INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Analyzing distributed denial of service attacks in cloud computing towards the Pakistan information technology industry

Kamran Ali Memon[1], Sijjad Ali Khuhro[2], Nasrallah Pirzada[3], Muhammad Aamir Panhwar[1]*, Masnizah Mohd[4], Kamlesh Kumar Soothar[1], Noor ul Ain[5]

1 School of Electronic Engineering, Beijing University of Posts and Telecommunications, China
2 School of Computer Science and Technology, University of Science and Technology of China, China
3 Department of Telecommunication Engineering, Mehran University of Engineering & Technology, Jamshoro, Pakistan
4 Faculty of Information Science and Technology, Universiti Kebangsaan, Malaysia
5 School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, China

OPEN ACCESS

Received: 16-07-2020
Accepted: 27-07-2020
Published: 11-08-2020

Editor: Dr. Natarajan Gajendran

Citation: Memon KA, Khuhro SA, Pirzada N, Panhwar MA, Mohd M, Soothar KK, Ain N (2020) Analyzing distributed denial of service attacks in cloud computing towards the Pakistan information technology industry. Indian Journal of Science and Technology 13(29): 2962-2972. https://doi.org/10.17485/IJST/v13i29.1040

***Corresponding author**.

maamirpanhwar@hotmail.com

Funding: National High Technology 863 program of China (No.2015AA124103) and national key R&D program no 2016YFB05502001

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: Cloud computing technology is in continuous development, and with numerous challenges regarding security. In this context, one of the main concerns for cloud computing is represented by the trustworthiness of cloud services in the Pakistan Information Technology (IT) industry. This problem requires prompt resolution because IT organizations in Pakistan adopting cloud services would be exposed to increased expenditures while at a higher risk. A survey conducted by International Data Corporation (IDC) in August 2008 confirms that security is the major barrier for cloud users in Pakistan. **Material/methods:** We have proposed the mathematical-based model for an estimate of our user's requirements regarding our resource investment based on queuing theory to overcome these security issues in cloud technology. We are adopting a system and real-world analysis using data set experiments. **Result:** In this article, we proposed a solution to overcome the Distributed Denial of Service (DDoS) attacks in a cloud computing environment in the Pakistan IT services; because along with discussed above phenomena, we also used DST and FTA (Fault Tree Analysis) for mentioned attacks. **Conclusion:** Our proposed solution based on Dempsters combination rule is to analyzed mixture proof of different types of cloud attacks in IT industries in Pakistan.

Keywords: DDoS attacks; IT Services; attack detection; cryptography; cloud computing

1 Introduction

In the age of 20th century, most of the recent extensive cyber-attacks issues in Pakistan, wherever particular hackers crossed into the banking sector of the safety system and try to compromises bank security. According to the recent research, banking sectors received a lot of complaints regarding the hackers. They hacked thousands of credit and debit cards of customer's confidential accounts data by applying the technique of breaking the security of passwords. Till now, more than 30 thousand debits cards have been compromised from different Pakistani Banks such as; NBP, UBL, HBL, .etc., according to the (PCERT-Pakistan Computer Emergency Response Team). According to the cyber-security forensic report, around 10 million dollars have been stolen from different bank accounts, this was organized by Bank of Islami through international ATMs services, and such types of banking cyber-crimes show the weaknesses at the national and international levels. However, the Pakistani cyber-crime team is also struggling to reduce such kind of extensive cyber-attacks due to a deficiency of ability and weakness within the country's cyber-security policies, and also, cyber-security is a multifaceted problem. Therefore, it needs an intense and highly researched plan to expose such kind of hacker's strategies and provide a more strong security firewall for our banking system [(1)]. We must have to understand that we are in the era of the 4th generation of computer knowledge, information, and technology, which is an advanced way of living our lives and the manner we can connect and broadcast public and private services in the modern world. In the 5th generation of computers, we must have reliable security methods and policies for our digital systems. The advancement and strictness of cyber-based attacks which are increasingly posing very severe attacks to the national economy, government sectors, international baking corporations.

The most advanced study titled 'Understanding the Cyber-security Threat Landscape in the Asia Pacific: Securing the Modern Enterprise in a Digital World', by Microsoft exposed that the possible financial damage across Asian countries and the Pacific region countries are the results of cyber-attacks. It is possibly hit around $1.745 trillion, with the total cost more than 7% of the region's additional GDP. The basic idea behind this research is to explain the business and government policies accordingly, particularly in the region of South Asian countries, to move existing defensive procedures to build a more secure firewall against the upcoming cyber-based attacks. In this well-ordered digital environment, cyber-security necessity makes an integral portion of our safety policies against hackers. Unfotunately, the National response center for cybercrime still do not have the deep understanding of numerous national and industrial technology policies. The organization needs to be incorporate their existing competence to challenge these developing issues. This is 5th generation that belongs to artificial intelligence technology, and many cyber-attacks are continuously evolving. They try to attack our confidential banking password and data very extensively day by day, so we must have a strong policy plan to handle these issues. Besides processes, trading sectors should be united through artificial intelligence and their security policies to control a vigorous cyber-security infrastructure insecure way.

This is a technological world where cyber-attacks are continuously growing and the attempts to attack surface is quickly increasing, it's essential to look forward to Artificial Intelligence (AI) technology which is a charming and effective modern technology against cyber-threats as this technology is capable of identifying and performance on the cyber-based attack against the confidential credit data and passwords insights. Also, banking or another organization should have to incorporate artificial intelligence within the security policies to handle a robust cyber-security infrastructure. The organization of The International Telecommunication Union (ITU), a dedicated agency of the United Nations-UN, is accountable for problems that are related to information and communication technologies- ICTs. In the recent research work regarding 'Global Cyber-security Index 2017′ categorized Pakistan at 67 out of 193 member countries in the world. This ranking analyses the obligation of the member regions towards cyber-security to increase consciousness about five supports of ITU's Global Cyber-security Agenda (GCA) which contain lawful, practical, structural, volume structure, and collaboration. The classification positioned Singapore country in the first country, which monitored by the United States of America and Malaysia as well. However, Iran, Korea, Bangladesh, China placed at different random places, respectively. Such type of South Asia ranking also shows that Pakistan region is behindhand in its region for its promises in the direction of cyber-security policies.

Also, international telecommunication unions published new research that delivers a summary of cyber-security advancement of related countries, which is founded on the five supports of the GCA. Emphasized possible areas for development and motivating cyber-security to the lead of regional strategies for the host country. Pakistan facing a lot of problem regarding cyber-security strategy according to the national and international wise. The main reason behind these issues is the weakness of the strategic framework for deploying globally acknowledged cyber-security ethics, the same as to guarantee and authorization of regional agencies as well as private and public sector experts within the respected country. The analysis shows that Pakistan still need officially recognized regional standards or referential for determining strategies about cyber-security issues within the country. Besides, within the country, the Pakistan government does not have any specific regional authority roadmap and particular documented agency for cyber-based security within the respected country. Though, if we see it the legal

way, particular lawmaking and authorities associated with cyber-security have been ratified from side to side the Prevention of Electronic Crime Act (PECA) 2016, which encompasses the entire country. Chapter 3, Section 26 of the PECA Article declares that the Federal government might launch or designate a law development agency as an examination agency for the determination of inquiry of crimes according to the article. However, the Federal government selected Federal Investigation Agency-FIA Cyber-Wing to examine crimes according to the article, but deficiency of capacity to answer and examine up-to-date cyber-based attacks.

Also, the country deficiencies a publicly recognized agency certified under globally documented principles for manpower improvement in cyber-security. Though Pakistan Computer Emergency Response Team and Pakistan Information Security Association are the only public information security sectors that deliver information security facilities and exercises to assist the public, government, and private organizations and provide a secure shape regarding data infrastructure. Nevertheless, the administration must take principal in creating an agency of global principles united with an extensive investigation and progress program to provide to the data security requirements of the respected country.

While it approaches global collaboration, Pakistan in recent times obtained a four-year term 2018 on the organizational council of international telecommunication union-ITU by obtaining 155 votes out of 177 to became one of the thirteen countries elected to this trans-governmental body from Asia continent and the Oceania-Pacific continent. This is surely an important accomplishment for a respected country, which can support the country to further progress its cyber-security shape as per global principles. In the year of 2012, a Senate Task Force on Cyber Security committee, containing around 40 specialists, was recognized to make cyber-security strategy, policy, rules, and nationwide Computer Emergency Response Team. The mission force consumed about two years and organized an outstanding draft on a cyber-security strategy which was offered to the House as a private member bill, but up till now to be considered. The draft bill was an inclusive manuscript, and with few necessary modifications can be considered nowadays. To encounter tasks, colleges and universities must train cyber experts and cyber administrators. Reason chambers, such as the Sustainable Development Policy Institute (SDPI) be able to check for research upkeep and evidence-based program guidance.

Here are numerous institutes working on cyber-security, be it civilian, military, or academia, nevertheless altogether of them are operational in separation. In this situation, they need robust coordination to manage the problem at hand. However, a crucial requirement is necessary for the respected country to build an agreement between investors to improve an inclusive nationwide policy for cyber-security. Similarly, the country wants to have a distinct sectorial level policy to challenge more sector-particular tasks. Educational institutes must emphasize more on cyber-security problems, and it should be trained as a subject in school and at the university level to raise consciousness between the communities at large. Also, to guarantee separate confidentiality and safety from cyber-threats.

Cloud computing is a novel Internet-based stage where dissimilar user services suppose as: network server, loading, cloud-based applications are common on Internet usage. These application trusts in distribution computer resources, it is disposed to numerous security attacks. In addition, most current study survey on the major 70 Internet-based users in the world designates that the amount of DDoS outbreaks is cumulative melodramatically. The main explanations are the open-access reserve model of the Internet; the other being the network community does not have effective and efficient trackback methods to locate attackers who disguise themselves. This is because of the stateless and anonymous nature of the Internet [(2)].

This paper is based upon noticing, analyzing, and preventing methods and methods to resilient the dispersed Denial of services attacks that ascends at the very high rate of powerlessly and cause the failure of a cloud computing environment. These types of attacks many times become the reason for service distraction. Among the many methods used, the topmost method is (IDS) Intrusion Detection System, to make sure the usability of cloud computing services. On the other hand, IDS sensors have the drawback of producing fault positive rates and high negative rates, and also they give up a massive amount of alerts [(3)]. Concerning proposed IDS issues, our paper will provide the solution to detect and analyze the Distributed Denial of services (DDoS) attacks in cloud computing by using the (DST). By using Dempster-Shafer Theory operations in 3-valued logic and (FTA) for VM intrusion detection system, we conclude the solution for detecting severe attacks of cloud computing environment [(4)].

The remainder of the paper consists of several other techniques for detecting and preventing DDoS attacks. Finally, in the end, the paper will present the concluding remarks about the proposed methods and their applications.

This implies our answer to DST meets the proficiency necessities as far as assaults location just as computational time. In related work, alongside numerous different methodologies, we additionally examined the software characterized organizing that with cooperation worked in the field of system security; however it did not give the best possible casing work to arrange security components [(5)]. Numerous another system, for example, Mitigation calculation, java-based filtration, and Distance-based DDoS are examined that gives some degree of data the executives in distributed computing yet does not have full fledge security prerequisite against DDoS assaults and vulnerabilities and improved extension in genuine work associations. Simultaneously,

other than the security requests, the ease of use prerequisites have been practiced in our proposed arrangement so that the distributed computing chairman's work is eased by the utilization of Dempster's principle of confirmation blend where the quantities of alerts are diminished [6].

2 Related Work

Several techniques have been proposed for the detection and prevention of DDoS attacks in the cloud computing environment. Some of the techniques only detect those attacks; others also provide some prevention criteria. A few also suggest a mitigating approach to these attacks. We have discussed some of these techniques in this paper.

In computing, distributed denial of services attack can cause of making machine or resource on the network is unavailable to its intended user. Generally, the DDoS attacks can be sent by more than two peoples or by bots and also can be sent by one system or person only [7]. Perpetrators of these attacks usually attack sites and services hosted by web servers. DDoS attacks are common in business, banks and card payment gateways, and others. In the Mitigation Algorithm, the IDEA (International Data Encryption Algorithm) is used. In this, instead of blocking or accepting the flows of bits of data, source IPs are shaped or molded in the desired shape [8]. Where conditional Legitimate Probability (CLP) is the probability of a flow to be legal. The other components that are used in the algorithm along with IDEA areas Traffic Shaping that are used for determining high packet rates by using a triggered function timer Handler to send packets. The third one is the shaping algorithm, which is used for function packet handling, which includes binary search. In the end, the evaluation takes place which is carried out to measure the throughput of a legal user on the link depending on the number of shaped IP ranges [9].

A study by Qiao Yan analyzes the relationship between Software-Defined Networking (SDN) and DDoS. It also studies how to launch DoS attacks on SDN and how to deal with this problem. Contradictory relationship between launch DoS attacks on SDN and how to deal with this problem. Another study presents that EDoS (Economic Denial of Sustainability) attack is the primary form of DDoS attack in cloud [10]. Therefore this EDoS can be studied to protect against DDoS attacks. The contradictory relationship between SDN and DDoS has not been well addressed in previous works, so this study can help to understand how to make good use of SDN's advantages to defeat DDoS attacks in cloud computing [11].

As we probably are aware the DDoS assaults influence the traffic of the system on distributed computing too, to forestall the DDoS assaults effectively the observing instrument can be utilized to recognize them and oppose them in the abnormal state by searching up for the irregular spikes in the voltage level [12]. In this respect, Stay cautions screen the traffic levels at the same time and makes and sets the doorstep for producing customized reports as indicated by explicit bots and assaults [13].

Among the different DDoS assaults counteractive action techniques, the most appropriate is the Content Conveyance Network . By identifying the following vulnerabilities in propelled system traffic conveys it to the outsider cloud framework on the system to stop the hacking procedure and other illicit works.

Another procedure in this period is the Virtual Private Administration (VPA). VPS has a more preparing force than a devoted server, and it has a claim processer, framework, and working framework tool [14]. By having its exceptional IP address disconnects it by different servers and from programmers on the system with ground-breaking abilities. What are more some supplier's additionally exceptional security administrations for facilitating Virtual Private Server (VPS). By utilizing the strategy of System Hardening the DDoS anticipation can be accomplished profoundly [15]. The framework ought to be made so secure and ought to be updated and redesign as far as hardware gadgets just as programming modules, including activity framework and different applications defenseless against hacking and assaults [16]. The framework ought to be refreshed occasionally for this reason. One ought to arrange its OS programming and another programming to be harder to the application layer DDoS assaults [17].

Presently days, various administrations are accommodated the hindering of mock IP addresses. Parodied addresses must be obstructed for that in parodying the gadgets, clients of cloud conditions or customers on the web are mental fortitude to uncover its data and other touchy information. Current arrangements request Deep Packet Inspection (DPI) to identify and hinder the Packets instead of IP address to make framework harder for the programmers and DDoS assaults [18].

3 Background of IT in Pakistan

In the 5th generation, IT is a growing industry that has the prospective to develop more in the artificial world. Problems concerning the IT industry are supervised by the Ministry of Information Technology-MoIT of Pakistan. However, the information technology industry is viewed as an effective sector of Pakistan, according to business-wise, though economic crisis. The major IT strategy and operation approach was accepted under the management of Prof. Atta-ur-Rahman, then Federal Minister of Science & Technology. However, at the beginning of the 20th century, which placed the fundamentals of the growth of the IT-information technology sector. Afterward, two basic strategies were launched by the Ministry of IT

under the management of Anusha Rahman Khan. She was the Federal Minister for IT and Telecommunication (2013-2018) during the PMLN league party period. IT principle and fundamental rights were published during the year of 12/2015, and well ahead of National Digital Pakistan Strategy that was officially permitted by the cabinet in 5/2018. At the beginning of the 20th century, a fifteen years tax day off was permitted to endorse the IT sector, which has mature from $30 million to more than $3 billion approximately during the last 20 years. A countrywide programmed started to give skills to the respected teachers was started by Intel Company in 3/2002 in Pakistan on the appeal of Prof. Atta-ur-Rahman according to his effort, 220,000 teachers got training crosswise 70 districts without cost to the government sector. The government of Pakistan has agreed to given incentives to IT stockholders in the region throughout the start of the 20th century until now. This was the main reason to provide support for the development of IT sectors. In the past decade, from 2003 to 2005, the Pakistani IT stakeholders realize the growth of 48.5 million dollars that was a great achievement for Pakistani IT sectors. According to the statistical report of The World Economic Forum, evaluating the growth of Information and Communication Technology-ICT within the country ranked Pakistan 111th among 144 countries in the Worldwide IT report of 2014. According to the analysis of IT research output of Pakistan, in contrast to China, India, and Brazil, the platform of Thomson Reuters has much-admired the growths that have occupied a place as a consequence of the improvements presented by Prof. Atta-ur-Rahman. Meanwhile Pakistan has developed as the country with the uppermost growth in the percentage of extremely cited papers in contrast to the ”BRIC” countries. IN the year of 2011, Pakistan has crossed 20 million internet consumers and is ranked as one of the highest countries that have registered a great progression rate in internet penetration. Generally, it has the 27th position of biggest population of internet consumers in the global. During the economic year 2012–2013, the Pakistan government's goal was to spend Rs. 4.6 billion on information technology developments, with importance on e-government, human resource, and infrastructure development and policies.

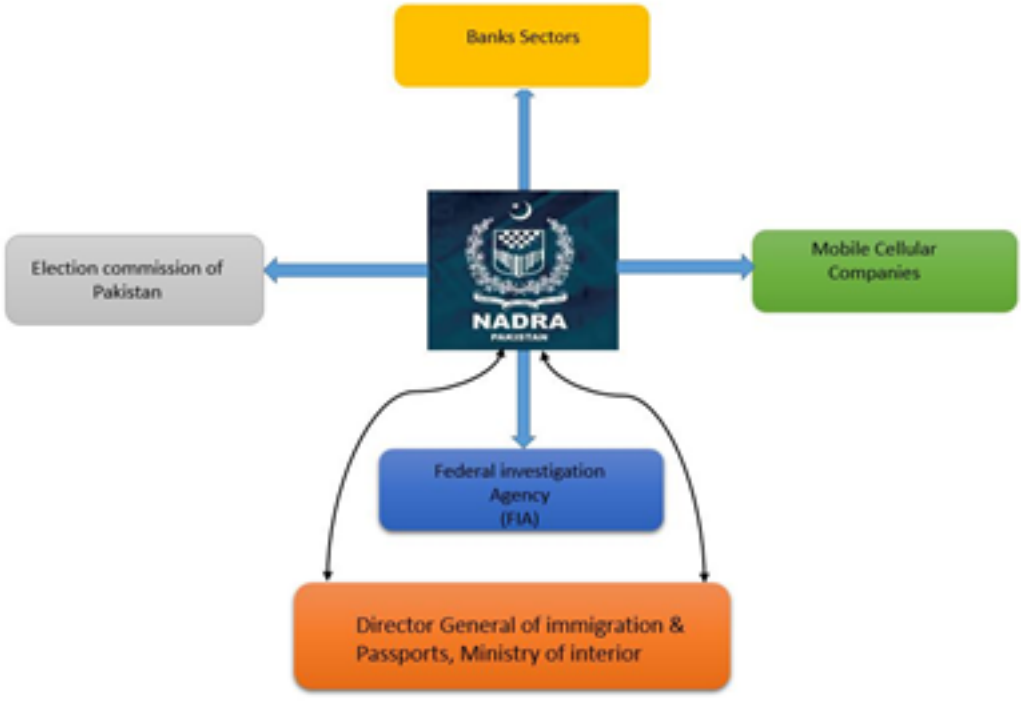

Fig 1. Pakistan IT service-connected to NADRA

The Pakistan Government has committed great significance to information technology sectors, as part of its struggles to progress a ”data/information age” within the region-wise. Also, an intricate nationwide IT strategy was verbalized under the management of Prof. Atta-ur-Rahman is the start of the 20th century, afterward Federal Minister of Science & technology. However, an emphasis on the scientific growth of information technology, the government goals to upsurge output in the public organization to progress the principles of IT structure within the country, and custom it as an administration tool for the advancement of decent authority in over-all. There has been extraordinary development in making operational computerized e-government infra-structure in Pakistan for chief sectors such as police departments, law enforcement agencies, intelligence

agencies, and district management. The respective institute of The National Database and Registration Authority-NADRA has also introduced computerized registration systems for distributing significant documents such as NIC-National Identity Cards, Passport ID, and permanent citizenship cards. IT has also been critically vital in successful work techniques of the civil service and other government-related fields.

According to the UN Economic and Social Commission for Asia and the Pacific (ESCAP) regions, Pakistan has been extremely exposed in information technology while following the ideas of e-governance and e-commerce. Pakistan's communication organization is also dependable. This has now fully advanced into the email, Internet, and IT culture parse. The country is very fast discovering the courageous innovative world of IT-information technology and intensely integrating the necessities of e-government and e-commerce. Information technology has unlocked a new commerce frontier for Pakistan's development. The Pakistan government is conveying very great importance to information technology together in terms of strategy attention and source distribution. Diagram of Pakistan IT services is given in Figure 1 .

4 DDoS Attacks

Distributed Denial of Service (DDoS) outbreaks have become a progressively regular disturbance of the worldwide Internet [MVS01]. They are steadfast to protect in contradiction of because they do not target exact susceptibilities of schemes, but relatively the fact that the target is linked to the whole network. Altogether known DDoS attacks takings benefit of the vast number of hosts on the Internet that have very poor or no safety; the committers break into such hosts, install slave curricula, and at the right time teach thousands of these slave programs to attack a particular destination. The attack does not have to exploit a security hole at the target to cause a problem (although that would Execrable the problem, to the attacks benefit[19].

Different most safety attacks, there is nearly nothing the victim can do to protect itself. What is being attacked is usually not a specific vulnerability, but rather the very fact that the victim is connected to the network. Under normal operating conditions, and assuming that its link(s) and processing capacity have been adequately provisioned, the standard, TCP-like congestion control ensures fair use of the available resources[20–22]. Under a DDoS attack, the arriving packets do not obey end-to-end congestion control algorithms; instead, they incessantly bombard the victim, causing the well-behaved flows to back off and eventually starve. Also, a large-scale DDoS attack not only causes trouble to its intended victim but also interferes with other traffic that may happen to share a portion of the network that is being heavily congested. The details diagram of DDoS attacks are shown in Figure 2 .

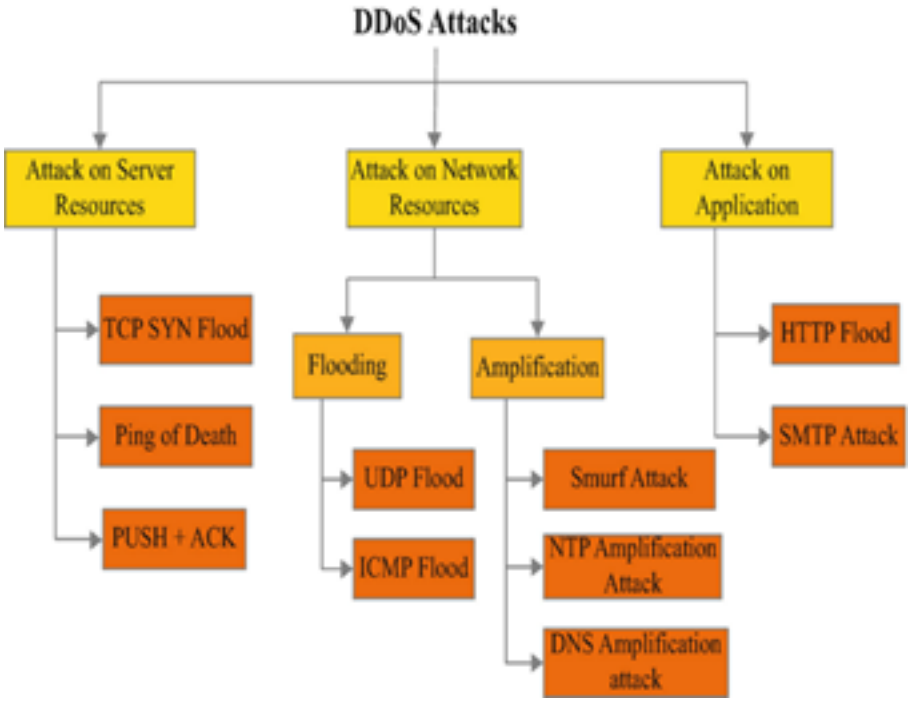

Fig 2. DDoS Attacks

5 Proposed Solution

A) DDoS attacks detection

To detect and examine the DDoS attack in a cloud computing environment where other many techniques and methodologies have been used, I proposed to discuss the IDS system executed on the nodes of VM (virtual machines) machines. In which, the intrusion detection system is installed and configured to come up with all the desired results. The attack estimation cycle or phase is handled internally in the front-end server, which is lied in the Cloud Fusion Unit (CFU).

The first step in the solution starts with the exploitation stage of a private cloud using Eucalyptus, which is the open-source version as 2.0.3. The topology that is used is a front end as well as back end (three nodes). Due to the advanced features, the Managed networking mode is chosen in this scheme. That is also used for virtualization. By installing and configuring the snort, the IDS VM-based IDS are formed. By using VM-based IDS, the overloading problem is overcome. This is the reason behind using these IDS location.

These IDSs will surrender the alerts; these alerts are stored in the database named as Mysql database. The Mysql database is placed in the Cloud Fusion Unit (CFU) of the front-end server. To eliminate or reduce the risk of losing data the single-end data is carried out in use; to maximize the resources usage inside the VMs and for simplifying the work of cloud administrator. A method of similar functionalities including as an IDS Management Unit is proposed in Dhage et al. (2011). Still, our solution adds the capacity to analyze the results by using the Dampster-Shafer theory of evidence in 3-valued logic.

The Cloud Fusion Unit (CFU) consists of three components, such as the Mysql database, BPA's calculation, and attack assessments.

1.Mysql Database

For the storage of alerts received from the VM-based IDS, the Mysql database is introduced in this mechanism. Further, these attacks are converted into Basic Probabilities Assignments (BPA), which will then be calculated by using the pseudo-code below.

2. Basic Probabilities Assignment (BPA's) Calculation

In this stage, for the calculation of basic probabilities assessment; first, we decide on the state space ϑΩ. We are using the DST operations in 3-valued logic in this paper, such as {True, False,(True, False)} for the following flooding attacks; TCP-flood, UDP-flood, ICMP-flood, for each VM-based IDS. For the sake of conversion, to convert the alerts which are received from IDS, pseudo-code is used. Pseudo-code is used for this purpose (conversion), into bpas. The purpose of this pseudo-code is to obtain the following probabilities of the alerts received from each VM-based IDS:

$$\begin{gathered}(m\upsilon DP(T),\ muPD(F),\ muDP(T,F)) \\ (mTCP(T),\ mTCP(F),\ mTCP(T,F)) \\ (mICMP(T),\ mICMP(F),\ mICMP(T,F))\end{gathered}$$

3. Shaping Algorithm

This is the shaping algorithm that is used to manage the data rate traffic in terms of packets. There are two types of algorithms that are used on the base of requirements. An algorithm which is used for the proposed solution is listed below:

Algorithm 1: Shaping algorithm

1: Function packet handler (Packet p)
2: r range including p source IP using binary search
3: if $r$not found then m
4: accept (p) and return
5: q queue of r
6: if not q empty or r sent $+p\ size\ >\ r$ limit then
7: if $q\ size\ >\ q\ max$ size then
8: $q\ push\ (p)$
9: steel (p)
10: else drop (p)
11: else
12: $r\ sent\ +=\ p\ size$
13: accept (p)
14: function $\rightarrow$ time handler

Continued on next page

Table 1 continued

15: for all ranges r do
16: r *sent* 0; finished false
17: q queue of r
18: while
19: not q empty and not finished do
20: p *and* q font()
21: if r *sent* $+$ p *size* $<$ r limit then
22: send (p)
23: $q.pop()$
24: r *sent* $+=$ p *size*
25: else finished true

After the calculation of Basic Probabilities Assignments, we will use the pseudo-code to convert these alerts into BPA's. Following is the pseudo-code that can be used for conversion.

For each node
Begin
For each x belongs to$\{UDP, TCP,$ *and* $ICMP\}$:
Begin

1. Query the alerts from the database when a X attack occurs for the specified hostname.
2. Query the total number of possible Xalerts or alarms for each hostname.
3. Query the alerts form database when X attack is unknown
4. Calculate the belief (True) for X, by dividing the result obtained at step 1 with the result obtained at step 2.
   Also, the probabilities that come from VM-based IDS are calculated as following the fault-tree that is discussed in the above section. This is done to obtain the probabilities for every attack packet.

4. Attacks assessment for evaluation

In this stage of DDoS detection and analysis process, the throughput of the whole system is analyzed and check either it is legal (not shaped) user on a desired data link capacity that is dependent on the number of shaped IP ranges. ".tc" throughput decreases at 400 shaped ranges that are not sufficient to moderate DDoS attack. An attack assessment is consists of data fusion of pieces of evidence that are obtained from the sensors. This is done by Dumpster's combination rule for maximizing the DDoS true positive rates and minimizing the false negative alarm rates, respectively.

B) DDoS attacks prevention

For DDoS Attacks prevention, in this project, we used average detachment estimation based on DDoS detection and exclusion method. In this technique, the mean value of distance in the next period is calculated. This is done by an exponential smoothing estimation technique. To estimate the traffic rates on the network for the smoothening the network security, the distance-based traffic separation DDoS detection technique uses MMSE (Minimum Mean Square Error, which is also called linear predictor to estimate the traffic rates.

We calculated the distance value that is based upon the TTL field of IP Header during transfer directly. In this process, each intermediate router is deducted from the TTL value of the IP packet. Therefore the distance of the packet is final TTL that is subtracted from the initial value of the IP header of the packet. The detection of anomaly depends upon the description of familiarity and deviation. It is stated that the smoothing exponential estimation technique is used due to successful requests in the real-time measurement of the round trip time RTT of the IP traffic.

To determine whether the current distance value is abnormal or not, Mean Absolute Deviation (MAD) can be utilized;

$$\frac{1}{n} = \sum_{n=1}^{n} |x_i - m(X)|$$

Where n is the number of all past errors, and m(X) can be the prediction error at time t. However, it is not realistic to maintain all past errors. For this purpose, we can use an exponential smoothing technique to calculate MAD based on the approximation equation where MADt is the MAD value at time t. r will be smoothing again for the best results. If the real value at the next moment is out of the legal scope, an anomaly situation is detected.

Following are the other techniques to prevent the DDoS attacks in cloud computing network:

As we know the DDoS attacks affect the traffic of the network on cloud computing as well, to prevent the DDoS attacks actively, the monitoring mechanism can be used to detect them and resist them at a high level by looking up for the abnormal spikes in the voltage level. In this regard, Stay alerts monitor the traffic levels simultaneously and create and set the doorstep for generating programmed reports according to specific bots and attacks.

Among the other DDoS attacks prevention methods, the most suitable one is the Content Delivery Network (CDN). By detecting the coming vulnerabilities in launched network traffic delivers it to the third-party cloud infrastructure on the network to stop the hacking process and other illegal works.

Another technique in this era is the Virtual Private Service (VPS). VPS has more processing power than a dedicated server, and it has its processer, infrastructure, and operating system as well. By having its unique IP address isolates it by other servers and from hackers on the network with powerful capabilities. Also, some provider's special security services for hosting to Virtual Private Server (VPS).

By using the technique of System Hardening, the DDoS prevention can be achieved highly. The system should be made so secure and should be updated and upgrade in terms of hardware devices as well as software modules, including operating systems and other applications vulnerable to hacking and attacks. The system should be updated periodically for this purpose. One should configure its OS software and other software to be tougher to the application layer DDoS attacks [23].

Nowadays, several services are provided for the blocking of spoofed IP addresses. Spoofed addresses must be blocked for that in spoofing the devices, users of cloud environment or clients on the Internet are courageous to expose their personal information and other sensitive data. Modern solutions demand Deep Packet Inspection (DPI) detect and block the Packets rather than IP address to make the system harder for the hackers and DDoS attacks.

6 Analysis

By defining the DDoS attacks and its effects in this given paper, we come in to know that with increasing the needs and requirements of the Cloud computing environments in the modern world. There is also a need for security is growing with the advent of modern apps and systems on the internet world [24–26]. To detect and remove these attacks from the networking infrastructure, different techniques have been used since the computing environment is come up with its leveraging services. In this paper, we discussed the existing system with its drawbacks in the sense of DDoS attacks and its severe threats than are not resolving yet.

To overcome these drawbacks, different mechanisms and methodologies we discussed are being used for the authenticity and availability of cloud resources. These techniques included DSP, IDS, Distance-based DDoS, Mitigation algorithm, and many other techniques with its applications and working environment. These are all using now a day in different fields of computing environment days. In the proposed solution, the methodology or technique we used the named as IDS with DST in VM-based machines to analyze the presence of DDoS attacks and its prevention is the most welcoming and using methodology with its Advantages. This uses the topology oriented IDS mechanism, which has the many components that work together comprehensively to detect the DDoS attacks. The Mysql database is used for the storing of alarms that are received from IDS and after that these are converted into BPA's using algorithms. Finally, in attacks assessment, we used the method to assess the output or throughput of the whole system while in the absence of these BPA (attacks). MAD algorithm made our process of defects detection and prevention more useful to execute the most significant values in terms of variables to compute the time and storage modules for the DDoS attacks.

In DDoS attacks prevention, we discussed different other techniques that are useful after reading the review papers published on the various forums through the Internet [27]. These techniques make our proposed work suitable to defend our topic in terms of attacks, its detection, and prevention. There are lots of services, techniques, and mechanisms offered nowadays to overcome the problem of DDoS attacks and its prevention [28]. We discussed some of them and tried to cover our topic at best as long as we did it.

7 Summary and Conclusion

Cloud computing is a new Internet-based platform of providing services such as a; a utility that is very efficient and scalable. However, there are some specific security issues related to cloud computing because of its resource sharing approach. One of such issues is Distributed Denial of Service or DDoS attacks in Pakistan IT sectors. Different approaches are presented for the detection and prevention of these attacks. Some techniques focus on mitigating these attacks. In this article, we used the same techniques such as; DST (Dempster-Shafer Theory) operations with the help of 3-valued logic for detection and analysis of the DDoS attacks, along Fault-Tree Analysis (FTA) approach for each VM-based Intrusion Detection System (IDS) technique for

the elimination of detected attacks. In overall sight, our article gives an overview of DDoS attacks, their origin, and after that the detection, prevention, and techniques by using secure and flexible mechanisms that can be intense and comprehend for future work.

Acknowledgments

The research work is financially supported by the National High Technology 863 program of China (No.2015AA124103) and national key R&D program no 2016YFB05502001 and carried out in state key Laboratory of Intelligent Communication, Navigation and Micro-Nano System, Beijing University of Posts and Telecommunications, Beijing, China.

References

1) Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*. 2017;107:30–48. Available from: https://dx.doi.org/10.1016/j.comcom.2017.03.010.
2) Sahi A, Lai D, Li Y, Diykh M. An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment. *IEEE Access*. 2017;5:1–1. Available from: https://dx.doi.org/10.1109/access.2017.2688460.
3) Iqbal S, Kiah MLM, Dhaghighi B, Hussain M, Khan S, Khan MK, et al. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*. 2016;74:98–120. Available from: https://dx.doi.org/10.1016/j.jnca.2016.08.016.
4) Rengaraju P, Ramanan VR, Lung CH. Detection and prevention of DoS attacks in Software-Defined Cloud networks. *2017 IEEE Conference on Dependable and Secure Computing*. 2017;p. 217–223. Available from: https://ieeexplore.ieee.org/document/8073810.
5) Gupta BB, Badve OP. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment. *Neural Computing and Applications*. 2017;28(12):3655–3682. Available from: https://dx.doi.org/10.1007/s00521-016-2317-5.
6) Agrawal N, Tapaswi S. Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing: A survey. *Information Security Journal: A Global Perspective*. 2017;26(2):61–73. Available from: https://dx.doi.org/10.1080/19393555.2017.1282995.
7) Zhang B, Zhang T, Yu Z. DDoS detection and prevention based on artificial intelligence techniques. *3rd IEEE International Conference on Computer and Communications (ICCC)*. 2017;p. 1276–1280. Available from: https://ieeexplore.ieee.org/document/8322748.
8) Somani G, Gaur MS, Sanghi D, Conti M, Rajarajan M, Buyya R. Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions. *IEEE Cloud Computing*. 2017;4:22–32. Available from: https://dx.doi.org/10.1109/mcc.2017.14.
9) Modi CN, Acha K. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. *The Journal of Supercomputing*. 2017;73(3):1192–1234. Available from: https://dx.doi.org/10.1007/s11227-016-1805-9.
10) Jaber AN, Zolkipli MF, Shakir HA, Jassim MR. Host based intrusion detection and prevention model against DDoS attack in cloud computing. In: International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Springer. 2017;p. 241–252. Available from: https://www.springerprofessional.de/en/host-based-intrusion-detection-and-prevention-model-against-ddos/15187626.
11) Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. Service resizing for quick DDoS mitigation in cloud computing environment. *Annals of Telecommunications*. 2017;72(5-6):237–252. Available from: https://dx.doi.org/10.1007/s12243-016-0552-5.
12) Bonguet A, Bellaiche M. A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. *Future Internet*. 2017;9(3):43–43. Available from: https://dx.doi.org/10.3390/fi9030043.
13) Alzahrani S, Hong L. A Survey of Cloud Computing Detection Techniques against DDoS Attacks. *Journal of Information Security*. 2018;09(01):45–69. Available from: https://dx.doi.org/10.4236/jis.2018.91005.
14) Badve OP, Gupta BB. Taxonomy of recent DDoS attack prevention, detection, and response schemes in cloud environment. In: Proceedings of the international conference on recent cognizance in wireless communication & image processing. Springer. 2016;p. 683–693.
15) Khan MA. A survey of security issues for cloud computing. *Journal of network and computer applications*. 2016;71:11–29. Available from: https://www.sciencedirect.com/science/article/pii/S1084804516301060.
16) Fakeeh KA. An Overview of DDOS Attacks Detection and Prevention in the Cloud. *International Journal of Applied Information Systems* . 2016;11(7):25–34. Available from: https://www.ijais.org/archives/volume11/number7/952-2016451628.
17) Balamurugan V, Saravanan R. Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation. *Cluster Computing*. 2019;22(6):13027–13039. Available from: https://link.springer.com/article/10.1007/s10586-017-1187-7.
18) Pillutla H, Arjunan A. Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing. *Journal of Ambient Intelligence and Humanized Computing*. 2019;10(4):1547–1559. Available from: https://dx.doi.org/10.1007/s12652-018-0754-y.
19) Wani AR, Rana QP, Saxena U, Pandey N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. *Amity International Conference on Artificial Intelligence (AICAI)*. 2019;p. 870–875. Available from: https://ieeexplore.ieee.org/document/8701238.
20) Ahmed P, Memon S. A Secure News Web-Based Application for Multiple users Sharing Information Publically. *Indian Journal of Science and Technology*. 2019;12:11–11.
21) Ahmed A, Khuhawar A, Kimlong N. OPAS: A Trusted Web-Based Online Property Advertising System. *Indian Journal of Science and Technology*. 2018;11:1–5.
22) Panhwar MA, Khuhro SA, Mazhar T. Virtual machine optimization to achieve energy efficient optimum resource utilization in cloud data center. *Indian Journal of Science and Technology*. 2020;(13):1423–1434. Available from: https://doi.org/10.17485/IJST/v13i13.211,2020.
23) Ahmed A, Khuhawar A, Hayat S. FGEHF: Authenticated Web Based Application for Human Resource Management System. *Indian Journal of Science and Technology*. 2018;11:1–12.
24) Rana K, Gulzar. Wireless ad hoc network: detection of malicious node by using neighbour-based authentication approach. *International Journal of Wireless and Mobile Computing*. 2018;14:16–24.
25) Khuhro S, Ali. MobiGuard: A mechanism for protecting and controlling user's personal data on android smartphones. *Imperial Journal of Interdisciplinary Research (IJIR) 3*. 2017;12:50–58.
26) Xie Y. Realize General Access Structure Based On Single Share. In: and others, editor. International Conference on Computer Technology, Electronics and Communication (ICCTEC). IEEE. 2017.

27) Panhwar M, Aamir. SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms. *International Journal of Computer Science and Network Security* . 2019;19:48–55.
28) Panhwar MA, Khuhro SA, Pirzada N, Memon KA, Zhongliang D, Ain N. Security Solutions for Classified Attacks in WSNs. *IJCSNS*. 2019;19(6).