INTRUSION DETECTION TECHNIQUES AND SWARM INTELLIGENCE CYBERSECURITY REVIEW

Zorana Krsmanović*,
[0009-0005-5642-8190]
Stojanka Tešanović,
[0009-0005-2371-3358]
Aleksandar Petrović,
[0000-0003-3324-3909]
Miodrag Živković,
[0000-0002-4351-068X]
Tamara Živković
[0000-0003-2969-1709]

Singidunum University,
Belgrade, Serbia

Abstract:

A computing and communications revolution at high speed has hastened the demand for effective security devices to protect networks from highly sophisticated cyberattacks. Intrusion Detection Systems (IDS) are an essential part of network traffic monitoring and network abuse detection. Traditional IDS techniques, however, such as signature-based and anomaly-based systems, experience severe limitations, including weak detection of novel attacks, high false positives, and high computational overhead. This survey provides a comprehensive overview of state-of-the-art hybrid machine learning (ML) methods with swarm intelligence (SI), a collection of metaheuristic optimization techniques inspired by collective behaviour in nature, for the enhancement of IDS. The examination is critical and covers hybrid models integrating supervised, unsupervised, and deep learning methods optimized using SI methods, such as crayfish optimization, firefly algorithm (FA), and social network search (SNS). Their key strengths and weaknesses and their applications in the real world are highlighted. Problems of computational complexity, scalability, and real-time use are also cited. The paper identifies critical areas for future research activity, such as improved feature selection methodology, real-time adaptability, distributed processing methodology, and large and diverse benchmark datasets. The survey highlights the immense scope for hybrid SI-based ML solutions to improve cybersecurity practice and research.

Keywords:

Intrusion Detection, Swarm Intelligence, Machine Learning, Metaheuristics, Cybersecurity.

INTRODUCTION

In today's era of rapid digital systems development, malicious activities constantly attempt to compromise data integrity, driven by financial gain, data theft, or other malicious motives. For this reason, special emphasis is placed on securing data and system infrastructure, where intrusion detection methods are used to identify unauthorized access. However, as these methods become more advanced, attackers continuously develop new techniques that must be countered to protect sensitive data from compromise. Intrusion detection can be classified into two categories, signature-based and anomaly-based techniques. Signature-based intrusion detection techniques rely on predefined rules and known attack patterns from an existing database but cannot detect unknown threats,

Correspondence:
Zorana Krsmanović

e-mail:
zorana.krsmanovic23@singimail.rs

DOI: 10.15308/Sinteza-2025-206-212

while anomaly-based techniques monitor network activity for deviations using methods like clustering and classification, both facing challenges from increasing data volume, and malicious behaviour, and the need to process numerous attributes [1]. Such traditional systems rely on previously known attacks and cannot effectively detect unknown, new, and sophisticated threats.

Although various methods based on statistics and machine learning (ML) exist, many still face challenges such as high false alarm rates and low accuracy in detecting new attacks [2]. Additionally, slow convergence and the lack of efficient techniques for optimization and feature selection are also challenges for intrusion detection [3]. Furthermore, many require significant computational resources and fail to find a balance between accuracy and efficiency, making them impractical for real-world implementation [4]. These challenges highlight the need for developing more advanced methods capable of better detecting threats in modern computer networks.

The applications of artificial intelligence (AI) and ML techniques are increasingly being used in the development of intrusion detection systems (IDS). According to Heidari et al. [5], ML is becoming a key component in network intrusion detection systems (NIDS) and intrusion prevention systems (IPS), providing greater accuracy compared to traditional rule-based methods. This shift is the result of the development of hardware accelerators and sophisticated ML algorithms [6], [7], [8], enabling more precise detection of network breaches and more efficient analysis of network traffic. AI-based systems have shown exceptional performance in anomaly detection and threat classification. The main goal initially was the implementation of traditional ML models such as decision tree (DT) [9] and support vector machine (SVM) in intrusion detection systems, to later introduce deep learning methods such as convolutional neural networks (CNN), long short-term memory networks (LSTM), and autoencoders [10]. However, despite significant potential, the application of such solutions in real operational environments still presents numerous challenges [11]. Therefore, a detailed review and analysis of state-of-the-art hybrid ML approaches for intrusion detection are essential for better understanding the real capabilities and limitations of AI.

Swarm intelligence (SI) is a branch of AI that focuses on optimization using metaheuristic methods inspired by collective behaviour in nature. Algorithms from the SI group rely on the idea that a group of individuals can find a better solution than a single individual. Each individual or agent in an SI algorithm represents a potential solution. Through constant interaction and exchange of information with other agents, the group evolves towards increasingly better solutions. This principle is inspired by the behaviour of animal communities, such as ants that communicate using pheromones while searching for food, marking the shortest and most efficient paths, or birds that move in flocks, adjusting their trajectory based on the position of their neighbours [12]. Thus, the basic principle is that many potential solutions are considered simultaneously and adjusted during each iteration, with collective behaviour finding a suboptimal global solution. The optimal solution is considered to be the best possible and often it is very hard and even impossible to reach. Hence approximation techniques target the suboptimal solution, which is considered to be very close to the optimal but it is reachable in polynomial time. Swarm Intelligence algorithms are based on two phases: exploration and exploitation. In the exploration phase, the algorithm randomly searches the entire search space, i.e., the space of all possible solutions. Each individual moves randomly through the space. The goal here is to ensure that the algorithm does not get stuck in the local optimum but explores a wide range of solutions. On the other hand, exploitation focuses on the most promising region of the search space and deepens the search within it. A balance between these two phases must exist so that the algorithm does not remain trapped in a local optimum or aimlessly wander through the entire search space [13]. One way to achieve a better balance is the process of hybridization, where the global search capability of one algorithm is combined with the efficient local search of another [14]. This approach is in line with the no-free lunch theorem (NFL) [15], which implies that no single optimization algorithm can outperform all others in every scenario. Because of this, combining different strategies is crucial for achieving better overall performance.

2. RELATED WORKS

As cyber threats are becoming more sophisticated, IDS have struggled due to their reliance on fixed signatures, limited detection of unknown attacks, and tendency toward high false positives. As a result, researchers are now exploring hybrid and adaptive approaches to make IDS more flexible and effective in real-time environments. Meanwhile, SI, inspired by natural group behaviours such as those of insects and birds, is emerging as a promising method for solving complex

optimization problems. These algorithms effectively balance broad exploration and focused searching, showing great potential in fields like cybersecurity, wireless sensor networks, medical diagnostics, and cryptocurrency forecasting.

2.1. INTRUSION DETECTION SYSTEMS

In today's rapidly evolving cyber landscape, it's clear that conventional network security methods struggle to keep pace with increasingly sophisticated and frequent attacks. Therefore, IDS, as a security tool, addresses these limitations by monitoring both internal and external network activities [16], [17]. They are used to observe network traffic for harmful actions, including data theft, censorship, or violation of network protocols. Traditional IDS solutions include network-based (NIDS), host-based (HIDS), wireless (WIDS), and network behaviour analysis (NBA) systems, employing signature-based (SIDS), anomaly-based (AIDS), or stateful protocol analysis (SPA) methodologies for threat detection.

Conventional approaches have demonstrated their effectiveness in detecting particular kinds of cyber threats, especially when utilizing established attack patterns. Traditional signature-based IDS effectively detect known cyber threats by comparing incoming packets with predefined signatures, but Kumar et al. [18] highlight their ineffectiveness against unknown or modified threats due to dependency on existing signature databases. Although effective in recognizing novel threats by identifying deviations from normal network activity, AIDS generates higher false-positive rates, increasing workload for security analysts, as noted by Narsingyani et al. [19].

Detection systems relying on protocol analysis, such as SPA, identify deviations from standard protocol behaviours, providing strong protection against unauthorized protocol usage and attacks. According to Nitin et al. [20], SPA is resource-intensive and vulnerable to advanced threats designed to mimic legitimate protocol behaviours. While NBA statistically profiles network traffic to detect significant threats like DDoS attacks, Moon et al. [21] point out its limitations in identifying subtle or covert cyber threats. As wireless communication becomes more widely used, WIDS has emerged as a critical part of network security, providing targeted monitoring for wireless traffic and detecting threats that are specific to wireless networks. Afzal et al. [22] emphasize that WIDS face difficulties in detecting passive monitoring attacks because of their dependence on static signatures, underlining the need for adaptive security approaches.

Hybrid IDS solutions, merging signature-based accuracy with anomaly-based flexibility, showcase the optimal balance of precision and resource effectiveness. Nonetheless, they demand considerable computational power, rendering them less appropriate for real-time use in resource-limited settings [23]. These findings emphasize the importance of enhancing IDS methods by incorporating explainability and efficiency to address the limitations of conventional strategies.

Even though they remain significant, traditional IDS systems encounter increasing difficulties in today's cybersecurity environments. One significant disadvantage is their computational and hardware constraints, especially for signature-based IDS, which necessitate regular database updates to stay effective against new threats like zero-day attacks [24]. This dependence on predetermined attack patterns limits their flexibility, rendering them susceptible to fast-changing malware. Anomaly-based IDS is more versatile yet faces scalability challenges because of its elevated false positive rate, requiring significant adjustments for use in dynamic network settings [25].

2.2. SWARM INTELLIGENCE

Metaheuristic techniques inspired by collective behaviours found in nature, particularly those observed in animals exhibiting swarm-like activities, form the basis of SI algorithms. Due to their effectiveness in addressing NP-hard problems, these algorithms have become highly popular for optimization purposes. Their performance can be further enhanced through the process of hybridization. This procedure involves the integration of various algorithms to harmonize their unique strengths and limitations. This hybridization is particularly valuable because swarm intelligence algorithms typically excel either in exploration (broadening the search space) or in exploitation (focusing on precise solutions), and finding the right balance between these two phases is critical for achieving optimal results [26], [27]. Despite their extensive applicability, the NFL theorem posits that no singular algorithm is able to consistently outperform all others. Applications cover areas including wireless sensor networks [28-29], cryptocurrency forecasting [30], optimization of neural networks [31], cloud-edge computing [32], and medical diagnostics [33].

3. APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The impact of AI on cybersecurity is profound and far-reaching. The use of AI technologies enables rapid detection of malicious behaviours for security teams to respond quickly before any real damage occurs. Applications powered by AI-driven technology can search through enormous amounts of data in real time, improving the detection of anomalies and possible threats [34]. Besides detection, AI is also used to predict future cyberattacks using behaviour patterns so that proactive security can be implemented. The development of artificial neural networks has improved malware analysis and made cloud security far more robust. However, AI in cybersecurity also presents challenges, as ethical concerns and the possibility of cybercriminals utilizing AI for negative purposes are significant threats [35].

The application of metaheuristic optimization techniques in cybersecurity has significantly enhanced the efficiency of ML models in detecting cyberattacks. Jokić et al. [36] present the application of a crayfish optimization algorithm (COA) and genetic algorithm (GA) for the optimization of extreme gradient boosting (XGBoost) in detecting structured query language (SQL) injection attacks. The method applies natural language processing (NLP) techniques to improve security against SQL-based cyberattacks, highlighting the power of metaheuristics in AI model optimization.

Similarly, Bačanin et al. [37] introduced a modified SNS algorithm for optimizing XGBoost for intrusion detection, emphasizing the advantages of swarm intelligence approaches in handling NP-hard security problems. Their study highlights how SNS-enhanced XGBoost outperforms conventional tuning techniques in detecting anomalies within internet of things (IoT) networks.

In another study, Savanović et al. [38] apply a modified firefly algorithm (FA) to optimize ML models for intrusion detection in Healthcare 4.0 Internet of Things (IoT) systems. The results indicate that FA-based metaheuristic tuning significantly improves accuracy and detection speed, making it a suitable solution for real-time cyber threat mitigation.

Finally, Živković et al. [39] propose a hybridized sine cosine algorithm (SCA) to fine-tune XGBoost in identifying vulnerabilities in IoT healthcare security, showcasing how metaheuristic approaches can enhance predictive performance and system resilience. These studies collectively underscore the growing importance of metaheuristic optimization in cybersecurity, particularly in hybridized AI-driven security solutions, where advanced optimization techniques ensure both efficiency and adaptability in modern cybersecurity defence frameworks.

4. COMPARATIVE ANALYSIS OF INTRUSION DETECTION TECHNIQUES

A structured comparison of these IDS methods, highlighting their strengths and limitations, is provided in Table 1. This comparison aims to illustrate the trade-offs between detection efficiency, resource consumption, and adaptability to emerging threats.

Table 1. Advantages and disadvantages of different IDS technologies

IDS Method	Reference Citation	Advantages	Disadvantages	Zero-Day Attack Detection	Resource Requirements	False Alarm Rate
Signature-Based IDS (SIDS)	[24]	Fast detection of known threats easy implementation	Cannot detect new threats, needs frequent updates	No	Low	Low
Anomaly-Based IDS (AIDS)	[25]	Can detect unknown threats, learns from behaviour	High false positive rate, difficult fine-tuning	Yes	High	High
Stateful Protocol Analysis	[24]	Effective against protocol deviations	High resource consumption, complex setup	Partially	High	Low
Network Behavior Analysis	[25]	Good for detecting DDoS, a traffic-based approach	Poor detection of low-intensity attacks	Partially	High	Medium
Wireless IDS (WIDS)	[23]	Specialized for wireless threats, enhances Wi-Fi security	Cannot detect passive attacks, limited scope	No	Low	Medium

As shown in Table 1, conventional IDS techniques provide different compromises regarding detection efficacy and computational performance. Signature-based IDS is the most efficient in terms of computation, yet it fails to defend against zero-day attacks because it depends on known signatures [24]. Conversely, anomaly-based IDS offers flexibility, but its elevated false-positive rate may cause alert fatigue in security analysts, diminishing overall efficiency in extensive implementations [25].

An overview of different metaheuristic technologies from the SI group of algorithms that are applied to the field of cybersecurity is provided. These types of algorithms have proven excellent optimizers, and each of the reviewed papers provides a high-performance solution for increasing cybersecurity. The role of SI in cybersecurity is therefore confirmed, and it can only increase as the future of cybersecurity will be AI. In the work of Jokic et al. [36] the authors explore security improvements through SI optimization by employing an SQL injection detection mechanism. Another approach based on the XGBoost algorithm and optimized by the SI algorithm is explored in the work of Bacanin et al. [37]. A different aspect of the intrusion detection is explored in the work of Savanović et al. [38], as the authors tackle the problem with a similar approach but for IoT systems. Lastly, a work by Zivkovic et al. [39] is reviewed in which the authors once more employ SI-optimized intrusion detection in IoT healthcare systems but this time a metaheuristic-math-based optimizer is employed for optimizing XGBoost.

These obstacles underscore the need for ongoing innovation in IDS development, especially in enhancing detection algorithms, minimizing false positives, and increasing computational efficiency. Future research pathways ought to emphasize hybrid and adaptive strategies that reconcile security efficacy with practical performance limitations.

5. CONCLUSION

Systems for detecting and preventing potential threats, known as IDS, play a crucial role in ensuring cybersecurity. This paper examined hybrid ML techniques for intrusion detection, highlighting their advantages over single techniques and traditional approaches. By integrating several techniques, hybrid models provide enhanced detection, fewer false positives, and greater responsiveness to evolving cyber threats.

Effective detection and prevention of cybersecurity attacks are crucial to maintaining network security. In this paper, focus was given to hybrid ML techniques for intrusion detection, pointing out the advantage of these over traditional methods. The study explored various intrusion detection methodologies, citing the limitation of signature-based and anomaly-based methods, especially their inability to detect sophisticated cyberattacks.

A review of recent research confirmed that hybrid solutions, which combine different ML methodologies, offer improved detection rates, fewer false alarms, and flexibility. In addition, the combination of SI and other nature-inspired optimization strategies was experimented and confirmed to improve IDS performance.

Despite advancements, challenges such as computational complexity, real-time processing constraints, and smaller dataset sizes remain. Optimizing hybrid systems through advanced feature selection, real-time tunability, and scalable computation methods would work in the future. Large-scale benchmark datasets, along with an exploration into transfer learning, could improve these systems' generalizability.

It is important to note that the evolving AI regulations use pose threat from cybersecurity as well as from the perspective of general security. Cybersecurity is a critical field even without implicating AI, which only increases the risk of mishap. However, this should not hinder the development of AI and cybersecurity, hence it is important to emphasise that this risk can be mitigated with proper regulations.

Lastly, hybrid ML techniques are a possible prospect for intrusion detection with greater accuracy and dependability. Continued innovation in the field will be essential to further strengthening cybersecurity defences against the ever-emerging world of cyber threats.

REFERENCES

[1] S. Sharma, V. Kumar, and K. Dutta, "Multi-objective optimization algorithms for intrusion detection in IoT networks: A systematic review," *Internet of Things and Cyber-Physical Systems*, 2024. doi: 10.1016/j.iotcps.2024.01.003

[2] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid deep learning-based intrusion detection system," unpublished, 2023. doi: 10.2139/ssrn.3994183

[3] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowl.-Based Syst.*, vol. 189, p. 105124, 2020. doi: 10.1016/j.knosys.2019.105124

[4] M. H. Nasir, S. A. Khan, M. M. Khan, and M. Fatima, "Swarm intelligence inspired intrusion detection systems—A systematic literature review," *Comput. Netw.*, vol. 205, p. 108708, 2022. doi: 10.1016/j.comnet.2021.108708

[5] A. Heidari, N. Navimipour, M. Unal, and G. Zhang, "Machine learning applications in Internet-of-Drones: Systematic review, recent deployments, and open issues," *ACM Comput. Surv.*, vol. 55, 2022, doi: 10.1145/3571728.

[6] S. Bukhari et al., "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," *Ad Hoc Netw.*, vol. 155, p. 103407, 2024, doi: 10.1016/j.adhoc.2024.103407.

[7] A. Hanafi et al., "Intrusion detection in Internet of Things using improved binary golden jackal optimization algorithm and LSTM," *Cluster Comput.*, vol. 27, pp. 1–18, 2023, doi: 10.1007/s10586-023-04102-x.

[8] M. Belouch and S. El Hadaj, "Comparison of ensemble learning methods applied to network intrusion detection," in *Proc. ACM Int. Conf. Computer Systems and Technologies*, 2017, pp. 1–4, doi: 10.1145/3018896.3065830.

[9] J. R. Quinlan, C4.5: Programs for Machine Learning, San Mateo, CA, USA: Morgan Kaufmann, 2014.

[10] M. Sajid et al., "Enhancing intrusion detection: A hybrid machine and deep learning approach," *J. Cloud Comput.*, vol. 13, no. 1, p. 123, 2024. doi: 10.1186/s13677-024-00685-x

[11] I. Goodfellow, Deep Learning, Cambridge, MA, USA: MIT Press, 2016.

[12] C. Wang et al., "Swarm intelligence: A survey of model classification and applications," *Chin. J. Aeronaut.*, 2024, Art. no. 102982. doi: 10.1016/j.cja.2024.03.019

[13] N. Bacanin et al., "Performance of a novel chaotic firefly algorithm with enhanced exploration for tackling global optimization problems: Application for dropout regularization," *Mathematics*, vol. 9, p. 2705, 2021, doi: 10.3390/math9212705.

[14] R. Shankar et al., "Hybridized particle swarm–gravitational search algorithm for process optimization," *Processes*, vol. 10, no. 3, p. 616, 2022. doi: 10.3390/pr10030616

[15] T. F. Sterkenburg and P. D. Grünwald, "The no-free-lunch theorems of supervised learning," *Synthese*, vol. 199, no. 3, pp. 9979–10015, 2021. doi: 10.1007/s11229-021-03233-1

[16] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), *NIST Special Publication* 800-90, 2007.

[17] F. Sabahi and A. Movaghar, "Intrusion detection: A survey," in *Proc. 3rd Int. Conf. Syst. Netw. Commun.*, Oct. 2008, pp. 23–26. doi: 10.1109/ICSNC.2008.44

[18] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using SNORT," *Int. J. Comput. Appl. Inf. Technol.*, vol. 1, no. 3, pp. 35–41, Nov. 2012.

[19] D. Narsingyani and O. Kale, "Optimizing false positive in anomaly based intrusion detection using genetic algorithm," in *Proc. IEEE 3rd Int. Conf. MOOCs, Innov. Technol. Educ. (MITE)*, Oct. 2015, pp. 72–77. doi: 10.1109/MITE.2015.7375291

[20] T. Nitin, S. R. Singh, and P. G. Singh, "Intrusion detection and prevention system (IDPS) technology-network behavior analysis system (NBAS)," *ISCA J. Eng. Sci.*, vol. 1, no. 1, pp. 51–56, 2012.

[21] D. Moon, H. Im, I. Kim, and J. H. Park, "DTB-IDS: An intrusion detection system based on decision tree using behavior analysis for preventing APT attacks," *J. Supercomput.*, vol. 73, no. 7, pp. 2881–2895, 2017. doi: 10.1007/S11227-015-1604-8

[22] Z. Afzal, J. Rossebø, B. Talha, and M. Chowdhury, "A wireless intrusion detection system for 802.2 networks," in *Proc. Int. Conf. Wireless Commun.*, Signal Process. Netw. (WiSPNET), Mar. 2016, pp. 828–834.

[23] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 112392–112415, 2022. doi: 10.1109/WiSPNET.2016.7566249

[24] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019. doi: 10.1186/s42400-019-0038-7

[25] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, pp. 1–27, 2021. doi: 10.1186/s42400-021-00077-7

[26] R. Poli, J. Kennedy, and T. Blackwell, "Swarm intelligence," *Particle Swarm Optim.*, vol. 1, no. 1, pp. 33–57, 2007.

[27] D. Karaboga, "Artificial bee colony algorithm," *Scholarpedia*, vol. 5, no. 3, p. 6915, 2010. doi: 10.4249/scholarpedia.6915

[28] N. Bacanin, E. Tuba, M. Zivkovic, I. Strumberger, and M. Tuba, "Whale optimization algorithm with exploratory move for wireless sensor networks localization," in *Proc. Int. Conf. Hybrid Intelligent Syst.*, Cham, Switzerland: Springer, Dec. 2019, pp. 328–338. doi: 10.1007/978-3-030-49336-3_33

[29] M. Zivkovic, N. Bacanin, E. Tuba, I. Strumberger, T. Bezdan, and M. Tuba, "Wireless sensor networks life time optimization based on the improved firefly algorithm," in *Proc. 2020 Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 1176–1181. doi: 10.1109/IWCMC48107.2020.9148087

[30] M. Salb, M. Zivkovic, N. Bacanin, A. Chhabra, and M. Suresh, "Support vector machine performance improvements for cryptocurrency value forecasting by enhanced sine cosine algorithm," in *Proc. CVR 2021*, Singapore: Springer, 2022, pp. 527–536. doi: 10.1007/978-981-16-8225-4_40

[31] N. Bacanin, T. Bezdan, M. Zivkovic, and A. Chhabra, "Weight optimization in artificial neural network training by improved monarch butterfly algorithm," in *Proc. ICMCSI 2021,* Singapore: Springer, 2022, pp. 397–409. doi: 10.1007/978-981-16-1866-6_29

[32] N. Bacanin, M. Zivkovic, T. Bezdan, K. Venkatachalam, and M. Abouhawwash, "Modified firefly algorithm for workflow scheduling in cloud-edge environment," *Neural Comput. Appl.,* vol. 34, no. 11, pp. 9043–9068, 2022. doi: 10.1007/s00521-022-06925-y

[33] T. Bezdan, M. Zivkovic, E. Tuba, I. Strumberger, N. Bacanin, and M. Tuba, "Glioma brain tumor grade classification from MRI using convolutional neural networks designed by modified FA," in *Proc. Int. Conf. Intell. Fuzzy Syst.*, Cham, Switzerland: Springer, Jul. 2020, pp. 955–963. doi: 10.1007/978-3-030-51156-2_111

[34] A. Oseni, N. Moustafa, H. Janicke, P. Liu, Z. Tari, and A. Vasilakos, "Security and privacy for artificial intelligence: Opportunities and challenges," *arXiv preprint arXiv:2102.04661*, 2021. doi: 10.48550/arXiv.2102.04661

[35] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023. doi: 10.1109/ACCESS.2023.3300381

[36] A. Jokic, N. Jovic, V. Gajic, and M. S. Milos, "Structured query language injection detection with natural language processing techniques optimized by metaheuristics," in *Proc. 2nd Int. Conf. Innovation Inf. Technol. Bus. (ICIITB 2024)*, Springer Nature, vol. 113, p. 155, Aug. 2024. doi: 10.2991/978-94-6463-482-2_11

[37] N. Bacanin, A. Petrovic, M. Antonijevic, M. Zivkovic, M. Sarac, E. Tuba, and I. Strumberger, "Intrusion detection by XGBoost model tuned by improved social network search algorithm," in *Proc. Int. Conf. Modelling Dev. Intell. Syst.*, Cham, Switzerland: Springer Nature, Oct. 2022, pp. 104–121. doi: 10.1007/978-3-031-27034-5_7

[38] N. Savanović, A. Toskovic, A. Petrovic, M. Zivkovic, R. Damaševičius, L. Jovanovic, et al., "Intrusion detection in Healthcare 4.0 Internet of Things systems via metaheuristics optimized machine learning," *Sustainability*, vol. 15, p. 12563, 2023. doi: 10.3390/su151612563

[39] M. Zivkovic, L. Jovanovic, N. Bacanin, A. Petrovic, N. Savanovic, and M. Dobrojevic, "XGBoost tuned by hybridized SCA metaheuristics for intrusion detection in Healthcare 4.0 IoT systems," in *Proc. Int. Conf. Eng., Appl. Sci. Syst. Model.*, Singapore: Springer, Apr. 2017, pp. 1–16. doi: 10.1007/978-981-99-8438-1_1