

AN EFFICIENT MECHANISM TO PROTECT CLOUD FROM INTERNET ATTACKS

Lokashree S¹, Lokana S², Dr.M V Sathyanarayana³

¹ PG Student, ² PG Student, Computer Science & Engineering,

Rajeev Institute of Technology, Hassan, Karnataka, (India)

³Technical Director, Rajeev Institute of Technology, Hassan, Karnataka, (India)

ABSTRACT

Due to rising threat of internet attacks, especially distributed denial-of-service (DDoS), traceback problem has become very relevant to internet security these days. The web services can get vulnerable to denial of services (DoS) or xml denial of services (xdos) attack which hamper web services by crashing the service provider and its services. In order to rescue from such attacks, there are some techniques that are being introduced such as traceback architecture, framework, grid, authentication and the validation. Simple Object Access Protocol (SOAP) allows the communications interaction between different web services. The messages of SOAP are constructed using either Hyper Text Transport Protocol (HTTP) and/or Extensible Mark-up Language (XML). In a way to find the real source of Internet attacks, we must be capable of discovering the origin of IP packets without having to rely on the source IP address field. This capability is known as IP trace back. To address the problem of kinds of internet attacks against cloud web services discussed above there is a need to differentiate the legitimate and illegitimate messages. This work has been used to not only trace DDoS attacking packets but it also enhances filtering attacking traffic. This holds a wide array of applications for other security systems. We have taken three types of filters namely MATCH, MARK, MAKE OVER and DUMP[13]. Then we use ECC algorithm to protect the genuine/legitimate data. The ECC algorithm will compress the original file, encrypts the plaintext data into cipher text and then hides the message being exposed to the attacker.

Keywords: *Traceback, SOAP, Ddos Attack, Filters, ECC Algorithm.*

I. INTRODUCTION

Cloud computing involves deploying groups of remote servers and software networks that allows centralized data storage and online access to computer services or resources. In a Cloud computing environment, resources are pooled to provide infrastructure, platform and software as services to many possible users by sharing the available resources. In this model customers sign in into the cloud to access IT resources that are priced and provided on-demand. Due to the rising threat of internet attacks, especially distributed denial-of-service (DDoS) attack, Traceback problem has become very relevant to internet security. Since the DDoS attackers spoof the source address, tracing them is very difficult. DDoS attack actually hamper web services by crashing the service provider and its services. The proposed approach is very simple to implement, scalable enough and helps rescue from DDoS attacks more effectively since these attacks can only be detected and cannot be prevented. This approach uses ECC(Elliptical Curve Cryptography)algorithm to compress/encrypt/hide the original data being exposed to the attacker.

1.1 Attributes of Cloud

Some of the essential attributes of the cloud model are security, reliability, availability, scalability, QoS, on-demand self service, broadband network access, resource pooling and rapid elasticity. The cloud can be characterized as private, public, community or uses. In public cloud computing model, services such as applications and storage, are available for general use over the Internet. Services of public cloud may be offered on a pay-per-usage mode or other purchasing models. IBM's Blue Cloud is an example of a public cloud. Private cloud is a virtualized data center that operates within a particular firewall. These types of cloud are highly virtualized, joined together by mass quantities of IT infrastructure into resource pools, and privately owned and managed. A hybrid cloud is a mixture of public and private clouds. Community cloud is an infrastructure shared by several organizations which supports a specific community. The cloud delivers its services in the form of software, platform and infrastructure. Costly applications like ERP, CRM will be offloaded onto the cloud by provider. They run at providers cost. Platform includes the languages, libraries etc. and the database, operating system, network bandwidth comes under infrastructure.

1.2 Security Concerns

Trustworthiness is one of the key concerns of the cloud service provider. Organizations are carefully deceiving both their sensitive and insensitive data to cloud to fetch required services. Cloud works on pay per use basis. Suppose a DoS attacker intentionally sends numerous requests to cloud then the owner of that particular cloud will have to process more requests at a time. Meanwhile, if other genuine users sends request to the server on cloud, their service will be denied since the server will be busy serving the DoS attacker. The other worst case is DDoS attack, where the attacker compromises some more hosts to send the flood request.

1.3 Denial-of-Service Attack/ Distributed Denial-of-Service Attack

A **denial-of-service attack (DoS attack)** or **distributed denial-of-service attack (DDoS attack)** is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. This attack hamper web services by crashing the service provider and its services. DoS attacks are illustrated in figure 1.3(a).

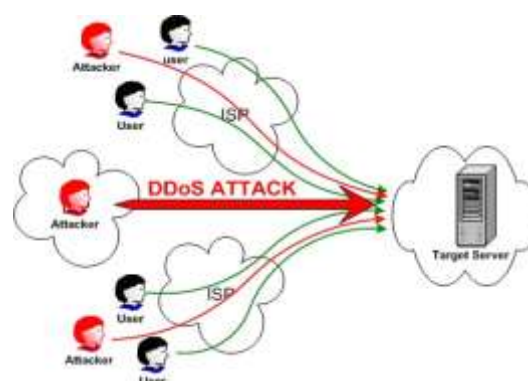


Fig1.3(a): DDoS Attack

1.3.1 Modes of Attack

In a denial-of-service attack, the attacker makes an explicit attempt to prevent legitimate users of a service from using that service. Two common forms of DoS attacks are: 1. those that crash services and, 2. those that flood services.

II. RELATED WORK

In a Cloud computing environment, cloud servers that provide requested cloud services, may sometime crash after they receive huge amount of request [16]. This situation is called Denial Of service attack. Cloud Computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. Cloud Computing is changing the IT delivery model to provide on-demand self-service access to a shared pool of computing resources (physical and virtual) via broad network access to offer reduced costs, capacity utilization, higher efficiencies and mobility. Recently Distributed Denial of Service (DDoS) attacks on clouds has become one of the serious threats to this buzzing technology. Distributed Denial of Service (DDoS) attacks continue to plague the Internet. Distributed Denial-of-Service (DDoS) attacks are a significant problem because they are very hard to detect, there is no comprehensive solution and it can shut an organization off from the Internet. The primary goal of an attack is to deny the victim's access to a particular resource. In this paper, we want to review the current DoS and DDoS detection and defence mechanism.

The main problem faced in a cloud environment is the Distributed denial of service (DDoS) [17]. During such a DDoS attack all consumers will get affected at the same time and will not be able to access the resources on the cloud. All client users send their request in the form of XML messages and they generally make use of the HTTP protocol. So the threat coming from distributed REST attacks are more and easy to implement by the attacker, but such attacks are generally difficult to detect and resolve by the administrator. So to resolve these attacks we introduce a specific approach to providing security based on various filters. We make use of five different filters which are used to detect and resolve XML and HTTP DDoS attack. This allows the security expert to detect the attack before it occurs and block or remove the suspicious client.

Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks [18]. DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not obeying traditional end-to-end congestion control, the problem must be handled by the routers. Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack.

Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router's resources be used to route legitimate traffic. In this paper we present an architecture for Pushback, its implementation under FreeBSD, and suggestions for how such a system can be implemented in core routers.

Cloud Computing is an emerging area nowadays. Researchers are working on all aspects of cloud viz [19]. cloud network architecture, scheduling policies, virtualization, hypervisor performance scalability, I/O efficiency, data integrity and data confidentiality of data intensive applications. The dynamic nature of cloud presents researchers new area of research that is cloud forensics. Cloud Forensics is the branch of forensics for applying computer science knowledge to prove digital artifacts. The DDOS is the widely used attack in cloud environment. To do the forensics of DDOS if it is identified a possible detection and prevention mechanisms would aid in cloud forensics solutions and evidence collection and segregation. This paper presents different types of DDOS attack at the different layers of OSI model with increasing complexity in performing attack and focuses more on prevention and detection of DDOS at different layer of OSI and effect of DDOS in cloud computing.

The theoretical background of our proposed work is taken from reference [13]. We are giving security to the confidential data by using ECC algorithm. This algorithm inhibits stronger encryption, efficient performance, high scalability and future of crypto tech.

III. PROPOSED WORK

Flaws either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched. Of the kinds of network attacks, denial-of-service flood attacks have caused the most severe impact. Cloud computing suffers from major security threat problem by HTTP and XML Denial of Service (DoS) attacks. The combination of HTTP and XML messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider is called as HX-DoS attack. To address this issue, there is a need to differentiate the genuine or legitimate message and illegitimate message.

HX-DoS attack involves an attacker who compromises a client having an account to access the cloud service provider server. Therefore, the attacker gets direct connection through the system. Then the attacker will install HX-DoS attack program at the user end and initiates it. The XDoS attack can take place in few ways: First, a network can be flooded with XML messages (instead of packets), in order to prevent legitimate users to network communication. Next, if the attacker floods the web server with XML requests, it will affect the availability of these web services. Finally, attackers manipulate the message content, so that the result web server gets crash. In order to differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH filter. MATCH filter is located one hop away from host. The rule set of MATCH filter has been built up over time to identify the known HDoS and X-DoS messages. The well known HX-DoS attack is XML injection or XML Payload Overload, MATCH filter is trained and tested to identify these known attacks. After the detection of HX-DoS message, MATCH filter drops the packet which matches the rule set. The packets are subjected to marking after they are examined by the MATCH filter. The ECC algorithm is used to convert the plaintext data into corresponding cipher text so that the attacker cannot view the original data being transmitted. The ECC algorithm will compress the file, encrypts it and hides the message from DDoS attacker.

IV. DESIGN CONSIDERATIONS

Consider two legitimate users and an attacker. User sends data through three filters namely, MATCH filter, MARK filter and MAKE OVER and DUMP filter to the server.

The message will be identified and if it is from an attacker then that message will be dropped before it reaches the server.

Modulo packet marking consists of two routers:

1. Edge router
2. Core router

On the victim side, by the time the victim starts collecting marked packets, all routers in the network will already have invoked the packet marking procedure. In extension, the victim does not have any knowledge about the real network or the attack graph. But the victim only knows the marking probability that the routers use.

It is appared with the ability to mark packets as in the original Probabilistic Packet Marking(PPM) algorithm where each router shares the same marking probability. In specific, a router can either be a transit router or a leaf router. A transit router is a router that forwards traffic from upstream routers to its downstream routers or to the victim, whereas a leaf router is a router whose upstream router is connected to client computers and not to routers and forwards the clients' traffic to its downstream routers or to the victim. Assuredly, the clients are mixed with genuine as well as malicious parties. Likewise, every router will be having only one outgoing route toward the victim named "outgoing route toward the victim" and this can be further justified by the fact that modern routing algorithms favor the construction of routing trees. The plaintext data inside the packet will be converted into cipher text data using ECC algorithm so that when an attacker tries to get the data, he will be unable to read the original plain text data. The most essential features of an ECC are as follows: stronger encryption, efficient performance, high scalability and future of crypto tech.

1. Stronger encryption:

- shorter key than RSA.
- 256-bit ECC = 3072-bit RSA.
- 10 times harder to crack than RSA 2048.
- meets NIST standards.

2. Efficient Performance:

- efficiency increases with higher server loads.
- utilizes less server CPU.
- ideal for mobile devices.

3. High Scalability:

- large SSL deployment without additional hardware.
- securing the enterprise: uses fewer resources, lower costs.

4. Future of crypto tech:

- viable for many years.
- built for internet of Things.
- supports billions of new devices coming online.
- Ideal for open networks.
- truly "future proof" trust infrastructure in place.

4.1 Goals

The denial-of-service (DDoS) attacks are addressed, where they try to suspend services of a host connected to the internet. The major goal of this project is to filter the genuine message from the message and pass that genuine message to the server, so that only genuine user can get resources of Cloud server. And the ECC algorithm is used so that the raw data is encrypted and is converted to cipher text so as to make it difficult the attacker to identify the message. Figure 4.1(a) demonstrates ECC.

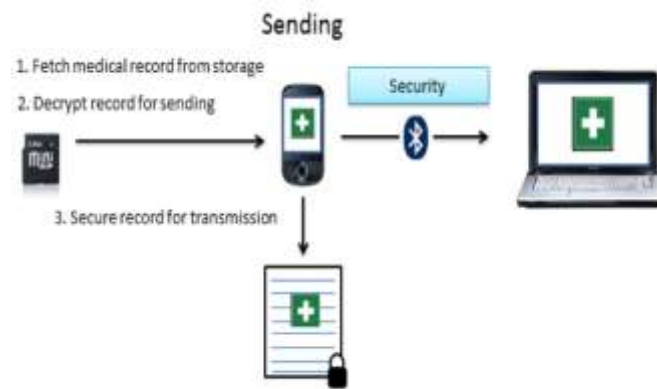


Fig4.1(1): Elliptical Curve Cryptography

4.2 Modules

In a DDoS attack, an attacker compromises a client who has an account to access the cloud service provider server. By this way they get a direct connection through the system. The attacker then installs the DoS attack program at the user end and initiates it. To differentiate them, the first method adopts Intrusion Detection System (IDS) by using a decision tree classification system called as MATCH. MATCH filter is located one hop away from host. MATCH's rule set has been built up over time to identify the known DDoS messages. With the help of known DDoS attacks like XML injection or XML Payload Overload, MATCH filter is able to be trained and tested to identify these known attributes. Upon detection of DDoS message, MATCH filter drops the packet which matches the rule set. After MATCH examines all the packets, they are subjected to marking. Next marking scheme is the Mark algorithm. As the packets travel via network, they are marked with router information using modulo technique. Upon trace-back request, reverse modulo is used to make over the path traversed by the packets. The marking is done on both edge and core routers. When an edge router decides to mark an incoming packet, it fetches the code to be marked that corresponds to physical address of the host from the lookup table and encodes it into the packet. The edge router requires one bit for indicating whether the packet is marked or not and few bits for marking code and it maintains a lookup table called MAC to ID table, which has physical address of the hosts attached to the network and equivalent numeric code for each of the physical addresses.

The core router marks the packet only if that packet has been already marked by the edge router. Else, it would simply forward the packets. Core router maintains a table called MAC to Interface which contains the physical addresses of all of its hardware input interfaces and link numbers assigned to each of these interfaces.

When a router decides to mark, it consults the table to find the link number assigned to the inbound interface.

The core router uses the modulo technique for marking is calculated as in Equation 1,

New marking information = current marking information \times number of interfaces on the router + the link number
(1)

Make over and Dump filter, which is built from the IDP and its location is one hop back from the victim. Specifically, the host follows the same path (shortest path) across the routers for sending the packet to its destination. Make Over and Dump component maintains the information about each host and its equivalent packet marking value. If the marking value matches the stored value, it forwards the packet to respective host. During the time of the attack, when host spoofs the IP address of another host, the packet marking value differs

from the value stored in the Make Over and Dump filter. This happens because: For marking, MATCH filter uses MAC address instead of the IP address. Therefore, the packets are dumped at the victim side and Make Over and Dump requests for the trace-back.

The ECC algorithm takes place in following steps [14]:

Step1: Select any master file from embed message.

Step2: Select a random picture from the local drive.

Step3: After master file has been selected, select output file to embed message.

Step4: If the file should be compressed, then click on check box compress.

Step5: If the message should be encrypted, then Click on checkbox encrypt message.

Step6: If the message should be hidden, then type message in message box and click on go button, then dialog will be appear with operation is successful or not.

Step7: Close embedding message window by clicking on close button.

Step8: To retrieving encrypted, hidden, compressed message click on retrieve message button and select the output file.

Step9: click on go button and enter the encrypted password for retrieving message.

ElGamal Elliptic curve encryption algorithm is as follows:

Input: Parameters field of elliptic curve (p, E, P, n) , public key Q , plain text m .

Output: Ciphertext $(C1, C2)$.

Begin

1. Represent the message m as a point M in $E(F_p)$
2. Select $k \in \mathbb{R}^+[1, n-1]$.
3. Compute $C1 = kP$
4. Compute $C2 = M+kQ$.
5. Return $(C1, C2)$

End.

ElGamal Elliptic curve decryption algorithm is as follows:

Input: Parameters field of elliptic curve (p, E, P, n) , private key D , cipher text $(C1, C2)$.

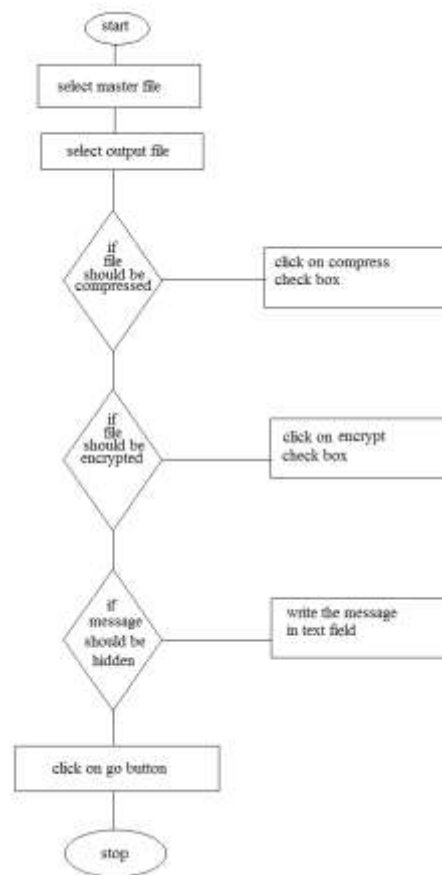
Output: Plain text m .

Begin

1. Compute $M = C2 - dC1$, and m from M .
2. Return (m) .

End.

4.3 Flowchart



Flow Chart

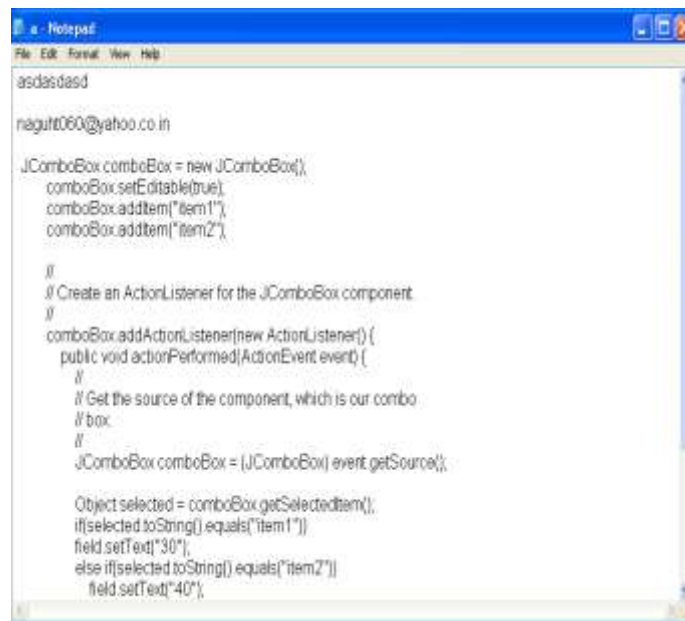
V. CONCLUSION

HTTP or XML-Based DoS attacks are one of the most serious threats to cloud computing. Detection of these attacks can be effectively done by using marking approach based on packets on the attacker side and the detected packets are filtered by dropping the marked packets on the victim side. Therefore, the packet marking overhead and the false positive rate of DoS attacks are effectively reduced. DDoS attack detection scenario is improved by replacing the Cloud Protector with Make Over and Dump on the victim side and the introduction of MATCH filter and MARK filter at the source side. By this, enhancement of the reduction of the false positive rate is done and increase in the detection and filtering of DDoS attacks is possible. By the use of ECC algorithm, the victim can never be able to access the original text. The future work can be extended by integrating the proposed system with the source end defensive systems to detect on MAC spoofing[13].

VI. SNAPSHOTS

The snapshots of the output after we apply ECC algorithm to our plaintext is as shown below:

Plain text for before applying ECC algorithm



```
arsdasdasd

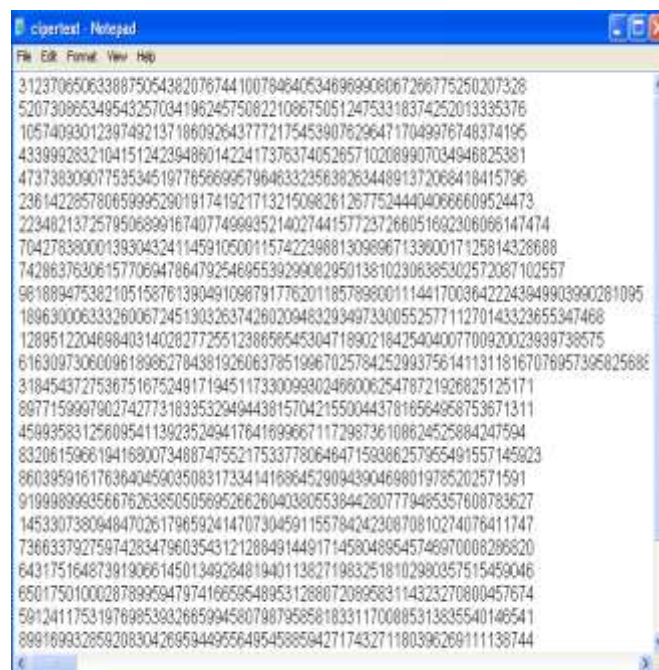
nagut060@yahoo.co.in

JComboBox comboBox = new JComboBox();
comboBox.setEditable(true);
comboBox.addItem("Item1");
comboBox.addItem("Item2");

//
// Create an ActionListener for the JComboBox component
//
comboBox.addActionListener(new ActionListener() {
    public void actionPerformed(ActionEvent event) {
        //
        // Get the source of the component, which is our combo
        // box.
        //
        JComboBox comboBox = (JComboBox) event.getSource();

        Object selected = comboBox.getSelectedItem();
        if(selected.toString().equals("Item1"))
            field.setText("30");
        else if(selected.toString().equals("Item2"))
            field.setText("40");
    }
});
```

Cipher text after applying the ECC algorithm



```
31237065063388750543820767441007846405346969908067266775250207328
52073086534954325703419624575082210667505124753318374252013335376
10574093012397492137186092643777217545390762964717049976748374195
43399928321041512423948601422417376374052657102089907034948625381
47373830907753534519778566995796463323563826344891372066418415796
236142285780659995290191741921713215068261267752444040666609524473
22348213725795068991674077499935214027441577237266051692306066147474
704278380001393043241145910500115742239881309696713360017125814326688
7428637630615770664786479254685539299082950138102306395302572087102557
9818894753821051587613904910987917762011857899001114417003642224384993990261095
189630006333260067245130326374280209483293497330055257711270143323655347468
12895122046984031402827725512386565453047189021842540400770092002389738575
616309730600981898627843819260637851996702578425299375614113118167078957386825886
318454372753675167524917194511733009930246600625478721926825125171
897715989790274277318335329494438157042155004437816564858753671311
45893583125609541139235249417641899667117298736108624525884247594
8320615968194169007348874755217533778064647159386257955491557145923
86039591617636404560350831733414168645290943904698019785202571591
91998999356676263850505695266260403805538442807779485357608783627
145330738064847026179659241470730459115578424230870810274076411747
736633792759742834796035431212884914491714580489545746970008296820
643175164873919066145013492848194011382719832518102980357515459046
650175010002878995947974166595489531288072089583114323270800457674
59124117531978995383266599458079879568818331170085313835540146541
898169932859208304269594495564954588594271743271180396269111138744
```

REFERENCES

- [1] A.Belenky and N.Ansari (2003), ‘Tracing Multiple Attackers with Deterministic Packet Marking (DPM)’, Proceedings of IEEE Pacific Rim conference on communications, computers and signal processing, Vol. 1, pp. 49–52.
- [2] A.Chonka W. Zhou and Y.Xiang (2008a), ‘Protecting Web Services with Service Oriented Traceback Architecture’, Proceedings of the IEEE eighth international conference on computer and information technology, pp. 706-711.

- [3] A.Chonka, W.Zhou and Y.Xiang (2008b), 'Protecting Web Services from DDoS Attacks by SOTA', Proceedings of the IEEE fifth international conference on information technology and applications, pp. 1-6.
- [4] A.Chonka, W.Zhou, J.Singh and Y.Xiang (2008c), 'Detecting and Tracing DDoS Attacks by Intelligent Decision Prototype', Proceedings of the IEEE International Conference on Pervasive Computing and Communications, pp. 578-583.
- [5] A.Chonka, W.Zhou and Y.Xiang (2009a), 'Defending Grid Web services from X-DoS Attacks by SOTA', Proceedings of the third IEEE international workshop on web and pervasive security (WPS 2009), pp. 1-6.
- [6] A.Chonka, W.Zhou and J.Singh (2009b), 'Chaos Theory Based Detection against Network Mimicking DDoS Attacks', Journals of IEEE Communications Letters, Vol. 13, No. 9, pp. 717-719.
- [7] A.Chonka, Y.Xiang, W.Zhou and A.Bonti (2011), 'Cloud Security Defence to Protect Cloud Computing against HTTP-DoS and XML-DoS attacks', Journal of Network and Computer Applications, Vol. 34, No. 4, pp. 1097-1107.
- [8] D.Dean (2002), 'An algebraic Approach to IP traceback', Journal ACM Transactions on Information and System Security', Vol. 5, No. 2, pp.119-137.
- [9] S.Savage, D.Wetherall, A.Karlin and T.Anderson (2000), 'Practical Network Support for IP traceback', Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 295-306.
- [10] H.Shabeeb, N.Jeyanthi and S.N.Iyengar (2012), 'A Study on Security Threats in Clouds', Journal of Cloud Computing and Services Science, Vol. 1, No. 3, pp. 84-88.
- [11] X.Xiang, W.Zhou and M.Guo (2009), 'Flexible Deterministic Packet Marking: an IP Traceback System to Find The Real Source of Attacks', Journal of IEEE Transactions on Parallel and Distributed Systems, Vol. 20, No. 4, pp. 567-580.
- [12] K.H.Choi and H.K.Dai (2004), 'A Marking Scheme using Huffman Codes for IP Traceback', Proceeding of 7th International Symposium on Parallel Architectures, Algorithms and Networks (SPAN'04).
- [13] E.Anitha and Dr.S.Malliga (2014), 'A Packet Marking Approach To Protect Cloud Environment Against DDoS' Computer Science and Engineering Department, Kongu Engineering College Perundurai, India mallisenthil@kongu.ac.in.
- [14] Randhir Kumar, Akash Anil (2011), 'Implementation of Elliptical Curve Cryptography' IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011 ISSN (Online): 1694-0814.
- [15] K.Santhi, (2013), 'A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks, volume 2, Issue 5, May 2013.
- [16] Nisha H. bhandari (2013), 'Survey on DDoS Attacks and its Detection & Defence Approaches' IJISME.
- [17] R. Vivek, R. Vignesh & V. Hema (2013), 'An Innovative Approach to Provide Security in Cloud by Prevention of XML and HTTP DDoS Attacks' ISSN(PRINT : 2320-8945, volume-1, Issue-1, 2013.
- [18] John Ioannidis, Steven M. Bellovin (2010) 'Implementing Pushback: Router-Based Defense Against DDoS Attacks' .
- [19] J.J. Shah, Dr. L.G. Malik (2013), 'Impact of DDOS Attacks on Cloud Environment', Communication Technology, vol 2, Issue 7, July-2013.