The Importance of IDS and IPS in Cloud Computing Environment: Intensive Review and Future Directions

Aws Naser Jaber[1](✉), Shahid Anwar[2], Nik Zulkarnaen Bin Khidzir[3], and Mohammed Anbar[4]

[1] Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, 16300 Bachok, Kelantan, Malaysia
naserjaber.a@gmail.com
[2] Department of Software Engineering, The University of Lahore, Lahore, Pakistan
[3] Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, 16300 Bachok, Kelantan, Malaysia
[4] Universiti Sains Malaysia, Gelugor, Penang, Malaysia

Abstract. Cloud computing paradigm produce several network access resources for example, storage server and networking. A vast number of transactions over the cloud computing attract the cyber criminals to attack on the sensitive credential of the users. Therefore, the users feel unsafe to store their data on the clouds, despite remarkable interest in the cloud-based computing. Data security is the main issue, since data of an organization provides an alluring target for cyber-criminals. It will cause to reduce the development of the distributed computing, in case the researchers failed to address these security issues on time. Thus, intrusion detection and prevention systems must be updated with the current advancement. In this paper we present an intensive review for the most related work done for IDS/IPS. Furthermore, it shows that IDS/IPS are under the deployment since four decades.

Keywords: Cloud computing · Distributed Denial-of-Service (DDoS) · IDS · IPS · IDPS

1 Introduction

With the steady increase in reliance on computer networks in critical systems and large computer networks distributed in all aspects of life. Computer networks have become more vulnerable to breakthroughs, exposing them to many major threats, especially in recent years such as side channel, covert channel, Denial of Service (DoS), Distributed DoS, botnets, malware threats [1–3]. Although there are different systems to protect networks from these threats, such as "firewalls, user authentication, and data encryption", these systems have not been able to fully protect networks and their systems from attacks that are more and more vulnerable over time [4]. However, the main purpose of intrusion detection systems (IDS) is to detect the unauthorized use of computer systems by all

M. Anbar et al. (Eds.): ACeS 2020, CCIS 1347, pp. 479–491, 2021.
https://doi.org/10.1007/978-981-33-6835-4_32

users of these systems, whether authorized users or external hackers [5,6]. IDS are based on comparing features available for user-authorized use and features that distinguish different types of attacks to distinguish whether the use being made is now a safe use or is a breach of network security [7]. Several breakthrough detection systems have been introduced in many previous studies based on different algorithms and designs, including good penetration detection [8,9]. Nonetheless, a certain type of threat or penetration from secure communication causes a decrease in the success rates of these systems and their ability to detect breakthroughs with high success rates, prompting many researchers to try to find the best set of features related to Various attacks.

However, the problem is that there is a huge amount of data traffic exchanged on the network, and data may be collected that contain irrelevant and redundant features. This affects the penetration rate and efficiency of these systems, and it consumes a high amount of system resources and causes in the slow process of training and testing of IDS. This will lead us to initiate this research, which aims to design and develop a model to select the best relevant features and identify the features which are most appropriate for IDS and breakthroughs. The identification of such features and features will help to use the developed model to build a breakthrough detection system characterized by speed, accuracy and non-consumption of system resources.

Although we have mentioned several features of this technology, it does not provide enough protection for organizations, although it can stop malicious programs, spyware, viruses, some types of DoS attacks, peer to peer and VoIP threats, Protection, not all, as to the size of the data that these systems can deal with? This varies depending on the manufacturer, but the rate starts from 50 MB to 15 GB per second. For thus, it has noted that the sales of IPS systems, IDS, are estimated to be about $ 1.6 billion, according to research by Infonetics, a telecommunications market research firm [10]. In this paper, DDoS is critically reviewed to show how these attacks influence the cybersecurity world and especially in cloud computing and summarizes the recent works related to IDS/IPS and DDoS attacks. With this ease certainly poses a danger big will be vulnerable to threats use the internet network. Many threats and attacks that come from the network itself even from Internet Network [11]. This happens because the existence of resources, services and others which is public, so it is needed special system for maintaining resources and services available on the network computer.

2 Intensive Review

In the year 2000 distributed attack on Yahoo, Amazon.com, CNN.com and other major websites till nowadays described methods and technique used in denial of service attack and possible way of defense against such attack [12]. Distributed computing is using to enhance the performance of educational organizations and other businesses [13]. It has become an effective approach that required minimum additional resources [14]. In this way, distributing computing helps the institutes in broadening their IT capabilities [15]. Significant concerns have developed to secure the sensitive credentials from both external such as malware attacks and internal such as botnet attacks over Internet [2,16,17]. Figure 1 shows how was the increase of DDoS attack based-on Kaspersky Q2 report in 2018.

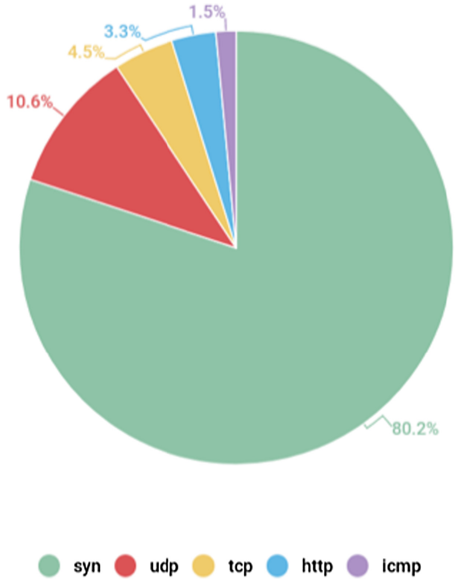


Fig. 1. Kaspersky DDoS Q2 report [18]

2.1 Types of Intrusions/Attacks

1. Active Attacks
   Routing and malicious packet dropping attacks are consider the active attacks. Furthermore, black hole, gray hole, rushing, man in the middle, sleep deprivation, spoof, and sybil are the types of routing attacks. These attacks are widely caused for dropping the network traffic, slowing the Internet speed, maximizing the power consumption, stealing data, bypass the access control and spreading malware [3].
2. Passive Attacks
   The attacks that hijack and examines the private communication as well as it expose the details about the network locations. Eavesdropping, traffic analysis and locations disclosure are the main types of passive attacks.
3. Insider attacks
   A malicious attack that access the normal users accounts inside the system and exploit some vulnerability. Furthermore, these types of attacks scan the less secure and free ports to perform flooding attacks which may cause to keep the system busy for most of the time.

4. Sniffer attacks
   This type of attack analyze network protocol and capture the network packets. The hackers use sniffing attack for reading the sensitive credentials such as bank account in formation, passwords, contacts and much more data within the network packets [19].
5. Probing
   This type of attack combine varies familiar techniques of dodging for network attacks.
6. Botnet attacks
   Botnet is a malicious program that is installed in an infected device or group of internet connected devices [17]. These infected devices then capable to perform different dangerous activities on the base of attacker's instructions in the form a groups. The very common ways of infection these devices are drive by download, access to the harm websites, spam emails, third parties applications and much more [2].

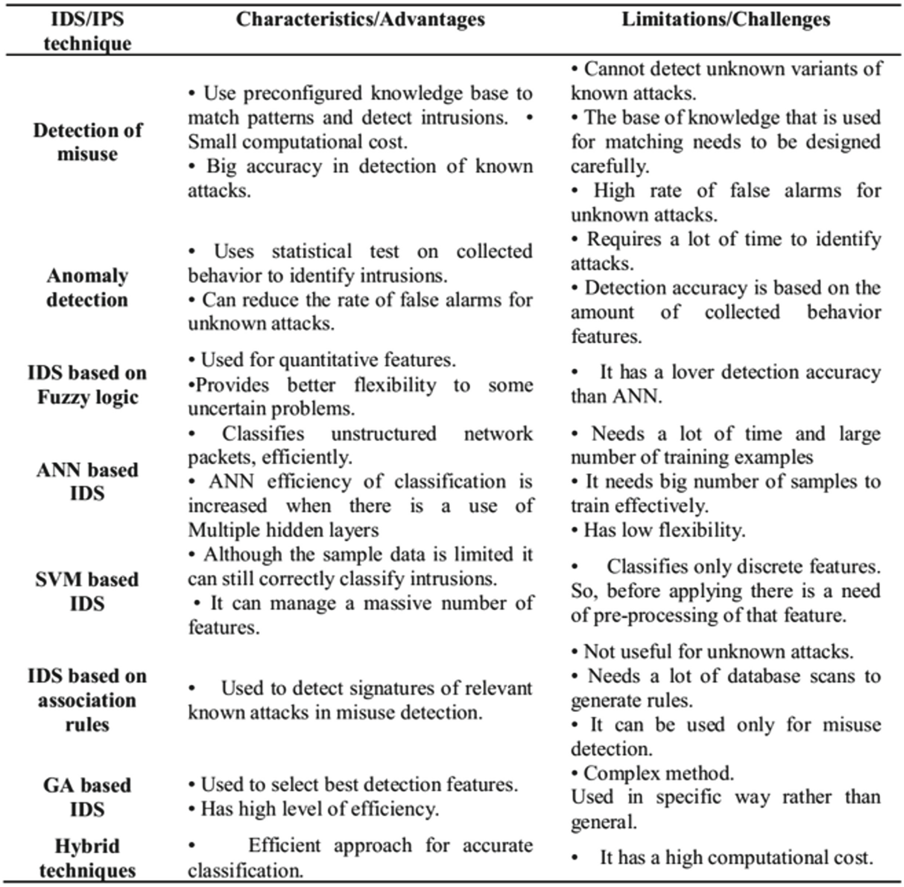
2.2 Intrusion Detection and Prevention System

An attack (intrusion) caused by a cybercriminal should be considered malicious due to highly skilled programming capabilities of cybercriminals [21]. There are several tools that can be used for network monitoring systems that impact attacks on computers, one of which is IDS-based Snort [22]. However, configuring and designing the previous researches Snort IDS is only used to monitor and detect attacks or intruders on the network, with the forensic network as a method to provide reports of attacks [23]. Depending on the source systems of intrusion detection divides into two different levels: Host-based (HBIDS) and network IDS (NIDS - Network Intrusion Detection) [10]. Nevertheless, these IDS and attacks shows in Fig. 2.

Machine learning is a ubiquitous mechanism which are vital in IDS. ANN, fuzzy logic, SVM, etc., have used in different ways in IDS and IPS. Anomaly detection, detection of misused.

To know of our best the reason for having an IDS are the alerts. True or false alerts are the two types of alerts that IDS triggers. These IDS generate huge number of alerts per day. This may cause to cost the organization in form of time and efforts. The system analysts some time consider these alerts as false positive alerts, however, they can be normal noise. These can be caused by the IDS (login failure on a password authentication server). There are four types of IDS/IPS alerts as shown in Table as shown in Table 1.

Different research groups from academic and industries have introduced many intrusion datasets for helping to assess many unknown attacks and intrusion detection methods [24]. Public, private and network simulation datasets are the three main categories of these datasets [25]. To develop the public and private datasets of intrusions a huge number of various tools are used. The tools which are used for generating these datasets are able to identify the victims, launch attacks of different types, capture and pre-process traffic, and monitor traffic patterns.



IDS/IPS technique	Characteristics/Advantages	Limitations/Challenges
Detection of misuse	• Use preconfigured knowledge base to match patterns and detect intrusions. • Small computational cost. • Big accuracy in detection of known attacks.	• Cannot detect unknown variants of known attacks. • The base of knowledge that is used for matching needs to be designed carefully. • High rate of false alarms for unknown attacks.
Anomaly detection	• Uses statistical test on collected behavior to identify intrusions. • Can reduce the rate of false alarms for unknown attacks.	• Requires a lot of time to identify attacks. • Detection accuracy is based on the amount of collected behavior features.
IDS based on Fuzzy logic	• Used for quantitative features. •Provides better flexibility to some uncertain problems.	• It has a lover detection accuracy than ANN.
ANN based IDS	• Classifies unstructured network packets, efficiently. • ANN efficiency of classification is increased when there is a use of Multiple hidden layers	• Needs a lot of time and large number of training examples • It needs big number of samples to train effectively. • Has low flexibility.
SVM based IDS	• Although the sample data is limited it can still correctly classify intrusions. • It can manage a massive number of features.	• Classifies only discrete features. So, before applying there is a need of pre-processing of that feature.
IDS based on association rules	• Used to detect signatures of relevant known attacks in misuse detection.	• Not useful for unknown attacks. • Needs a lot of database scans to generate rules. • It can be used only for misuse detection.
GA based IDS	• Used to select best detection features. • Has high level of efficiency.	• Complex method. Used in specific way rather than general.
Hybrid techniques	• Efficient approach for accurate classification.	• It has a high computational cost.

Fig. 2. Machine learning in IDS/IPS

Table 1. IDS/IPS alerts in machine learning

	Alert type	Decryption
1.	False Negative	Bad traffic but no alert is raised
2.	True Negative	Good traffic, and no alert is raised
3.	True Positive	Bad traffic which triggers an alert
4.	False Positive	Good traffic which triggers an alert

2.3 Cloud Computing Security and Intrusion Detection System

Cloud computing security is the combination of control based technologies and guidelines describe to observe to managing compliance rules and secure instructions, data applications and infrastructure identify with cloud computing use.

As shown in Fig. 3, few of the very common security risks of cloud computing that prevail users are- loss of sensitive credentials [26].

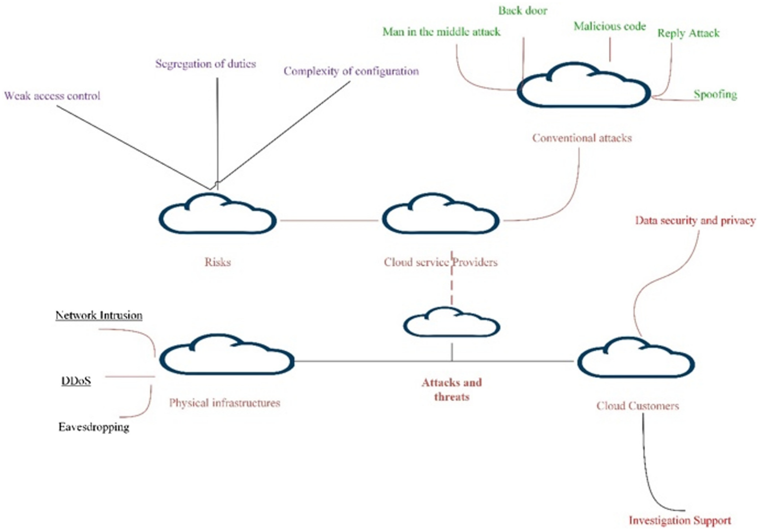


Fig. 3. Cloud computing security and attacks

IDS/IPS in cloud computing can detects several DDoS traffic with the least amount of time must be developed carefully. Nevertheless, it still leaks in term of efficiency which can be narrowed as follows:

1. The drawback of the IDS and IPS lies in their weakness in detecting sophisticated attacks, which are TCP flooding and UDP flooding. Furthermore, differentiating between false alarms and true positives and blacklisted IPs over cloud computing is a difficult task. However, one of well-known classifier which is artificial neural network (ANN) suffering from the multiple local minimum (due to the implementation of declivity based technique to know the weights of the neurons).
2. Leaks of a few necessary features would result in a wrong IDS/IPS if many unnecessary features are selected and the computation time increases, thereby leading to a slower IDS/IPS that performs erroneous detection and prevention. Therefore, the necessary and notable features (optimized) should be selected to ensure correct detection of anomalies.
3. To date, no solution has been provided for widespread novel attacks. The existing IDS/IPS systems for anomalous approach involve the following steps to fight intrusions: training phase, detection phase, and prevention phase. The detection phase uses either supervised, semi-supervised, or unsupervised methods to detect an anomaly. Costly loss of resources and services occurs because the current IDS/IPS solutions are inefficient in detecting novel attacks.

2.4 DDoS Attack

DDoS Attacks can take place for a prolonged time that could actually lead to a financial loss in your online business [27] Buffer overflow, user datagram protocol (UDP) and synchronize (SYN) flooding are the dominant types of DDoS attacks [20]. The buffer boundary is overrun by a program and it also overwrite the memory location of the adjacent buffer. However, during the performing UDP attack the hacker send a huge number of packets to different random ports. Furthermore, the SYN flooding attack consume more than enough resources of the server and keep the server busy to legitimate traffic.

For instance, when customers get in your website, they will immediately see a warning sign saying that they cannot enter the website temporarily because of the high volume of users. In certain cases, some users and technical staff could also fail to realize that the website is already under attack. Although there are different vectors for DDoS attacks, all of them aim to overwhelm servers, firewalls, or other perimeter defined devices by sending request packets at high packet rates [28]. The network becomes overwhelmed to the point where a website is not accessible [29]. According to Black Lotus, the UDP flooding attack rate reached 53% in 2017 [30]. Meanwhile, the rates of transmission control protocol (TCP) and hypertext transfer protocol (HTTP) were 33% and 14%, respectively. Table 2, classified a different types of DDoS attacks which have described by [31].

Table 2. DDOS attack types

DDoS attack	DDoS characteristics and types			
	Infrastructure	Application	Direct	Reflection
UDP Flood	✓	✓	✓	✓
TCP flood	✓		✓	
HTTP flood	✓	✓	✓	
ICMP flood	✓		✓	
XML flood		✓	✓	
Ping of death	✓	✓		
Smurf	✓			✓

The network's existing resources are the target of these types of attacks. However, various Internet-connected devices are used to initiate this task. In an attempt to get malicious packets served to the victim, cybercriminals flood the victim with overwhelming amounts of fake packets. The congestion or unavailability of resources causes benign traffic on the other side, which can adversely affect the end users' quality of service (QoS) experience.

2.4.1 Volumetric Attack

The attackers' aim in this type of attack is to consume the bandwidth of the victim's network by injecting a large number of traffic. Different amplification techniques can be employed to easily launch such type of attack [32]. It is the simplest form of attack that allows a cybercriminal to utilize a reflection medium through which gigabits of traffic can be generated using a small amount of traffic. In targeting a service, reflection-based volumetric attacks usually apply a spoofed source IP address to send genuine requests to a Network Time Protocol (NTP) or Domain Name System (DNS) server. The intensity of this attack can be determined in bits per second. NTP amplification and UDP flood are classic examples of this kind of attack.

2.4.2 Protocol Attack

The weakness of transport and network layers of the protocol stack is exploited in this attack [33]. It is normally perpetrated through several control packets like ICMP, UDP or TCP. This attack is targeted at consuming the resources or intermediate sensitive resources of the server, such as firewall and load balancer. Packets/sec forms the basis for measuring the magnitude of this attack. ICMP Smurf attack represents a good example of this attack.

2.4.3 Application Layer Attack

In this kind of attack, the possible flaws of the application layer of the protocol stack are exploited. The attack is often aimed at draining the server resources in order to disrupt the services of legitimate users [34]. Bandwidth between secondary memory and main memory, input and output bandwidth, the memory in use, and the CPU processing speed are some of the resources targeted by this attack. Attackers who utilize this type of attack are very experienced and knowledgeable about the complexity of the protocol or application. The number of requests received by the server per second can be used to measure the severity of this attack. Typical examples of this attack include DNS flood and HTTP flood.

Aside the attacks mentioned above, some popular types of DDoS attack are presented below: UDP (User Datagram Protocol) flooding: UDP is an unreliable protocol that requires no session. It is employed for sending short messages known as datagrams [35]. During UDP flooding attack, UDP packets are sent to capture random ports of the network through a fake IP address. Thus, the victim is inundated with many datagrams, which leads to buffer overflow.

2.4.4 ICMP (Internet Control Message Protocol) Flood Attack

ICMP is normally used to check the responsiveness of a system in the network [36]. This begins by sending an ICMP echo request packet to a system. An ICMP echo reply packet will then be returned by the system if it successfully receives the packet. A DDoS attack occurs during this request-reply process if an attacker uses ICMP echo requests to hijack a target system which becomes unable to access benign traffic.

2.4.5 Smurf Attack

A smurf attack is another form of an ICMP flood attack where spoofed ping messages are used to flood a system [37]. It is an attack that utilizes a reflection medium. In this attack, the victim's IP address is used by the attacker to send ICMP echo requests to various systems. As a result, numerous ICMP echo replies are sent back to the victim from the random hosts.

2.4.6 Slowloris Attack

This attack involves the slow exchange of requests and responses in the form of HTTP messages [38]. With the help of at least one system, it is capable of shutting down a server. At first, the attacker sends a few HTTP requests and gradually increases the request. The attacker will keep doing this until the requests acquire all the server's sockets. The TCP (transmission control protocol) is then exploited by the attacker through its open connection. Instead of sending the requests, it starts reading the responses gradually. It uses a window size that is smaller than the victim's buffer. Hence, an attack is eventually created, as the server is compelled to open the connection.

2.4.7 TCP-SYN Flooding Attack

The focus of this attack is to exploit the vulnerability of stateful network protocols, such as TCP, since resources are consumed by these protocols to maintain the states [39]. The client gets a SYN message to initiate the handshake in the three-way handshake (i.e., TCP connection sequence). Next, the server sends an acknowledgment (ACK) to the client to acknowledge their message, and the connection is then closed by the client. However, the connection is still very much open because spoofed IP messages are dispatched at a fast rate in a SYN flood. Thus, the victim cannot provide services because it cannot accept any new incoming connection. NTP (Network Time Protocol) amplification: In this type of volumetric attack, the target is overwhelmed with UDP traffic through the exploitation of network protocols and NTP servers that are utilized in synchronizing system clocks [40]. A spoofed IP receives an acknowledgment from the server in any reflection attack. Here, there is a huge disparity between the query-to-response ratio and the original requests (which range from 1:20 to 1:200 (or more)). This means that an attacker can easily carry out a high-volume DDoS attack if they make use of a tool like Metasploit to get a list of unclosed NTP servers. Zero-day attack: It refers to an unprecedented attack for exploiting weaknesses that have no pre-existing patch. It is also called the zero-minute attack.

2.5 Other Related Works for IDS/IPS in Cloud Computing

Furthermore, Sharma et al., used artificial bee colony (ABC) as an attack classifier through H-IDPS on private cloud server [41]. They employed their own testbed to generate the dataset. Kazemi et al., used signature-based and genetic-based techniques for intrusion detection [42]. Their cloud intrusion detection datasets can detect cloud attacks. Cloud-based IDSs could detect 94% of random sets of cloud attacks. By adding the background traffic retrieved from DARPA, IDS could detect the same amount of attacks and no false positive alarm was raised while filtering the background traffic.

Ramteke et al., proposed an open source security event correlator for H-IDPS; however, the effectiveness of their work is not clear [43]. In addition, their work did not make use of features because they depended only on a real-time virtual machine.

Nicholas J, Puketza et al. devise a methodology for testing intrusion detection system (IDS's), the technique used for testing the IDS's was adopted from the field of software testing, the testing is best done in an isolated local area network (LAN) because it requires direct control over computing activity in that environment. There is a need for these tests because of the growing numbers of organization reliant on IDS's for their computer system security. The testing methodology can be used to reveal information about an IDS and its capability. [44] in the advent of the failing preventive measure to detect malicious attack and the ever-increasing cyber-attack on data-intensive applications, in a bid to solving the problem of relative long detection latency in database system presented a multi-phase damage confinement approach to solve this problem.

3 Conclusion

In this paper shows how an intensive review for cloud computing IDS/IPS and DDoS. In fact, DDoS and IDS/IPS in cloud computing have had immense cybersecurity stories and will never end. It has been obvious that the distributed and open structure of cloud computing and services becomes an attractive target for potential cyber-attacks by intruders. IDS/IPS are largely inefficient to be deployed in cloud computing environments due to their openness and specific essence. In future studies. In future work will focus in COVID-19, which contagion has brought in extraordinary and special social and financial conditions leveraged by cyber-crime. Thus, a new modern mechanism should proposed for the IDS/IPS in cloud computing through the pandemic cybersecurity attacks. Also, we need more to concentrate about the blockchain, which playing an important role in cloud computing. Especially when an encrypted transaction accrues between cloud and user and how will IDS/IPS will cooperate with this technique. Nevertheless, there is a relationship between IDS/IPS with blockchain.

References

1. Liew, C.S., Ang, J.M., Goh, Y.T., Koh, W.K., Tan, S.Y., Teh, R.Y.: Factors influencing consumer acceptance of internet of things technology. In: Handbook of Research on Leveraging Consumer Psychology for Effective Customer Engagement: IGI Global, pp. 186–201 (2017)
2. Anwar, S., Zolkipli, M.F., Inayat, Z., Odili, B., Ali, M., Zain, J.M.: Android botnets: a serious threat to android devices. Pertanika J. Sci. Technol. (2017)

3. Anwar, S., et al.: From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms **10**(2), 39 (2017)
4. Jaber, A.N., Zolkipli, M.F.B.: Use of cryptography in cloud computing. In: 2013 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 179–184. IEEE (2013)
5. White, G.B., Fisch, E.A., Pooch, U.W.: Computer System and Network Security. CRC Press, Boca Raton (2017)
6. Inayat, Z., Gani, A., Anuar, N.B., Khan, M.K., Anwar, S.: Intrusion response systems: foundations, design, and challenges. J. Netw. Comput. Appl. **62**, 53–74 (2016)
7. Aljawarneh, S., Aldwairi, M., Yassein, M.B.: Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J. Comput. Sci. **25**, 152–160 (2018)
8. Singh, R., Kumar, H., Singla, R.K., Ketti, R.R.: Internet attacks and intrusion detection system: a review of the literature. Online Inf. Rev. **41**(2), 171–184 (2017)
9. Anwar, S., et al.: Cross-VM cache-based side channel attacks and proposed prevention mechanisms: a survey. J. Netw. Comput. Appl. **93**, 259–279 (2017)
10. Zhang, Z., Meddahi, A.: Security in Network Functions Virtualization. Elsevier, Amsterdam (2017)
11. Tripathi, M., Mukhopadhyay, A.: Vulnerable Paths Assessment in Cloud for DDoS Attacks (2018)
12. Saxena, R.: Analysis on distributed denial of service attack prevention in cloud computing. J. Comput. Hard. Eng. **1** (2018)
13. Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management, and Security. CRC Press, Boca Raton (2016)
14. Woodruff, D.P., Zhang, Q.: When distributed computation is communication expensive. Distrib. Comput. **30**(5), 309–323 (2017). https://doi.org/10.1007/s00446-014-0218-3
15. Kaul, S., Sood, K., Jain, A.: Cloud computing and its emerging need: advantages and issues. Int. J. Adv. Res. Comput. Sci. **8**(3) (2017)
16. Anwar, S., Mohamad Zain, J., Zolkipli, M.F., Inayat, Z.: A review paper on botnet and botnet detection techniques in cloud computing. In: ISCI 2014 - IEEE Symposium on Computers & Informatics, no. Comptuer and Informatics, p. 5 (2014)
17. Anwar, S., Zain, J.M., Inayat, Z., Haq, R.U., Karim, A., Jabir, A.N.: A static approach towards mobile botnet detection. In: 2016 3rd International Conference on Electronic Design (ICED), 11–12 August 2016, pp. 563–567. https://doi.org/10.1109/ICED.2016.7804708
18. Kosowski, D., Kołaczek, G., Juszczyszyn, K.: Evaluation of an impact of the DoS attacks on the selected virtualization platforms. In: Borzemski, L., Świątek, J., Wilimowska, Z. (eds.) ISAT 2018. AISC, vol. 852, pp. 30–40. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-99981-4_4
19. Zhao, Z., Gong, D., Lu, B., Liu, F., Zhang, C.: SDN-based double hopping communication against sniffer attack. Math. Probl. Eng. **2016** (2016)
20. Zhang, M., et al.: Poseidon: mitigating volumetric DDoS attacks with programmable switches. In: Proceedings of NDSS (2020)
21. Kamat, P., Gautam, A.S.: Recent trends in the era of cybercrime and the measures to control them. In: Handbook of e-Business Security, pp. 243–258. Auerbach Publications (2018)
22. Jaber, A.N., Zolkipli, M.F., Majid, M.A., Anwar, S.: Methods for preventing distributed denial of service attacks in cloud computing. Adv. Sci. Lett. **23**(6), 5282–5285 (2017)

23. Mohamad Fadli, Z., Jaber, A.N.: Hypervisor IDPS: DDoS Prevention Tool for Cloud Computing (2017)
24. Jaber, A.N., Zolkipli, M.F., Shakir, H.A., Jassim, M.R.: Host based intrusion detection and prevention model against DDoS attack in cloud computing. In: Xhafa, F., Caballé, S., Barolli, L. (eds.) 3PGCIC 2017. LNDECT, vol. 13, pp. 241–252. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-69835-9_23
25. Hussein, M.K., Zainal, N.B., Jaber, A.N.: Data security analysis for DDoS defense of cloud based networks. In: 2015 IEEE Student Conference on Research and Development (SCOReD), pp. 305–310. IEEE (2015)
26. Naser, A., Majid, M.A., Zolkipli, M.F., Anwar, S.: Trusting cloud computing for personal files. In: 2014 International Conference on Information and Communication Technology Convergence (ICTC), pp. 488–489. IEEE (2014)
27. Jaber, A.N., Zolkipli, M.F.B., Majid, M.B.A.: Security everywhere cloud: an intensive review of DoS and DDoS attacks in cloud computing. J. Adv. Appl. Sci. (JAAS) **3**(5), 152–158 (2015)
28. Saied, A., Overill, R.E., Radzik, T.: Detection of known and unknown DDoS attacks using artificial neural networks. Neurocomputing **172**, 385–393 (2016)
29. Freedman, A.T., Pye, I.G., Ellis, D.P.: Network Monitoring, Detection, and Analysis System, ed: Google Patents (2017)
30. Lotus, B.: Level 3®DDoS Mitigation (2017)
31. Bhardwaj, A., Subrahmanyam, G., Avasthi, V., Sastry, H., Goundar, S.: DDoS attacks, new DDoS taxonomy and mitigation solutions–a survey. In: 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), ITM (part of Centurion University Of Technology & Management) Village Alluri Nagar, pp. 793–798. IEEE (2016). https://doi.org/10.1109/SCOPES.2016.7955549
32. Alharbi, T., Aljuhani, A., Liu, H., Hu, C.: Smart and lightweight DDoS detection using NFV. In: Proceedings of the International Conference on Compute and Data Analysis, pp. 220–227. ACM (2017)
33. Shakir, H.A., Jaber, A.N.: A short review for ransomware: pros and cons. In: Xhafa, F., Caballé, S., Barolli, L. (eds.) 3PGCIC 2017. LNDECT, vol. 13, pp. 401–411. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-69835-9_38
34. Duessel, P., Gehl, C., Flegel, U., Dietrich, S., Meier, M.: Detecting zero-day attacks using context-aware anomaly detection at the application-layer. Int. J. Inf. Secur. **16**(5), 475–490 (2016). https://doi.org/10.1007/s10207-016-0344-y
35. Rosli, A., Taib, A.M., Ali, W.N.A.W.J.S.H.: Utilizing the enhanced risk assessment equation to determine the apparent risk due to user datagram protocol (UDP) flooding attack, vol. 9, no. 1–4 (2017)
36. Kamboj, P., Trivedi, M.C., Yadav, V.K., Singh, V.K.: Detection techniques of DDoS attacks: a survey. In: 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), pp. 675–679. IEEE (2017)
37. Wankhede, S.B.: Study of network-based DoS attacks. In: Nath, V., Mandal, J.K. (eds.) Nanoelectronics, Circuits and Communication Systems. LNEE, vol. 511, pp. 611–616. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-0776-8_58
38. McGregory, S.J.N.S.: Preparing for the next DDoS attack. Netw. Secur. **2013**(5), 5–6 (2013)
39. Shah, D., Kumar, V.: TCP SYN Cookie Vulnerability (2018)

40. Sharma, R., Guleria, A., Singla, R.K.: Characterizing network flows for detecting DNS, NTP, and SNMP anomalies. In: Bhalla, S., Bhateja, V., Chandavale, A.A., Hiwale, A.S., Satapathy, S.C. (eds.) Intelligent Computing and Information and Communication. AISC, vol. 673, pp. 327–340. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7245-1_33
41. S. Sharma, A. Gupta, and S. Agrawal, "An Intrusion Detection System for Detecting Denial-of-Service Attack in Cloud Using Artificial Bee Colony," in Proceedings of the International Congress on Information and Communication Technology, 2016: Springer, pp. 137–145
42. Kazemi, S., Aghazarian, V., Hedayati, A.: Improving false negative rate in hypervisor-based intrusion detection in IaaS cloud. IJCAT - Int. J. Comput. Technol. **2**(9), 348 (2015)
43. Ramteke, S., Dongare, R., Ramteke, K.: Intrusion detection system for cloud network using FC-ANN algorithm. Int. J. Adv. Res. Comput. Commun. Eng. **2**(4) (2013)
44. Lee, W., et al.: A data mining and CIDF based approach for detecting novel and distributed intrusions. In: Debar, H., Mé, L., Wu, S.F. (eds.) RAID 2000. LNCS, vol. 1907, pp. 49–65. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-39945-3_4