



Intrusion Detection Systems

Dr. Sonal Ayare, Aakash Mansing Mane, Pankaj P. Gavit

Dr. Sonal Ayare, Assistant Professor, Kolhapur Institute of Technology's College Of Engg, Kolhapur.

Aakash Mansing Mane, Kolhapur Institute of Technology, Kolhapur, Maharashtra

Pankaj P. Gavit, Kolhapur Institute of Technology, Kolhapur, Maharashtra.

Date of Submission: 06-05-2025

Date of Acceptance: 17-05-2025

ABSTRACT: Intrusion Detection Systems (IDS) have become a cornerstone of modern cybersecurity, providing essential monitoring and detection capabilities to safeguard networks and systems from malicious activities. As cyber threats grow in complexity and frequency, IDS technologies are evolving to incorporate advanced techniques such as machine learning, artificial intelligence (AI), and big data analytics. Despite their critical role, IDS face challenges such as high false-positive rates, scalability issues, and the need for real-time threat detection. This paper explores the historical development, future prospects, applications, challenges, and implications of IDS, referencing key studies in the field.

KEYWORDS: *Intrusion Detection System (IDS), Network Intrusion Detection System (NIDS), Host Intrusion Detection System (HIDS), Signature-based IDS, Anomaly-based IDS, and tools like Snort and Suricata*

I.INTRODUCTION

Intrusion Detection Systems (IDS) are security mechanisms designed to detect unauthorized access, malicious activities, or policy violations within a network or system. With the increasing sophistication of cyberattacks, IDS have become indispensable for organizations aiming to protect their digital assets. The integration of AI and machine learning has enhanced the capabilities of IDS, enabling them to detect previously unknown threats and reduce response times. However, challenges such as false positives, resource constraints, and the need for continuous updates remain significant hurdles. This paper examines the evolution of IDS, their future potential, and the challenges that must be addressed to ensure their effectiveness in the face of evolving cyber threats.

Annual scientific production

In the previous 10 years, reliable ML in intrusion detection has advanced. In particular, the annual scientific output depicted in 2 provides an explanation for the emergence of earlier theoretical and practical investigations on reliable ML. The annual scientific output for intrusion detection is depicted in . The number of papers published in 2018 and 2019 reached approximately 23 papers, it can be seen that the quantity of publications has significantly expanded in recent years. There was an increase in the number of articles published in 2020 and 2021. In 2022, the number of articles grew even further, reaching a notable high of 138 papers. This pattern persisted in 2023, where 95 papers were published. The increase in research output suggests a growing interest and emphasis on the development and improvement of IDS over the years. Furthermore, specific authors have contributed significantly to this field, with some focusing on optimization and feature selection based on intrusion detection, while others have concentrated on IDS for Internet of Things (IoT) based on DL. These authors have achieved high accuracies in their research, indicating the advancement and effectiveness of the techniques employed in IDS. Overall, the observed publication trends demonstrate a substantial growth in research output in the field of IDS from 2018 to 2023, reflecting an increasing focus on enhancing the reliability and effectiveness of intrusion detection techniques. shows authors' production over time, where Motwakel published seven papers in 2022 and 2023 and he focused in his research on optimization and feature selection based on intrusion detection. In his research, the highest accuracy he reached was 99.87 using sand paper optimization. As for Al_Qaness , he published five papers in 2021–2023) and he focused on IDS for IOT based on DL. In his research, he reached the highest accuracy of 99.997 using swarm intelligence optimization. Bacaninhas published five papers



DOI: 10.35629/5252-45122323 | Impact Factor value 7.429 | ISO 9001: 2008 Certified Journal | Page 51



Growth of IDS in Past Years

The development of IDS has progressed significantly since their inception in the 1980s. Early IDS relied on signature-based detection methods, which were effective against known threats but struggled with new or evolving attacks. Over the years, the adoption of anomaly-based detection and behaviour analysis has improved the ability of IDS to identify zero-day attacks and sophisticated threats. According to industry reports, the global IDS market was valued at approximately \$4.5 billion in 2020 and is projected to grow at a compound annual growth rate (CAGR) of 10% over the next decade. The rise of cloud computing, IoT, and 5G networks has further driven the demand for advanced IDS solutions capable of securing complex and distributed environments.

References

- [1]. Motwakel, A. (2022-2023). Research on optimization and feature selection based on intrusion detection. (Multiple papers, highest accuracy: 99.87% using sand paper optimization).
- [2]. Al-Qaness, M.A.A. (2021-2023). Research on IDS for IoT based on deep learning. (Highest accuracy: 99.997% using swarm intelligence optimization).
- [3]. Bacanin, N. (2020-2023). Research on optimization algorithms and feature selection for intrusion detection. (Highest accuracy: 99.6878% using GOA and MPO).
- [4]. Chen, H. (2020-2023). Research on intrusion detection using hybrid algorithms. (Highest accuracy: 99.44% using COBYLA optimization).
- [5]. Dahou, A. (2021-2023). Research on IoT IDS using deep learning and optimization. (Highest accuracy: 99.997% using swarm intelligence optimization).
- [6]. Fang, Y. (2018, 2020, 2022). Research on optimization algorithms for feature selection in network intrusion detection. (Highest accuracy: 97.89% using WOA and OPS optimization).
- [7]. Hilal, A.M. (2022-2023). Research on deep learning algorithms optimization for intrusion detection. (Highest accuracy: 99.77% using IFSO-FS).
- [8]. Zivkovic, M. (2022-2023). Research on intrusion detection for optimization algorithms and feature selection. (Highest accuracy: 99.6878% using GOA and MPO).
- [9]. Al-Janabi, S. (2020-2021). Research on IDS, optimization algorithms, and feature selection. (Highest accuracy: 100% using NTLBO optimization).
- [10]. Om Kumar, C. (Referenced for KDD Cup 99 dataset).
- [11]. Li, J. (Referenced for NSL-KDD dataset).
- [12]. Li, W. (Referenced for UNSW-NBIS dataset).
- [13]. Yousef, M. (Referenced for CICIDS 2017 dataset).
- [14]. Yin, C. (2017). Deep learning approach for intrusion detection using recurrent neural networks (RNN-IDS).
- [15]. Vasan, D. (Referenced for CNN applications in IDS).
- [16]. Mirsky, Y. (2018). Autoencoder-based online IoT IDS.
- [17]. Benkhelifa, E. (2018). Centralized IDS deployment in IoT.
- [18]. Bhuyan, M.H. (2014). Limitations of NIDS in high-bandwidth networks.
- [19]. Khraisat, A. (2019b). IoT security challenges and attacks.
- [20]. Liao, H.J. (2013a). IoT system architecture layers and attacks.