IJE TRANSACTIONS B: ApplicationVol. 27, No. 8, (August 2014) 1179-1184

International Journal of Engineering

Journal Homepage: www.ije.ir

# Reputation Based Service for Cloud User Environment

N. Jeyanthi*, H. Shabeeb, M. A. Saleem Durai, R. Thandeeswaran

*School of Information Technology and Engineering, VIT University, Vellore – 632 014, Tamilnadu, India*

*PAPER INFO*

*Paper history*:
Received 12 November 2013
Received in revised form 18February 2014
Accepted in 06March 2014

*Keywords*:
Cloud Computing
DDoS Attack
Network-level Attack
Service-level Attack
Authentication
Credits

*ABSTRACT*

Exceptional characteristics of cloud computing have replaced all traditional computing. With reduced resource management and without advance investment, it has been victorious in making the IT world to migrate towards it. Microsoft announced its office package as Cloud, which can prevent people moving from Windows to Linux. As this drift is escalating in an exponential rate, the cloud environment has also become a target for attackers. Hence to acquire the best use of the cloud services, the security issues have to be dealt with first. Among various security threats faced by the cloud environment, this paper focuses on the most dangerous one, Distributed Denial of Service attack, DDoS. In DDoS attack, a victim is targeted simultaneously by numerous hosts distributed across the network. An attacker compromises the vulnerable systems in the network and infects those systems with malicious code which can trigger these systems, called zombies, to send requests in huge numbers to choke the target. This type of attack can happen both at network as well as service level. Network level attack is achieved by sending simultaneous invalid or incomplete requests, whereas in service level attacks, the target will be flooded with complete request for services provided by the CSP, but with malicious intent. These two types of attack trafficshave to be filtered out at different levels. In this paper, a three phase authentication scheme, REputation based Service for Cloud User Environment (RESCUE) has been proposed that can help the cloud service provider to detect and mitigate both the aforesaid types of DDoS attacks. RESCUE, the proposed scheme authenticates the users in three different phases. The simulation results presented here exhibits the strength of the proposed method in detection and prevention of DDoS attack in cloud computing environment.

*doi: 10.5829/idosi.ije.2014.27.08b.03*

## 1. INTRODUCTION

In this era of global economic recession, industries are on the lookout for novel and commercial ways to chop down the investments at the same time as to expand up the benefits. Cloud computing has been accepted as the prominent technology of all traditional computing paradigms by the IT world. It can be described as the supply of on-demand scalable resources as 'services' on 'pay-as-you-go' basis. Users can access these services anytime, anywhere provided they have an internet enabled system, without worrying about what is happening behind the screen.

Besides these benefits, the security concerns have become an overwhelming challenge for cloud service providers (CSP). These issues have been given light in the literature [1]. Distributed Denial of Service attacks are the most hazardous of all, in a cloud environment. This kind of attack stifles the CSP in a way that the datacenter resources will get exhausted and it fails to serve the service request from legitimate users. The attackers usually execute this by compromising insecure systems distributed across the network and install malware applications in those systems which are capable of sending multiple requests to the CSP simultaneously. The DDoS can occur in two different levels, one at Network Level and the other at Service Level.

- In Network Level DDoS, the attackers will try to send some invalid requests with the aim of flooding the CSP; e.g., requests for a half open connection.
- In Service Level DDoS, the attacker will be

*Corresponding Author's Email: njeyanthi@vit.ac.in (N. Jeyanthi)

Please cite this article as:N. Jeyanthi, H. Shabeeb, M. A. Saleem Durai, R. Thandeeswaran, Reputation based Service for Cloud User Environment. International Journal of Engineering (IJE) Transactions B: Applications Vol. 27, No. 8, (2014): 1179-1184

sending requests that seem to be legitimate. Their content will be similar as a request made by a legitimate user. Only their intention is malicious.

But, CSP would not be able to discriminate this kind of requests for services. Thus, it is high time now to devise some techniques to eradicate these two kinds of DDoS attacks and make the cloud 100% secure from DDoS.

RESCUE authenticates users in both of the above mentioned form of DDoS. The compromised system can be either human controlled or a robot. This can be judged by inquiring the clients to solve puzzles or simple mathematical equations, which will not entail more processing time. The robots can perform only the tasks assigned to them, i.e., to send request as per the bot master's command, fails to solve the puzzle. The requests coming from these systems can be dropped immediately and their IP address is blacklisted for blocking them in future also. Human controlled systems could solve the puzzle; succeed in this phase. Hence, this phase is able to segregate man and machine but fails to identify the zombies. The proposed reputation based authentication mechanism could discriminate them by assigning credits to the requester based on which they are classified as well-reputed, reputed or ill-reputed.

In case of Network Level DDoS, the similarity exhibited in request traffic flow is used as a criterion for discriminating DDoS traffic from Flash Crowd,as the attacker installs malware in the zombies and attack is set based on the instructions in the program code. It is assumed that the request traffic from zombies controlled by a bot-master will show signs of resemblance.

In case of Service Level DDoS, this criterion fails. As all users, no matter good or bad, will be sending request for services to CSP, the traffic flow analysis will yield same result. So, we have used another decisive factor. The intervals between successive requests from each aggressive user are found out. Those who exhibit fixed time periods are suspected whereas others are considered as impatient legitimate users. After authenticating the users, they are given credits and based on these credits, the users are provisioned services.The rest of this paper is organized as follows: section 2 presents the related works, section 3 describes REputation based Service for Cloud User Environment (RESCUE) proposed framework, section 4 analyzes the performance of the proposed solution and section 5 concludes the paper with future work.

## 2. RELATED WORK

DDoS attack in cloud is a crucial issue that bothers most CSPs. This type of attack brings down their datacenters and/or crashes the systems permanently which can cause severe loss to small and large organizations that offload the tasks to this attacked cloud. CSPs will suffer from both financial and reputational losses. Numerous research works have been taking place in various parts of world to rescue the cloud from this threat.

Overcourt [2] defends the network from DDoS threat. The users are given credits based on the response they receive from the protected server and are classified as well-behaving and ill-behaving, accordingly. VIP path with full access to protected servers is assigned to well-behaving clients and Non-VIP path with limited access is assigned to ill-behaving clients. The clients whose credits got exhausted meanwhile are blocked. The method has various advantages such as no need of changing the underlying infrastructure, credit decaying mechanism to deal with issue of dynamic IP allocation, etc. But the criterion chosen by the authors to discriminate attack traffic from legitimate will not sound good in all cases. The chances are high that even an attacker gets responses. Liu et al.[3] suggested a 'Trust Guard' which gives credits to users who show miscellany in the size of request packets. They assumed that the attackers always send small sized packets which are numerous in number. The method fails if the attacker sends large sized packets or mimics the legitimate packets. Natu and Mirkovic[4] used ticket granting mechanism based on credits and penalties acquired by the clients during their past interactions with the protected server. The attacker can turn hostile after attaining the ticket and also the scheme fails if the attacker is a human. The information distance [5], flow correlation coefficient [6] and inter arrival time of packets are various other methods proposed in this regard. Inanother work [7], the authors have used the expectedness of packet arrival rates to discriminate between attackers and legitimates. Al-Duwairi and Manimaran [8] used search engines for authenticating users. The users are given access to the protected server only through search engines and this search engines will ask users to solve some reverse turing test. The users authenticated this way are given services after white listing them and others are blocked. A major advantage of this method is thatthe attack traffic and legitimate traffic are distinguished at the entry level themselves using the search engine and edge routers. This will reduce the traffic aggregation near the victim. Communication overhead among the edge routers is also a problem here. This method fails in front of human intelligence. In another work [9], Walfish et al. proposed 'speak up' mechanism which encourages the users to send more and more request using the available resources. It is assumed that attackers will be using all the available resources and legitimate users will have spare resources. So, those who respond to this encouragement are classified as legitimate users and others as attackers. The method is simple to implement and attackers cannot fool the defensive mechanism by any means. The increased cost at server, network as well as end user, uncertainty of extra resource availability and failure in discriminating DDoS from

Flash crowd are the limiting factors.

Dinesha and Agrawal [10] have proposed a multilevel authentication mechanism by providing different passwords to different levels of users in an organization. This method reduces the probability of breaking the credentials as multiple level passwords are there. Strict authentication and authorization are possible with this method. As authentication is at different levels, each user does not need to know all passwords. But this kind of authentication would not work when there isno intermediate level between end user and CSP. Schneider and Koch [11] propose 'HTTP reject' to discriminate DDoS from Flash crowd. They have suggested that when flooding is detected, the server should provide each user with a small but informative message about the situation. It is assumed that a legitimate user will not retry again, whereas the attackers do and hence the requests from such users can be dropped.

From survey, it has been observed that each of these methods have their own pits and falls and can be a standalone defense toward off DDoS in Cloud. RESCUE, a new framework which washes out all the disadvantages of above described methods, has added hallmark.

## 3. REPUTATION BASED SERVICE FOR CLOUD USER ENVIRONMENT (RESCUE): PROPOSED SOLUTION

**3. 1. Working Mechanism** RESCUE, REputation based Service for Cloud User Environment, is an authentication based approach that classifies the users into three ranks of reputation, viz. well-reputed, reputed and ill-reputed. In the first phase, puzzle solving is used as an entry level authentication to discriminate human beings and robots. The requests from users who are unable to solve the puzzle are dropped instantly. The second phase identifies the network level attack traffic based on the homogeneity of traffic flow under the assumption that the same malicious programs installed in zombies generates similar pattern of invalid request. The user's requests which contribute to such similar patterns are suspected. The requests filtered at this phase are given to the third phase authentication. The service level attack is trapped at this phase based on the observation that the malicious program generated requests exhibit fixed interval between the consequent service requests. Credits are given to senders of requests based on these three authentications. The users are classified into three ranks of reputations according to which they are provisioned CSP resources. The method helps to filter out the attack traffic and passes the legitimate requests only to the CSP. The users, whose credits go down beyond a certain limit, are blocked and blacklisted, so that they cannot cause further attacks.

The users are given credits for this classification. The lower limit of credit is $L_{VALUE}$and upper limit is. $H_{VALUE}$. Initially all users are given credit equal to $M_{VALUE}$ which is the mean of $L_{VALUE}$ and $H_{VALUE}$., $P_{VALUE}$, a predetermined value ($M_{VALUE}$< $P_{VALUE}$< $H_{VALUE}$) is the deciding factor for reputation. The users who acquired credit value greater than $P_{VALUE}$ are designated as well reputed and are given full access to CSP resources. The users with credit value between $L_{VALUE}$and $P_{VALUE}$ are given limited access by classifying them under group reputed. The users, whose credits are less than $L_{VALUE}$ are blocked and blacklisted.

### 3. 2. Assumptions

i. *To Defend Network-Level DDoS Attack*
The attackers form botnets by compromising vulnerable systems distributed across the network and install malicious program codes in those systems. Impersonation can happen with or without the knowledge of the legitimate system. Whatever the case maybe, the instructions in codes will make the systems to flood the target server. So, it is assumed that these request patterns will exhibit signs of similarity as they are the result of legal program code installed in all zombies.

ii. *To Defend Service Level DDoS Attack*
Whether it is the legal program code or botmaster that triggers all zombies, there will be a periodicity in the inter-arrival time between consequent requests from a user.

### 3. 3. Crediting Mechanism

**1. Initialize**

$M_{VALUE} = ( L_{VALUE} + H_{VALUE} )/2$

**2. incrCredit()**

$Credit_{new} = min(credit_{old} + Incr * credit_{old}, H_{VALUE})$

**3. decrCredit()**

$Credit_{new} = max(credit_{old} - Decr * credit_{old}, L_{VALUE})$

Note: Incr & Decr are increment and decrement factors

**3. 4. REputation based Service for Cloud User Environment (RESCUE) Architecture** In the RESCUE architecture shown in Figure 1, the request from the users will be accepted by a proxy server which performs entry level authentication. Man and machine are distinguished by their problem solving skill. The request initiator will be invited to do minor computations such as puzzle solving or factorization which do not consume much of the user time. After this phase, the bad traffic is trashed and others are given to a component called Resource Overload Monitor (ROM). Based on the volume of requests, ROM will detect the

presence of flooding. Upon flood detection and resource overload, the flow routers at datacenter perform flow analysis and feed the result to the Coordinator Router (CR). The CR compares the inputs from all flow routers. If the requests with similar contents are valid requests, they are concluded to contribute service level flooding. Invalid requests contribute to network level flooding. The details of discarded and accepted flows are communicated to the ROM and it will add or deduct credits of users accordingly. In case of service level attack, the flow router reports the inter-arrival time between requests from each aggressive user to the CR. The CR discards the requests from users who send requests in fixed intervals. The details of discarded and accepted flows are communicated to the ROM and it will add or deduct credits of users accordingly.

3. 5. RESCUE Framework The RESCUE framework, shown in Figure 2, authenticates the users in three phases -

3. 5. 1. Phase I: Discriminate Human from Robot The proposed frame work first finds out whether the incoming requests are sent by a human user or programmed robot. This is done by presenting the sender of requests a puzzle or mathematical sum. Only human beings can succeed this test. So, it can be easily confirmed that others who fail in the test are robots with malicious intent. Such senders are blocked and their IP addresses are blacklisted immediately. This can be considered as an entry level authentication.

3. 5. 2. Phase II: Discriminate Legitimate and Attacker After authenticating the users based on the above test, the system detects whether there is flooding or not, based on the volume of incoming traffic. In case of flooding, the system has to analyze the flow similarity. If the flow analysis yields similar results, the system checks the content of requests. The valid requests are given for phase III authentication. The senders of invalid requests with similar content are suspected and those requests are dropped. The credits of such senders are decremented. Also, well reputed users are notified about the possibility of malware in their system so that they can take necessary actions to rescue their systems and hence avoid further decrements in credits.In case if the flow analysis gives different results, that flow can be concluded as coming from different users and those users are legitimate. The credits of such users are incremented and services are provisioned accordingly.

3. 5. 3. Phase III: Discriminate Impatient Legitimate and Legitimate In case, there is no network flooding, the system has to check for service level flooding in which the attackers will flood the system with 'legitimate like' requests. Phase II authentication fails in such cases. Then the system finds the aggressive users first. Non aggressive users are considered harmless, and based on the credits they have, the services are provisioned to them. Aggressive users can be attackers or impatient but legitimates. Such users' credits are decremented first. Then the inter-arrival period between requests are identified. Those who send requests in random interval are 'impatient legitimate'. They are given service according to their credits and others are suspicious clients. Their requests are dropped and credits are further decremented. Well reputed clients are then given notification. The users whose credits got exhausted are blocked and blacklisted.

## 4. PERFORMANCE EVALUATION

The advantages of the proposed RESCUE solution for DDoS attack in cloud have been highlighted in this section by analyzing the simulation results obtained from CloudSim Simulation.

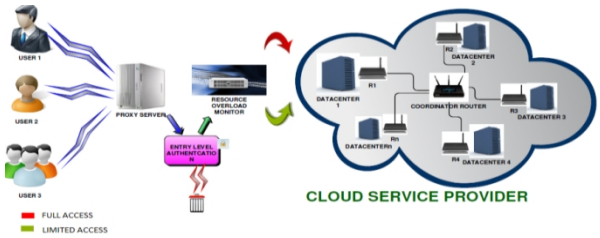


**Figure 1.** RESCUE architecture

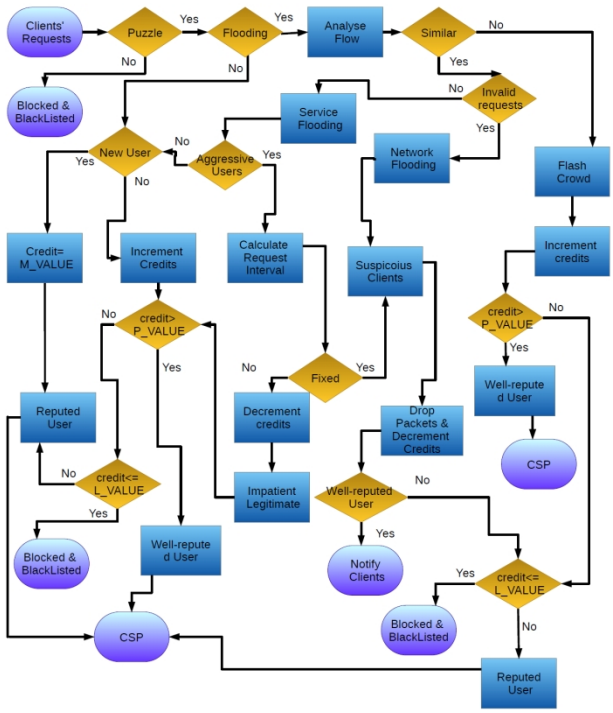


**Figure 2.** Flow diagram of RESCUE framework

4. 1. Traffic at Datacenter The traffic at datacenter is measured by analyzing the number of requests reaching the various datacenters owned by the CSP in a particular time interval.The request reaching the CSP during a time period of 1 second is observed here. Figure 3 shows the number of requests arrived at the datacenters during various scenarios. Figure 3(a) shows that during non-attack period, at peak times the count of requests is in between 4 to 5 request per second. But, the increased spike in Figure 3 (b) shows that the system is under attack. The strength of the proposed method is depicted in Figure 3 (c). It shows that all the requests that have contributed to flooding at CSP datacenters have been completely eliminated and the system under attack is enabled to work as if in normal non-attack environment. This ensures high performance of the CSP datacenters even during the DDoS attack.

4. 2. Resource Utilization based on Credit The resources here refer to the CPU, RAM and Bandwidth. The utilization in percentage (%) according to the credits attained by users is observed. As per the proposed solution, the well reputed users with higher credits are given full access to these resources. The graph in Figure 4 depicts that the users whose credits increment with time and cross a certain prefixed limit are allowed to access the 100% CSP resources. The reputed users are allowed to use the CSP resources in a limited manner. Also, the ill-reputed users whose credits got exhausted are totally debarred. The proposed scheme emphasizes strict following of this rule so that the users will get serviced based on the reputation, and no attacker is being served unnecessarily which was the case before implementation of the proposed approach in a cloud environment.

4. 3. Distribution of Flow to Flow Routers One of the key aspects of the proposed scheme is that flow routers are used to analyze the incoming flow, and this is done before the traffic reaches the datacenters. The flow is given to these flow routers in a circular manner after finding the free flow routers.It has been observed from Figure 5 that the flow is distributed uniformly among the Flow Routers (FRs) so that there would not be any overhead for any particular FR at any instant. At the same time, this ensures fast flow analysis as multiple flow routers are deployed at various sites near the CSP datacenters.From the above discussion, it is very clear that the proposed scheme can aid the CSPs to get rid of the hazard of DDoS attack completely.

## 5. CONCLUSION AND FUTURE WORK

Distributed Denial of Service attack in cloud is one of the most dangerous security issues that prevails in cloud computing environment. Although numerous researches which have been undergoing in different parts of globe have come with innovative solutions, none of them proved to be 100% effective in defending this attack. RESCUE, the proposed three-phase authentication scheme, helps to discriminate the DDoS traffic from flash crowd. Credits are given to the authenticated users and users are categorized into various reputation classes based on the credits. Service provisioning depends on the reputation of user. The method deals with both network as well as service DDoS. There is no need of maintaining any traffic profile for comparison purpose. Multi-level authentication helps in more efficient validation of legitimate users. The method does not involve any complex computation and memory overhead. RESCUE is expected to detect, discriminate and prevent DDoS attack and ensure 100% protection from the overwhelming threat of DDoS in cloud. Above experimental results strengthen the claim. In future, RESCUE, defense mechanism will be extended to the federated cloud environment where the CSPs share the credits attained by users in a secure way.

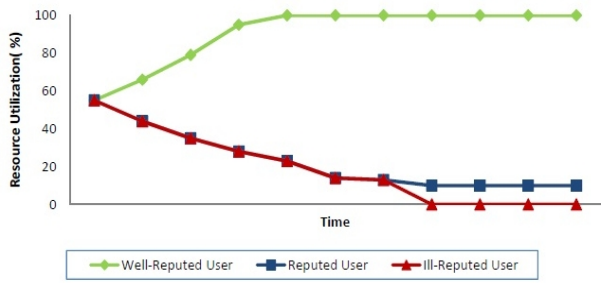


**Figure 4.** Resource (CPU, RAM and Bandwidth) utilization based on credits

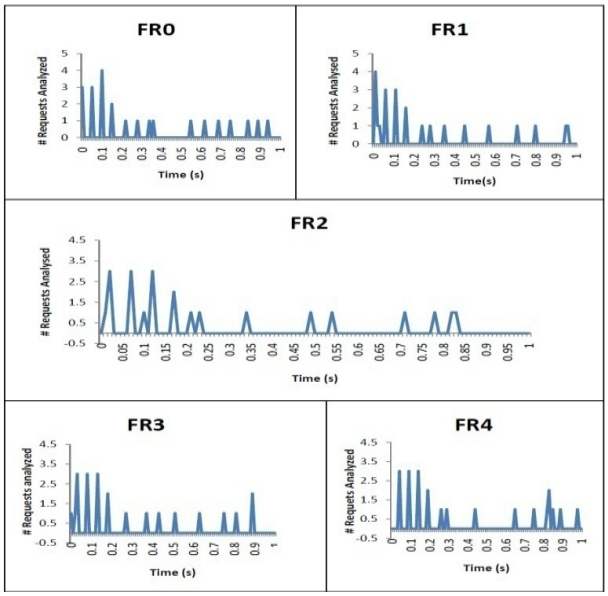


**Figure 5.** Flow router performance

## 6. REFERENCES


1. Jeyanthi, N., Shabeeb, H. and Iyengar, N.C.S., "A study on security threats in cloud", ***International Journal of Cloud Computing and Services Science (IJ-CLOSER)***, Vol. 1, No. 3, (2012), 84-88.
2. Du, P. and Nakao, A., "Overcourt: Ddos mitigation through credit-based traffic segregation and path migration", ***Computer Communications***, Vol. 33, No. 18, (2010), 2164-2175.
3. Liu, H., Sun, Y., Valgenti, V.C. and Kim, M.S., "Trustguard: A flow-level reputation-based ddos defense system", in Consumer Communications and Networking Conference (CCNC), IEEE, (2011), 287-291.
4. Natu, M. and Mirkovic, J., "Fine-grained capabilities for flooding ddos defense using client reputations", in Proceedings of the workshop on Large scale attack defense, ACM. (2007), 105-112.
5. Yu, S., Thapngam, T., Liu, J., Wei, S. and Zhou, W., "Discriminating ddos flows from flash crowds using information distance", in Network and System Security,. NSS'09. Third International Conference on, IEEE. (2009), 351-356.
6. Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y. and Tang, F., "Discriminating ddos attacks from flash crowds using flow correlation coefficient", ***Parallel and Distributed Systems, IEEE Transactions on***, Vol ,۲۳ .No. 6, (2012), 1073-1080.
7. Thapngam, T., Yu, S., Zhou, W. and Beliakov, G., "Discriminating ddos attack traffic from flash crowd through packet arrival patterns", in Computer Communications Workshops (INFOCOM WKSHPS), Conference on, IEEE., (2011), 952-957.
8. Al-Duwairi, B. and Manimaran, G., "Just-google: A search engine-based defense against botnet-based ddos attacks", in Communications. ICC'09. IEEE International Conference on, (2009), 1-5.
9. Walfish, M., Vutukuru, M., Balakrishnan, H., Karger, D. and Shenker, S., "Ddos defense by offense", in ACM SIGCOMM Computer Communication Review, ACM. Vol. 36, (2006), 303-314.
10. Dinesha, H. and Agrawal, V., "Multi-level authentication technique for accessing cloud services", in Computing, Communication and Applications (ICCCA), International Conference on, IEEE. (2012), 1-4.
11. Schneider, J. and Koch, S., "Httpreject: Handling overload situations without losing thecontact to the user", in Computer Network Defense (EC2ND), European Conference on, IEEE., (2010), 29-34.


# Reputation based Service for Cloud User Environment


N. Jeyanthi, H. Shabeeb, M. A. Saleem Durai, R. Thandeeswaran

*School of Information Technology and Engineering, VIT University, Vellore – 632 014, Tamilnadu, India*



*P A P E R  I N F O*

*Paper history:*
Received 12 November 2013
Received in revised form 18February 2014
Accepted in 06March 2014

*Keywords*:
Cloud Computing
DDoS Attack
Network-level Attack
Service-level Attack
Authentication
Credits



**چکیده**

ویژگی های استثنایی محاسبات ابری جایگزین تمام محاسبات سنتی شده است. با کاهش مدیریت منابع و بدون سرمایه گذاری اولیه، مهاجرت در ساخت جهانITیک پیروزی بوده است. مایکروسافت بسته افیس خود را به عنوان "ابر" اعلام کرد که می تواند از حرکت کاربران از ویندوز به لینوکس جلوگیری کند. از آنجا که این جریانبا یک نرخ نمایی در حال افزایش است، محیط ابری یک هدف برای مهاجمان نیز می باشد. از این رو برای به دستآوردن بهترین استفاده از خدمات ابری، مسائل امنیتی باید در اولویت نخست باشد. در میان تهدیدات امنیتی مختلف که محیط ابری با آن مواجه است،این مقاله روی خطرناک ترین آنها، DDoS،تمرکز دارد. در حملهDDoS، قربانی به طور همزمان توسط میزبان های متعدد در سراسر شبکه هدف قرار می گیرد. یک مهاجم با آلوده کردن سیستم های آسیب پذیر در شبکه با کد های مخرب می تواند این سیستم ها را که زامبی نامیده می شوندفعال کند تا تعداد زیادی درخواست برایمسدود کردن هدف ارسال کند. این نوع حمله می تواندهم در شبکه و همچنین در سطح خدمات اتفاق بیفتد. حمله به سطح شبکه با ارسال درخواست های نامعتبر و یا ناقص به طور همزمان صورت می گیرد، در حالی که در حملات سطح سرویس، هدف با سیلی از درخواست های کامل برای خدمات ارائه شده توسطCSP، اما با سوء قصد مواجه می شود. این دو نوع از ترافیک حمله باید در سطوح مختلف فیلتر شود. در این مقاله، یک طرح احراز هویت سه بخشی، اعتبار خدمات مبتنی بر محیط کاربریابری (RESCUE)مطرح شده است که می تواند به ارائه دهنده خدمات ابریدر شناسایی و کاهش هر دو نوع فوق از حملاتDDoSکمک کند.RESCUE طرح پیشنهادی اثبات صحت کاربران در سه فاز مختلف است. نتایج شبیه سازی ارائه شده در اینجا نشان از قدرت روش پیشنهادی در تشخیص و جلوگیری از حملهDDoSدر محیط محاسبات ابریدارد.



doi:*10.5829/idosi.ije.2014.27.08b.03*