iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.34935

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Study of Intrusion Detection System

Miss. Manoshri A. Ghawade[1], Dr. S. S. Dhande[2]
[1]*PG Scholar, Sipna College of Engineering & technology, Amravati (M.S), India*
[2]*Professor of Computer Science & Engineering, Sipna College of Engineering & technology, Amravati (M.S), India*

***Abstract:** An intrusion detection system (IDS) could be a device or software application that observes a network for malicious activity or policy violations. Any malicious activity or violation is often reported or collected centrally employing a security information and event management system. Some IDS's are proficient of responding to detected intrusion upon discovery. These are classified as intrusion prevention systems (IPS). A system that analyzes incoming network traffic is thought as Network intrusion detection system (NIDS). A system that monitors important software files is understood as Host intrusion detection system (HIDS). Wireless sensor networks (WSNs) are vulnerable to different kinds of security threats which will degenrate the performance of the entire network; that may lead to fatal problems like denial of service (DoS) attacks, direction attacks, Sybil attack etc. Key management protocols, authentication protocols and secure routing cannot provide security to WSNs for these varieties of attacks. Intrusion detection system (IDS) could be a solution to the present problem. It analyzes the network by collecting sufficient amount of knowledge and detects abnormal behavior of sensor node(s).*
***Keywords:** Intrusion detection, Wireless Sensor Network (WSN), HIDS, NIDS.*

I. INTRODUCTION

Intrusion detection is that the act of detecting unwanted traffic on a network or a tool. An IDS will be a bit of installed software or a physical appliance that monitors network traffic so as to detect unwanted activity and events like illegal and malicious traffic, traffic that contravene security policy, and traffic that contravene acceptable use policies. Many IDS tools will store a detected event in an exceedingly log to be reviewed at a later date or will combine events with other data to create decisions regarding policies or control. There's also subset of IDS types. The foremost common variants are supported signature detection and anomaly detection.

1) *Signature-based:* Signature-based IDS detects possible threats by trying to find specific patterns, like byte sequences in network traffic, or known malicious instruction sequences employed by malware. This terminology originates from antivirus software, which refers to those detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it's impossible to detect new attacks that no pattern is on the market. These systems have an unified database or library of signatures or properties exhibited by known intrusion attacks or malicious threats. Signature-based IDS observes all the network packets and detects potential malware by analyzing if these signatures match the suspicious activities happening.
2) *Anomaly-based:* A more recent technology designed to detect and adapt to unknown attacks, primarily thanks to the explosion of malware. This detection method uses machine learning to form an outlined model of trustworthy activity, so compare new behavior against this trust model. While this perspective enables the detection of previously unknown attacks, it can suffer from false positives: previously unknown legitimate activity can accidentally be classified as malicious. This kind of IDS is predicated on a way or an approach where the program monitors your ongoing network traffic and analyzes its pattern against predefined norms or baseline. It then recognizes and alerts the admins to unusual behavior across network bandwidth, devices, ports, protocols, etc.

Intrusion Detection Systems are broadly classified into two categories:

a) *Network intrusion detection systems (NIDS):* A system that analyzes incoming network traffic. Network IDS is deployed across your network infrastructure at specific strategic points like the subnets most liable to an exploit or attack. A NIDS placed at these points monitors the whole inbound and outbound traffic flowing to and from the network devices.
b) *Host-based intrusion detection systems (HIDS):* A system that monitors important package files. On the opposite hand, Host IDS is configured altogether the client computers (called hosts) running within your network environment. HIDS monitors the devices with access to your internal network and therefore the internet. As it's installed on networked computers, HIDS can detect malicious network packets transmitted within the organization (internally), including any infected host attempting to poke into other computers. NIDS usually fails to try to that.

The intrusion detection application concerns how briskly the intruder may be detected by the WSN. If sensors are deployed with a high density so the union of all sensing ranges covers the complete network area, the intruder may be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and will be even unaffordable for an outsized area. In fact, it's not necessary to deploy numerous sensors to hide the whole WSN area in many applications, since a network with small and scattered void areas will be ready to detect a moving entire WSN area in many applications, since a network with small and scattered void areas will be ready to detect a moving intruder within a particular intrusion distance. During this case, the applying can identify a required intrusion distance within which the intruder should be detected. As shown in Fig. 1, the intrusion distance is referred as D and defined because the distance between the points the intruder enters the WSN, and therefore the point the intruder is detected by the WSN system. This distance is of central interest to a WSN nearly new for intrusion detection. During this paper, we derive the expected intrusion distance and evaluate the detection probability in several application scenarios. For instance, given an expected detection distance, we will derive the node density with relevance sensors' sensing range, thereby knowing the whole number of sensors required for WSN deployment. In a WSN, there are two ways to disclose an object (i.e., an intruder): single-sensing detection and multiple-sensing detection. Within the single-sensing detection, the intruder is successfully detected by one sensor. On the contrary, within the multiple-sensing detection, the intruder can only be detected by multiple collaborating sensors .In some applications, the sensed information provided by one sensor could be inadequate for recognizing the intruder. It's because individual sensors can only sense some of the intruder. As an example, the placement of an intruder can only be determined from a minimum of three sensors' sensing. In sight of this, we analyze the intrusion detection problem under two application scenarios: single-sensing detection and multiple-sensing detection. In line with the potential of sensors, we consider two network types: homogeneous and heterogeneous WSNs We define the sensor capability in terms of the sensing range and also the transmission range. During a heterogeneous WSN some sensors have a bigger sensing range and more power to realize an extended transmission range. During this paper, we show that the heterogeneous WSN increases the detection probability for a given intrusion detection distance. This motivates us to investigate the network connectivity during this paper. Furthermore, during a heterogeneous WSN, high capability sensors usually undertake more important tasks (i.e., broadcasting power management information or synchronization information to all or any the sensors within the network), it is also desirable to define and examine the printed reachability from high-capability sensors. The network connectivity and broadcast reachability are important conditions to confirm the detection probability in WSNs. they're formally defined and analyzed during this paper. To the most effective of our knowledge, our effect is that the first to handle this issue in a very heterogeneous WSN.

II. WORKING

Intrusion detection systems are accustomed detect anomalies with the aim of catching hackers before they are doing real damage to a network. They will be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system occupy on the network.

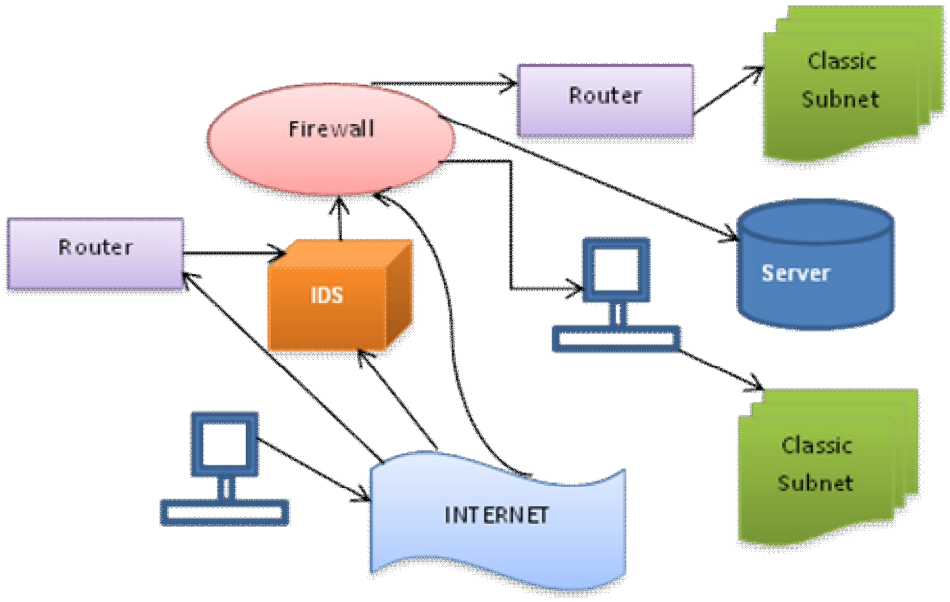
Intrusion detection systems work by either searching for signatures of known attacks or deviations from normal activity. These divergence or abnormality are pushed up the stack and examined at the protocol and application layer. They will successfully identify events like Christmas tree scans and name system (DNS) poisonings. An IDS could also be executed as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are available to guard data and systems in cloud deployments.

An intrusion detection system could be a monitor-only application designed to spot and report on anomalies before hackers can damage your network infrastructure. IDS is either installed on your network or a client system (host-based IDS).Typical intrusion detection systems rummage around for known attack signatures or abnormal deviations from set norms. These anomalous patterns within the network traffic are then sent up within the stack for further investigation at the protocol and application layers of the OSI (Open Systems Interconnection) model.

An IDS is placed out of the real-time communication band (a path between the data sender and receiver) within your network infrastructure to figure as a detection system. It instead leverages a SPAN or TAP port for network monitoring and analyzes a duplicate of inline network packets (fetched through port mirroring) to create sure the streaming traffic isn't malicious or spoofed in any way. The IDS efficiently detects infected elements with the potential to impact your overall network performance, like malformed information packets, DNS poisonings, Xmas scans, and more.

Intrusion detection systems serve three essential security functions: they monitor, detect, and reply to unauthorized activity by company insiders and outsider intrusion. Intrusion detection systems use policies to define certain events that, if identified will issue an alert.

In other words, if a specific event is taken into account to constitute a security incident, an alert are issued if that event is detected. Certain intrusion detection systems have the potential of sending out alerts, so the administrator of the IDS will receive a notification of a possible security incident within the sort of a page, email, or SNMP trap. Many intrusion detection systems not only recognize a selected incident and issue an appropriate alert, they also respond automatically to the event. Such a respond might include logging off a user, disabling a user account, and launching of scripts.



In terms of response IDS classified as:

1) *Passive System:* Passive system: in an exceedingly passive system, the IDS detect a possible security breach, log the data and signal an alert.
2) *Reactive System:* in a very reactive system, the IDS answer the suspicious activity by logging off a user or by reprogramming the firewall to dam network traffic from the suspected malicious source. This will happen automatically or at the command of an operator. In reactive intrusion detection system is one during which if the intruder or attacks is detected it doesn't alert the user rather responds to the elegant activity for shows a strict reaction. Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall therein a firewall looks outwardly for intrusions so as to prevent them from happening. Firewalls limit access between networks to forestall intrusion and don't signal an attack from inside the network. An IDS evaluates a suspected intrusion once it's taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. this can be traditionally achieved by examining network communications,

III. WIRELESS SENSOR NETWORK

A wireless sensor network (WSN) may be a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, like temperature, sound, vibration, pressure, motion or pollutants, at different locations the event of wireless sensor networks was originally motivated by military applications like battlefield surveillance. However, wireless sensor networks are now employed in many civilian application areas, including environment and habitat monitoring, health-care applications, home automation, and control. Additionally to at least one or more sensors, each node in an exceedingly sensor network is often equipped with a radio transceiver or other wireless communications device, a little micro-controller, and an energy source, usually battery. The envisaged size of one sensor node can vary from shoe box-sized nodes right down to devices the dimensions of grain of dust although functioning 'motes' of genuine microscopic dimensions have yet to be created. The price of sensor nodes is similarly variable, starting from many dollars to some cents, looking on the dimensions of the sensor network and therefore the complexity required of individual sensor nodes. Size and value constraints on sensor nodes end in corresponding constraints on resources like energy, memory, computational speed and bandwidth.

A sensor network normally constitutes a wireless ad-hoc network, meaning that every sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the bottom station).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

IV. SUPREMACY OF IDS

A. Monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms.
B. Allows administrator to tune, organize and comprehend often incomprehensible software system audit trails and other logs.
C. Can make the protection management of systems by non-expert staff possible by providing nice user friendly interface.
D. Can recognize and report alterations to data files.
E. Comes with extensive attack signature database against which information from the shoppers system is matched.
F. It provides time to time information, it recognize attacker (intrusion) & report alteration to data files.
G. IDS generate alarm and report back to administrator that security is breaches and also react to intruders by blocking them or blocking server.

V. PITFALLS OF IDS

A. Intrusion detection systems are able to detect behavior that's not normal for average network usage. While it's good to be able to detect abnormal network usage, the disadvantage is that the intrusion software can create an oversized number of false alarms.
B. The IDS has no impact on traffic.
C. The IDS doesn't stop malicious traffic.
D. The IDS works offline using copies of network traffic.
E. The IDS requires other devices to reply to attacks.
F. The IDS analyzes actual forwarded packets.
G. Limited visibility. Most intrusion detection systems are focused on the perimeter attack surface threats, starting together with your firewall. that gives protection of your network's north-south traffic, but what it doesn't take into consideration is that the lateral spread (east-west) that a lot of network threats today make the most of as they infiltrate your organization's network and remain there unseen.
H. Delays in response. When an IDS detects suspicious activity, the violation is often reported to a security information and event management (SIEM) system where real threats are ultimately determined amid benign traffic abnormalities or other false alarms. However, the longer it takes to differentiate a threat, the more damage are often done.
I. Threat containment. As mentioned earlier, IDS-only environments have an honest handle on monitoring north-south network traffic and therefore the typical surface threats. But east-west traffic is created of a number of the foremost fluid traffic paths and unmonitored devices.

VI. CONCLUSION

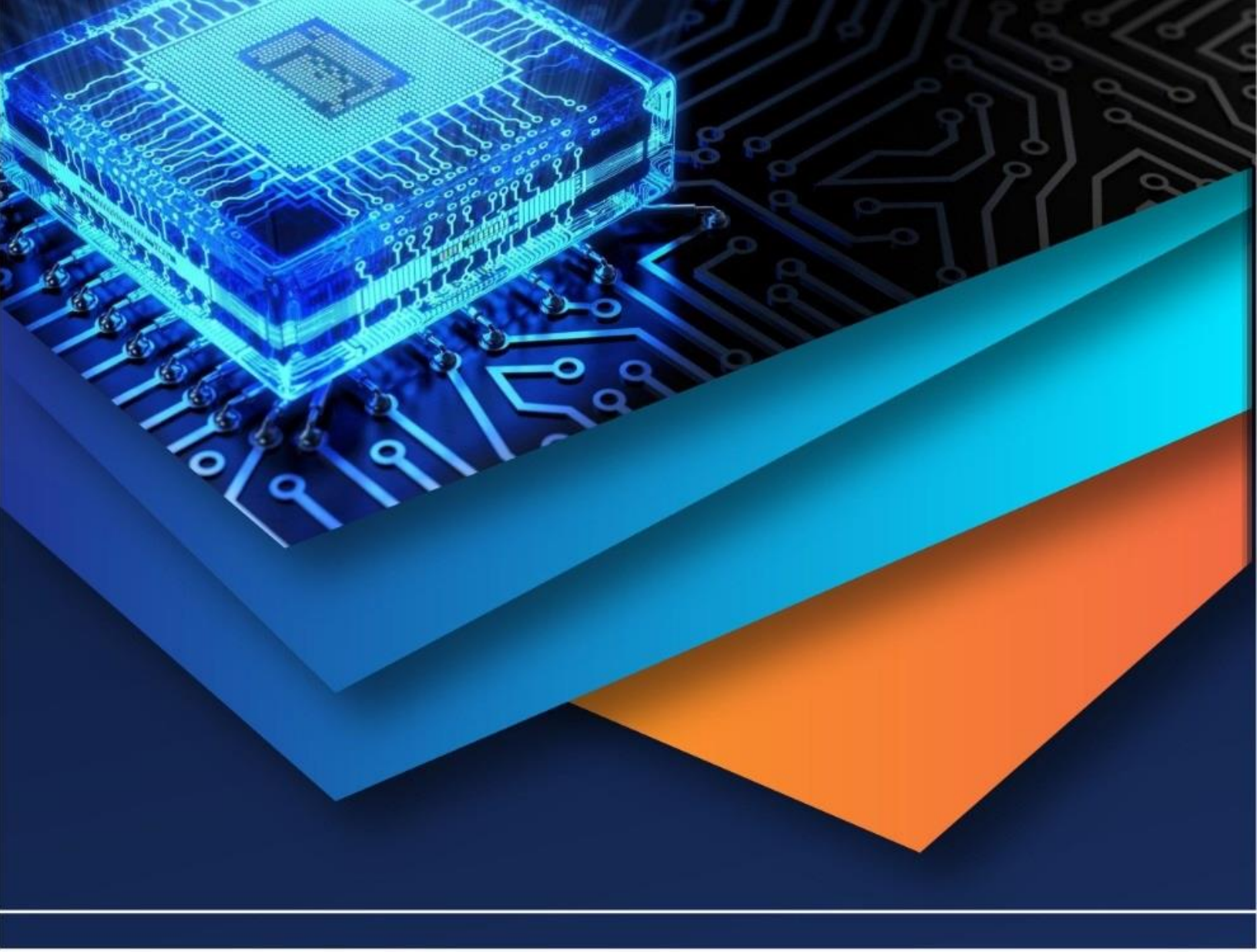
As security incidents become more numerous, IDS tools are getting increasingly necessary. They round out the protection arsenal, working in conjunction with other information security tools, like firewalls, and permit for the whole supervision of all network activity.

A. IDS have come a protracted way
B. Still an extended thanks to go
C. Many different products on the market
D. Many different uses
E. Open source solutions are very fashionable
F. No easy or long-term solution to network security
G. Vigilance will should be maintained

Intrusion detection systems add an early warning capability to your defenses, alerting you to any form of suspicious activity that typically occurs before and through an attack. Since most cannot stop an attack, intrusion detection systems shouldn't be considered an alternate to traditional good security practices. there's no substitute for a carefully thought out corporate security policy, secured by effective security procedures which are dole out by skilled staff using the mandatory tools. Instead, intrusion detection systems should be viewed as an extra tool within the continuing battle against hackers and crackers

REFERENCES

[1] Dr. Manish Kumar and Ashish Kumar Singh, "Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure" Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020)
[2] A. A. Titorenko and A. A. Frolov, "Analysis of modern intrusion detection system," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 142-143.
[3] Alexopoulos, Nikolaos & Vasilomanolakis, Emmanouil & Réka Iványkó, Natália & Mühlhäuser, Max. (2018). Towards Blockchain- Based Collaborative Intrusion Detection Systems: 12th International Conference, CRITIS 2017, Lucca, Italy, October 8-13, 2017.
[4] Axelsson, Stefan. Intrusion detection systems: A survey and taxonomy. Vol. 99. Technical report, 2000.
[5] H. M. Anwer, M. Farouk and A. Abdel-Hamid, "A framework for efficient network anomaly intrusion detection with features selection," 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, 2018, pp. 157-162.
[6] H.Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of Intrusion Detection Systems", Computer Networks, vol 31, n0. 8, pp. 805-822, 1999.
[7] Holtz, Marcelo D. ; Bernardo David ; Sousa Jr., R. T. . Building Scalable Distributed Intrusion Detection Systems Based on the MapReduce Framework. Telecomunicacoes (Santa Rita do Sapucai), v. 13, p. 22-31, 2011.
[8] J. Dean and S. Ghemawat, MapReduce: Simplified Data Processing on Large Cluster, USENIX OSDI,2004. Proceedings of the Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020) IEEE Xplore Part Number: CFP20J32-ART; ISBN: 978-1-7281-5518-0 978-1-7281-5518-0/20/$31.00 ©2020 IEEE 251 Authorized licensed use limited to: Carleton University. Downloaded on August 05,2020 at 15:36:09 UTC from IEEE Xplore. Restrictions apply.
[9] J. Yang, C. Shen, Y. Chi, P. Xu and W. Sun, "An extensible Hadoop framework for monitoring performance metrics and events of OpenStack cloud," 2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA), Shanghai, 2018, pp. 222-226.
[10] K. Kato and V. Klyuev, "Development of a network intrusion detection system using Apache Hadoop and Spark," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, 2017, pp. 416-423.
[11] Konstantin Shvachko, Hairong Kuang, Sanjay Radia, and Robert Chansler, "The Hadoop Distributed File System," IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST), pp.1-10, 2010.
[12] S. Ghribi, A. M. Makhlouf and F. Zarai, "C-DIDS: A Cooperative and Distributed Intrusion Detection System in Cloud environment," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, 2018, pp. 267-272.
[13] Suah Kim, Beomjoong Kim, and Hyoung Joong Kim. 2018. Intrusion Detection and Mitigation System Using Blockchain Analysis for Bitcoin Exchange. In Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things (CCIOT 2018). ACM, New York, NY, USA, 40-44.
[14] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," in IEEE Access, vol. 6, pp. 10179-10188, 2018.
[15] Yeonhee Lee and Youngseok Lee. 2012. Toward scalable internet traffic measurement and analysis with Hadoop. SIGCOMM Comput. Commun. Rev. 43, 1 (January 2012), 5-13.
[16] Zohreh Abtahi Foroushani and Yue Li. 2018. Intrusion Detection System by Using Hybrid Algorithm of Data Mining Technique. In Proceedings of the 2018 7th International Conference on Software and Computer Applications (ICSCA 2018). ACM, New York, NY, USA, 119-123.
[17] R. Hemenway, R. Grzybowski, C. Minkenberg, and R. Luijten, "Optical-packet-switched interconnect for supercomputer applications,"OSA J. Opt. Netw., vol. 3, no. 12, pp. 900–913, Dec. 2004.
[18] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, M. Gusat, P.Dill, I. Iliadis, R. Luijten, B. R. Hemenway, R. Grzybowski, and E.Schiattarella, "Designing a crossbar scheduler for HPC applications,"IEEE Micro, vol. 26, no. 3, pp. 58–71, May/Jun. 2006.
[19] E. Oki, R. Rojas-Cessa, and H. Chao, "A pipeline-based approach formaximal-sized matching scheduling in input buffered switches," IEEE Commun. Lett., vol. 5, no. 6, pp. 263–265, Jun. 2001.
[20] C. Minkenberg, I. Iliadis, and F. Abel, "Low-latency pipelined crossbar arbitration," in Proc. IEEE GLOBECOM 2004, Dallas, TX, Dec. 2004, vol. 2, pp. 1174– 1179.
[21] C. Minkenberg, R. Luijten, F. Abel, W. Denzel, and M. Gusat, "Current issues in packet switch design," ACM Comput. Commun. Rev., vol. 33, no. 1, pp. 119–124, Jan. 2003.
[22] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, and M. Gusat,"Control path implementation of a low-latency optical HPC switch," inProc. Hot Interconnects 13, Stanford, CA, Aug. 2005, pp. 29–35.
[23] C.-S. Chang, D.-S. Lee, and Y.-S. Jou, "Load-balanced Birkhoff-von Neumann switches, part I: One stage buffering," Elsevier Comput.Commun., vol. 25, pp. 611–622, 2002.
[24] A. Tanenbaum, Computer Networks, 3rd ed. Englewood Cliffs, NJ: Prentice Hall.
[25] R. Krishnamurthy and P. Müller, "An input queuing implementation for low-latency speculative optical switches," in Proc. 2007 Int. Conf.Parallel Processing Techniques and Applications (PDPTA'07), Las Vegas, NV, Jun. 2007, vol. 1, pp. 161–167.
[26] H. Takagi, Queueing Analysis, Volume 3: Discrete-Time Systems. Amsterdam: North-Holland



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY