Cloud Protector Using Ids in WEKA

[1]Reena, [2]Parbhat Verma

[1]Research Scholar, [2]Head of Department
MIET Computer Science & Engineering, Kurukshetra University

***Abstract* - Distributed Denial of Service (DDoS) attacks have become a large problem for users of computer systems connected to the Internet. DDoS attackers hijack secondary victim systems using them to wage a coordinated large-scale attack against primary victim systems. In this paper, we propose a framework integrating network intrusion detection system (IDS) in the Cloud. Our IDS module consists of DARPA Set [i] algorithm. It generates new rules from captured packets. It aims to detect known attacks and derivative of known attacks in Cloud by monitoring network traffic, while ensuring low false positive rate with reasonable computational cost**

***Keywords* - CLOUD, Security, DDOS, DARPA, Weka**

I. INTRODUCTION

Cloud Computing is getting prevalent in the business and IT industry. Cloud Computing can be defined as an Internet based computing where Virtual shared servers provide software, infrastructure, platform devices and other resources[2]. The main concern of Cloud Computing is that the customers use only what they want and pay only for what they use. Resources are available to the customer any time they want and at any location. It also aims at cutting down the cost of maintenance and operation of any software service. Cloud Computing customers need not to own the physical infrastructure; rather they rent usage from a third-party provider i.e. Cloud provider. This reduces the cost of infrastructure and maintenance.

Layers of Cloud Computing

Cloud computing basically consists of three layers:

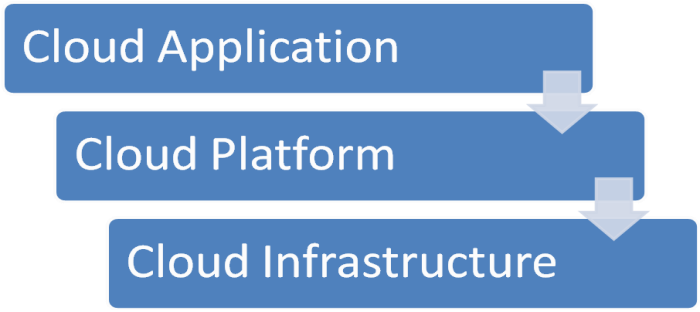


Fig 1 layers of Cloud Computing

- **Cloud Application** - This is the top most layer of the Cloud. The applications and services of the cloud are accessed here via web browser, hosted desktop or remote client. It eliminates the need of installing and running the application on customer's computer & thus removes the burden of software maintenance, ongoing operation and support services.
- **Cloud Platform** - This is the middle layer of the Cloud. This layer provides the computing platform as a service. A Cloud Computing platform makes changes in the server's configuration and settings according to the increase and decrease in the demand.
- **Cloud Infrastructure** - The lower most layer of the Cloud is Cloud Infrastructure. The basic function of this layer of cloud is to provide IT infrastructure through Virtualisation. Virtualisation means dividing or splitting single piece of hardware independent, self-governed environments, which can be scaled in terms of CPU, RAM, Disk and other elements. Virtualisation is the creation of a virtual (rather than actual) version of something, such as a hardware platform, Operating System, storage device, or network resources. These are then interlinked with others for resilience and additional capacity [3].

II. SECURITY IN CLOUD

Security Threats in Cloud

The foremost concern in cloud computing is security. There have been survey works in the past that classifies security threats in cloud based on the nature of service models of cloud computing system. The security is needed at various levels of Cloud-Network level, Host level and Application level. At these level various security breaches can occur which are classified as follows. This classification is done on the basis of discussion in [2] for Amazon EC2 cloud and as in [1].

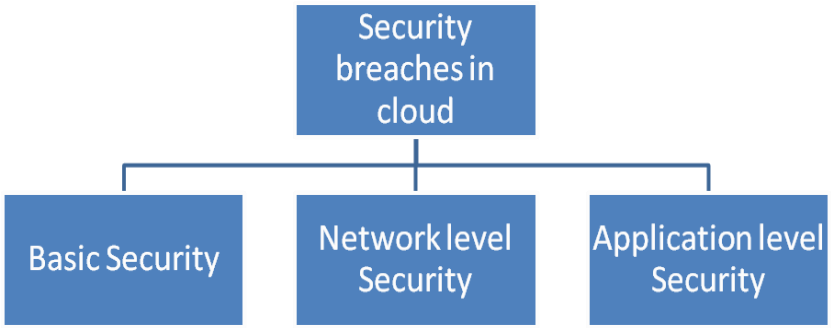


Fig 2 Security breaches in Cloud

Basic Security

With prevalence of latest Web technologies like Web 2.0 security has become more important. The attacks observed over the Web application are:

1. **SQL Injection attacks:** are those attacks in which an attacker gains unauthorised access into a database through malicious code inserted into a standard SQL code.
2. **Scripting attacks**: In this a malicious script is injected into the Web content and user considering it to be authentic executes it over his own machine, thus giving either control of the machine or exposure of confidential information to the attacker.
3. **Man in the Middle attacks**: In this attack an intruder interferes in the ongoing conversation between the sender and receiver and makes them believe that conversation is taking place between them only.

Network Level security

Problems associated with network are:

1. **DNS attacks:** A DNS (Domain Name Server) server translates domain name into the IP address. Domain name are much easier to remember. But sometimes it happens that on calling server by the domain name the user is routed to some other evil cloud.
2. **Sniffer attacks**: It is a kind of application program which captures the packets flowing in the network and reads the information in it if it is not encrypted.
3. **Issue of Reused IP Addresses:** When a particular user moves out of a network his IP address is issued to another user. It may lead to security threat to the previous user as there is certain time lag between the change of IP address in DNS and clearing of the IP address from the DNS caches. Thus there are chances that the data of the previous user may become accessible by the new user.
4. **BGP Pre fix Hijacking**: The Internet relies on the Border Gateway Protocol (BGP) to convey routing information across Autonomous Systems (ASes).As a BGP propagates the entire AS path used to reach each destination network (represented by an IP address prefix). A prefix hijack occurs when a BGP router R announces a route to prefix P but R does not provide data delivery to P. Such a false route may appear more attractive to some other BGP routers than the actual route to P, thus influencing them to choose the route announced by R instead of the actual route. As a result, packets from these affected routers would then be forwarded towards R instead of the true destination, leading to serious security and privacy breaches.

Application level Security

Application level security to the use of software and hardware to provide security to applications. The threats to Application include level security includes:

1. **DENIAL Of SERVICE ATTACKS**: A DoS attacks is to make services unavailable to an authorised user by flooding the server with large number of requests
2. **COOKIE POISIONING:** Cookie poisoning attacks are basically manipulation and forging the cookies to achieve an unauthorised application or website.
3. **BACKDOOR ATTACKS**: During the development of an application or Operating System program a backdoor is left intentionally by the developer for different purpose. These backdoors enables attacker to bypass the normal authentication and gain access.
4. **DISTRIBUTED DENIAL Of SERVICE ATTACKS:** A DDoS attack is the one in which the collection of compromised systems attack the one target system, thus denying the services from the targeted system to the authorised users.
5. **CAPTCHA BREAKING:** CAPTCHA's were developed to prevent spam and overexploitation of network resources by bots. But recently it has been observed that these CAPTCHAs can also be broken by the spammers

III. Related Work

Bhaskar Prasad Rimal et.al [1] in 2009 provided a taxonomy of cloud computing and information to evaluate and improve the existing and new cloud systems. The goal of cloud computing is to make an efficient use of distributed resources with minimum of wastage in order to get high throughput and to tackle a large scale problem with ease. Cloud Computing makes use

of, some of the basics like Virtualization, interoperability, scalability, quality of service, fail over mechanism and the cloud delivery model. Clouds have layered architecture which basically consists of Software as a Service, Platform as a Service, Infrastructure as a Structure and Hardware as a Service. Cloud Modes are basically public, private and hybrid. Cloud have some disadvantages too like low fault tolerance rate and security issues etc. Some other issues of the Cloud include load balancing, interoperability, scalable data storage. There are many cloud service provider in the market like Amazon EC2, GigaSpaces, GAE, Sun Cloud etc. Each service provider has its own advantages and disadvantages.

Roschke et.al [2] in 2009 proposed a deployment architecture of Intrusion Detection Systems in the Cloud. He proposed the deployment of IDS on each layer of the cloud to gather the alerts from the sensors deployed in the cloud. For each layer there should be Network-based sensors and host based sensors. Thus IDS VM (IDS Virtual Machine) management system was proposed. It includes IDS Sensor VMs and an IDS Management Unit. The IDS sensors identify malicious behaviour and generate alerts which will be processed by the Event Handler. These alerts are stored in the Event Database storage. The analysis component analyzes the events. It can be configured and controlled by the user. Information such as VM (Virtual Machine) status, VM workload, and IDS –VM assignments can be monitored. The involved IDS VMs can be stopped, started and recovered by the management system. The challenges faced during the implementation of this ID are: the output of different sensors is not standardized; communication between sensors and the management component is not much flexible, complex architecture with multiple sensors.

Du Ping et.al[3] in 2010 presented a cloud based system called Cloud Based attack Defense System (CLAD) which runs on cloud infrastructures as a network service to protect Web Servers. Defense against network –layer attacks depends on the execution environment of the cloud infrastructure. It is desirable to run CLAD on execution environment. When a new connection request arrives, the cloud infrastructure will first check whether it is an HTTP request. Since the cloud infrastructure only allows Web traffic to pass through it, only HTTP requests can reach CLAD system. Other non-HTTP traffic such as network-layer attack packets will be dropped by the cloud infrastructure. The drawback of this architecture is that it is applicable on small sized companies only.

W.Yassin et.al [4] in 2012 suggested a Cloud based Intrusion Detection framework (CBIDS). This framework has three main components: User Data Collector (UDC), Cloud Service Component (CSC), and Cloud Intrusion Detection Component (CIDC). The UDC is a server in which a group of necessary information is contained. It standardizes and filters the collected packets of information. CSC analyzes and validates information from UDC to find out the any external intrusion and then determines whether to delete the information or forward the information to appropriate IDS. The CIDC is the main component of intrusion detection. It further has four modules: Analysis Engine, Service Console, Signature Database and User Database. In this framework sensitive information is first copied and then forwarded to the proxy UDC. Then UDC collects the information and sends it to CSC through VPN switch. CIDS then provide a complete defensive mechanism and detects the entire attacks based on the information collected from user in the real time. The drawback of this framework is that it is described from theoretical perspective.

IV. PURPOSED WORK

Cloud Protector

CTB does not directly eliminate a DDoS attack message. This is left for the filter section of a defense system called Cloud Protector. The Cloud Protector is a trained back propagation neural network (NN), to help detect and filter out DDoS messages. A neural network is a set of connected units made up of input, hidden and output layers [8] [9]. Each of the connections in a neural network has a weight associated with it. In a neural net the focus is on the threshold logic unit (TLU). The TLU inserts input objects into an array of weighted quantities and sums them up to see if they are above the threshold. The cloud protector system is implemented in five different phases as shown in Fig.3 and described below

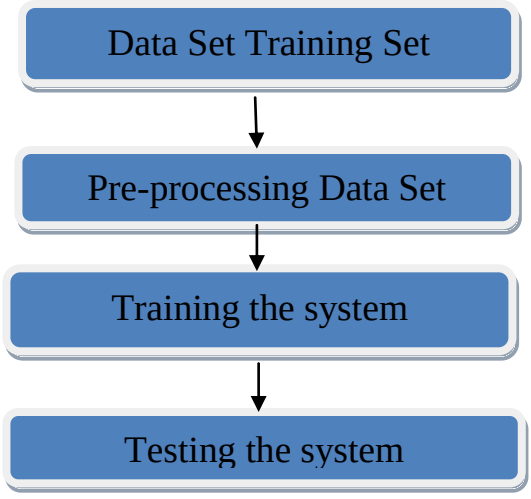
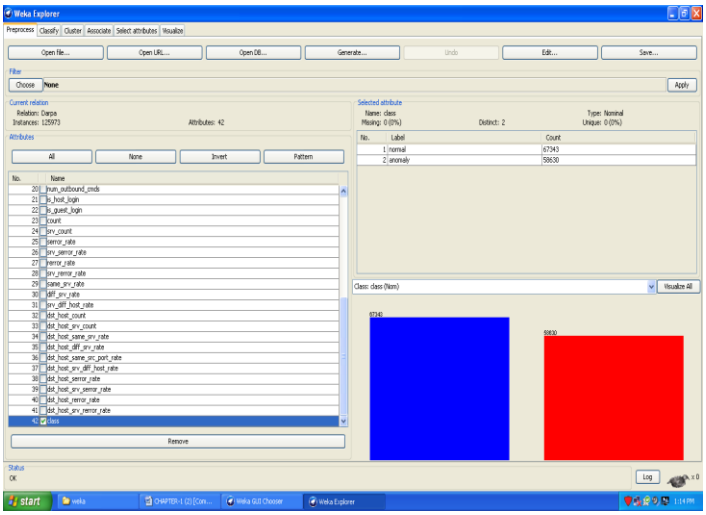
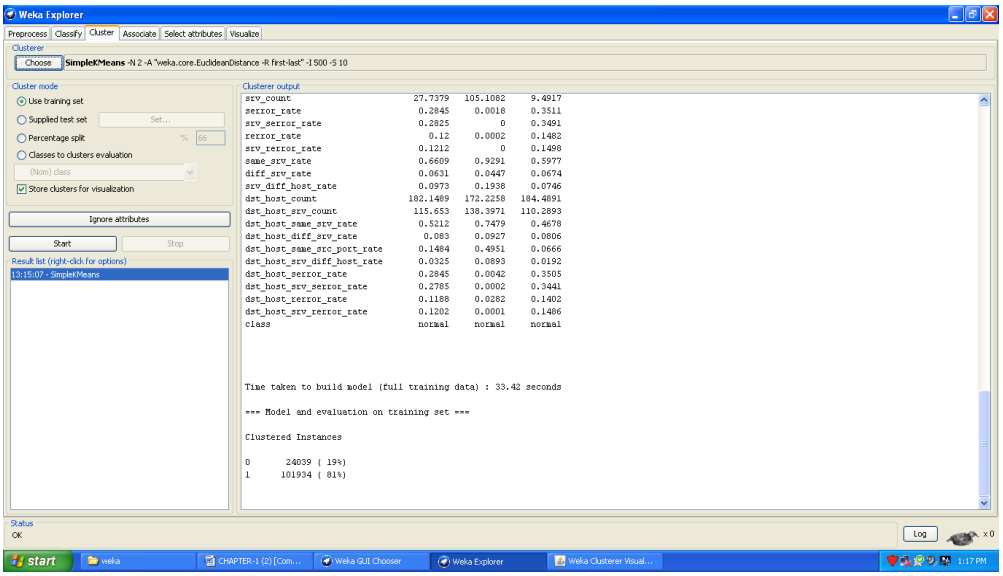


Fig 3 Implementation phases

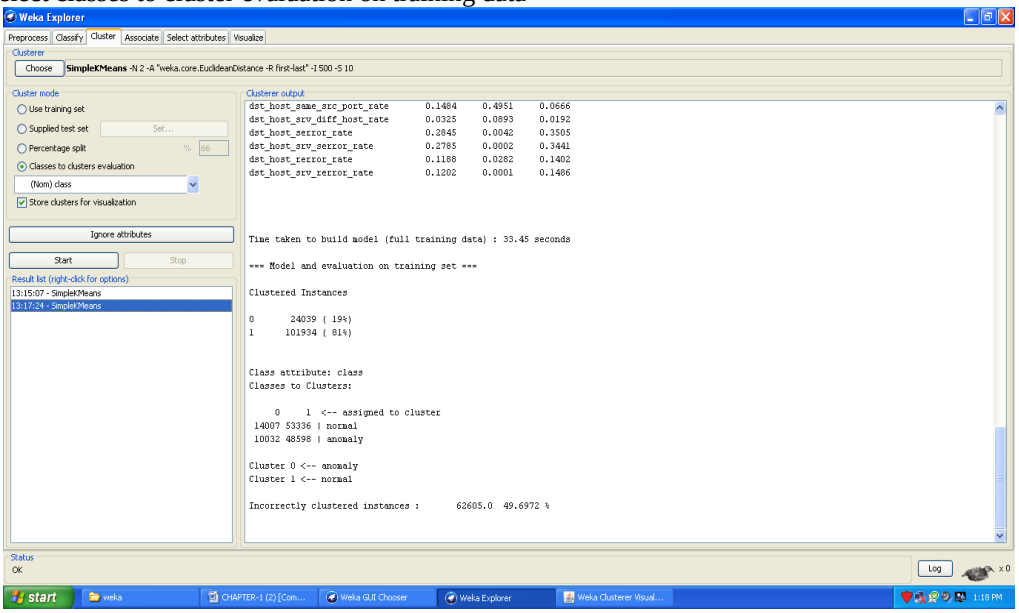
Step1 Weka3.6.2 is used for DARPA weka explorer with dataset loaded .We used K-mean Clustring alogrthim K=2,Normal and Anomoly.



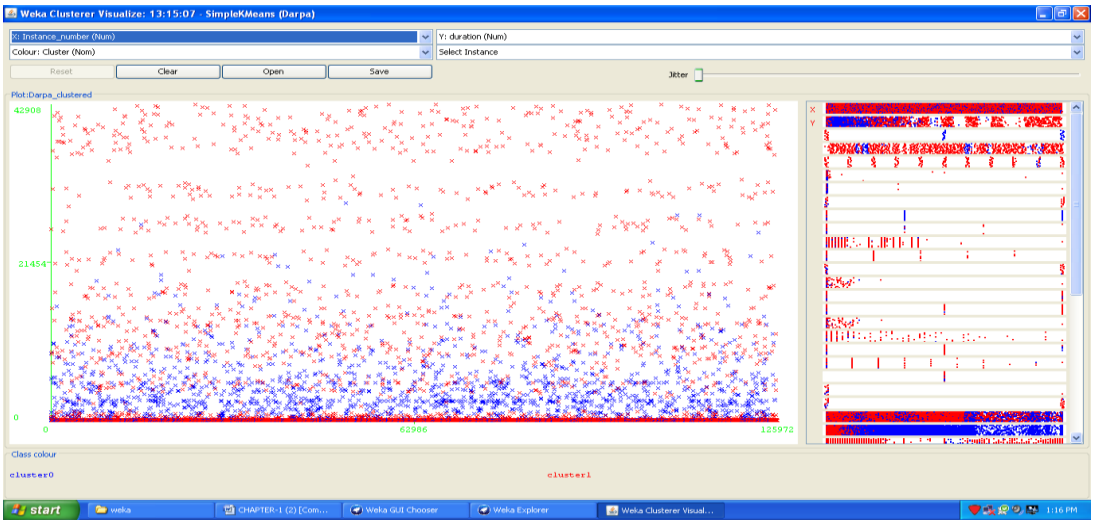
Step2: Now we select classes to cluster evaluation. Then we choose k-mean and we find out accuracy. We use 42 Attribute in DARPA

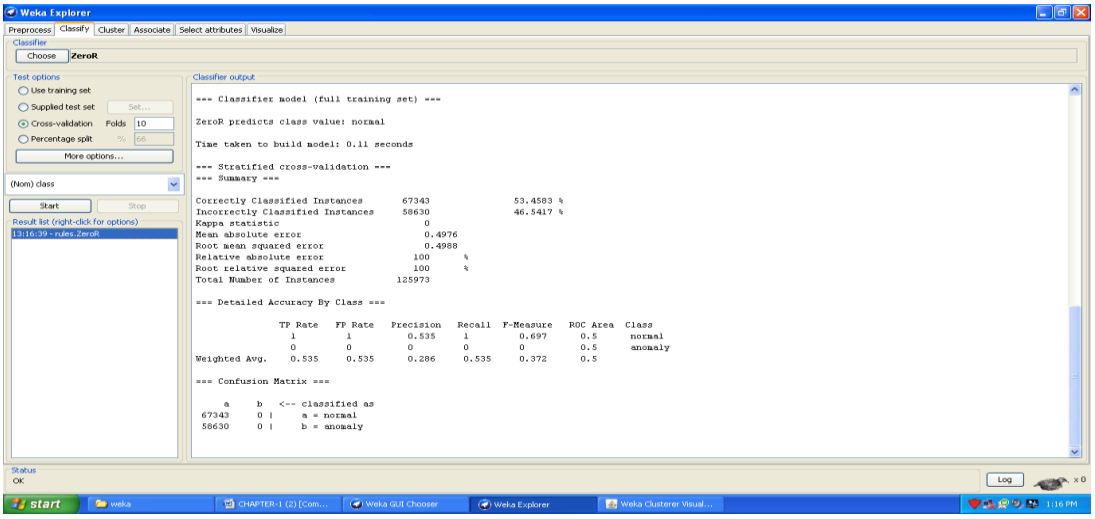


Step3: Now we select classes to cluster evaluation on training data



Step 4:Now we find cluster visual assignment





V. CONCLUSION

The efficiency of the algorithm with which intrusions are detected is around 90%-95%. The accuracy of this algorithm depends on the training data taken. If the number of instances of a particular type is equal to that of the other then there is an algorithm based on the k-mean clustering for analysing program behavior in intrusion detection is evaluated by experiments. The preliminary Experiments with the Darpa Data Set audit data have shown that this approach is able to effectively detect intrusive program behaviour.

In the near feature, we will conduct more experiments. We'd like to test the time based features on different sizes as on DARPA dataset. We will also study the impact of different normalization methods and the impact of weighted features.

REFERENCES

[1] Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, "A taxonomy and Survey of Cloud Computing Systems". In *Fifth International Joint Conference on INC, IMS, and IDC*. pp. 44-51, IEEE, 2009

[2] Sebastian Roshke, Feng Cheng, Christoph Meinel, "Intrusion Detection in the Cloud". In *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. - 729-734, IEEE, October 2009

[3] Ping Du, Akihiro Nakao, "DDoS Defense as a Network Service". In *International Conference on Network Operations and Management Symposium*, pp.-894-897, IEEE, April 2010

[4] W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, M.t. Abdullaha, "Cloud-Based Intrusion Detection Service Framework". In the *Proceedings of the International Conference on Cyber Security*, pp. 213-218, IEEE, June 2012

[5] Abhishek Jain, Ashwani Kumar Singh, "Distributed Denial of Service (DDOS) Attacks – Classification And Implications". In *Journal of Information and Operations Management*, ISSN: 0976-7754 & E-ISSN: 0976-7762, Vol. 3, Issue 1, pp 136-140, 2012

[6] http://www.symantec.com/connect/articles/justifying-expense-ids-part-one-overview-rois-ids

[7] http://netsecurity.about.com/cs/hackertools/a/aa030504.htm

[8] Sanjay B Ankali, Dr. D V Ashoka, "Detection Architecture of Application Layer DDoS Attack for Internet". In International Journal of Advanced Networking and Applications, Vol-o3, Issue: 01, pp. 984-990, 2011.

[9] Aderemi A. Atayero, Oluwaseyi Feyisetan,"Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", In *Journal of Emerging Trends in Computing and Information Sciences*, Vol-2, No.10, pp.546-552, October 2011

[10] Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue, "Security Issues and Solutions in Cloud Computing". In *32nd International Conference on Distributed Computing System Workshops*, pp.573-577, 2012 (2012)