International Journal of Computer Networks and Communications Security

VOL. 3, NO. 10, OCTOBER 2015, 403–411
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Studying the Efficiency of using Private Certificate to Solve the Peer-to-Peer Distributed Denial of Service Attack on Cloud Computing

Nazar Kamal Khorsheed[1], Omeed Kamal Khoursheed[2], Dr.Taher Tawfeek Hamza[3] and Dr. Magdi zakaria Rashad[4]

[1, 2] Koya university, Dep of S\W engineering, [3, 4]AlMansoura University, Dep.of Computer Science

E-mail: [1]onizarkhorshd@yahoo.com, [2]omeed_khorsheed@yahoo.com, [3]taher_hamza@yahoo.com, [4]magdi_z2011@yahoo.com,

ABSTRACT

This paper presents a treatise about cloud computing security risk and attack, we explained the definition of cloud computing and the P2P network in order to understand the infrastructure and how Denial of Service attacks consumes and confuses the network infrastructure, the two type of Denial of Service attack DoS and DDoS aimed to flood the network storage and to exhaust the network resource. Among the available solutions is SSL certificates but we found It's not enough to solve and to prevent DDoS/DoS attacks, that due to the existence of SSL handshake attack. The ideal solution for Denial of Service attacks is by using private certificate protected from third party or to use multi-type and multi-level of private certificate keys. For strengthening our work we took two study cases Prolexic cloud and Parse cloud.

Keywords: *NIST, Self-Provisioning, DoS, Distributed, DDos, Fully-Qualified Domain Name, Certificates, Authorities Domain, Wildcard, SAN, UCC, Prolexic , Handshake.*

1 INTRODUCTION

Denial of Service (DoS) attack has overwhelmed the cloud computing environment, from the beginning of the internet and Denial of service attack cloud servers, database servers and even P2P network, the attackers aim to dilapidate the network resources by flooding the routers and servers with malicious requests until the target server could not response to any requests even if it was a normal and legitimate request from legitimate user.

Denial of Service attackers are experience with hacking knowledge, but their primary goal is to disrupt the network infrastructure without obtaining any further information, so they are vandals for the purposes of sabotage, So they are wasting time and suffering stressful work to upload junk data to flood the network storage, after that they will exhaust the network bandwidth by downloading the junk data , undoubtedly they are using special tool to help them in split files into small parts thus, the attack will be faster.

There is more dangerous and more destruction type of Denial of Service when several attackers from several places attack one cloud or network at the same time, with this multi-attack the cloud will face Distributed Denial of Service (DDoS) with faster impact and more destruction of network infrastructure.

Fortunately DDoS or DoS attacks are commonly used with non-HTTPS protocol that because the SSL Certificates, however HTTPS and SSL are based on TCP protocol which can be breakthrough with TCP handshake attack, after handshake completed the attacker can open SSL layer and attack it with SSL handshake attack.

2 LITERATURE REVIEW

2.1 Cloud Computing

Cloud Computing is a new technique for providing suitable access level to shared computing resources over the internet, the NIST (National Institute for Standards and Technology) defined the cloud computing as “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1,2].

Cloud Computing can be used within the large corporations or in small companies, even the autonomous users can find their resources in the clouds like torrent file sharing sites. In IT development business cloud computing taken into consideration when we care about increase the capacity or we need to add more capabilities to our cloud system without the complications of system infrastructure expansion, with cloud computing we don’t need license for new operating system or software even the training isn’t necessary and all the updated services will be online right away over the Internet.

Cloud Computing is cloud self-provisioning which means it allows the end users to set up and launch applications and services in a cloud computing environment without any involvement of the service provider or administrator privileges [1,2,13,15].

2.2 Cloudself- Provisioning Models [1,2,11]:

- *Public model:*

In the public model of cloud self provisioning the services provider provide all resources to the general public users over the Internet. These resources could be free of charge or they are available as pre-payment services. This model does not require any financial cost since all costs of hardware and software are covered by the services provider.

Public model is more scalability and not expensive because the user only pay for what he has from resources.

- *Private model*

This type provides the same services provided by public model, but not in public level, services are available only for private category of users pre-defined.

- *Hybrid model*

This model is a combination type of public model and private model; it allows the user at any time to choose between the public model or the private model in order to match the system requirements, of course the cost is changed depending on the type of services required.

2.3.Cloud Computing Service Model Categories:

In general cloud computing services model are divided into three categories [1,2,11].

- *Software as a Service (SaaS)*

Software as a Service is a distribution model, which means the cloud applications are available over the Internet as a web service (examples: email, Virtual desktop, gaming, communications). Cloud user could not control the servers, operating systems, storage of cloud infrastructure so the cloud services are accessible through a thin client and the user can access them directly from web browser or he can call the service from any developing application, online email services is a good example for (SaaS) model.

- *Platform as a Service (PaaS)*

Some cloud users need to create their own applications using programming language and utility so they will need support from the cloud provider who host the hardware and software infrastructure (example: database, web server, dev tools).

Platform as a Service relieves cloud users from hardware provision and installation problem, for the same reason (PaaS) provide the programming language utility and tools so the developer cloud user can create and run their own applications on cloud provider hardware and software infrastructure.

- *Infrastructure as a Service (IaaS)*

Infrastructure as a Service is used when cloud provider provides virtualized computing resources in his cloud computing(example : virtual machines, servers network, storage), in such virtualized environment user can maintenance and backup his cloud resources using a third-party utility and hardware. IaaS model provide a flexible resources that can be adjusted on-demand especially for businesses that require a lot of adjustment.

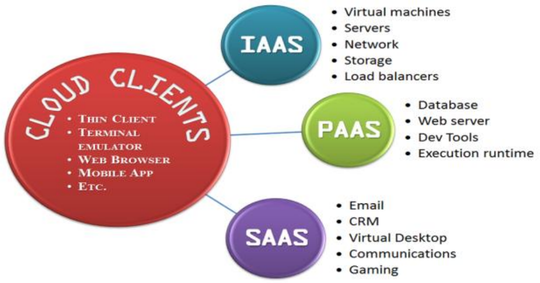


Fig. 1. Cloud Computing Services Model.[http://ohioerc.org / ? page_id=187]

3 DIGITAL CERTIFICATES

In cloud computing, identity credentials expressed by the expression Digital Certificates .those digital certificates are small data files stored in users device or on some cloud servers, each file contains certificate key to define the user identity and the access level (Authorities). The certificate key must be verifiable so that the websites or internet-based services can authorize the user identity to take trusted transactions online. In this trusted transactions information are protected and encrypted by Certificate Authorities (CAs) key [3,4,6].

When the user try to access any internet-based services the web browser will verify the digital certificate data and modify user session automatically. If user is using HTTP (HyperText Transfer Protocol) he will be transfer immediately to the secure session HTTPS. In HTTPS all transactions data between user and the internet-based services are encrypted and secure through SSL (Secure Sockets Layer) communication.[3,4,6]

SSL Certificates are valid for a finite period of time like twelve months or more, and SSL certificates are restricted to unique domain name to ensure that the user is accessing the domain which included in the certificate. In fact the unique domain name suffer from the sub-domain problem, in this situation sites need to use sub-names prefix with the same root name and that means cloud site with multi sub-domain requires multi SSL certificate , therefore certificates will be expensive and time-consuming .

To solve multi certificate problem, certificate providers have tow type of multi-use SSL certificate [3,4,6,7]:

- *Wildcard Certificates*

In Wildcard Certificates allthe sub name embedded in a certificate must be in the FQDN format followed by Fully-Qualified domain name. This type needs a single certificate to secure domain and its own sub-domains.

Wildcard certificate does not require all website service names, we can use a wildcard character (*) instead of the prefix name of the sub-domain name

Example:

We have the domain google.com which has the mail service as a sub-domain mail.google.com so in Wildcard it will be *.google.com , at the same time this Wildcard for google.com will cover any presented service and all the future services automatically.

- *Multi-Domain Certificates*

In multi-domain certificates we can include all multi FQDN (Fully Qualified Domain Names) within the same certificate, one multi-domain certificate can support up to 100 different FQDN and each domain is declared a single primary service with additional entry called SAN (Subject Alternative Name) or UCC (Unified Communications Certificates),with this type of multi-domain if we change any service name we have to change the certificate and to update the new certificate to all devices[3,4,6] .

Multi-domain certificate does not support sub-domain and wildcard characters is not permitted.

Multi-domain certificate with shared SSL is often used in the web hosting domains like HostGator domain, HostGator host a lot of site and each site can have its own private SSL ,but there is a shared SSL customized for the purposes of site management and Cpanel administration . In other words all hosted site will use the same shared SSL despite the difference in their domain names.

4 CERTIFICATE AUTHORITY PRIVATE KEY AND PUBLIC KEY MECHANISM

Certificate Authority (CA) has three keys private, public and symmetric, all of them to identify the security of transactions, CA mechanism is as follows [3,6,7,16]:

- User browser requests a secure page like https://mail.google.com.
- Domain sends its public key with its certificate.
- User browser checks if the certificate is still valid and if the certificate is related to the domain contacted.
- User browser uses the public key to encrypt a new random symmetric key.

- User browser sends the symmetric key to the server with the encrypted required url.
- Domain decrypts the symmetric encryption key using its private key.
- Domain uses the symmetric key to decrypt the url.
- Domain sends back the requested html document and http data encrypted with the symmetric key.
- User browser decrypts the http data and html document using the symmetric key and displays the information.

5 PEER-TO-PEER CLOUD

Peer to Peer (P2P) Cloud is a decentralized communications cloud model, in P2P we called the party as (a peer), and each a peer has the same privilege and capabilities in the network architecture, any peer can start a communication session. Contrast to the client-server cloud model where the client makes a service request and the centralized server, the server responds the client request with HTTP response, in P2P cloud architecture each a peer will do the necessary operations to keep the network continuance through implementation of the functions of server and functions of client [5,8,9,12].

5.1 Peer-To-Peer Models

- *Hybrid P2P model*

In the hybrid P2P model network has a centralized server which keeps information about the all peers in network, and the peers are answerable for storing their information on the server. When a peer wants to contact with another peer it will request server for the address as a query, after the server response they can contact directly.

- *Pure P2P model*

In pure model there isn't any centralized server. Each peer plays the role of client and the role of server at the same time.

- Mixed P2P model

In the Mixed model network has clustering without any centralized server. Each cluster is a group of pure nodes.

P2P Cloud Benefits

- P2P cloud provide anonymous routing of network traffic.
- P2P cloud ensures massive parallel computing environments.
- P2P cloud is a distributed storage over the Internet.
- P2P cloud considered as media sharing cloud.

5.2 P2P Cloud Disadvantages

- P2P cloud associated with software piracy.
- P2P cloud most of the time violate software and media copyright.
- P2P cloud is permeable cloud.
- P2P cloud does not guarantee the contents of files.
- P2P cloud files may contain viruses or backdoor spy files.

6 ATTACKS ON P2P CLOUD AND SECURITY ISSUES

Cloud computing broadly implicate many technologies including networks, databases, operating systems, multi-media , virtualization, resource scheduling, transaction management, Streaming , load balancing, concurrency control and memory management, therefore there are many security issues in cloud computing and the cloud computing has to be secure and trusted[5,9,10]. For the same reasons there are different types of attack in cloud computing [5,11,12]:

- Null Prefix Attack.
- Cloud Malware Injection Attacks.
- Flooding Attacks.

In this paper we will focus on "denial of service" flooding attack .

6.1 Denial of Service Attack (DoS and DDoS)

The DoS (Denial of Service) attack is an flooding attack on a cloud computing or a network , DoS causes loss of a service. In the of P2P cloud DoS attack is an attempt to flood the cloud with bogus packets in order to prevent the natural transaction in the network [10,11,12,15].

DoS attacker aim to fill the cloud space with junk data in the format of big files , after that the attacker will use malicious peer or node to request the junk files from the cloud. Depending on the size and number of junk files the cloud will be flood and become heavy so it could not transfer the data for all users.

It may happen that the cloud users trying to download these junk files , which leads to waste time and consumes cloud bandwidth.

There is another way to DoS attack which is to overload the cloud with account data request to be overstuffed and could not respond to any other request.

Compounding the problem that in P2P cloud there is no centralized server to verify the requests and services or to check the junk files and this is invaluable gift to the attacker .

DoS attacks will be more efficient if there are multiple attacker with multiple host involved in the attack, multiple attacker with multiple host that mean we facing a distributed denial-of-service (DDoS) ,DDoS caused network overstuffed in a short period of time[13,15] .

So that we can overcome DoS attack if we have a mechanism to verify the user who is sending the files or request services instead of verifying the data itself.

6.2 Denial of Service Attack Defenses

Protect against DoS or DDoS attacks are very difficult ,That because it's hard to classified the attack requests from the normal and legitimate requests.

If we visit digitalattackmap.com on the URL http://www.digitalattackmap.com/#anim=1&color=2&country=ALL&list=0&time=16690&view=map

We can see the "Top daily DDoS attacks worldwide" as shown in Fig 2

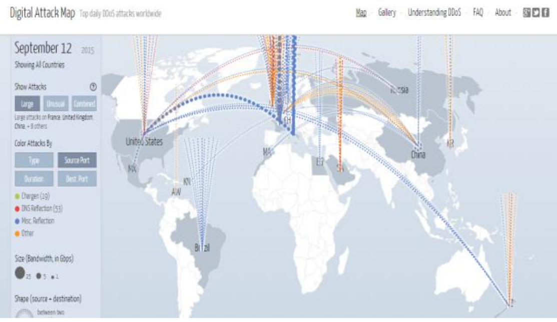


Fig. 2. Top daily DDoS attacks worldwide [http://www.digitalattackmap.com]

Digital Attack Map visualizing the tens of thousands of attacks against the websites of newspapers, businesses and charities every day, and it describes DDoS as "A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information"[14].

From the visualize map of raw data behind DDoS attacks we conclude it is a complex issue , and it is hard to understand the challenge of distributed denial of service .Map shows that word cloud computing all the time in digital conflicts.

6.2.1 DDoS / DoS Detection Techniques

The important step in defenses against DDoS is detection the attack, there are accredited techniques in DDoS attack detection include:

1. Anomaly/ abnormal detection:

This technique detects DDoS attacks by recognizing the anomaly or abnormal behaviors performance of the cloud computing. The detection mechanism done by comparing current values with previously detected normal cloud computing performance values [15,16,18].

2. Misuse Detection:

This technique detects the DDoS attacks depending on intrusion detection system (IDS) , the IDS gathers information and analyzes it by compare the information with large databases of attack signatures looking for a specific attack documented [15,16,18].

If DDoS attack is detected then we have to block the attack and trace the attacker id and location.

6.2.2 DDoS / DoS and SSl:

In the early appearance of Denial of Service attacks fortunately SSl was secured and Denial of Service attacks succeed just with non-HTTPS, But with the evolution of attack techniques ,Attack elevated to disrupt both secured and clear text services and exceeded that to attack SSL itself, taking advantage of traditional TCP handshake attack.

TCP layer is the most targeted of Denial of Service attacks. Despite of the different methods of attack but they all share one distinctive which is to attack the capacity of the network infrastructure which support concurrent TCP connection[16,18] .

No matter how many firewalls on the network the ability to maintain TCP connections is limited and insufficient.
In case one TCP handshake attack succeed it will open a network SSL session ,the attacker gets a chance to access this session and he will start with dangerous type of attacks which is SSL handshake attack. The attacker will exhaust network resources by sending junk data to the SSL server, so the SSL rules undertake to process the junk data as a legitimate data, what compounding the problem is the attacker has a completed TCP handshake so the firewall will not interfere to block the attack.

6.2.3 DDoS / DoS and JavaScript

Many people may believe that attack cloud with DDoS requires superior technical skills. But the truth, the process really simpler than that especially if it was organized and found a lacuna in the cloud system.

Several lines of JavaScript can constitute a large DDoS attack , the main idea is to do infinite or repeatedly request the cloud URL or (any sub-domain cloud) , in the next example of code we will see a basic attack on cloud called demo.com ,on demo cloud there is a page called user_documents.php which request the user Id as GET parameter and it response all the documents of this id (demo.com/ user_documents.php?Id=1).

```
$(document).ready(function () {
        var url =
'http://www.demo.com/user_documents.php';
        var repeat= true;
        var id = 0;
        while (repeat) {
           id++;
           var temp=";
           $.get(url + "?ID=" + id, function
(files) {
                if (files != ") {
                  ///....JavaScript to download all
files in the page
                  //.... Download (files)
                  //.........
                }
           });
                  }
      });
```

By this example any user opens the script page he will download all the documents for all user in demo.com cloud , In fact subject may be easier than that, look to the next code :

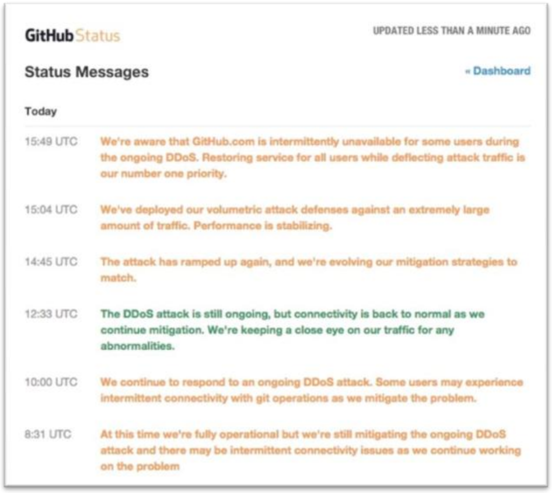
```
<script type="text/javascript">
 while (true){
 document.write('<iframe
src="http://www.demo.com/" width="0"
height="0" frameborder="0"
scrolling="no"></iframe>');
}
</script>
```

The above code will call demo.com millions of times, in all cases the malicious script will exhaust demo.com bandwidth.

How the attacker organized his malicious JavaScript to be distributed attack?
The answer is quite simply, the attacker has his one proxy site, which proved open blocked sites service, the proxy customer just went any tool to open his blocked site and he does not care if this tool attack others in background. Like those script need lass then 20 hours to fooled could an take it done (depending cloud sources) we try one html injected with DDoS JavaScript-based to attack a local cloud and this html page distributed on 50 site then we request the 50 page from on site in JavaScript IFrame , the result was 15 hours to prevent the cloud service.

6.2.4 The latest DDoS Attack Statistics

According to the latest statistics from the security companies that Github cloud is fighting the largest DDoS attack in 2015, but it halted most of the attack traffic. The attack was advanced JavaScript hosted by Chinese anti-censorship projects. The attack started at 19/3/2015:3 AM. However Github cloud continued to provide services for all users , at the same time it track the attack source and it's end aim to find that the attacker try to fooled tow projects hosted by Github cloud GreatFire project and the CN-NYTimes project. So Because the Github has become saturated it send a Twitter message contain " The DDoS attack has evolved and we are working to mitigate" this massage was at 30/3/2015:8:50AM.



GitHub Status

UPDATED LESS THAN A MINUTE AGO

Status Messages

« Dashboard

Today

15:49 UTC We're aware that GitHub.com is intermittently unavailable for some users during the ongoing DDoS. Restoring service for all users while deflecting attack traffic is our number one priority.

15:04 UTC We've deployed our volumetric attack defenses against an extremely large amount of traffic. Performance is stabilizing.

14:45 UTC The attack has ramped up again, and we're evolving our mitigation strategies to match.

12:33 UTC The DDoS attack is still ongoing, but connectivity is back to normal as we continue mitigation. We're keeping a close eye on our traffic for any abnormalities.

10:00 UTC We continue to respond to an ongoing DDoS attack. Some users may experience intermittent connectivity with git operations as we mitigate the problem.

8:31 UTC At this time we're fully operational but we're still mitigating the ongoing DDoS attack and there may be intermittent connectivity issues as we continue working on the problem

Fig. 3. GITHUB Status During Tthe Attack [http://www.theregister.co.uk/2015/03/27/github_under_fire_from_weaponized_great_firewall/]

GreatFire project received more than 2.6 billion requests per hour which is about 2500 times more than normal levels, all of that flood because GreatFire project fighting against anti-censorship in China, so the purpose of the attack became clear.

After six days GreatFire project faced attack from CNNIC (China Internet Network Information Centre)

In order to stop the attack Github appealed the third party Insight-labs (a group of security organizations) which confirmed that the attack is from China with malicious JavaScript hosted by www. baidu.com (baidu search engine) and the script works to hijack HTTP connections.

6.2.5 Private Certificate and Third Party Solution

After we identified the problem and found that the firewall alone is not enough and even with the use of SSL the opportunity for DDoS/DoS attacks is available[18].

Most of relevant authorities to information security found the best solution to solve and prevents DDoS/DoS attacks is by using private certificate in collaboration with a third party. In the next paragraphs we see Prolexic as third party and how it reduces the risk of DDoS/DoS attacks. Prolexic is a cloud with five technical centers around the world, Prolexic abilities to dedicate Denial of Service in network with a capacity of more than 1.8 Terabits in one second. Prolexic has huge anti-DDoS bandwidth, so it can protect concurrent DDoS attacks on multiple clients cloud in seconds.

When Prolexic detects that your cloud already attacked it will immediately reroutes the attacking traffic to the nearest Prolexic technical center where it is can be cleaned and then routed back to your network.

Prolexic has SSL certificate key sharing tools which authorize cloud customers to have control and maintain their SSL keys at all times, and this sharing tools includes [19] :

- PLXabm (Prolexic Application Based Monitoring) service
- PLXproxy SSL Manager service
- Prolexics on-demand
- Symmetric DDoS mitigation service

With these serves Prolexic can detect and stop DDoS attacks , the first step from the cloud customer is to upload his SSL keys and certificates to PLXproxy SSL Manager and then he must deploy the certificates key with two options:

- Stored securely for reuse.
- Provide temporary certificates and keys to by revoked after Denial of Service attack is stopped.

After that cloud customer can access his SSL keys and certificates through the PLXportal online with the visibility to mitigation Denial of Service attacks.

Another example for third party certificates is Parse.com, Parse is a cloud where the users can build and power applications for any platform , Parse provides three type of services Core Data , Push Notifications and Analytics, Parse customers must get Parse certificate keys to authorizes access.

Cloud like Parse is all the time under Denial of Service attack, this is because must off the Parse customers create a web-service on their domain and this web-service request one of Parse services, it could happen that the free-customer himself attack Parse cloud or any attacker aim to attack the customers web-service, consequently he will attack the Parse itself with customer authorizes. To solve this problem Parse used several certificate keys [20]:

- CSR (Certificate Signing Request), which allows the customer to access Parse services though HTTPS and apply SSL certificate.

- Application ID Key, it is the main identifier that uniquely specifies customer application.

- Client Key, to be used in consumer clients of customer application.

- JavaScript Key, to be used in JavaScript SDK applications.
- Windows Key, to be used in the Windows 8 and Windows Phone 8 SDK.
- REST API Key, to be used when making requests to the REST API
- Master Key, This key is only allowed to access the REST API and does not adhere to object level permissions. This is equivalent to admin level access and should be kept secret.

When these keys work together Parse can protect the cloud and reduces Denial of Service attacks.

7 CONCLUSION

Within this paper we found that protecting cloud computing against Denial of Service attacks is very difficult and there isn't an integrated solution to end Denial of Service attacks, All solutions are offered only to minimize the impact of Denial of Service attacks, that because it’s impossible to detect the malicious requests from the normal and legitimate requests.

As a result, cloud computing with traditional firewalls can't reduce Denial of Service attacks especially the distributed attack , even if cloud computing used SSL certificate the opportunity for Denial of Service attacks is available as long as the traditional TCP handshake attack existing.

We also found that the solutions which adopt the idea of a third party certificate are more useful and feasibility to stop DDoS or Dos, in this paper we considered Prolexic as one of the leader in certificate security third party field .so we learned about the way that it protects its customers from DDoS.

In the end, we can say that Denial of Service attacks can't be stopped no matter what methods we used keys, certificate and firewalls, all we can do is to reduce the risks of attacks.

8 REFERENCES

[1] The NIST Definition of Cloud Computing (SP 800-145),” http://csrc.nist.gov/publications/PubsSPs.html#800-145.”

[2] SO, K. "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks, 2011.

[3] Phong Q. Nguyen, David Pointcheval ," Public Key Cryptography - PKC 2010", International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010

[4] Professor Ninghui Li ,"Computer Security-Public Key Encryption and Digital Public Key Encryption and Digital Signatures", cs.purdue.edu 2010.

[5] H. Schulzrinne,E. Marocco, E. Ivov "Security Issues and Solutions in Peer-to-Peer Systems for Realtime Communications", Internet Research, ISSN: 2070-1721 February 2010

[6] Franck Martin, " SSL Certificates HOWTO" , The Linux Documentation Project LDP 2002

[7] Zhou, Jianying, Young, Moti (Eds.),"Applied Cryptography and Network Security" 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010

[8] http://www.wikipedia.com," Peer-to-peer".

[9] Prashant Dewan and Partha Dasgupta “P2P Reputation,"Management Using Distributed Identities and Decentralized Recommendation Chains” IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 22,NO. 7, JULY 2010

[10] R. K. Balachandra, P. V. Ramakrishna and A.Rakshit. “Cloud Security Issues.” In PROC‘09 IEEE International Conference on Services Computing, 2009, pp 517-520

[11] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. “On Technical Security Issues in Cloud Computing” In PR OC 09 IEEE International Conference on Cloud Computing, 2009pp 110-112 pp.109-116, Sep 2009

[12] Xiang Fan ,Yang Xiang “Modeling the propagation of Peer-to-Peer worms” Future Generation Computer Systems Volume 26 Issue 8, October, 2010

[13] Sabu M. Thampi, Albert Y. Zomaya, Thorsten Strufe, Jose M. Alcaraz-Calero, Tony Thomas,"Recent Trends in Computer Networks and Distributed Systems Security",International Conference, SNDS 2012, Trivandrum, India, October 11-12, 2012

[14] http://www.digitalattackmap.com

[15] Saman Taghavi ,James Joshi, David Tipper,"A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS , 2013.

[16] Dr. Karen Collins,"Introduction to Business", section 15.6 "Security Issues in Electronic Communication”, 2012

[17] Vangie Beal ,” How to Protect Your Business Against Cyber Attack”, Webopedia.com.

[18] Jonathan Lewis ,"DDoS Attacks on SSL: Something Old, Something New", arbornetworks , 04/24/2012

[19] http://www.prolexic.com/

[20] https://parse.com/questions/what-is-the-purpose-of-the-different-types-of-parse-application-keys.