OPEN ACCESS

Volume: 11

Special Issue: 1

Month: July

Year: 2023

E-ISSN: 2582-0397

P-ISSN: 2321-788X

Impact Factor: 3.025

Received: 12.05.2023

Accepted:16.06.2023

Published: 01.07.2023

Citation:
Deepa, KR, and P. Ashish Krishna. "NFV-Based Attack Defence Architecture for SDN Management Layer." *Shanlax International Journal of Arts, Science and Humanities*, vol. 11, no. S1, 2023, pp. 24–30.

DOI:
https://doi.org/10.34293/sijash.v11iS1-July.6311

NFV-Based Attack Defence Architecture for SDN Management Layer

Deepa K.R
Department of Computer Applications
Rajarajeswari College of Engineering, Bengaluru

Ashish Krishna P
Department of Computer Applications
Rajarajeswari College of Engineering, Bengaluru

Abstract

Software-defined networking With the goal to improve network reliability and security, tech is an internet management approach that enables dynamic, programmatically effective network architecture. monitoring, similar to cloud computing. CoFence, our proposed DDoS defence mechanism, enables a domain-helps-domain collaboration network across NFV-based domain networks. CoFence enables domain networks to assist one another in dealing with massive volumes DDoS assaults by combining capabilities. We develop a particular variable resource distribution method. for domains that is fair, efficient, and incentive compatible. The resource provider domains decide how much resource to give to each seeking peer by optimising a reciprocal-based utility function.All domains have a degree of control in this game to maximise their own usefulness. The resource provider domains decide how much resource to give to each seeking peer by optimising a reciprocal-based utility function. The resource demanding domains, determine the degree of demand to convey to the resource supplier domains in order to achieve adequate support.The results of our simulation show that the intended resource distribution is effective, incentive compatible, fair, and reciprocal.

Keywords: DDOS, NFV Domain.

Introduction

Networking Defined by Software (SDN) is a game-changing concept that is propelling moving the social media sector ahead. SDN benefits come in two forms: For starters, it facilitates quick innovation by dismantling ossified old infrastructures. the data and control planes have traditionally been closely coupled on Rendering it impossible and overly costly to swap devices rebuild. SDN, however, isolates both surfaces by delegating power to a different, based on software computer. As a result, SDN challenges the rigidity of traditional networks and provides new possibilities. possibilities.

The SDN concept provides per-flow monitoring with fine resolution and control, in addition to centralised control. Because it is highly challenging, if not unattainable, for rules published effectively beforehand that encompass the entire packet header area, a pure proactive rule deployment is extremely uncommon.

Reactive and hybrid rule deployment are therefore more common in actual use. The controller in these two instances works reactively to setup new processes that aren't governed by regulations that have been proactively publicised.Only when the transaction has been completed can following packets in be that flow handled appropriately.

Literature Survey

According to V K A Sandor [1,] attribute-Atomic cryptography (ABE) is frequently employed for cloud-based storage in order to secure data confidentiality and to achieve fine-grained access control over data. Although just one attribute agency may allocate user characteristics, single-authority attribute-based encryption (SA-ABE) has an evident drawback in that this enables data to be shared only within the attribute authority's management domain, while multiple attribute authorities are unable to share the data. Multi-authority attribute-based encryption (MA-ABEcontrasted with, provides benefits over SA-ABE. It can not only meet the demand for fine-grained access in command and data confidentiality, but it can also make data available to numerous attribute authorities. Existing MA-ABE systems, however, are inappropriate for hardware with constrained resources since they all rely on costly bilinear pairing. Furthermore, attribute revocation is a big difficulty for the MA-ABE method. So far, several solutions in this area have been ineffective. In this research, we offer an efficient revocable multi-authority attribute-based encryption (RMA-ABE) system for cloud storage based on elliptic curve cryptography. According to the security study, the suggested system is indistinguishable under adaptive selected plaintext attack, assuming the difficulty of the decisional Diffie-Hellman issue. In comparison to the previous methods, the suggested approach has the benefit of being more cheap in computation and storage.

Advantages

Filtering, exchanging, and integrating sensor inputs in an efficient manner.

Excellent performance.

Disadvantages

The speed will be slowed while distributing a significant volume of data over networking.

Fine-grained control of access in a multi-user system required to prevent unauthorised data consumption. We provide an escrow-free traceable attribute-based Using proven external decryption and multiple keywords subset search system (EF-TAMKS-VOD) in this work. The key generation centre (KGC) may be effectively stopped from searching for and decoding all user-encrypted data by using the key escrow-free strategy.

Existing Model

In our current setup, Attacks using Distributed Denial of Service (DDoS) continue to be a major security threat due to the magnitude of DDoS attacks increases all the time, with the SYN Flood attack being the most popular form.Traditional DDoS defence solutions may not be ideal since they need highly competent hardware resources, in a high cost and a lengthy implementation cycle. Our existing system may capable of integrate NFV tiers and security. A domain-specific method for allocating resources ensures the system is fair, efficient, and incentive-compatible.

Section V presents the evaluation findings of our resource allocation approach and Stackelberg game model. Finally, we end the study in SectionDDoS attacks may be loosely split into two categories: IP spoofing attacks and actual IP address assaults.

In our current framework, we may implement the (NFV) Technology security level but not the Security-based levels entirely.

The existing technique generates the DOS attack deduction, however it does not display full DOS details and attacked information.The emergence of Network Function Virtualization (NFV) technology opens up new possibilities for reducing the amount of proprietary hardware required to launch and manage network services.

Proposed Methodology

CoFence, our proposed DDoS defence mechanism, enables a “domain-helps- domain” collaboration network across NFV-based domain networks. CoFence enables domain networks to assist one another in dealing with massive volumes of DDoS attacks by pooling resources. We specifically create a dynamic resource allocation system for domains that is fair, efficient, and incentive compartible. The resource provider domains decide how much resource to give to each seeking peer by optimising a reciprocal-based utility function.

Our testing Findings demonstrate that our proposed method effectively reduces DDoS attack flow to the targeted site, and the resource distribution is fair and offers an incentive for domains to aid other domains in need as much as possible. This study makes the following contributions: Based on network function virtualization technology, this is a revolutionary collaborative DDoS defence network. A domain-specific dynamic resource allocation technique that ensures the system is fair, efficient, and incentive-compatible. An assessment of our suggested solutions using simulation To guarantee their efficacy,fair, and incentive compatible.

Our suggested system may implement the NVF Security Level and Firewall Security Efficiency, allowing for a high level of security.The data node’s transmission speed may be high, allowing data packets to easily flow from source to destination. Our objective will be to model and analyse the attack and defence activities that occur between the IDS and an attacker, with the analysis results potentially assisting in the implementation of strategic measures for the IDS.

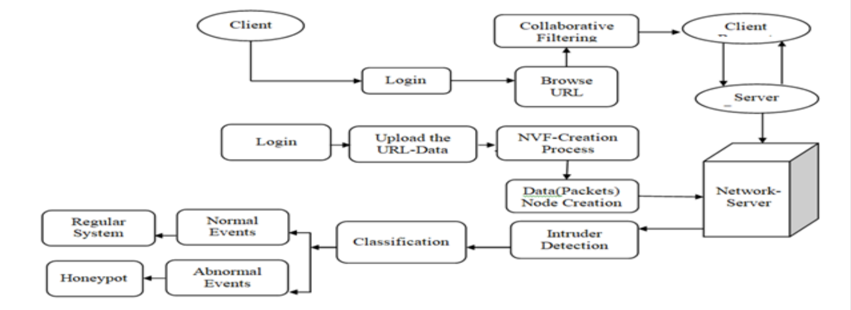


Figure 1 Proposed Architecture

Implementations

Admin and User Login

Logging in (or logging in or signing in or signing on) is the procedure by which an individual receives access to a computer system by identifying and authenticating themselves in computer security.The user credentials are normally some sort of “username” and a matching “password”, and these credentials are also referred to as a login (or a logon, sign-in, or sign-on).

Server Creation and Allocation

A web server’s principal duty is to store, process, and distribute web pages to clients. The Hypertext Transfer Protocol (HTTP) is employed to keep in touch with the client and the server.

Pages are typically HTML pages that may include graphics, style sheets, and scripts in addition to text content. A user agent, which is often a web browser or web crawler, begins communication by sending an HTTP request for a specific resource, and the server responds with the content of that resource or an error message if that request is not successful.

The resource is usually a genuine file on the server's disc.

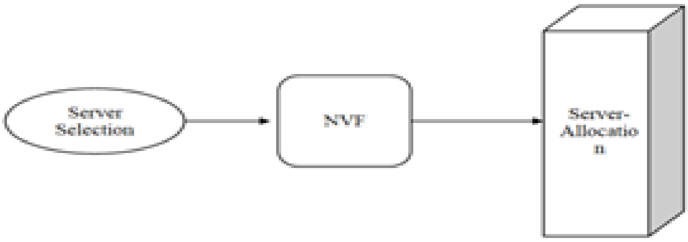


Figure 2 Server Creation and Allocation

Node Creation

A physical network node in data communication can be either a data communication equipment (DCE) such as a modem, hub, bridge, or switch; or a data terminal equipment (DTE) such as a digital telephone handset, printer, or a host computer, such as a router, workstation, or server.

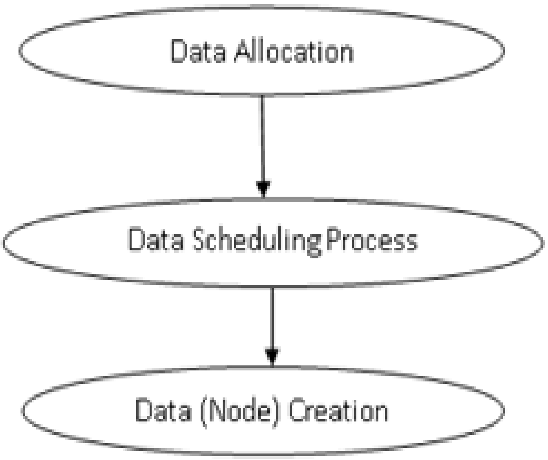


Figure 3 Node Creation

NVF Creation

Network functions virtualization (NFV) is the network architectural concept that use IT Using virtualization technologies virtualize entire categorization of network node functionality into potential building components linked to chained both to form communication services.

NVF Firewall Creation

A firewall is a network security tool that keeps track of and regulates incoming and outgoing network traffic based on predefined security rules in computing. A firewall is often used to create a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is not presumed to be safe or trustworthy. Firewalls are frequently classified such as network firewalls or host-based firewalls.

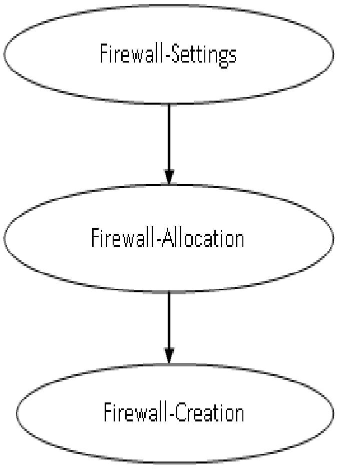


Figure 4 Firewall Creation

Intruder Detection

Finally, the intruders are detected using the honeypot. It is mostly used to provide security in networking. It detects harmful internet activity and displays the results in a report format.

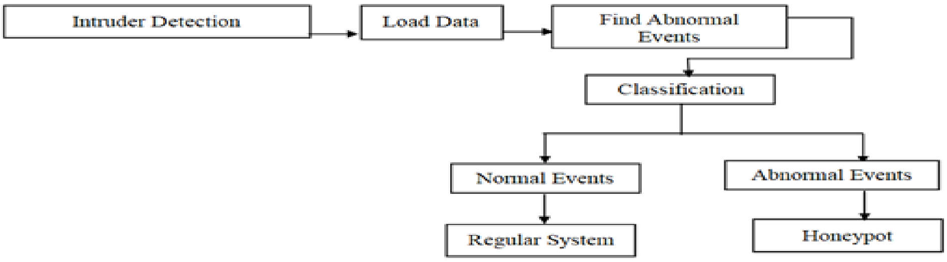
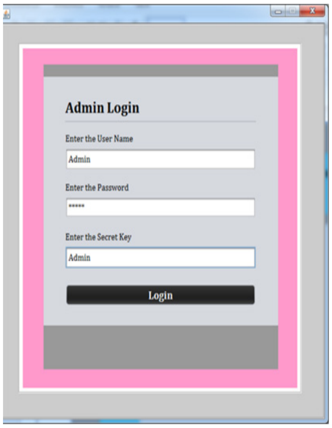


Figure 5 Intruder Detection

Results

Here are some general outcomes:



Admin Login

Enter the User Name

Admin

Enter the Password

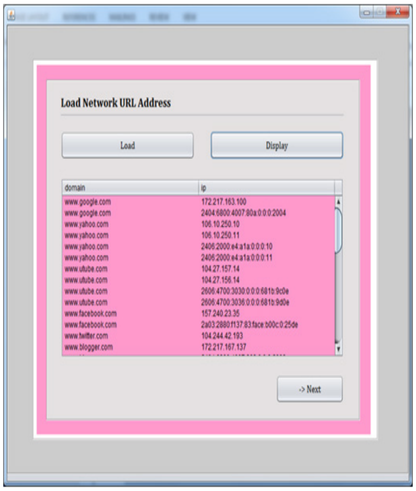
*****

Enter the Secret Key

Admin

Figure 6 Admin Login

Figure 6 Admin login Shows the Administrative access to the SDN controller or management system. Securing the admin login page to prevent unauthorized access and potential access.



domain	ip
www.google.com	172.217.163.100
www.google.com	2404:6800:4007:80a:0:0:0:2004
www.yahoo.com	106.10.250.10
www.yahoo.com	106.10.250.11
www.yahoo.com	2406:2000:e4:a1a:0:0:0:10
www.yahoo.com	2406:2000:e4:a1a:0:0:0:11
www.utube.com	104.27.157.14
www.utube.com	104.27.156.14
www.utube.com	2606:4700:3030:0:0:0:681b:9c0e
www.utube.com	2606:4700:3036:0:0:0:681b:9d0e
www.facebook.com	157.240.23.35
www.facebook.com	2a03:2880:f137:83:face:b00c:0:25de
www.twitter.com	104.244.42.193
www.blogger.com	172.217.167.137

Figure 7 View Network Url Shows the Network Activity

Figure 7 describes to a specific web address that can be accesssed on the internet . It is unique identifier that points to particular web page or resource on a network.

Conclusions

We propose CoFence, a collaborative network based on network virtualization technology that defends against DDoS assaults by redirecting excessive traffic to other cooperating domains for filtering. We concentrate on the resource allocation process, which specifies how much resource one domain should supply to requesters in order for the resource to be dispersed effectively, equitably, and with incentives.

We used the stakelberg game model for collaboration in order to optimise resource allocation. To make the collaboration more equitable, we developed a QoS framework on which domain networks should agree. Our assessment findings show that the collaborative DDoS defence can successfully mitigate the effects of assault and that the suggested resource allocation system may achieve the design aim. To improve the fairness and effectiveness of our credit evaluation method, we will incorporate the influence of link bandwidth.

References

1. ONF stands for Open Networking Foundation. Software-Defined Networking Is the New NetworkStandard. [Online]. The following link is available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdnnewnorm.pdf
2. D. Drutskoy, E. Keller, and J. Rexford, "Scalable network virtualization in software-defined networks," IEEE Internet Comput., vol. 17, no. 2, March 2013, pp. 20-27.
3. M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: Dynamic flow scheduling for data centre networks," USENIX NSDI Proceedings, 2010.
4. Y. Zhang et al., "StEERING: A software-defined networking for inline service chaining," in Proceedings of the 21st IEEE International Conference on Network Protocols (ICNP), Oct. 2013.

5. M. Arumaithurai, J. Chen, E. Monticelli, X. Fu, and K. K. Ramakrishnan, “Exploiting ICN for Flexible Management of Software-Defined Networks,” in Proc. 1st International Conference on Information-Centric Networks (INC), 2014.
6. X. Chen et al., “Design of a protocol to enable economic transactions for network services,” IEEE Int. Conf. Commun., Jun. 2015.
7. N. McKeown et al., “OpenFlow: Enabling Innovation in Campus Networks,” ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, April 2008, pp. 69-74.
8. S. H. Yeganeh, A. Tootoonchian, and Y. Ganjali, “On the Scalability of Software-Defined Networking,” IEEE Communications Magazine, vol. 51, no. 2, Feb. 2013, pp. 136-141.
9. “Scotch: Elastically scaling up SDN control-plane using vSwitch,” A. Wang, Y. Guo, F. Hao, T. V. Lakshman, and S. Chen.
10. T. Wolf and J. Li, “Denial-of-service prevention for software-defined network controllers,” in Proceedings of the 25th International Conference on Computer Communications and Networking (ICCCN), Aug. 2016.
11. “DevoFlow: Cost-effective flow management for high performance enterprise networks,” in Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw. (Hotnets), 2010.
12. D. Kreutz, F. M. V. Ramos, and P. Verissimo, “Towards secure and dependable software-defined networks,” in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw.
13. T. Wang, Z. Guo, H. Chen, and W. Liu, “BWManager: Mitigating denial of service attacks in software-defined networks through bandwidth prediction,” IEEE Trans. Netw. Service Manage., vol. 15, no. 4, December 2018, pp. 1235-1248.