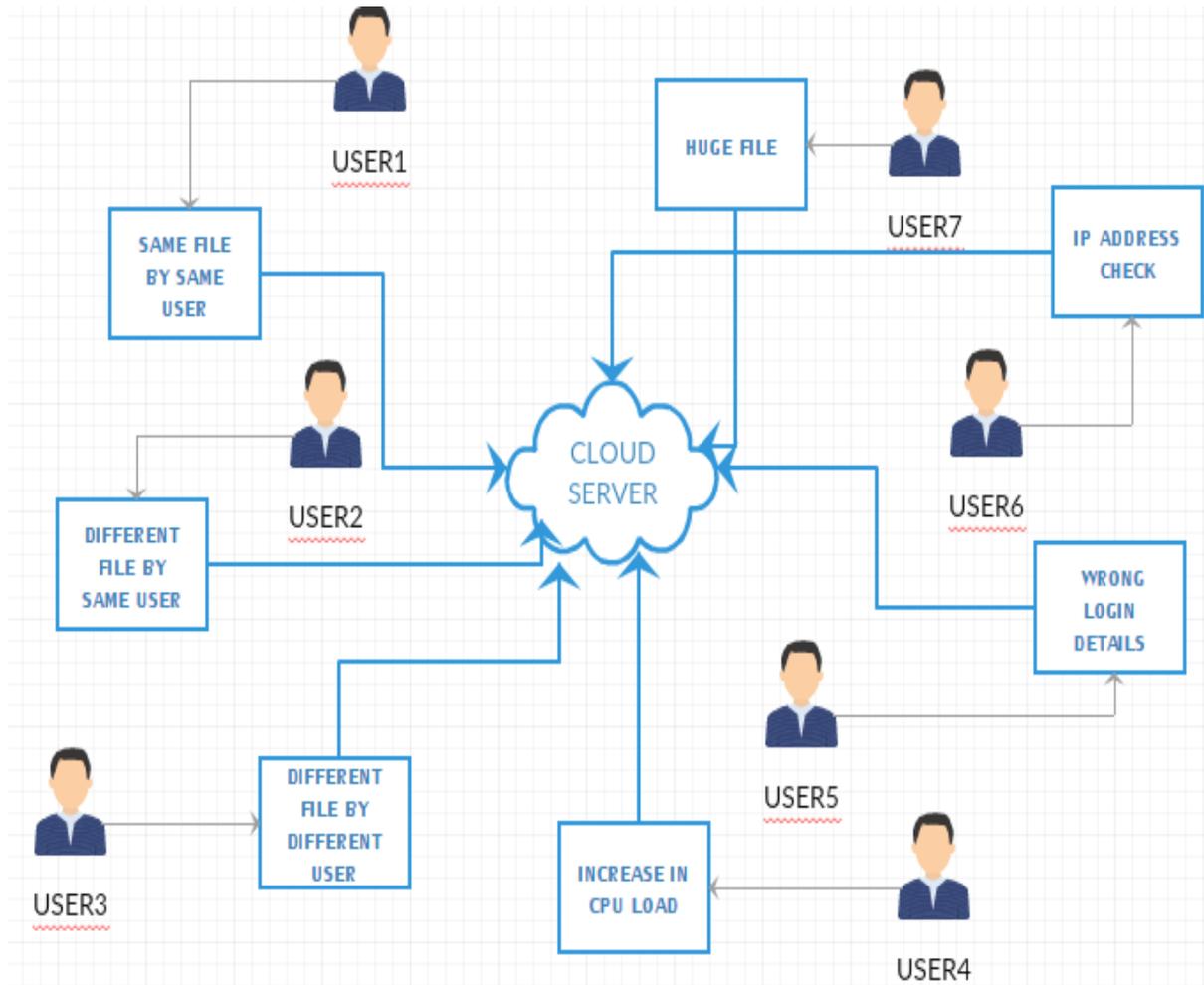
Host-based IDS require establishment with respect to the specific gadget that you wish to secure. In the event that, for instance, we own a HR server, and need secure it, we need to introduce intrusion methodology on the server. Numerous associations don't have the budgetary assets to secure whole system portions utilizing host-based frameworks.

These associations should precisely pick which frameworks to secure. This can leave wide crevices in ID scope, on the grounds that, for instance, an aggressor on a neighbouring be that as it may, unprotected framework can sniff validation data or other delicate material from the system. At last, have based frameworks endure, to a significantly more noteworthy degree, from nearby vision limitations.

They are absolutely insensible system space. Consequently, examination periodneeded to assess harm from a probable interruption increments directly within quantity secured hosts. human requires significant investment examine occurrence framework, it will take 2 to research two frameworks, 3 to explore 3 frameworks, etcetera.

**Module Description**

**System Architecture**



**Existing System**

A distributed denial of maintenance attack accounts to large amount of traded off structures attack a singular aim, in this way processing on framework. The flow of accessing reports to the aim of the structure actually forces it to contiguous period, consequently avoiding reinforcement to the framework to accurate users in the existing system, DDOS Attack in a Client Server Environment would Collapse the Entire System, however to the extent Cloud is concern it is not that Effective but rather still it will attempt to Disturb the Regular Activity of the System.

**Disadvantages**

- Increase CPU load
- Congestion
- Time consuming process
- Less effective
- Less security

## Proposed System

In the proposed system, we Deploy User's Request which could likewise expand the CPU Load of the Cloud Server. Filters the Request taking into account it then conducts and advances to the relating Servers through Cloud Server. Each Server would have designated Certain Space in Cloud Server. Our framework screens the Activity of the Users to Avoid DDOS Attacks. Through this system we can minimise the distributed denial of service attacks and the server will continuously monitor the system.

## Modification Process

In this part once information proprietor transfer their information alongside their catchphrase information put away in isolated server. We execute seven sorts of attacks to detect the attack and to prevent the attacks. 1. Persistent and same solicitation from single client in a state of time. 2. Diverse inquiry from the same client inside a timeframe. 3. Distinctive inquiries from various clients however from same IP. 4. Solicitation of immense estimated record past the allowed. 5. Wrong login credentials for more than 4 times. 6. IP location of the enrolled client. 7. CPU usage of the client's solicitation.

## Advantages

- Congestion is avoided
- Less Time consuming process
- Effective
- Provides security

## Modules

1. Cloud server positioning
2. Space assignment
3. Client mustering
4. Positioning of multiple IPS
5. DDOS attack from one user
6. DDOS attack from many users
7. Attack sieving model

**Cloud Server Positioning:** Cloud Service Provider will contain the considerable measure of data in their information channel. Moreover the Cloud benefit supplier keep up every customer information for checking the customer when

they are accessed into their record. The customer information is secured in the Database of the Cloud benefit user.

Similarly the Cloud host occupies the customer requested occupation whereas in surrogate Accessing plan to set up the User requested Job. The Request of the significant number of Users will handle by the appliance Accessing plan.

To talk with the Client and the with exchange modules of the Cloud Network, the Cloud Server will develop relationship within them. Due to this reason we are going to make a User Interface Frame. Furthermore the Cloud Service Provider will send the User Job sales to the appliance Access plan in Fist come first serve method

### **Space Assignment**

Cloud Servers is a cloud framework benefit that permits clients to send "one to several cloud servers in a flash" and make "propelled, high accessibility models" .The "cloud servers are virtual machines running on the hypervisor for Linux-based occasions, and Xen Server for Windows and Linux occurrences. Every quad center equipment hub has somewhere around 16 and 32 GB of RAM, taking into account designations between 256 MB and 30 GB. Circle and CPU designations scale up with memory, with plate sizes running from 10 GB to 620 GB. Different circulations of Linux are upheld, and every client space designation with various band width is allotted so they uses inside the transmission capacity

### **Client Mustering**

1. Track Users amid an Emergency
2. Guarantee no one is left in threat zone
3. Lessen Paperwork/Human Error amid
4. Information accumulation and reporting.
5. Get specialists over into office in a sheltered and convenient way

### **Positioning of Multiple IPS**

In this module we execute various IPS ie interruption security framework that used to ensure the client shape the assaults .in existing they were utilizing single to output the inquiry of a cloud client. in any case, in this proposed module various IPS is sent to screen the client question so that it effortlessly discover the foreswearing of attack

### **DDOS Attack from One User**

DDOS is a kind of attack where various traded off structures and they normally polluted with infection are used to concentrate on a single structure providing a Denial of Service. Actually this assault consist of both the last focused on framework so every frameworks vindictively used and supervised by the coding team in the dispersed assault. in

this assault, the adventing activity congestion the casualty provides within the multiple range of sources that are provided over the attacks

### DDOS Attack from Many Users

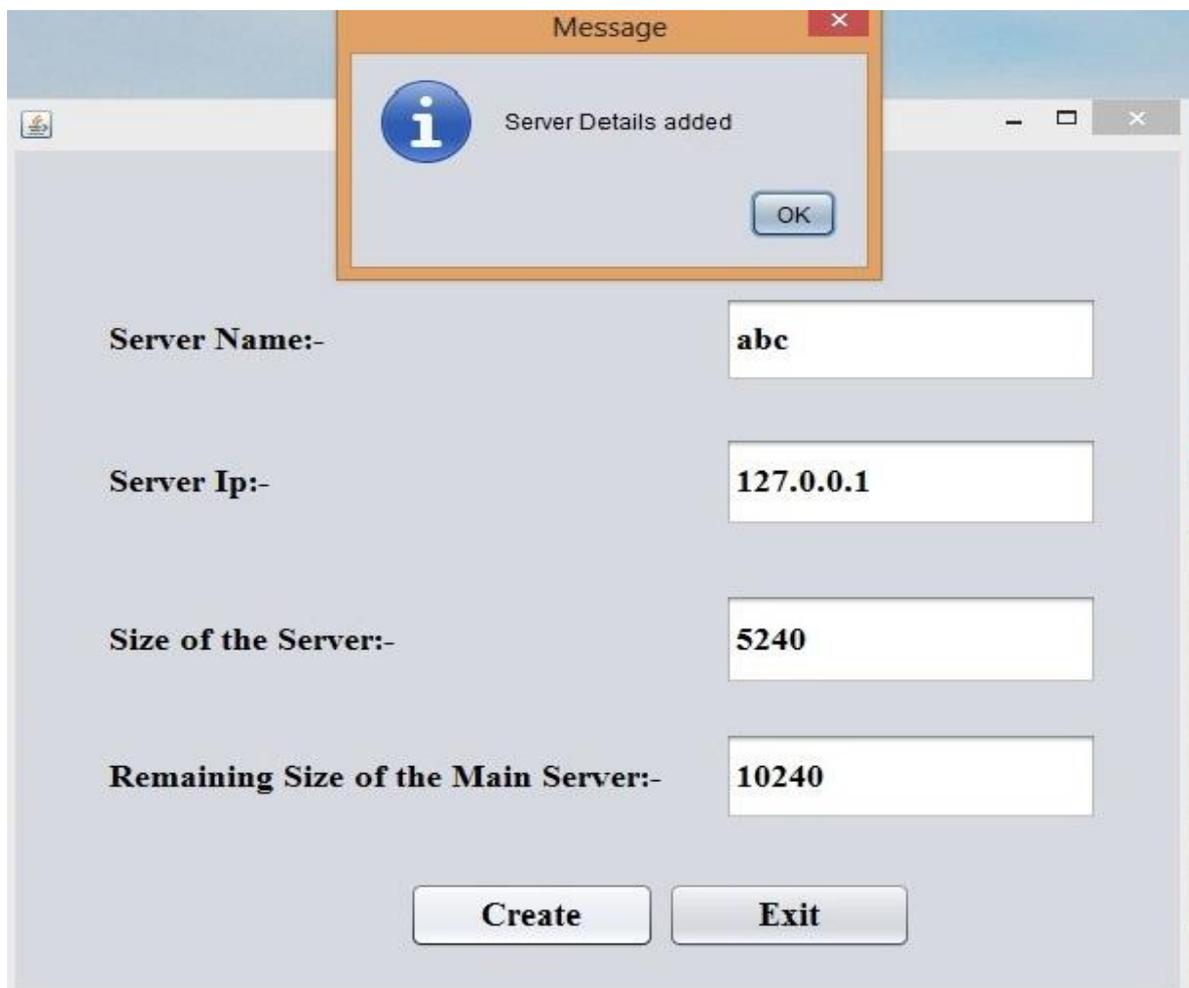
To dispatch a DDoS attack, malevolent clients first form a system of PCs that an expansive number of traded off hosts to test and check the same locations in timeframe, the spreading rate lessens in light of the fact that the quantity of the new IP .in this different will be login in the same ip address and send question so it will see the record and it will prompt over-burden on the disjoin. in out proposed we screen the inquiry originating from numerous client frame the same ip .And we investigation ip location to discover the DDOS assault

### Attack Sieving Model

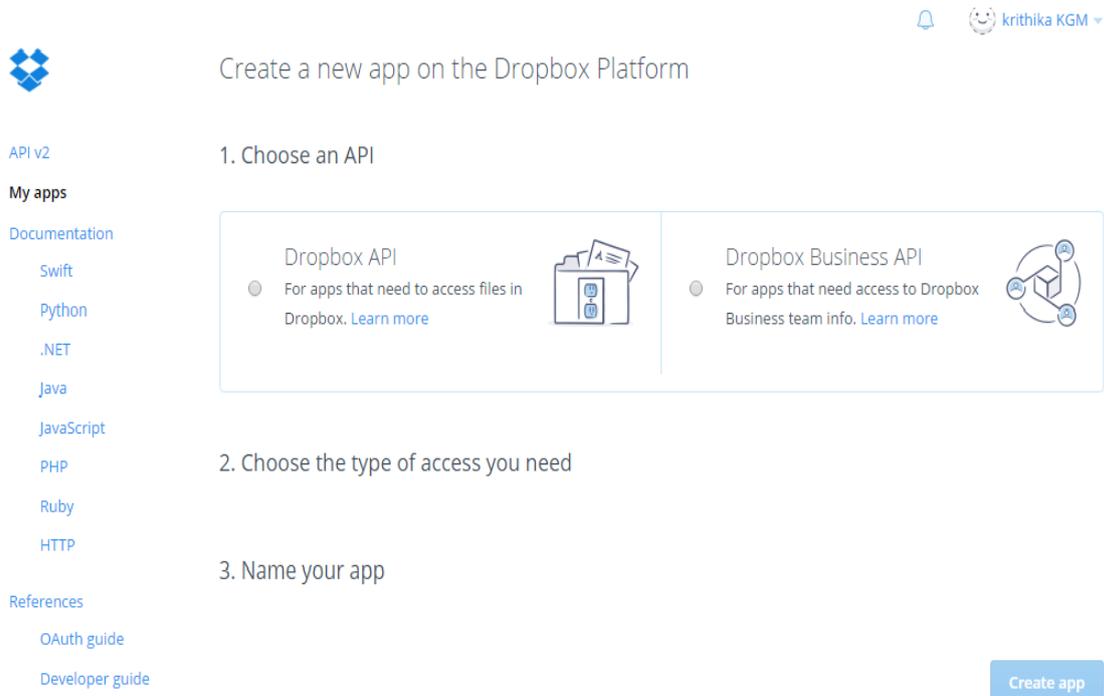
We introduce a probabilistic bundle sifting (PPF) system to safeguard the Web server against Distributed Denial-of-Service (DDoS) attacks. In the attack sifting model we execute the asked for enormous measured record past the allowed. In view of these examples client conduct is checked DDOS attack is evaded in cloud.

### Screenshots

#### 1. Constructing a Database and Uploading Server Details

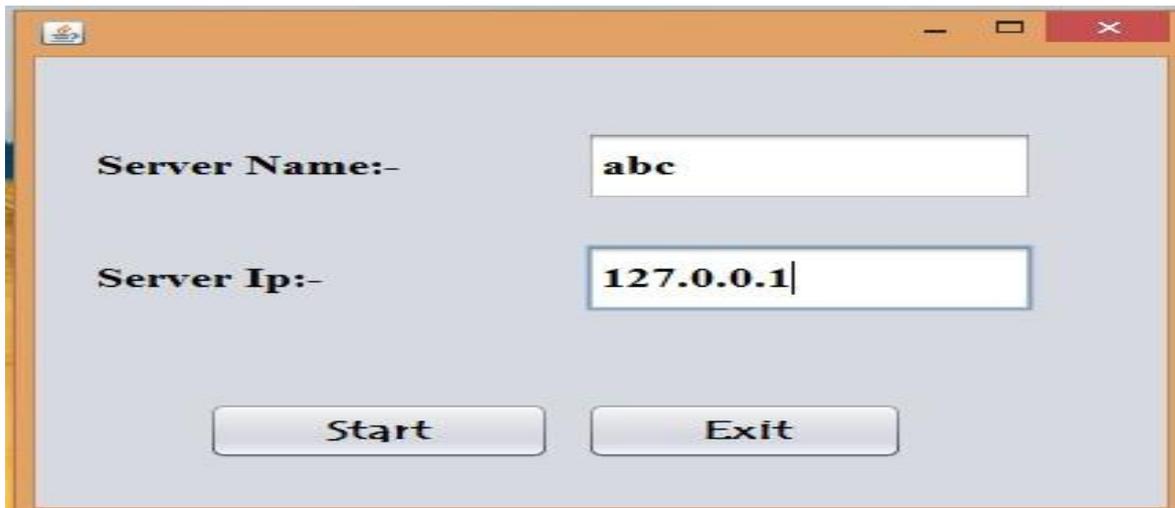


## 2. Creating an App in the Cloud

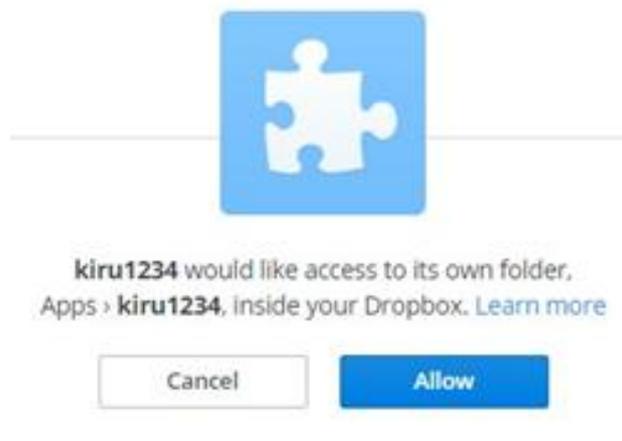


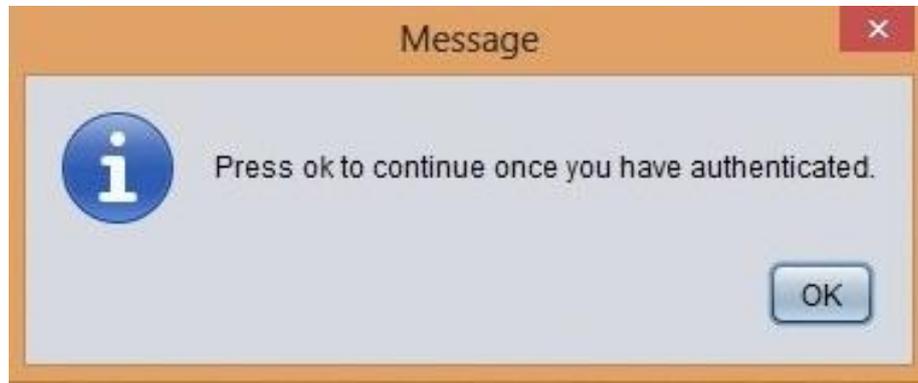
The screenshot shows the Dropbox Developer Console. At the top right, there is a notification bell and a user profile for 'krithika KGM'. The main heading is 'Create a new app on the Dropbox Platform'. On the left, there is a navigation menu with categories: 'API v2', 'My apps', 'Documentation', and 'References'. Under 'Documentation', there are links for Swift, Python, .NET, Java, JavaScript, PHP, Ruby, and HTTP. Under 'References', there are links for 'OAuth guide' and 'Developer guide'. The main content area is titled '1. Choose an API' and contains two options: 'Dropbox API' (selected) and 'Dropbox Business API'. The 'Dropbox API' option is described as 'For apps that need to access files in Dropbox. Learn more' and features an icon of a folder with a document. The 'Dropbox Business API' option is described as 'For apps that need access to Dropbox Business team info. Learn more' and features an icon of a cube with people. Below this, there are steps '2. Choose the type of access you need' and '3. Name your app'. A blue 'Create app' button is located at the bottom right.

## 3. Connecting Server IP to Dropbox



## 4. Authenticating Access To Drop Box





### 5. Creating Attacks (DDOS ATTACKS)



### 6. DDOS Attack Mitigation



## Conclusion and Future Work

Here, we propose a system to actualize stealthy attack designs, which show a gradually expanding polymorphic conduct that can avoid, or in any case, extraordinarily defer the strategies scheduled with written in recognize less-mode assaults. Misusing a helplessness objective usage, a tolerant with a smart assailant could coordinate modern streams of messages, undefined from true blue administration demands. Specifically, the proposed attack design, rather than going for making the administration distracted, it goes for abusing the cloud adaptability, compelling the administrations to scale up and expend a larger number of assets than required, influencing the cloud client more on monetary angles than on the administration accessibility

## Future Enhancement

Later on work, we go for extending the way to deal with a bigger arrangement of use level vulnerabilities, and characterizing a modern technique ready to identify attacks in the distributed computing environment.

## References

1. N.Ch.S.N. Iyengar, Arindam Banerjee and Gopinath Ganapathy ,”A Fuzzy Logic based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment” , Vol. 6, No. 3,December 2014.
2. A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment by MuhammadShahid, Younis Abbas and IqraSattar Volume 115 – No. 8, April 2015.
3. Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme by Mieso K. Denko Department of Computing and Information Science University of Guelph, Guelph, Ontario, Canada, N1G 2W1.
4. Haiqin Liu, Yan Sun, and Min Sik Kim,” Fine-Grained DDoS Detection SchemeBased onBidirectional Count Sketch”, School of Electrical Engineering and Computer ScienceWashington State University,Pullman, Washington, U.S.A.
5. ]“International Journal of Advanced Research in Computer Science and Software Engineering”,NeelamPaliwal,Ramesh Singh Rawat andDeepak Singh Ra Volume 4, Issue 5, May 2014.
6. M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson,“Security and privacy governance in cloud computing via SLASand a policy orchestration service,” in Proc. 2nd Int. Conf. CloudComput. Serv. Sci., 2012, pp. 670–674.
7. F. Cheng and C. Meinel, “Intrusion Detection in the Cloud,” in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec.2009, pp. 729–734.

8. C. Metz. (2009, Oct.).DDoS attack rains down on Amazon Cloud[Online].
9. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoSattacks for large-scale internet," *Comput. Netw.*, vol. 51, no. 18, pp. 5036–5056, 2007.
10. H. Sun, J. C. S. Lui, and D. K. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in *Proc. 12<sup>th</sup>IEEE Int. Conf. Netw. Protocol.*, 2004, pp. 196-205.
11. A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeteddenial of service attacks: The shrew vs. the mice and elephants,"in *Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun.*,2003, pp. 75–86.
12. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction ofquality (RoQ) attacks on internet end-systems," in *Proc. IEEE Int.Conf. Comput. Commun.*, Mar. 2005, pp. 1362–1372.
13. X. Xu, X. Guo, and S. Zhu, "A queuing analysis for low-rate DoSattacks against application servers," in *Proc. IEEE Int. Conf. WirelessCommun., Netw. Inf. Security*, 2010, pp. 500–504.
14. K.Santhi," Efficiently Allocating the Virtual Machines in Cloud enironment", *International journal of applied engineering research* , Feb 2014.
15. Manoj Prabhakar, K.R., LawanyaShri,M."Implementation of an issue tracking system in privatecloud", *international journal of applied engineering research*, 2014.
16. Tarun Kumar, K.S., Vignesh Kumar, P., LawanyaShri, M.," An implementation of storage provisioning in private cloud",*international journal of applied engineering research*, 2014.
17. M. B. BenjulaAnbu Malar, M. LawanyaShri,M. Deepa, K. Santhi "Approach for Secure AuthorizedDeduplication using Hybrid Cloud ", *INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH*, 2016.
18. K.Santhi, M.Deepa, M.LawanyaShri, M. B. BenjulaAnbuMalar ," An Efficient active audit services for achieving Data Integrity in Cloud System", *International Journal of Pharmacy and Technology*, 2016.

**Corresponding Author:**

**Deepa Mani\***,

**Email:** [mdeepa@vit.ac.in](mailto:mdeepa@vit.ac.in)