An Improved Framework for Cloud Data Security using Frequency Variation and Hard Logarithmic based Algorithm

Ankur Jain\textsuperscript{1}, Asst. Prof. Dr. L. K. Vishwamitra\textsuperscript{2} \\
\textsuperscript{1,2}Department of Computer Science & Engineering, Oriental College of Technology, Bhopal, India

Abstract—Retreat is a significant anxiety throughout the broadcast of statistics whether in strengthened or in wireless communication. Numerous methods are intended for the safe communication but several biases are conceivable in these systems. The mock-up is founded on the cross combinatorial technique of Pre shared key replace and entropy dissimilarity by Interconnecting Federated Clouds. The information to be directed is first authentic by the indigenous agents of the Clouds by associating the communal key among them. The Proposed Methodology implemented here is more efficient as compared to the existing framework in terms of number of percentage of attacks blocked and accuracy.

Keywords: Cloud Computing, CCAF, Frequency Variation, DDoS, Viruses, Trojans.

I. INTRODUCTION

The express increase of the Internet and the appearance of cloud calculating have permitted an innovation drift of acquiring and overwhelming Material Knowledge amenities. Cloud calculating has transported new chances to the Material and Announcement Knowledge industry permitting productions to subcontract their IT amenities to cloud wage-earners and circumvent high-class up-front assets of founding their own infrastructures and resulting costs of conservation and advancements. By earnings of cloud amenities, cloud clientele can admittance all their obligatory competences i.e., computational resources, information, and submissions over the Internet, use what they necessity, and recompense for what they use deprived of anxiety with the fundamental organization (see Figure 1). As a consequence, patrons involve the coziness of outmoded conveniences such as water, electricity, gas, and telephony. Compensation such as a utility representation in totaling to convenience, scalability, and ease of organization have fashioned an industry-wide modification concerning cloud figuring explanations. Cloud computing initiates a foremost transfer in the IT liberation representation by donation computing possessions for hosting requests as an effectiveness which provides businesses and organizations to admittance sophisticated IT amenities existing by shade provider without the exclusive up-front reserves obligatory to create their own communications [1].

Figure 1: Cloud computing model

Now-a-days the use of internet has to change the way information is exchanged communicate with each other and all over the world, all of them can do their work over the internet, and there is much more dependent on the Internet. One of the most important safety measures troubles in the present Internet is the denial-of-service (DoS) attack always attempts to stop the victim from serving genuine users. One of the most universal types of cyber-threats to these situations is recognized as a Denial of Service (DoS) attack—an assault preventing users from accessing an organization for an epoch of time. Denial of Service (DoS) attacks exploit internet to target critical Web services [2, 3, 4]. This category of assault is planned to put off rightful manipulators from retrieving a specific organization replacement or embarrassment standard amenities for genuine operators by distribution enormous unsolicited circulation to the fatality (apparatuses or systems) to fatigue military and association capability or the bandwidth.
Cumulative movement of these DoS bouts has made waitpersons and system devices on the internet at superiordanger. Current DoS bouts have leftwardgreatbusiness and management web sites unreachable to clientele, associates, and operators for times or days, subsequent in noteworthymonetary, reputational, and other wounded. The increasing use of mist computing facilities and communalsubstructure is additionalcumulative the position of consuming a measuredstrategy for management such DoS bouts. The eventual purpose of a DoS bout is to avert users from retrieving anorganization or reserve, and the possible cost to hazardousinfrastructures can be significant. The smash of stoppage to hazardoustransportationsadministrations may not be imperfect to lost incomes and sympathy, but can encompass to community and hominoid costs. Internet-dependent and schmososedsubstructuremachineries are normally most at danger of a DoS bout.

II. DENIAL OF SERVICE (DOS)

Denial of Service (DoS) bouts are a period of attacks on boards, which purposes at fatiguingboardpossessions, in that way disallowing provision to lawfulworkers. The boardcapitals might be in rapport of time and space. For instance, waitpersons as long as SSL service might be time-attacked by creating them to achieve a portion of luxurious cryptographic in that way stopping them from portion their honestcustomers. Every other, servers could also be interplanetaryconfronted by fatiguing their assembly buffers or bandwidth with lot of fake needs/packages.

Distributed Denial of Service (DDoS) attacks are becoming a more and more frequent disturbance of the global internet and it is a distributed great balance effort by spiteful users to overflow the injured party complex with anmassivequantity of packages. This fatigues the wounded of systempossessions such as bandwidth, calculatinginfluence, etc. the affronted is not competent to supply military to its authentic users and systempresentation is greatly declined. Attacks against network resources are current in common internet dependent are launched for a variety of reasons, together with cost-effective gain, maliciousness, deception, disagreement and to gain an economic advantage. Attacks are directed at compromising the availability, integrity and confidentiality of networks and their property fall into the subsequent four wide-ranging categories are Denial of examine bother, refutation attack, variation attack, and admittance attacks. Some well-known DOS attacks are sync food, tear drop, black holes, octopus, ping of death, shork, ARP cache poisoning.

DDoS attacks are huge form of DOS attack where assailants produce anenormousquantity of necessities to injuredthroughcooperatedcongregation called zombies against computers (zombies), with the intend of deny ordinary examine or belitting of the eminence of armed forces. Disseminated Denial of Service (DDoS) bouts are a mounted form of DoS bouts where manifold attack bots2are working in an prearrangedmanner to method an attack system for aggressive a specific board. DoS and DDoS attacks are unfortunate for the most of the part after that to be an appropriate for very much perceptive intentions similar to Critical Information Infrastructure (CII). A fine and conventional communication is an example of a DoS attack is a SYN flooding attack [5], which is nearly everyone admired. A piece of information which is frequently acknowledged by safety measures investigators over and done with the globe is no difficulty by means of which grave DoS and DDoS occurrences can be doubtlesspermitted.

Additionally, the analysis [6] also instigate that the crest of 40 gigabit DDoS attacks almost creased in 2008 associated with the previous year. The grounds following this singularities is that the arrangement safety measures people does not have positive and resourceful suggestion back methods to establish attackers as it is informal for aggressors to camouflage themselves by enchantingrecompenses of the predispositions of the World Wide Web, such as the self-motivated, circumstances, and indeterminate countrysid of the Internet[7][8].
Denial of service is an intentional attempt to entirely interrupt or worsen accessibility of package/possessions to genuine/authorized user by attackers. DoS attacks more insensitive and easy to execute. On the other hand, with the ahead of certainty progress of the Internet throughout the recent years, a progressively more large number of susceptible systems are now available to attackers. Attackers can now employ a large number of these susceptible hosts to launch an attack as an alternative of using an on its own server, an approach which is not very valuable and become aware of easily. Generally, this type of attacks create a problem during at system downtime, missing profits, and the substantial effort fit into placed to be acquainted by means of and formulate moving ahead creating such attacks.

III. LITERATURE SURVEY

In this thesis suggests [9] an interconnection clarification for Cloud coalitions based on allocate/recruit military. Here they introduced a original flexible amalgamated Cloud building in which the sustenance bounded by the obsessional society is based on a ascendable distribute/promise middleware for active and translucent interconnection of manifold classes of incomes/objects over mixed Internet-based announcement structures. The projected [9] IntCloudWare contexttheoretical and recapitulates the interacted possessions accessible within the coalesced Cloud into controllable and energetically provisioned objects, enable relaxed and low-priced descriptions that make imaginable perpendicularly and straight announcement amongst the intricate wage-earner's distributed complete appropriate borders, supportive the mandatory trustworthiness and ease of use environments of present-day location-independent Cloud tenders.

On the additional pointer such construction suggests new approaches for realizing DoS boudiscovery, anticipation, and salvage. Here they established that in an interconnection organization for joined Clouds the penalties of a DoS dose can broadcast inversely contingent on influences for instance communication gratified and the upkeep of national in the machineries of the middleware. Untried consequence demonstrations that the stuff of DoS bouts that mature the dispersed brokerage, the communication content-complexity and the location defense. Specific retrievals gadgets have to be designed with the determination of withstand predictableregulator over presentation and answer periods of such compound organizations.

In amalgamated Cloud, breadwinners can reciprocally cooperate to portion their incomes and accomplish the requestamong teach other’s.

For occurrence, a wage-earner can subcontract requirements to other workers when obliging requirements within indigenous substrates is not conceivable for instance in crowning hours. Unquestionably, this is the circumstance when the foreseebale incomes from these purchasers’ requirements is greater than the custody of subcontracting them. Consequently, the worker attains developed revenues since it can deliver provision for more patrons without opposite principal costs of gaining IT apparatus which capacity be costly. Similarly, a provider that has underutilized belongings might license part of them to other earner in the alliance [10]. The effectiveness of a miscontractor in a amalgamates situations except for being contingent on widespread range of strictures such as the breadwinner’s conventional assignment, the charge of subcontracting added incomes, the income of rental underutilized volume, or the cost of preserving the wage-earner’s possession effective. Consequently, cloud workers necessitate partaking an understandableness of the disadvantage of every conclusion they make. Goiri et al. [10] commend a monetary symbol that symbolizes circumstances that assist conclusions in an amalgamated incomprehensible, such as when to commission possessions to other wage-earners, when to acknowledge requirements from other wage-earners, and how much volume to underwrite to the coalition.

S. Yu, et al. [11], planned a self-motivated stock portion method for defensive discrete clientele of mistruth throughout DDoS attack safeguarding excellence of provision throughout attack. The cloud setting is accomplished of supervisory the reserved distributions since it has huge amount of possessions to apportion to separate operator. The standby helping method used in clouds theaters vigorous role in extenuating the impression of dose by philanthropic admission to capitals. In cloud situation the accomplishment of attack or protection be contingent upon who is property more resources, aggressor or cloud user. The active further stand by portion averts malnutrition, thus defensive in contradiction of DDoS boat. They also accessible queue based classical of reserve apportionment under numerous attack situations. They used dependable planet statistics set standing on DDoS attack for investigation of reserve apportionment. In average municipal of activities, the real-world associated in mist has disturbance prevention organization (IPS) for sanctuary determination and column that preserves the list of received packets.

324
Through attack conditions, great number of package licenses finished the column as botnets are used for introduction DDoS attacks there ascend a need of replicating the possessions to upsurge the intrusion expectation systems. This is made conceivable by go-ahead reserve provision. They appraised the exhibition of developed mock-up through limitations in standard and bountiful circumstances and using Amazon EC2 cloud for procurement consequences.

M. Glenn [12], in “A instant of DOS/DDOS avoiding, nursing and alleviation technique in an overhaul supplier atmosphere”, demonstrates that the incidence and intricacy of Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) on the Internet are quicksilvernowballing. Provisionwage-earners are below cumulative force to avoid, mitigate and monitor DoS/DDoS attacks heading for in the direction of their clientele and their organization. The Internet is portion of the thoughtful countrywide organization but is exclusive in that it has no unvarying limitations to guard it from doses. Attacks that are production a dissimilarity every day on the Internet include philosophical attacks, shortest attacks, remote controlled attacks, viruses and worm. Explicit attacks expressed at a service provider’s infrastructure can be very damaging and cause wide spread. Here this paper covers these attacks and talk about techniques to avoid attacks as well as good safety measures policies, latest updated product safety measures tough, and space supervision, spoofed container dropping (uRPF) and IPS/IDS/firewall use in a examine contributor environment. Security of the provider’s communications is another key characteristic and that is addressed in this paper.

Fasheng Yi, et al. [13], in “Source-Based Filtering Scheme against DDOS Attacks”, describes that IP address spoofing is make use of a lot of DDoS attack tools. Generally of the existing research on DDoS attack packet filtering depends on collaboration among routers, which is inflexible to achieve in authentic promotions. Consequently, in this dissertation proposition a narrative filtering format based on starting place in sequence in this dissertation to care for against different source IP deal with spoofing.

C. Lin, et al [14], in “An efficient main concern Queue-Based method to lessen spiteful Packet Flows from disseminated DoS Attacks”, demonstrates that a DoS attack affects the resources or bandwidth of a targeted system. By flooding networks and distracting access to services, it may reason that harm on multimedia network services and Internet Service Providers.

In this paper, the authors propose to evaluate the activities of packet flows and implement a main concern queue-based procedure that allocate packet from standard users to a elevated main concern row and packets from supposed attacker to a low main concern queue. Here they justify by using NS2 simulator to proposed priority queue-based scheme is valuable in blocking attacking traffic while maintaining constant flows for legal users.

Yi Xie, et al [15], in “Monitoring the Application-Layer DDoS Attacks for Popular Websites”, illustrates that Distributed denial of service (DDoS) attack is a continuous dangerous threat to the Internet. Originated from the low layer, new application-layer-based DDoS attack make use of legal HTTP requests to overcome victim resources are more untraceable. The case may be more serious when such attacks take off or occur during the flicker crowd occurrence of a popular Website. Mainly these attacks are focusing on the detection for such new DDoS attacks; a design based on manuscript reputation is established. An Access Matrix is defined to imprison the spatial-temporal patterns of a common blaze host. Autonomous constituent psychotherapy and most important constituent psychiatry are practical to theoretical the multidimensional admittance Matrix. A work of fiction anomaly detector based on concealed semi-Markov model is proposed to explain the dynamics of Access Matrix and to detect the attacks. The entropy of manuscript attractiveness correct to the reproduction is used to identify the budding function layer DDoS attacks. Some results based on real Web traffic data are presented to express the effectiveness of the proposed method.

T. Peng, et al [16], “Protection from distributed denial of service attacks using history-based IP filtering” describes that this paper, introduce a convenient design to protect against dispersed refutation of service (DDoS) attacks based on IP foundation lecture to filtering. The boundary router keeps a history of all the legal IP addresses which have formerly become visible in the network. When the boundary router is exceed, this record is used to choose whether to acknowledge an incoming IP packet. Distinct additional proposals to defend against DDoS attacks, here there proposal works well during highly-distributed DDoS attacks, i.e. from a large number of sources. The author nearby quite a lot of heuristic methods to create the IP address database correct and robust, and the experimental results shows that effectiveness of their design in defending against highly-distributed DDoS attacks.
Saman Taghavi Zargar et al.[17] were focus on DDoS flooding attacks and defense mechanisms in wired networked systems. Here, there goal is to categorize the existing DDoS flooding attacks and to provide a broad ranging survey of defense mechanisms categorized based on where and when they become aware of and take action to DDoS flooding attacks. Such a learning of DDoS flooding attacks and the current survey is important to identify with the significant issues related to this essential network security problem so as to put together additional extensive ranging and valuable defense mechanisms. When they avoid, detect, and respond to the DDoS flooding attacks. Furthermore, they highlight do with for a broad distributed and joint defense approach. Our most essential purpose for this work is to support the research community into developing inspired, widespread prevention, detection, and response mechanisms, valuable, proficient, and that address the DDoS flooding problem before, during and after an authentic attack.

DefCOM [18,19] is a distributed framework for DDoS defense. It contains assorted resistance nodes prearranged in a peer-to-peer complex, communicate to realize a energetic supportive resistance and it approved out fatality end, source end, and network core defenses mechanisms to perform attack detection, traffic differentiation and rate-limiting, respectively.

IV. PROPOSED METHODOLOGY

Here the proposed code is based on the concept of computing normal and abnormal behavior of packets that flow in these Interconnected Federated Clouds.

The Proposed algorithm consists of following steps:
1. Select and Configure number of Data Centers and Brokers and Virtual Machines and setup an Interconnected federated Cloud.
2. The algorithm is tested on KDDCup99 Dataset with number of attributes and classes for the prediction of normal and abnormal behavior of packets.
3. The rule sets are computed for each packet of the Dataset in KDDCup99.
4. Selection of Dependent Features attributes from the Datasets on the basis of which prediction of DDoS attacks can be categorized.
5. Reducing the number of other Feature attributes from the dataset.
6. Classification rules are then generated using Classification Tree.
7. Each of the testing packets is then compared with the rule sets generated using Classification tree and finally DDoS attacks can be classified.
8. All the packets which are Categorized as Normal packets, then Frequency of each of these packets is again computed to check the behavior of these packets.

Proposed Algorithm for Feature Selection

Let ‘t’ be the total number of attributes available and ‘C’ be the number of classes available in dataset. Since there are ‘t’ attributes in the dataset so $2^t$ possible feature subsets are possible. There would be two its bits used ‘0’ and ‘1’ for the representation of attribute is selected or not. The Fitness Function can be computed on the basis of below criteria:

$$fitness(x) = accuracy(x) - \frac{cost(x)}{accuracy(x) + 1} + cost_{max}$$

Where fitness (x) is the fitness of the feature subset represented by x, accuracy (x) is the test accuracy of the trained network classifier trained using DistAl using the feature subset represented by x, and costmax is an upper bound on the costs of candidate solutions.

1. Procedure GA(Population)
2. T $\leftarrow$ 0
3. InP Population(t) $\rightarrow$ Initialization of Population randomly
4. F(t) = Com_Fitness (Population(t))
5. While not terminated do
6. t $\leftarrow$ t + 1
7. Population(t) $\leftarrow$ crossover(Population(t-1))
8. Population(t) $\leftarrow$ mutate (Population(t))
9. F(t) $\leftarrow$ ComputeFitness (Population(t))
10. end while
11. return bestPopulation $\rightarrow$ return the best individual population
12. end procedure

J48graft Decision Tree

A Classification tree is a recursive form of the tree consisting of nodes and leaves on the basis of which a decision is taken from the dataset. It is constructed on the basis of the characteristic with the uppermost standardized evidence gain ratio which will be taken as the root node and the dataset is split based on the root element values. Again the data gain ratio is intended for all the sub nodes independently and the procedure is frequent until the calculation is accomplished.

J48graft.Decision_Tree (Training dataset features, Features selected from algorithm above, Output classified features, Non Classified Features)
1. Start with the construction of an empty Tree ‘t’ t → ∅
2. From the ‘F’ selected features from the training Dataset from the Feature Selection algorithm above.
3. Compute the Information gain ratio

\[ I(C1,C2) = - \frac{C1}{C1 + C2} \log \left( \frac{C1}{C1 + C2} \right) - \frac{C2}{C1 + C2} \log \left( \frac{C2}{C1 + C2} \right) \]

Where, I is the Information and C1 and C2 are the classes in the dataset.

\[ E(\text{attribute}) = \sum_{c \in \mathcal{C}} p(c)I(c) \]

Where, E is the Entropy and P is the occurrence of any attribute in dataset and I is Information.

\[ \text{Gain} = I - E \]

4. Select the attributes with highest information gain.
5. Update the tree ‘t’ the attribute as the root node to ‘t’.
6. Remove the attribute from the relation set.
7. End

**Prediction of Normal Packets using Frequency behavior**
1. For each of the Normal (packets) selected from Classification algorithm above.
2. Compute Frequency of each of the normal packet at time ‘tm’ till ‘threshold time’.
3. Compare the total frequency of each of the Normal packet Fpack >>> Fpack+1
4. Select the Normal Packet as Abnormal and comes in the category of DDoS Attack.

V. RESULT ANALYSIS

**Table 1.**
Analysis of Execution Time in Hrs

<table>
<thead>
<tr>
<th>Execution time in Hrs</th>
<th>Existing Work</th>
<th>Proposed Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>24</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>48</td>
<td>37</td>
</tr>
<tr>
<td>4</td>
<td>60</td>
<td>52</td>
</tr>
<tr>
<td>5</td>
<td>60</td>
<td>54</td>
</tr>
<tr>
<td>6</td>
<td>60</td>
<td>57</td>
</tr>
<tr>
<td>7</td>
<td>75</td>
<td>68</td>
</tr>
<tr>
<td>8</td>
<td>100</td>
<td>85</td>
</tr>
<tr>
<td>9</td>
<td>125</td>
<td>118</td>
</tr>
</tbody>
</table>

![Comparison of Execution Time](image)

**Table 2.**
Analysis of number of viruses & Trojans Blocked

<table>
<thead>
<tr>
<th>Layers</th>
<th>Existing Work</th>
<th>Proposed Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>5500</td>
<td>6000</td>
</tr>
<tr>
<td>Identity</td>
<td>3800</td>
<td>4000</td>
</tr>
<tr>
<td>Encryption</td>
<td>900</td>
<td>1000</td>
</tr>
</tbody>
</table>

![Figure 3. Comparison of Execution Time](image)
VI. CONCLUSION

This proposed methodology implemented here is a novel method for optimization of detecting intrusion in the web log data on the basis of preshared exchange of keys between sender and local router and the by checking the entropy variation of message. The proposed methodology implemented here is feasible for large datasets also and provides high alarm rate and accuracy of detecting intrusions. The result analysis shows the performance of the proposed methodology. The proposed methodology is compared with the existing entropy variation based intrusion detection and proposed methodology provides more security and provides high alarm rate and detection ratio as compared to the existing technique.

Although the technique implemented here for the detection of intrusions using entropy variation and pre shared key exchange provides high classification ratio, but further enhancements can be done for the detection of intrusions using more generalized detection algorithm such that it provides high detection ratio but also reduces computational overhead and time.

REFERENCES