Brief Report

Intrusion Detection Systems: Categories, attack detection and response.

Natalia Lewandowska *

Posted Date: 1 February 2024

doi: 10.20944/preprints202402.0008.v1

Keywords: Intrusion Detection Systems (IDS); Intrusion Prevention System (IPS); Intrusion Response System (IRS); Anomaly (AIDS); Signature (SIDS); Heuristic; Network (NIDS); Host (HIDS); Hybrid; Cloud (CIDS)

Brief Report

Intrusion Detection Systems: Categories, Attack Detection and Response

Natalia Lewandowska

Correspondence: nlewando99@gmail.com

Abstract: This report covers the analysis of Intrusion Detection Systems nowadays. Therefore, it focuses on the IDS classification, which includes not only a well-known explanation of Network/Host-Based IDS type but also cloud- based solutions. The paper explores ways of intrusion detection, providing examples of the best detecting tools (OSSEC, Snort or Bro (ZEEK)). Another aspect covered in this report is the juxtaposition of three systems: IDS, IPS and IRS and their response. Finally, there will be presented Intrusion Detection Systems' evasion techniques and challenges, followed by critical conclusions.

Keywords: Intrusion Detection Systems (IDS); Intrusion Prevention System (IPS); Intrusion Response System (IRS); Anomaly (AIDS); Signature (SIDS); Heuristic; Network (NIDS); Host (HIDS); Hybrid; Cloud (CIDS)

1. Introduction

An Intrusion Detection System is a security tool or software that is designed to monitor network traffic or system activities for sign of malicious or unauthorised activities. Its primary purpose is to detect and alert suspicious or potentially harmful activities that could indicate a security breach, intrusion, or cyber-attack [1]. There are many functions of Intrusion Detection Systems, which include monitoring/analysing user and systems activities, its vulnerabilities, and configurations or recognising patterns and abnormal activities. All collected data helps to improve IDS performance, which means higher system security and accurate prediction of network attacks [2].

However, the prediction aspects are not always faultless and identified intrusions might give false alerts. Depending on different alertion circumstances, we can distinguish four intrusion reporting situations:

- True Positive,
- True Negative,
- False Positive,
- False Negative.

In the case of True Positive, the Intrusion Detection Systems report will appear while the attack actually happened. The True Negative case scenario will generate no alert, meaning that, in fact, there was no attack. The first two distinguished situations will report only the actual system status, which had occurred [24]. In the case of a False Positive and False Negative reports, the first one will inform about occurred attack, while it did not take place. The second one will report about normal system state (no attack), while the intrusion occurred [3]. It is essential to understand that as a security tool, which IDS is, one of the main systems' goals is to maximize the occurrence of two first cases: TP/TN, and minimalize the last two: FP/FN.

2. IDS CATEGORIES AND ANALYSIS

Intrusion Detection Systems classification is more complex than it seems to be. The choice of IDS type and deployment depends on the specific security requirements and constraints of an organisation. There might be many ways of categorising it based on its scope, destination, methodology or intrusion detection approaches. Knowing the IDS background, and its system

 doi:10.20944/preprints202402.0008.v1

purposes but also following rapid technology development there was produced ensuing systems categories, classified by:

- *Types of IDS.*
  - Host-based (HIDS),
  - Network-based (NIDS),
  - Cloud-based (CIDS).
- *Ways of detecting intrusion. (Chapter III)*
  - Anomaly detection (AIDS),
  - Signature detection (SIDS),
  - Heuristic detection,
  - Hybrid detection.

A. *Host-based IDS (HIDS)*

Host-based Intrusion Detection Systems are introduced on a specific server (host), therefore they monitor any activities on individual hosts for signs of intrusion. Its main purpose is to detect and examine file integrity, system logs or any host-related data. So, as it says, it provides only information about host-level activities [5]. In the case of an attack on the server, HIDS will use any tools installed on this server e.g. OSSEEC, Samhain or SolarWinds. Subsequently, it will track suspicious files, examine them by looking at any recorded differences and alert the human. However, Intrusion Detection Systems based on this kind of model have some strengths and weaknesses based on their server limits. Since HIDS are host-dependent, they may be difficult to manage. Moreover, being installed on the specific host may significantly slow down the system and take up quite a lot of disc space. On one hand, being host dependent is its vulnerability to attacks against host operating systems, hence DoS attacks for instance. Finally, it cannot identify attacks outside of its local host e.g. network related [21]. On the other hand, HIDS are effective for detecting unauthorized access and changes. Based on host behavior it can easily identify zero-day attacks and it makes them free from the bandwidth. It is a great alternative for detecting local attacks before they reach the network, and it also provides a low False Positive rate [6].

B. *Network-based IDS (NIDS)*

Network-based Intrusion Detection Systems focus on network traffic and based on them, it identifies suspicious patterns or behaviors that may indicate an intrusion or security risks. It provides a perfect solution for network- level threats such as DoS attacks and port scans. NIDS works by analyzing the traffic and capturing data packages, which are inspected by looking at where they came from, and what their destination IP addresses, ports and protocols are [25]. It usually happens between the firewall and the Switch, where NIDS is placed, so it can allow the traffic to go through it [13].

Network-based IDS use two types of intrusion detections:

- Anomaly (Unknown)-based system, which detects any abnormal activity. It works by looking at the usual network behaviors, and highlighting deviations from the baseline.
- Signature (Known)-based system, which compares patterns in the network, relying on a signature database of well-known attacks.

It uses the above detection methods to give an alert about real-time attacks and store detailed data about the attack that occurred [22].

Placed below Figure 1., presents two mentioned models: Host-based and Network-based IDS.

 doi:10.20944/preprints202402.0008.v1

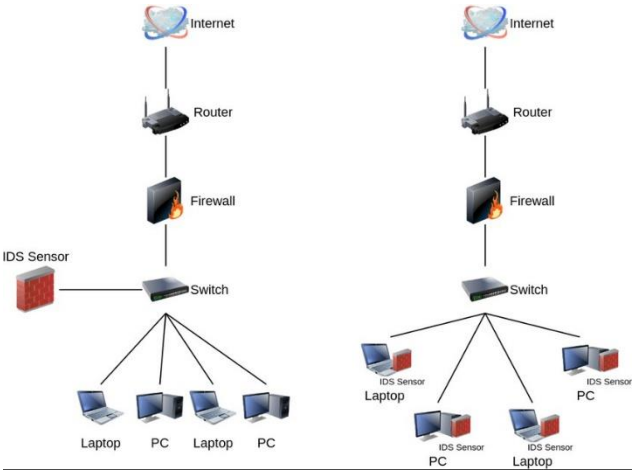

Figure 1. An example of NIDS (left) and HIDS (right). Source: [20].

Both models include the Internet source, Router, Firewall, Switch and Personal Devices: Laptops and PCs. Each of them also has an IDS Sensor placed depending on the used system. As mentioned before the NIDS model, which is presented on the left side monitors the network traffic and, hence is placed between Firewall and the Switch to let the traffic go through it. The model placed on the right side (HIDS) is strictly limited to the local host. So, Fig.1. shows the sensor placed where its host is, Laptop/PC in that case.

C. Cloud-based IDS (CIDS)

Cloud-based Intrusion Detections Systems focus on protecting cloud infrastructures. Its purpose is to identify and mitigate security threats specific to cloud- based environments. It is not an official type of IDS, although it is known as one of NIDS' approaching methods and it provides futuristic solutions. Most importantly, CIDS offer faster performance and lower maintenance costs [17]. There are still a few cloud- based IDS issues, which are explained below.

Relating to M. Bharati and other authors, who specifically highlighted the security problems of CIDS usage, the most significant ones appear to be safeguarding data confidentiality, potential host and network attacks and the need for effective evaluation process. Another aspect of cloud-based IDS are challenges of gathering activity NIDS in the cloud, which M. Bharati addressed concerns related to encrypted traffic, effective virtualization, and resource utilization, which are crucial to assure the data integrity of the cloud environment [5].

However, Zhiqiang Liu and other authors, in their article focus more on the beneficial side of CIDS in the computing world like fast systems arrangement, big storage capacity and relatively easy access to the system [26]. They also mention its security issues, but it is not considered as an unsolvable problem. Authors highlight chances that CIDS might offer in the future and lists all the system aspects which in their opinion impact the cloud-based IDS performance. These are presented in the below chart (Figure 2.) and analyzed.

 doi:10.20944/preprints202402.0008.v1

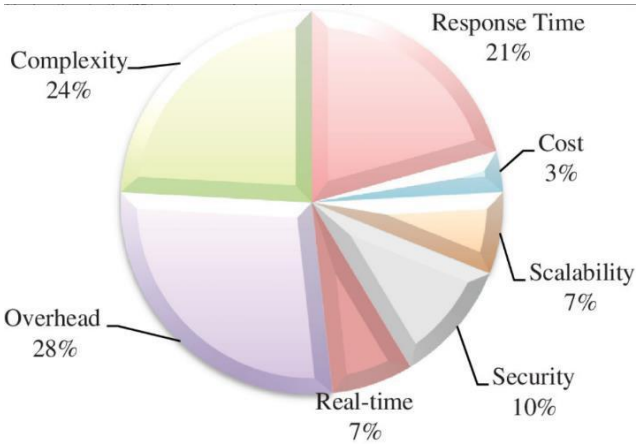

Figure 2. CIDS criteria defining/impacting the systems performance. Source: [23].

Figure 2. Presents seven criteria which purpose is to help analyze CIDS in terms of advantages/ disadvantages in these categories. Based on Z Liu's chart, the following criteria:

- Overhead (28%) - related to the system's cost, which as mentioned before is relatively low.
- Complexity (24%) - which are related to scalability, integration and real-time monitoring challenges, appear to be rather beneficial for cloud-based IDS.
- Response Time (21%) – which as mentioned earlier is relatively fast [23].

The above aspects appear to impact the system the most significantly. All three criteria constitute 3/4 of the total chart percentage, while the security aspects appear to be only 1/10 of the total. Relating to the above analyze [27], there are clearly more benefits out of using cloud-based systems than flaws, especially looking at the presented chart. The security issues and challenges related to NIDS implementation in cloud environment, the system has the appearance to be futuristic solution, especially because cloud systems are still comparatively a 'fresh ground', but its potential and general adaptation to the environment assures wide and long-term usage. The aim of mentioning CIDS was to give the best security monitoring tool [28]. However, the analysis of all three IDS types gave a clear conlusion that there is no one "correct" answer for this question. The tool effectiveness depends on the institution's unique requirements and its environement. If the establishment base more on the hosts security, HIDS is desirable. In the case of depending on the network-centric model, NIDS would be the best security support. However, the best option would be combaining these tools to create properly layered defence.

3. Attack detection techniques

Detecting intrusions is a main purpose of IDS. The importance of choosing detection techniques lies in *Early Threat Identification, Adaptability, Reduced False Positives, Response Time and Systems Monitoring*. Based on these criteria, there is going to be performed the investigation of different types of intrusion detection techniques and analyze their general performance. As mentioned before, there is four kinds of intrusion detections: Anomaly (AIDS) and Signature (SIDS – which both were shortly explained before), Heuristic and Hybrid detection techniques.

A. Anomaly-based detection (AIDS)

A characteristic feature of AIDS is detecting unknown/new attacks, which makes them very useful during detecting zero-day attacks. By identifying new kinds of threats, these systems are able to create an intrusion signature for them, so they may be easily detected by SIDS as well [12]. Analysing normal system behaviour and raising alert for deviations from established baseline involves machine-learning in that case. Having no specified detecting guidelines requiers additional training. It means, if there is not enough system training provided, it may wrongly identify occurred events and give a False Positive alert [4]. Below there is presented anomaly-based system example, Figure 3.

 doi:10.20944/preprints202402.0008.v1

B. Signature-based detection (SIDS)

SIDS detection method to perform well, it requires a database with a list of known attacks – signatures. These are also know as Knowledge-based or Misuse Detections. This technique is especially effective against recognised threats by providing accurate malware detection, viruses or common attack methods. On one hand, the need of signature, limits its performance, which make it useless in detecting zero-day attacks. Moreover, to be relatively usable for detecting newly created threats, its Signature database requires to be regularly updated. On the other hand, if the system will give an allert, there is high probability of its accurance. Therefore it limits False Positive alerting, opposite to Anomaly-based detection systems [8].

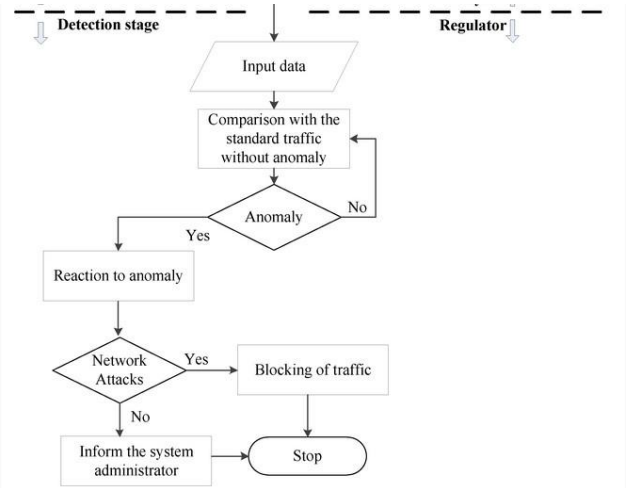

Figure 3. Anomaly-based detection system example. Source: [11].

C. Heuristic-based detection

Heuristic-based detection differ from SIDS/AIDS by looking for identified patterns and behaviours. It also establishes a baseline like AIDS but it focuses on the mentioned abnormal behaviours. Another aspect, which makes the system unique is the way it adapts to new and envolving threats. It finds a way to be effective against complex threats and zero-days attacks. On the other hand, heuristic-based detection may be problematic during the training phase. It is caused by using machine learning techinques, known from Anomaly-based detection method.[18]. This system is able to detect both not-known and signature-based attacks, but it requires database (signatures) and experience (Machine Learning). However, some of the attackers may use metamorphic strategies, which makes them more difficult to detect even by heuristic method [21].

D. Hybrid-based detection

Hybrid-based detection is a perfect solution to create high-performance working tool for identifying malware and accurate alerting. On one hand, that detection technique usually combines two or three different detecting tools like AIDS/SIDS or heuristic/behavioral-based method to overcome all the systems weaknesses and combine all the beneficial aspects into one working system. On the other hand, this solution may involve high maintenance costs, which are also related to the system complexity [15] Besides, this method seems to be the most effective. Figure 4. compares SIDS and AIDS detecting method, showing their strenghts and weaknesses in terms of False Positive and False Negative alerts. As presented below, combining these two could effectively work together by using SIDS low FP and AIDS low FN, thus creating Hybrid detecting system.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 February 2024 doi:10.20944/preprints202402.0008.v1

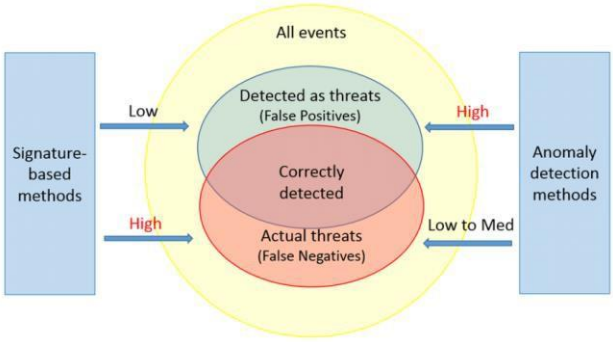

Figure 4. Juxtaposition of SIDS and AIDS. Source: [10].

4. IDS VS IPS VS IRS AND THEIR RESPONSE

So far, the report explained what Intrusion Detection Systems are, its types and attack detection techniques. The following part of this paper will elaborate why detecting is not the only solution to secure systems.

A. IPS – Intrusion Prevention System

It is a security tool, which as its name says – prevents the upcoming threat. So, instead of just detecting and alerting as the IDS is doing, IPS actively prevents and blocks the attack in real-time [7]. Figure 5. presents IDS/IPS and their positions/roles in the network security. As shown, the IDS is detecting malware activities and sending an alert, then the IPS reacts by actively preventing/blocking the threat and it sends the report about the occurred event.

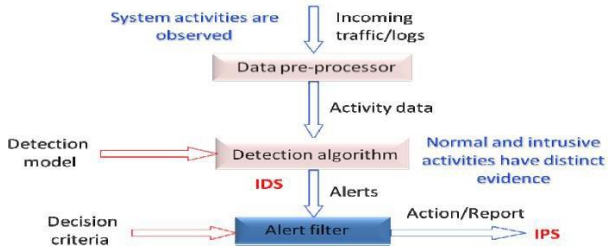

Figure 5. IDS vs IPS roles in network security. Source: [9].

B. IRS- Intrusion Response System

IRS is a system tightly paired with IDS. As its name highlights, it is responsible for responding to the malware detection. After the Intrusion Detection System identifies the threat, the IRS takes over and reacts in a passive or active way. It could either passively record , or actively mitigate the attack [14].

C. Which of the systems is best?

There is no direct answer for this question. All three systems exists for a reason and they have their own equally important roles. As mentioned, IDS focus on the detecting and alarming part, IRS takes over IDS to response after malware is detected and IPS blocks the attack in real-time [29]. That makes IDS passive, which is observing and reporting, IRS could be passive or active, depending on its response, while IPS is an active automatic system. Although, all three of them could work together and become one combined system, it is called IDPRS – Intrusion Detection Prevention Response System (Figure 6.), or combination of IDS and IPS (IDPS) which could be used for example with wireless networks. IDPS system combination is effective, taking into account slow down network performance caused by IPS inline delays. Whereas, IDS does not impact the network traffic, so it does not stop its detecting effectiveness [7]. However, IDPRS is even more effective in terms of communicating with firewall and inbound/outbound monitoring of traffic [16].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 1 February 2024 doi:10.20944/preprints202402.0008.v1

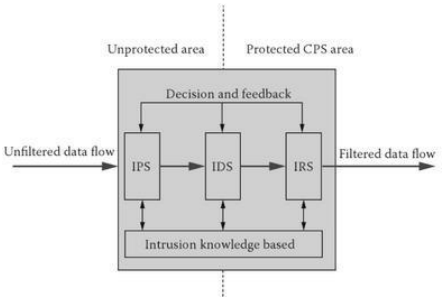

Figure 6. An example of IDPRS model. Source:[16].

5. THE BEST IDS TOOLS

In this chapter there is going to be presented three most commonly used IDS tools: OSSEC, Snort and Bro (ZEEK) and shorty compared in the Table 1. [17], [19].

Table 1. Juxtaposition of OSSEC, Snort and Bro IDS tools.

Feature	OSSEC	Snort	Bro
Type	HIDS	NIDS	NIDS
Protocol support	N/A	TCP, UDP, IP, ICMP	SNMP, FTP, DNS, HTTP
Suported platform	Unix, Windows, Linux, MacOs	Unix, MacOs, Windows, Linux, FreeBSD	Unix, Linux, MacOs
Open source	yes	yes	yes
Performance	Generaly good, easily scallable	Good, extensive rule sets	Good, efficient for high speed
IPS feature	no	yes	no
SIDS/AIDS	SIDS/AIDS	SIDS	AIDS

At first, it is not clear which of these is best, taking into account their general good performance. The choice of which should be used is rather personal and should be based on specific requirements of the establishment. OSSEC is a host-based security tool, easily scalable and flexible enough to adapt to different needs. That tool provides a real-time monitoring and alerting system. However, it may not be as good as BRO or SNORT in terms of network-based monitoring. So, OSSEC is a good choice in case if the establishment is looking for host-based security. However, if the company focuses on the ability to detailed insights into network traffic, BRO(Zeek) would be a good fit [30]. Especially because it provides comprehensive network visibility and protocol analysis. Finally, SNORT would be a great choice for signature- based detection. It also provides large and active community support.

6. Evasion techniques

Evasion techniques are ways that attackers use to avoid being detected, for instance by: Encryption, Obfuscation, Fragmentation or Flooding techniques.

- Encryption – IDS is not able to read encrypted files, thus attackers can encrypt malicious payload to make it harder to inspect the content.

 doi:10.20944/preprints202402.0008.v1

- Obfuscation- the attacker use obfuscation to make the malicious payload difficult to read and understand. Its aim is to have a code, which functionality is malicious but difficult to detect by IDS.
- Fragmentation- that technique of evasion is used by the attacker to divide the malicious payload into smaller packages- fragments and this way avoid Signature-based detection.
- Flooding – the attacker wil try to overload the target causing IDS failure. It could be achieved by using UDP or ICMP protocols [4].

Cyber criminals are very creative with avoiding detections and every day they discover new ways of evasion. Certainly, there is more ways of them, which we could be not aware of. However, The above four evasion techniques are the most common attackers choices to be familiar with.

7. Disscusion and Conclusions

This paper explained Intrusion Detection Systems, its types and detection techniques. Besides HIDS and NIDS types of IDS, there was analyzed cloud method, which offer futuristic solutions. Subsequently, the report elaborated and compared IDS to IPS and IRS in terms of their roles in the network and responses to the threat. Finally, the paper listed and collated the most common IDS tools: OSSEC, Snort and Bro.

This report's aim is not only to present facts about Intrusion Detection Systems, but also to help understand the importance of network protection and that there is not one ,,correct,, solution which would provide 100% secureness. As mentioned before, the IDS main goal is to minimalize the False Positive/Negative alerts, so the systems reports can be 100% accurate. Unfortunately, looking at the systems flaws, there is still lots of work to achieve such a result. Through the report, we analyzed HIDS, NIDS and CIDS in terms of their way of work, strengths and weaknesses. In a similar way, there were discovered: AIDS, SIDS, Heuristic-based and Hybrid- based detections. Each of them standalone are not good enough, with a big room for development. However, using hybrid solutions supported by Machine Learning, where there could be combined two or three different systems as proposed before: IDPS or IDPRS, hybrid of SIDS and AIDS, would create a properly build security layer.

Certainly, each establishment lists different requirements and is in need of different security techniques/level. However, they need to be aware of the rapid technology development and attackers new ways to be not detected – evasion techniques. This kind of security challenges force us to develop new security technologies, reuse and improve the old ones and look for completely new solutions like proposed CIDS.

References

1. Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Bryan D. Payne. 2015. Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices. ACM Comput. Surv. 48, 1, Article 12 (September 2015), 41 pages.
2. Ashoor, A. S., & Gore, S. (2011, January). Importance of Intrusion Detection System (IDS). Editor Ijser.
3. Diab, D. M., AsSadhan, B., Binsalleeh, H., Lambotharan, S., Kyriakopoulos, K. G., & Ghafir, I. (2019, August). Anomaly detection using dynamic time warping. In 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (pp. 193-198). IEEE.
4. G. Meena and R. R. Choudhary, "A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA," *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, Jaipur, India, 2017, pp. 553-558,
5. Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019).
6. M. Bharati and S. Tamane, "Intrusion detection systems (IDS) & future challenges in cloud based environment," 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), Aurangabad, India, 2017, pp. 240-250, doi: 10.1109/ICISIM.2017.8122180.

7. Aparicio-Navarro, F.J., Kyriakopoulos, K.G., Ghafir, I., Lambotharan, S. and Chambers, J.A., 2018, October. Multi-stage attack detection using contextual information. In MILCOM 2018- 2018 IEEE Military Communications Conference (MILCOM) (pp. 1-9). IEEE.
8. Eve, A. and Abaci, I.N. (2022) Comparison of the Host-Based Intrusion Detection Systems and Network-Based Intrusion Detection Systems.
9. Coulibaly, K. (n.d.). An overview of Intrusion Detection and Prevention Systems. Bradford; Bradford University.
10. Lefoane, M., Ghafir, I., Kabir, S. and Awan, I.U., 2021, December. Machine learning for botnet detection: An optimized feature selection approach. In The 5th International Conference on Future Networks & Distributed Systems (pp. 195-200).
11. Einy, S., Oz, C. and Navaei, Y.D. (2021) 'The anomaly- and signature-based ids for network security using Hybrid Inference Systems', Mathematical Problems in Engineering, 2021, pp. 1–10. doi:10.1155/2021/6639714.
12. Ashoor, A.S. and Gore, S. (2011) 'Intrusion Detection System (IDS) &Intrusion Prevention System (IPS): Case Study'. IJSER.
13. Degeler, Victoria & French, Richard & Jones, Kevin. (2016). Self- Healing Intrusion Detection System Concept. 351-356. 10.1109/BigDataSecurity-HPSC-IDS.2016.27.
14. Zhang, Y., Yang, Q., Lambotharan, S., Kyriakopoulos, K., Ghafir,
15. and AsSadhan, B., 2019, October. Anomaly-based network intrusion detection using SVM. In 2019 11th International conference on wireless communications and signal processing (WCSP) (pp. 1-6). IEEE.
16. Song, W.; Beshley, M.; Przystupa, K.; Beshley, H.; Kochan, O.; Pryslupskyi, A.; Pieniak, D.; Su, J. A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection. *Sensors* 2020, *20*, 1637.
17. R. Samrin and D. Vasumathi, "Review on anomaly based network intrusion detection system," *2017 International Conference on*
18. *Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, Mysuru,
19. India,2017,pp.141-147
20. Eltanani, S. and Ghafir, I., 2020, November. Coverage Optimisation for Aerial Wireless Networks. In 2020 14th International Conference on Innovations in Information Technology (IIT) (pp. 233-238). IEEE.
21. S. Kumar, S. Gupta and S. Arora, "Research Trends in Network- Based Intrusion Detection Systems: A Review," in *IEEE Access*, vol. 9, pp. 157761-157779, 2021,
22. N. B. Anuar, M. Papadaki, S. Furnell and N. Clarke, "An investigation and survey of response options for Intrusion Response Systems (IRSs)," *2010 Information Security for South Africa*, Johannesburg, South Africa, 2010, pp. 1-8,
23. Santhosh Kumar, S.V.N., Selvi, M. and Kannan, A. (2023) A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things, Computational Intelligence and Neuroscience.
24. Lefoane, M., Ghafir, I., Kabir, S. and Awan, I.U., 2022. Unsupervised learning for feature selection: A proposed solution for botnet detection in 5g networks. IEEE Transactions on Industrial Informatics, 19(1), pp.921-929.
25. Pathan, A.-S.K. (2016) 'IDPRS for CPSs', in Securing Cyber- Physical Systems. CRC Press, pp. 380–384. [Online] Available:https://books.google.co.uk/books?hl=en&lr=&id=wB6vCgAAQBAJ&oi=fnd&pg=PA371&dq=IDPRS+system+in+cyber+ security
26. M. Ozkan-Okay, R. Samet, Ö. Aslan and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," in *IEEE Access*, vol. 9, pp. 157727-157760, 2021
27. Z. Bazrafshan, H. Hashemi, S. M. H. Fard and A. Hamzeh, "A survey on heuristic malware detection techniques," *The 5th Conference on Information and Knowledge Technology*, Shiraz, Iran, 2013, pp. 113-120,
28. D. A. Bhosale and V. M. Mane, "Comparative study and analysis of network intrusion detection tools," *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Davangere, India, 2015, pp. 312-315, doi: 10.1109/ICATCCT.2015.7456901.
29. Eltanani, S. and Ghafir, I., 2021, May. Aerial Wireless Networks: Proposed Solution for Coverage Optimisation. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.
30. Integrating an Intrusion Detection System with Heterogeneous IoT Endpoint Devices - Scientific Figure on ResearchGate.Available: https://www.researchgate.net/figure/Network-based-IDS-left-vs- Host-based-IDS-right_fig5_346499141 [accessed 1 Dec, 2023]
31. Ozkan-Okay, M. et al. (2021) 'A comprehensive systematic literature review on Intrusion Detection Systems', IEEE Access, 9,
32. pp. 157727–157760.

 doi:10.20944/preprints202402.0008.v1

33. S. Kumar, S. Gupta and S. Arora, "Research Trends in Network- Based Intrusion Detection Systems: A Review," in *IEEE Access*, vol. 9, pp. 157761-157779, 2021.
34. Liu, Z. et al. (2021) 'Intrusion Detection Systems in the cloud computing: A comprehensive and deep literature review', Concurrency and Computation: Practice and Experience, 34(4).