ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

ATTACKS and THEIR EFFECT on SECURITY of DATA in CLOUD COMPUTING

Priyanka Jairath[1], Rajneesh Talwar[2]

Student, Computer Science, C.G.C. Landran, Mohali, India [1]

Principal, Chandigarh University, Mohali, India [2]

Abstract: Cloud computing has become widespread in recent years because of the value and speed. However Security challenges are still among the most important obstacles as attacks are a part of each net user's life. This paper explores the identification of Dos and DDos attacks by victimisation CUSUM algorithmic rule. DoS attacks are a category of attacks initiated by individual or cluster of people exploiting aspects of the web Protocol to deny alternative users from legitimate access to systems and knowledge. DDoS on the opposite hand may be a combination of DoS attacks staged or disbursed collectively from varied hosts to penalise the target host from any serving its perform DDoS is term coined once the supply of the attack isn't returning from one supply, however multiple sources. Consistent with the applied approach, Black and White List is formed to spot the attacker and legitimate users supported their weights. To validate our methodology, after we notice the attacker or legitimate users, then we have a tendency to apply CUSUM algorithmic rule to spot the sort of attack that's DOS & DDOS attack and empirical results show the sort of attack.

Keywords: Cloud Computing, Attacks, Detection, Dos, DDos, CUSUM Algorithm

I. INTRODUCTION

Cloud computing could also be a rising model of business computing. It's turning into a development trend. It will connect million of computers to a superb cloud. It provides a secure and dependable information storage centre that saves users time of storing information and killing virus, this kind of task is additionally done by professionals. It's not necessary for the users to grasp however the cloud runs. Cloud service suppliers doesn't ought to prepare methodology ahead for hardware provisioning as cloud computing offers infinite computing resources on demand as a results of its high measurability in nature. Merely simply just in case of cloud service suppliers, want the necessity of any quite commitment isn't there as they'll begin from tiny firms and increase hardware resources as long as there's an increase in need. The costs deem computing resources usage on a short basis and will unharnessed computing resources as they have. This might be the sole real reason cloud supply services like data as a service (daas), coding system as a service (saas), and platform as a service (paas)). There unit of activity several cloud computing platforms that unit of activity growing terribly quickly. The cloud computing infrastructure encompasses a nice impact on varied vital areas

Of it, like security, infrastructure investments, business application development, and much of many. Over the past two decades, the sophistication of exploits that attack the memory of a running method has fully grown considerably. Hardware vendors, like Intel, have frequently tried to stay pace with the most recent attack by introducing measures to beat specific exploits, like the no-execute bit developed to mitigate buffer overflows. Unfortunately, new vulnerabilities and ways to use them have continued to stay pace.

In this paper we have a tendency to establish varied attacks on cloud computing supported the principles of cusum algorithm and we have a tendency to establish the attacks.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

A denial-of-service attack is characterized by a precise try by attackers to forestall legitimate users of a service from victimization that service. There are two general types of dos attacks: those who crash services and those that flood services. Dos attacks these days are a unit part of each net user's life. They're happening all the time, and every one the web users, as a community, have some half in making them, plagued by them or perhaps loosing time and cash as a result of them.

A distributed denial of service attack (Ddos) happens once multiple systems flood the information measure or resources of a targeted system,

The main contributions of this paper are:
(i) Identification of attacker and legitimate user.
(ii) Discussion on the attacks on varied informatics addresses in cloud;
(iii) Identification of attack by cusum algorithm.

II. RELATED WORK

A. Distributed Denial of Service: Taxonomies of Attacks

Many researchers have projected the DDoS attack models and propose taxonomies to characterize the scope of DDoS attacks, the characteristics of the software system attack tools used, and therefore the countermeasures obtainable. These taxonomies illustrate similarities and patterns in numerous

DDoS attacks and tools, to help within the development of a lot of generalized solutions to countering DDoS attacks, together with new spinoff attacks.

Some previous studies have centered on the attacks and detection of attack by watching behaviour of knowledge. Sephen M. Specht et al enforced paper that describes taxonomies of DDoS attacks, tools, and countermeasures. They describe categories of DDoS attack architectures that's the Agent-Handler model and therefore the net Relay Chat (IRC)-based model. They describe the software system characteristics for DDoS attack tools action however these tools are setup on secondary victim systems.

Raja Azrina et al describes the various forms of Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attack. They illustrate the various approaches and variations of DoS attacks so as to produce an overall recovery steps and best observe in networking to forestall high impact disaster against such attacks by ways that of technology and legal framework.

Mehmud Abliz describes one in every of the most important security threats within the net - denial of service. He analysed the initial style goals of the net and the way they'll have contributed to the challenges of the DoS downside.

There are alternative studies that additionally specialize in the various attack, however those studies outlined the behaviour of attacks otherwise.

B. Botnet primarily based Distributed Denial of Service

Botnets are prevailing mechanisms for the facilitation of the distributed denial of service (DDoS) attacks on computer networks or applications. Currently, Botnet-based DDoS attacks on the appliance layer are latest and most problematic trends in network security threats. Botnet-based DDoS attacks on the appliance layer limits resources, curtails revenue, and yields client discontent, among others.

Esraa Alomari et al describes the Botnet primarily based DDOS attacks. The goal of a Botnet primarily based DDoS attack is to entail harm at the victim aspect. They describes the design of Botnet primarily based attacks that's Agent Handler Model, Internet Relay Chat, net primarily based Model. They present numerous Botnet primarily based DDOS attack Tools and additionally numerous incidents relating to these attacks.

III. SCOPE

For attacks detection, DOS attacks are congestion based as same identifies Denial of Service that addresses to the congestion in the network and overloading of requests for the server and the host. So, identification of DOS & DDoS attacks is important in moderate conditions as extreme ones are easily identifiable**.**

File Access Path is vital proof for characteristic the system activity. It plays major role to find unidentified intruders who try to sneak into the atmosphere. There are number of ways to identify the intruder. One of this is based on load monitoring. By monitoring the weights, we can

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

identify about the attacker or legitimate user and the proposed system identifies this. Attacker identification is done by using CUSUM algorithm. This algorithm is sequent analysis algorithm that is usually used for modification detection. Cumulative sum (CUSUM) algorithm is employed within the internal control. They're well matched for checking a measuring instrument operating for any departure from some target or specific values and are wide used for detecting the little and moderate mean shifts By using this algorithm, we can detect the change and find the attacker i.e. DOS & DDOS attack.

A. Attacks & their Effect

1. In all previous techniques like log in passwords, or trap file mechanism the user can be identified if make a mistake of entering a wrong password too many times or open a file that he is not supposed to respectively.

2. So we need to have a method that is able judge the user and the attacker by seeing the data access or the file access pattern.

IV. PROPOSED WORK & METHODOLOGY

A. Attack Analysis

The legitimate user's access is additionally restricted; solely the authorized will have each browse and write/ modify permissions. For redaction the file or document, there's once more a security check. To spot the user is associate degree assailant or legitimate user we tend to analyse the access behaviour of every user who logins. This monitoring of user behaviour is completed through CUSUM algorithm. The data access patterns are identified and legitimacy of the user is checked on the idea of modification purpose that's in step with the typical fluctuation within the pattern. Accordingly, a black list and white list of IP addresses is made to identify the load. If the user will access the trap file it'd be thought-about as associate degree abnormality and there'll be a modification purpose within the graph of average fluctuation. The second case is that if the assailant opens a true or confidential file and tries to breach the authorization barrier then again the system would analyse abnormality within the access behaviour of the user. Then any, we tend to added a feature of fog computing that's checking the user location if the access behaviour are abnormal. Through IP address we are able to verify the user's location and additionally trace the attacker's location.

The system is secure therefore whenever the assailant enters the system he can open the files to that the access is open and can search in an exceedingly random manner, however here within the system we've got left solely those files receptive that are trap files. Therefore once the assailant can open the trapped file, the abnormality in user behaviour will be detected. With CUSUM modification purpose will be detected.

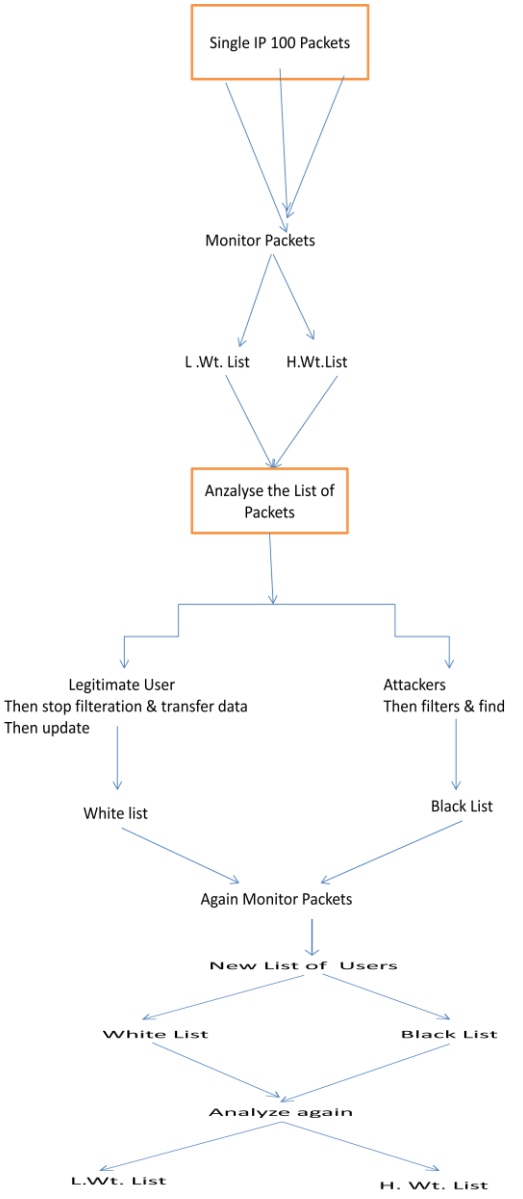

Fig1. Technique explained in the form of process

DOI 10.17148/IJARCCE.2015.43153

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

B. Methodology

In this section, we explain the method by explaining our algorithm that is CUSUM algorithm which is used to detect the change in the network and help to find the attacker by load balancing.

CUSUM ALGORITHM

CUSUM is Cumulative **S**ummation. For applying cusum on N no of observations.

Let initial average av 1 -> N =0;
Sump=Sum till previous observations =0;
For loor n=1 -> N
Sump =sump (previous)+Current(n)
av(n)=sump/N
end for loop

Now av is the cumulative summation averages and difference in two consecutive averages gives the fluctuation.

General sort of a consecutive amendment detection algorithmic program.

Two necessary steps seem during this algorithmic program:

1. Detection step: The way to decide between H0 and H1?
2. Estimation step: The way to expeditiously estimate the amendment time?

These steps are a unit more elaborate within the two following sections:

1. Detection step

The problem here is to make your mind up between 2 potential hypothesis H0 and H1 from the measured samples x[0]; : : : ; x[k], that is additionally termed a binary hypothesis testing drawback. The answer, given by the detection theory, is to use the so-called probability magnitude relation check testing drawback. The answer, given by the detection theory, is to use the so-called probability magnitude relation check.

2. Estimation step

Once H1 has been determined and an abrupt amendment has been detected, the matter is to efficiently estimate the amendment time American state from the measured samples x[0]; : : : ; x[k].A way to unravel this drawback is to use its most likelihood estimate, that is that the worth of American state maximising the probability

Setting the parameters

The CUSUM algorithmic program has many standardization parameters the user needs to properly set:

1. In any case the detection threshold h,

2. Just in case of the given suboptimal CUSUM algorithmic program, ten or equivalently the change. The previous section shows that the user should have a priori data concerning the signal to properly set this parameter. Indeed, an efficient setting for the change is that the a priori possibly amendment magnitude that ought to seem within the signal. Just in case many magnitudes of jump are potential, the simplest selection is that the minimum one. In any case, the ensuing change observation algorithmic program is simply optimum to consecutive detect the chosen change magnitude.

V. RESULTS

Process for showing the attacks:

1. Initial of all there's no. of IP addresses that generates packets when filtering. Our theme distinguishes between Light-Weight Weight IP address & Heavy Weight IP address. Some load of traffic will be reducing by this mechanism.

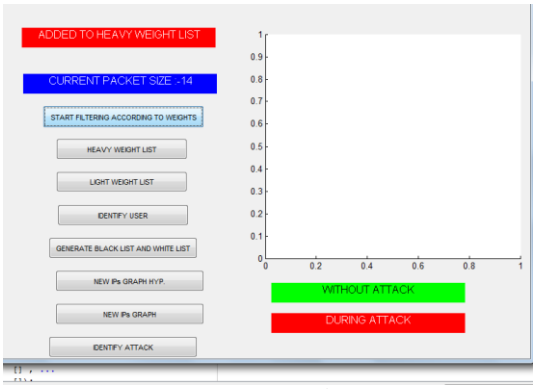

Fig.2 Start Filtering of Packets

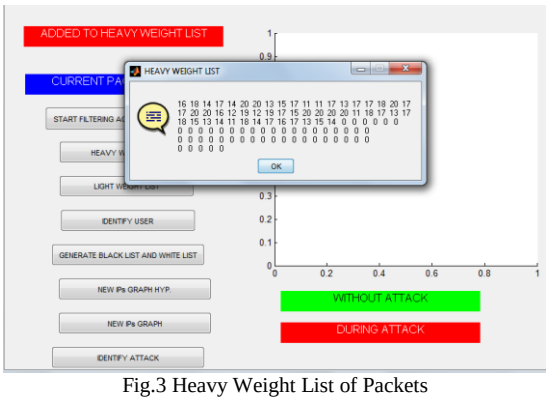

Fig.3 Heavy Weight List of Packets

DOI 10.17148/IJARCCE.2015.43153

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

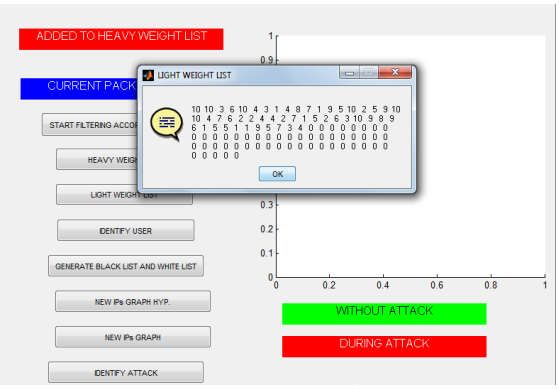

Fig.4 Light Weight List of packets

2. After it, we tend to apply Non-Parametric CUSUM algorithm & identifies attackers & legitimate users.

3. After it, within the case of Legitimate user we tend to produce White list that embody explicit legitimate user, that facilitate in resolving traffic in future.

4. Additionally creation of Blacklist happens that embody explicit Attacker that additionally facilitate in resolving future issue.

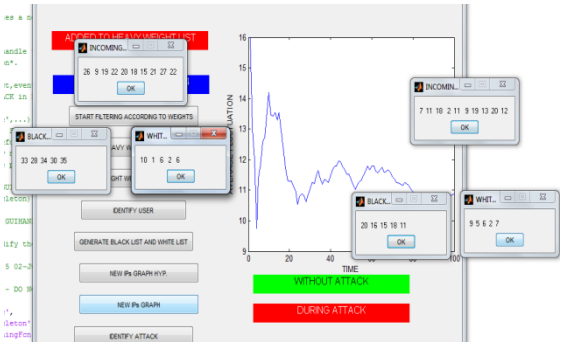

Fig. 5 Incoming Packets with White & Black List

5. Then IP Hypothesis graph shows the Attacker& Legitimate users.

Fig.6 Result shows the Attacker

6. New IP graph shows that at -1 worth, there's no Attack and at 1 worth, there's associate degree of attack happens.

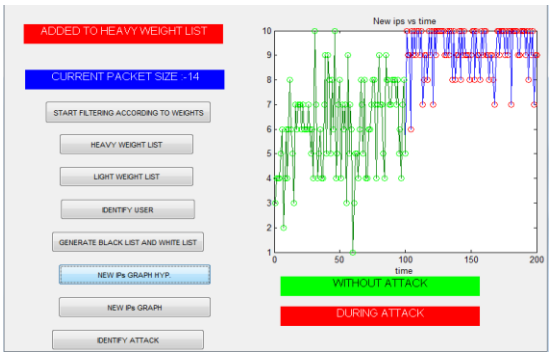

Fig. 7 New IP Graph Hypothesis

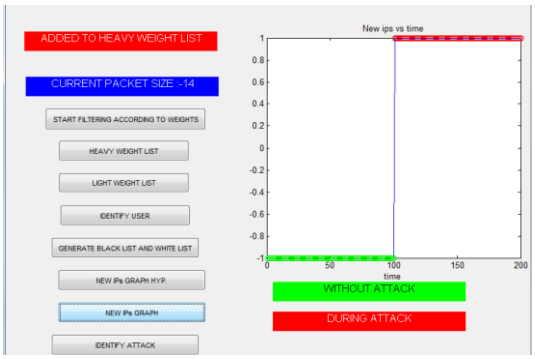

Fig.8 New IP Graph

7. Once the attacker is identified then, when it DOS & DDOS identified thus, we will able to detect single source or cluster of source which might cause attack.

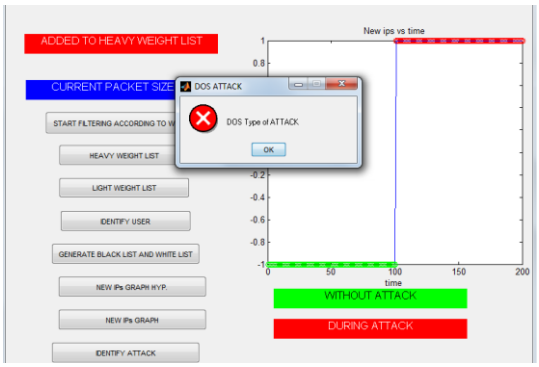

Fig.9 Result Shows DOS Type of Attack

VI. EXPERIMENT & COMPARISON

In comparison with previous technique, we perform a test on 18 computers in which we apply our and previous technique 100 times. Out of those 100 times, 50 times legitimate user use the computer & 50 times attackers use the computer. If system is right then our result is more accurate than the previous one as result shows.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

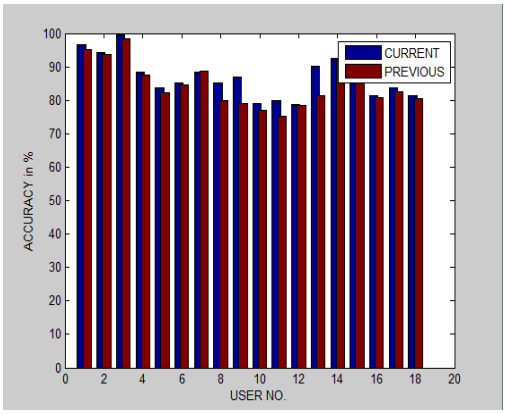

Fig. 10 Comparison Graph of Previous & Our Technique

TABLE I
COMPARISON TABLE OF PREVIOUS & OUR TECHNIQUE

User No.	Accuracy of our technique	Accuracy of previous technique
1	96.7	95.2
2	94.3	93.6
3	99.5	98.3
4	88.3	87.5
5	83.6	82.3
6	85.2	84.7
7	88.5	88.6
8	85.3	79.9
9	86.9	79.1
10	79.1	76.9
11	79.9	75.3
12	78.6	78.5
13	90.2	81.5
14	92.5	91.8
15	90.7	89.5
16	81.5	80.7
17	83.8	82.5
18	81.5	80.5

VII. CONCLUSION & FUTURE WORK

The detection criteria should be such that the abnormality or any anomaly is detected accurately. By increasing the number of user's cases we can get more accurate results. The system should be able to recognize the pattern generated earlier when the legitimate user had accessed the file system. For these reasons proper learning should be provided to the system so that it could detect the abrupt changes in behaviour of the user if it is not authorized or is an insider. The results determined when applying CUSUM algorithm for monitoring user's profile are successfully detecting the abnormalities and abrupt changes if the attacker tries to enter into system and intent to alter the documents. Within the accuracy comparison with results of the base paper, our technique has shown more accuracy than the previous one. Therefore, by following this method user information can be protected against insider theft attacks and any malicious activity can often be detected. As within the analysis, the average fluctuation shows the distinction between the access behaviour of the user and therefore the decoy technology is additionally effective in confusing the attacker and making the attacker believe that it's a useful file for the attacker. Through this analysis we concluded that decoy technology and fog computing together will provide security to real world problems like insider theft attacks.

ACKNOWLEDGMENT

I express my sincere gratitude to the **Punjab Technical University**, Jalandhar for giving me the opportunity to work on this during my final year of M.Tech. I would also like to express my sincere gratitude to the **CGC College of Engineering**, Landran, Mohali (Punjab) for giving me this opportunity and its faculty for full support in dissertation.

REFERENCES

[1] Alomari, E.,Manickam,S.,Gupta, B., Karuppayah, S., and Alfaris, R. (2012) *"Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art"* International Journal of Computer Applications(0975 – 8887) Volume 49– No.7, July 2012, pp. 24-32.

[2] Bishnoi, N., and Sehrawat, A., (2013), *"Cloud and its Security Concerns"* International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) Vol. 3, Issue 3, Aug 2013, pp. 79-84.

[3] Wang, H.,and Zhang, Y., (2014), *"COMMENTS On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage"* IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014, pp. 264-267.

[4] Yu, J., Lu, P., Zhu, Y., Xue, G.,and Li, M (2013) *"Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data"* IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013, pp. 239-250.

[5] Nourian, A.,and Maheswaran, M.(2012) *"Using segmentation for confidentiality aware image storage and retrieval on clouds"* Globecom 2012 - Communication and Information System Security Symposium, pp. 758-763

[6] Yang, K., and Jia, X. (2013) *"Expressive, Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage*" IEEE Transactions On Parallel And Distributed Systems, pp. 1-11.

[7] Kanter, M., and Taylor, S. (2013), *"Attack Mitigation through Diversity"* IEEE Military Communications Conference 2013 pp. 1410-1415.

[8] Raje, S., Patil, N., Mundhe, S., Mahajan, R. (2014), *"Cloud Security Using Fog Computing"* IRF International Conference, 30th March-2014 pp. 5-7.