International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 3(E); March 2018; Page No. 10779-10783
DOI: http://dx.doi.org/10.24327/ijcar.2018.10783.1843

Research Article

A SURVEY ON MECHANISM TO MITIGATE FRC ATTACK IN CLOUD COMPUTING

Sandeep Singh Rana[1] and Brij Mohan Singh[2]

[1]Maharishi Markandeshwar University, Ambala
[2]College of Engineering Roorkee, Roorkee

ARTICLE INFO

Article History:

Received 25th December, 2017
Received in revised form 18th January, 2018 Accepted 14th February, 2018
Published online 28th March, 2018

Key words:

Cloud Computing, FRC Attacks, Confidentiality, Integrity, Distributed Denial of Service (DDoS) attack.

ABSTRACT

Computing services that were traditionally hosted on organization's private servers and networks are being outsourced to third party Cloud Service Providers (CSPs). Initial threat modeling on CSPs has concentrated on both the confidentiality (keeping data secret) and integrity (making sure the data has not changed) of data hosted in the public cloud. While these threats present real concerns, missing from threat models is the consideration of external threat sources that can affect the availability of Internet-facing cloud services. Availability in this context is not solely restricted to system downtime as a result of a Distributed Denial of Service (DDoS) attack, but also the long-term financial viability of being able to host services in the cloud due to Fraudulent Resource Consumption (FRC) attack.

INTRODUCTION

As our lives become more and more connected, network security becomes more andmore challenging. Security has become an integral part of any network service. With the rapidly increasing number of transactions happening on the Internet, security hasbecome an essential part of everyday life. The context of network security becomes much more difficult to control when the environment becomes as dynamic and emanding as cloud computing.

The main aim of cloud computing is cost reduction and efficiency improvement. This cost reduction is not only in terms of computing resources, but also in termsof helping its users to focus on the business instead of the information technology enabling this business. Cloud computing is the result of developments in many technology directions such as virtualization, autonomic-computing, grid-computing, and many other technologies.

As always, with every new technology, new challenges arise. A very important challenge is providing adequate security to that cloud to perform in alliance with business objectives.

At the start of our discussion, we must be familiarwiththree basic concepts: vulnerability, threats, and attack.

In the Internet EngineeringTask Force (IETF) RFC 2828 [1], a vulnerability is defined as a flaw or weaknessin a system's design, implementation, or operation and management that could beexploited to violate the system's security policy. A threat is identified as a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. On the other hand, the same RFC identifies an attack as an assault on system security that derives from an intelligentthreat, i.e., an intelligent act that is aeliberate attempt to evade security services and violate the security policy of a system. In general, computer security identifies three main objectives-

Confidentiality: Assuring that data are available only to eligible entities and nounauthorized access to data can be obtained.

Integrity: Assuring that data have not been altered in any way while it is stored orwhile its transport over the network.

Authentication: Assuring the identity of the entity involved in the communication.

One of the major reasons why organizations decide to switch to a cloud environmentis the you-pay-for-what-you-use business model. No one likes paying forresource that are not very well utilized. Hence, when an attack such as Denial-of-Service (DoS) attack happens, not only availability is targeted. enial of Service (DoS) attacks aim at making a certain network service unavailableto its legitimate users. In its basic form, these attacks keep the resources busysuch that these resources

Corresponding author:* **Sandeep Singh Rana
Maharishi Markandeshwar University, Ambala

become unavailable to the users this service was aimed to serve. Using DoS attacks on the cloud, the attacker can cause huge financial implications by consuming high resources in the trial of making the service unavailable. So, for the organization using the cloud, it is a doubled loss. The organization will be paying a lot of money for the resources consumed by the attack and, after a while, the organization's service will be unavailable due to theDoS attack. This type of attacks is referred to as Fraudulent Resource Consumption(FRC) [3].

LITERATURE SURVEY

In April 2004, J. Mirkovic and P. Reiher *et. al.* [1], focused on Distributed denial-of-service (DDoS) problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. They presented two taxonomies for classifying attacks and defenses, and thus provided researchers with a better understanding of the problem and the current solution space. The attack classification criteria were selected to highlight commonalities and important features of attack strategies, that define challenges and dictate the design of countermeasures.

In 2005, S. Kandula, D. Katabi, M. Jacob, and A. Berger *et. al.* [2], presented the design and implementation of Kill-Bots, a kernel extension to protect Web servers against DDoS attacks that masquerade as flash crowds. Recent denial of service attacks are mounted by professionals using Botnets of tens of thousands of compromised machines. To circumvent detection, attackers are increasingly moving away from pure bandwidth floods to attacks that mimic the Web browsing behavior of a large number of clients, and target expensive higher-layer resources such as CPU, database and disk bandwidth. The resulting attacks are hard to defend against using standard techniques as the malicious requests differ from the legitimate ones in intent but not in content.

In 2008, C. Hoff *et. al.* [3], proposed that through an EDoS attack, the adversary class reserves a large pool of resources (within the service level agreement of the service provider) in order to make it financially unviable for the service provider to sustain further services for its user. The EDoS is defined as an attack that targets the service provider's economic resources by sending a huge number of requests that appear to be legitimate, exploiting the auto-scale feature of the cloud infrastructure, analogous to traditional DDoS attacks.

In Feb 2009, S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly *et. al.* [4], focused on sophisticated attacks that are protocol-compliant, non-intrusive, and utilize legitimate application-layer requests to overwhelm system resources. In this paper, authors explored the vulnerability of systems to sophisticated layer-7 DDoS-attacks which are both protocol compliant as well as non-intrusive. These attacks mimic legitimate clients and overwhelm the system resources, thereby substantially delaying or denying service to the legitimate clients. They developed a framework to classify these resource attacks as one of request flooding, asymmetric workload, repeated one-shot attacks or combinations there-of, on the basis of the application workload parameters that they exploit. Since these resource attacks are undetectable via sub-layer-7 techniques, authors developed DDoS-Shield, a counter-mechanism which assigns a suspicion measure to a session in proportion to its deviation from legitimate behavior and uses a DDoS resilient scheduler to decide whether and when the session is serviced. Using a web application hosted on an experimental test bed, they demonstrated the potency of these attacks as well as the efficacy of DDoS-Shield in mitigating their performance impact.

In 2009, G. Oikonomou and J. Mirkovic *et. al.* [5], proposed defenses against flash-crowd attacks via human behavior modeling, which differentiate DDoS bots from human users. Flash-crowd attacks are the most vicious form of distributed denial of service (DDoS). They flood the victim with service requests generated from numerous bots. Attack requests are identical in content to those generated by legitimate, human users, and bots send at a low rate to appear non-aggressive these features defeat many existing DDoS defenses. Prior approaches to human-vs-bot differentiation, such as graphical puzzles, are insufficient and annoying to humans, whereas they supposed that their defenses are highly transparent.

In 2010, Khaled M. Khan and QutaibahMalluhi *et. al.* [6], focused on challenges in cloud computing introduced by different type of trust scenario. Today, the problem of trusting cloud computing is a paramount concern for most enterprises. It's not that the enterprises don't trust the cloud providers' intentions; rather, they question cloud computing's capabilities. Yet the challenges of trusting cloud computing don't lie entirely in the technology itself. The dearth of customer confidence also stems from a lack of transparency, a loss of control over data assets, and unclear security assurances. Unfortunately, the adoption of cloud computing came before the appropriate technologies appeared to tackle the accompanying challenges of trust. This gap between adoption and innovation is so wide that cloud computing consumers don't fully trust this new way of computing. To close this gap, they discussed the trust issues associated with cloud computing from both a technology and business perspective.

In 2011, Bernd Grobauer, Tobias Walloschek, and ElmarStöcker *et. al.* [7], presented in this paper author discussed basic architectural model of clouds. The essential characteristics of cloud as determined by US National Institute of Standards and Technology (NIST) which are as follows:*On-demand self-service.* Users can order and manage services without human interaction with the service provider, using, for example, a Web portal and management interface. Provisioning and de-provisioning of services and associated resources occur automatically at the provider. *Ubiquitous network access.* Cloud services are accessed via the network (usually the Internet), using standard mechanisms and protocols.

In 2011, J. Idziorek and M. Tannian *et. al.* [8], focused on attack by which an attacker subtly exploits a fundamental vulnerability of current utility compute models over a sustained period of time. Internet-accessible cloud services expose resources that are metered for billing purposes. These resources are subject to fraudulent resource consumption that is intended to run upthe operating expenses for public cloud service customers. The details and significance of this attack are discussed as well astwo detection methodologies and there respective experimental results. This work investigates a potentially significant vulnerabilityof the cloud computing model that could be exploited fromany Internet connected host. Well-crafted transactions that only differ in intent but not in content are challenging to differentiateand thus this attack may be difficult to detect and prevent.

In 2011, M. Sqalli, F. Al-Haidari, and K. Salah *et. al.* [9], proposed a mitigation technique called EDoS-Shield to protect the cloud against EDoS attacks. The Key factor proposed for differentiating between legitimate and EDoS requests is through verification of human presence to control an end-user machine. A Virtual Firewall (VF) and a Verifier Node operate in tandem to perform the EDoS mitigation tasks. The firewall filters incoming request on a white list and black list. The verifier node verifies the incoming requests using a Turing test, during first client access. If a user passes the Turing test, its IP address will be held in the white list and subsequent requests from the same address will be forwarded to the cloud scheduler for providing necessary services. In contrast, if a user fails the Turing test, itsIP address will be held in the black list and subsequent requests from this address will be dropped by the firewall. However, the proposed approach has a few shortcomings. One of them is its vulnerability to IP spoofing. This problem might cause and EDoS attack if an attacker spoofs an IP address belonging to the white list of the verifier node.

In 2012, F. Al-Haidari, M. Sqalli, and K. Salah *et. al.* [10], presented enhanced edos-shield for mitigating edos attacks from spoofed ip addresses. Its is enhanced version of the technique discussed in their previous paper [9]. In enhanced EDoS-Shield technique a Time To Live (TTL) field is appended alongside the IP address of cloud service requests. Through such an approach, the authors attempt to thwart the threat of spoofed IP address, as the distinctness in IP addresses when accompanied with a TTL field will help differentiate malicious spoofing clients from legitimate ones.

In March 2012, S VivinSandar and SudhirShenai *et. al.* [11], focused on threats and the counter measures of the prevailing DDoS attacks on the Cloud Environment as well as the Cloud Specific Vulnerabilities to these attacks. “Cloud Computing”, a new wave in the Internet revolution, transforms the kind of services provided over the Internet. The Cloud Services can be viewed from two perspectives, one as Cloud Service Provider and the other as Cloud Service Consumer. Assurance of security in the Cloud Service is a major challenge for the Providers, as it’s the biggest concern for the Consumers to opt for the service, which in turn decides the prospects of the business in Cloud Service. The Security can be administered in the Cloud at various levels and for several types of attacks. The threats and the attacks on the Cloud service can be common prevailing attacks in the internet or can be cloud specific.

In 2013, FarhadAhamed, SeyedShahrestani and AthulaGinige [12], focused on security and reliability of cloud computing services which remain among the dominant concerns inhibiting their pervasive adaptation. The distributed and the multi-tenancy nature of the cloud computing paradigm can be considered as the root causes for their increased risks and vulnerabilities. Resource sharing and virtualization can also be mentioned as additional main factors contributing to or augmenting cross-site scripting and other cloud vulnerabilities. Cloud are also exposed to the risks and liabilities faced by other networked systems. Poorly designed APIs that may cause security problems or distributed denial of services attacks are the examples of this category that are considered in this paper. Public key infrastructure provides the foundations for provision of some essential security services. These include services such as confidentiality, authentication, and privacy that are of vital importance for establishing trust and confidence between the cloud providers and their clients. In this work, authors have discussed the potential flaws of this infrastructure and examined how they may deteriorate the security and reliability levels of the cloud environments. To enable a comprehensive study of the challenges in security and reliability of the cloud computing environments, authors categorized the risks and vulnerabilities they face. Traditional techniques, based on cryptography, can address some of these challenges to a certain degree. Authors have argued that they may not be efficient for use in cloud environments.

In 2013, Zhifeng Xiao and Yang Xiao *et. al.* [13], gave a comprehensive review of the existing security and privacy issues in cloud environments. They have identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). Beginning with these attributes, they presented the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defense strategies in a cloud scenario. Future research directions are previously determined for each attribute.

In November 2014, F. Al-Haidari, M. Sqalli and K. Salah *et. al.* [14], studied the impact of EDoS attacks on the cloud computing services, considering only a single class of service. They developed an analytical model verified by a simulation model to study such impact of EDoS attacks on the cloud computing. The analytical model relies on the queuing model that captures the cloud services and considers a number of performance and cost metrics including end-to-end response time, utilization of computing resources, throughput, and the incurred cost resulting from the attack.

In 2015, Andrew Carlin, Mohammad Hammoudeh and Omar Aldabbas proposed that Cloud computing offers users high-end and scalable infrastructure at an affordable cost. Virtualization is the key to unlocking cloud computing. Although virtualization has great benefits to the users, the complexity in its structure, introduces unseen anforcible threats to the security of the data and to the system infrastructure. This investigates the exploitation of compromise virtual machines to execute large-scale Distributed Denial-of-Service (DDoS) attacks. A critical review of most recent intrusion detection and prevention systems to mitigate potential DDoS attacks is presented.

In November 2016, Gaurav Somani, Manoj Singh Gaur, DheerajSanghi and Mauro Conti proposed that the effects of distributed denial-of-service (DDoS) attacks on cloud computing are not very similar to those in traditional fixed on-premise infrastructure. In the context of DDoS attacks in multi-tenant clouds, we argue that, instead of just the victim server, multiple other stakeholders are also involved. Some of these important stakeholders are co-hosted virtual servers, physical servers, network resources, and cloud service providers. In this paper, we show through system analysis, experiments, and simulations that these stakeholders are collaterally affected, even though they are not the real targets of the attack. Damages/effects to these stakeholders include performance interference, web service performance, resource race, indirect EDoS (economic denial of sustainability), service downtime, and business losses.

In November 2017, Marco Antonio Sotelo Monge, Jorge Maestre Vidal and Luis Javier GarcíaVillalba suggest that In recent years, an important increase in the amount and impact of Distributed Denial of Service (DDoS) threats has been reported by the different information security organizations. They typically target the depletion of the computational resources of the victims, hence drastically harming their operational capabilities. Inspired by these methods, Economic Denial of Sustainability (EDoS) attacks pose a similar motivation, but adapted to Cloud computing environments, where the denial is achieved by damaging the economy of both suppliers and customers. Therefore, the most common EDoS approach is making the offered services unsustainable by exploiting their auto-scaling algorithms. In order to contribute to their mitigation, this paper introduces a novel EDoS detection method based on the study of entropy variations related with metrics taken into account when deciding auto-scaling actuations. Through the prediction and definition of adaptive thresholds, unexpected behaviors capable of fraudulently demand newresource hiring are distinguished. With the purpose of demonstrate the effectiveness of the proposal, an experimental scenario adapted to the singularities of the EDoS threats and the assumptions drivenby their original definition is described in depth. The preliminary results proved high accuracy.

CONCLUSION

Security issues related to the cloud computing are relevant to various stakeholders for an informed cloud adoption decision. Apart from data breaches, the cyber security research community is revisiting the attack space for cloud-specific solutions as these issues affect budget, resource management, and service quality. Distributed Denial of Service (DDoS) attack is one such serious attack in the cloud space. In this paper, we present developments related to DDoS attack mitigation solutions in the cloud. In particular, we present a comprehensive survey with a detailed insight into the characterization, prevention, detection, and mitigation mechanisms of these attacks. Additionally, we present a comprehensive solution taxonomy to classify DDoS attack solutions. We also provide a comprehensive discussion on important metrics to evaluate various solutions. This survey concludes that there is a strong requirement of solutions, which are designed keep ingutility computing models in mind. Accurate auto-scaling decisions, multi-layer mitigation, and defense using profound resources in the cloud, are some of the key requirements of the desired solutions. In the end, we provide a definite guideline on effective solution building and detailed solution requirements to help the cyber security research community in designing defense mechanisms. To the best of our knowledge, this work is an ovelattempt to identify the need of DDoS mitigation solutions involving multi-level information flow and effective resource management during the attack.

References

1. J. Mirkovic and P. Reiher, “A taxonomy of ddos attack and ddos defense mechanisms,” SIGCOMM Comput. Commun. Rev., vol. 34, pp. 39–53, April 2004.
2. S. Kandula, D. Katabi, M. Jacob, and A. Berger, “Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds,” in Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2, ser. NSDI’05, 2005, pp. 287–300.
3. C. Hoff., “Cloud computing security: From ddos (distributed denial of service) to edos (economic denial of sustainability)” 2008.
4. S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, “DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection”, IEEE/ACM Trans. Netw., vol. 17, pp. 26–39, February 2009.
5. G. Oikonomou and J. Mirkovic, “Modeling human behavior for defense against flash-crowd attacks,” in IEEE International Conference onCommunications, 2009, pp. 1–6.
6. Khaled M. Khan and QutaibahMalluhi, “Establishing Trust in Cloud Computing”, IEEE Computer Society, 2010
7. Bernd Grobauer, Tobias Walloschek, and ElmarStöcker, “Understanding Cloud Computing Vulnerabilities”, IEEE Computer and Reliability Societies, 2011.
8. J. Idziorek and M. Tannian. Exploiting cloud utility models for profit and ruin. In Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing (CLOUD ’11), pages 33–40, 2011.
9. M. Sqalli, F. Al-Haidari, and K. Salah, “Edos-shield: a two steps mitigation technique against edos attacks in cloud computing”, in fourth IEEE International Conference on Utility and Cloud Computing (UCC), pages 49-56, 2011
10. F. Al-Haidari, M. Sqalli, and K. Salah, “Enhanced Edos-shield for mitigating edos attacks originating from spoofed ip addresses”, in 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages 1167-1174, 2012
11. S VivinSandar and SudhirShenai, “Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks”, in International Journal of Computer Applications (0975 – 8887), Volume 41– No.20, March 2012.
12. FarhadAhamed, SeyedShahrestani and AthulaGinige, “Cloud Computing: Security and Reliability Issues”, Vol. 2013, Article ID 655710, 12 pages, 2013
13. Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing”, in IEEE Communications Surveys & Tutorials, Volume 15, No. 2, Second Quarter 2013.
14. F. Al-Haidari, M. Sqalli and K. Salah, “Evaluation of the Impact of EDoS Attacks Against Cloud Computing Services”, in Arab Journal Science and Engineering, November 2014
15. NASA Server Traces. [Online] Available: http://ita.ee.lbl.gov/html/contrib/nasa-http.html.
16. S.-M. Huang, D. C. Yen, L.-W. Yang, and J.-S. Hua. An investigation of zipf’s law for fraud detection. Decision Support Systems, 46:70–83, December 2008.
17. P. Mell and T. Grance. The NIST Definition of Cloud Computing (Draft).
18. [Online] Available: www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf., Jan. 2011.
19. G. K. Zipf. Human Behavior and the Principle of Least Effort. Addison-Wesley, 1949.
20. J. Idziorek, M. Tannian, D. Jacobson, Attribution of fraudulent resource consumption in the cloud, in Proceedings of the IEEE 5th International Conference on Cloud Computing (CLOUD), 2012, pp. 99–106.

21. Pimentel, M.A.F.; Clifton, D.A.; Clifton, L.; Tarassenko, L. A review on novelty detection. Signal Process. 2014,99, 215–249.
22. Hillmer, S.C.; Tiao, G.C. An ARIMA-Model-Based Approach to Seasonal Adjustment. *J. Am. Stat. Assoc.*1980, 77, 63–70.
23. Ong, C.S.; Huang, J.J.; Tzeng, G.H. Model identification of ARIMA family using genetic algorithms.*Appl. Math. Comput*. 2005, 164, 885–912.
24. Hyndman, R.J.; Koehler, A.B.; Ord, J.K.; Snyder, R.D. Prediction intervals for exponential smoothing statespace models. *J. Forecast*. 2005, 24, 17–37.
25. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly Detection: A Survey. ACM Comput. Surv. 2009, 41doi:10.1145/1541880.1541882.
26. Open Source Sotware for Creating Private and Public Clouds. Available online: https://www.openstack.org (accessed on 28 November 2017).
27. Kang, S.; Lee, K. Auto-scaling of Geo-based image processing in an OpenStack cloud computing environment.Remote Sens. 2016, 8, 662.
28. Krieger, M.T.; Torreno, O.; Trelles, O.; Kranzlmuller, D. Building an open source cloud environment withauto-scaling resources for executing bioinformatics and biomedical workflows. Futur. Gener. Comput. Syst.2017, 67, 329–340.
29. Flask-A Python Microframework. Available online: http://flask.pocoo.org (accessed on 28 November 2017).
30. Webster, W.P. MERRA analytic services: Meeting the big data challenges of climate science throughcloud-enabled climate analytics-as-a-service. Comput. Environ. *Urban Syst*. 2017, 61, 198–211.
31. Fielding, R.T.; Taylor, R.N.; Erenkrantz, J.R.; Gorlick, M.M.; Whitehead, J.; Khare, R.; Oreizy, P. Reflections onthe REST architectural style and principled design of the modern web architecture (impact paper award).In Proceedings of the 11th Joint Meeting on Foundations of Software Engineering, Paderborn, Germany,4–8 September 2017; pp. 4–14.
32. Barakat, C.; Thiran, P.; Iannaccone, G.; Diot, C.; Owezarski, P. Modeling Internet backbone traffic at the flowlevel. IEEE Trans. Signal Process. 2003, 51, 2111–2124.
33. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the ioT: Mirai and other botnets. Computer 2017,50, 80–84.
34. Wei, W.; Chen, F.; Xia, Y.; Jin, G. A rank correlation based detection against distributed reflection DoS attacks.*IEEE Commun. Lett*. 2013, 17, 173–175.
35. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutor. 2013, 15, 2046–2069.
36. Baig, Z.A.; Sait, S.M.; Binbeshr, F. Controlled access to cloud resources for mitigating Economic Denial ofSustainability (EDoS) attacks. *Comput. Netw*. 2016, 97, 31–47.
37. Chris, H. Cloud Computing Security: From DDoS (Distributed Denial Of Service) to EDoS (Economic Denialof Sustainability). 2008.
38. Reuven, C. Cloud Attack: Economic Denial of Sustainability (EDoS). Available online: http://www.elasticvapor.com/2009/01/cloud-attack-economic-denial-of.html (accessed on 28 November 2017).
39. Singh, P.; Manickam, S.; Rehman, S.U. A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture. In Proceedings of the IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), Noida, India, 8–10 October 2014;pp. 1–4.
40. Bremler-Barr, A.; Brosh, E.; Sides, M. DDoS attack on cloud auto-scaling mechanisms. In Proceedings ofthe IEEE Conference on Computer Communications (INFOCOM 2017), Atlanta, GA, USA, 1–4 May 2017;pp. 1–9.
41. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M. DDoS attacks in cloud computing: Collateral damage tonon-targets. *Comput. Netw*. 2016, 109, 157–171.
42. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Comput. Commun*. 2017, 107, 30–48.
43. Singh, A.; Chatterjee, K. Cloud security issues and challenges: A survey. *J. Netw. Comput. Appl*. 2017, 79,88–115.
44. Berezinski, P.; Jasiul, B.; Szpyrka, M. An entropy-based network anomaly detection method. *Entropy*. 2015,17, 2367–2408.
45. Bawa, P.S.; Manickam, S. Critical Review of Economical Denial of Sustainability (EDoS) Mitigation Techniques. *J. Comput. Sci*. 2015, 11, 855–862.
46. Idziorek, J.; Tannian, M.; Jacobson, D. Attribution of fraudulent resource consumption in the cloud.In Proceedings of the IEEE 5th International Conference on Cloud Computing, Honolulu, HI, USA,24–29 June 2012; pp. 99–106.
47. Koduru, A.; Neelakantam, T.; Bhanu, S.M.S. Detection of Economic Denial of Sustainability Using TimeSpent on a Web Page in Cloud. In Proceedings of the IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 16–18 October 2013; pp. 1–4.
48. Al-Haidari, F.; Sqalli, M.H.; Salah, K. Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, 25–27 June 2012; pp 1167–1174.
49. Singh, K.J.; Thongam, K.; De, T. Entropy-Based Application Layer DDoS Attack Detection Using Artificial Neural Networks. Entropy 2016, 18, 350.
50. Idziorek, J.; Tannian, M. Exploiting Cloud Utility Models for Profit and Ruin. In Proceedings of the IEEE International Conference on Cloud Computing (CLOUD), Washington, DC, USA, 4–9 July 2011; pp. 33–40.
51. Yu, S.; Tian, Y.; Guo, S.;Wu, D.O. CanWe Beat DDoS Attacks in Clouds? IEEE Trans. *Parallel Distrib. Syst.*2014, 25, 2245–2254.
52. Khor, H.; Nakao, A. Spow: On-demand cloud-based eDDoS mitigation mechanism. In Proceedings ofthe IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), Lisbon, Portugal, 29 June–2 July 2009.