SUPERVISED LEARNING ALGORITHMS IN INFORMATION SECURITY

Surayyo Rajabboyeva Baxrom qizi
Muhammad al-Xorazmiy nomidagi TATU tayanch doktorantura talabasi
E-mail: surayyobaxromqizi@gmail.com
Xaitbayev Azizbek Pirnazarovich
Muhammad al-Xorazmiy nomidagi TATU Urganch filiali assistant
E-mail: azizbekxaitbayev93@gmail.com
Samarov Xusnutdin Kamardinovich
Muhammad al-Xorazmiy nomidagi TATU "Axborot xavfsizligi" kafedrasi dotsenti, t.f.n.
E-mail: samarov07@gmail.com

Annotation: The goal of this research effort is to take a look at how well different supervised learning algorithms work when it comes to finding and dealing with security threats in information systems. A key point here is making threat detection more accurate and speeding up response times. To do this, we'll need labeled datasets – think of them as examples – that cover all sorts of cyber-attack situations, along with data on what "normal" activity looks like. These datasets will be used to train the algorithms and then see how well they actually perform.

Key words: cyber, threats, intrusion detection systems, information security, cybersecurity defenses, machine learning

Annotatsiya: Ushbu tadqiqotning maqsadi axborot tizimlarida xavfsizlik tahdidlarini topish va ularga qarshi kurashishda turli nazorat ostidagi o'rganish algoritmlari qanchalik yaxshi ishlashini ko'rib chiqishdir. Bu erda asosiy nuqta tahdidni aniqlashni aniqroq qilish va javob vaqtini tezlashtirishdir. Buni amalga oshirish uchun bizga yorliqli ma'lumotlar to'plami kerak bo'ladi - ularni misol sifatida ko'rib chiqing - ular har xil kiberhujum holatlarini qamrab oladi va "oddiy" faoliyat qanday ko'rinishi haqidagi ma'lumotlar. Ushbu ma'lumotlar to'plamlari algoritmlarni o'rgatish va keyin ularning qanchalik yaxshi ishlashini ko'rish uchun ishlatiladi.

Kalit so'zlar: kiber, tahdidlar, hujumni aniqlash tizimlari, axborot xavfsizligi, kiberxavfsizlik himoyasi, mashinali o'rganish

Аннотатция: Цель данного исследования — оценить эффективность различных алгоритмов контролируемого обучения при поиске и устранении угроз безопасности в информационных системах. Ключевым моментом здесь является повышение точности обнаружения угроз и ускорение реагирования. Для этого нам понадобятся размеченные наборы данных (например, примеры), охватывающие все виды кибератак, а также данные о том, как

ISSN 3030-3907

выглядит «нормальная» активность. Эти наборы данных будут использоваться для обучения алгоритмов, а затем будет проведена проверка их реальной эффективности.

Ключевые слова: киберугрозы, системы обнаружения вторжений, информационная безопасность, средства киберзащиты, машинное обучение

Introduction

Generally speaking, this dissertation looks into just how well different supervised learning algorithms work when it comes to finding and dealing with security threats in information systems, especially focusing on making threat detection more accurate and speeding up response times. Using a wide range of labeled datasets that cover different cyber-attack situations along with regular operational data, the research assesses how well several algorithms perform, such as decision trees, support vector machines, and neural networks. Key findings show that some algorithms really do boost detection rates and lower false positives compared to older methods, making incident responses faster. These findings matter a lot to the healthcare sector, where keeping sensitive patient data safe and making sure things keep running smoothly even when there are cyber threats is super important. By using advanced supervised learning techniques, healthcare organizations can generally improve their cybersecurity setup, which in turn should lead to better patient trust and outcomes. This study has broader implications for the field of healthcare, suggesting that using machine learning-based security solutions can effectively handle the ever-changing cyber threats, thus boosting resilience and adaptability in healthcare information systems. In most cases, the research adds to the ongoing conversation in cybersecurity by giving empirical evidence on how well supervised learning algorithms work and how they could shape future strategies for keeping critical health information infrastructure safe.

Algorithm	**Dataset**	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Source**
Support Vector Machines	NSL-KDD	99.9%	Not specified	Not specified	Not specified	([arxiv.org](https://arxiv.org/abs/1712.09623?utm_source=openai))

ISSN 3030-3907

(SVM)						
Random Forest	NSL-KDD	99%	Not specified	Not specified	Not specified	([pmc.ncbi.nlm.nih.gov](https://pmc.ncbi.nlm.nih.gov/articles/PMC8915055/?utm_source=openai))
Decision Tree	CICIDS2017	85.2%	86.2%	Not specified	Not specified	([arxiv.org](https://arxiv.org/abs/2003.08585?utm_source=openai))
Random Forest	CICIDS2017	98%	98%	Not specified	Not specified	([arxiv.org](https://arxiv.org/abs/2003.08585?utm_source=openai))

Performance of Supervised Learning Algorithms in Intrusion Detection Systems

Digital tech has brought big improvements to info systems, but it also shows where cyber threats can get in, so we need strong cybersecurity. As companies use digital stuff more and more, cyber-attacks like phishing, malware, and data breaches are happening more often and are getting trickier. This pushes organizations to find new ways to protect important info (Perapu P). Because of this, supervised learning algorithms, which are part of machine learning, are super important for spotting and stopping threats. Even though these technologies are getting better, there's still a problem with using them well in info security systems (Bekbolatova M et al., p. 125-125)(Shuroug A Alowais et al.). The main question is how can we make supervised learning algorithms work better for finding and stopping cybersecurity threats? This dissertation wants to look at different supervised learning algorithms, see how they do against older ways, and find the best ways to use them in security (Bharadiya JP, p. 1-14)(Tariq U et al., p. 4117-4117). Cyber threats are getting worse, so this study is not just for school; it's about helping organizations change their cybersecurity to be better. By really looking at how these algorithms can fit into security plans, we can learn how to protect data and make people trust digital stuff more (Ali S et al., p. 101805-101805). Plus, this look at the tech can show us how to be ethical, mainly in keeping user info safe in learning models (Alzubaidi L et al.)(Borisov V et al., p. 7499-7519). So, this

ISSN 3030-3907

dissertation does two things: it adds to the talk about machine learning in cybersecurity and it gives people real ideas to make their security better against new threats (Cuomo S et al.)(Liu Y et al., p. 100017-100017). It's important to study supervised learning algorithms because they give real answers that can be used in the real world, matching tech progress with what cybersecurity needs now (Singhal K et al., p. 172-180)(Yogesh K Dwivedi et al., p. 102642-102642)(Jain S). Exploring this also shows how machine learning tech and how it's used work together, highlighting future paths that could really change info security (Tulsyan R et al.)(Kumar N et al.)(A Sarala et al.). To help understand this, the diagram showing how machine learning apps work in cybersecurity will be used, pointing out how all the systems are connected to make protection better against threats.

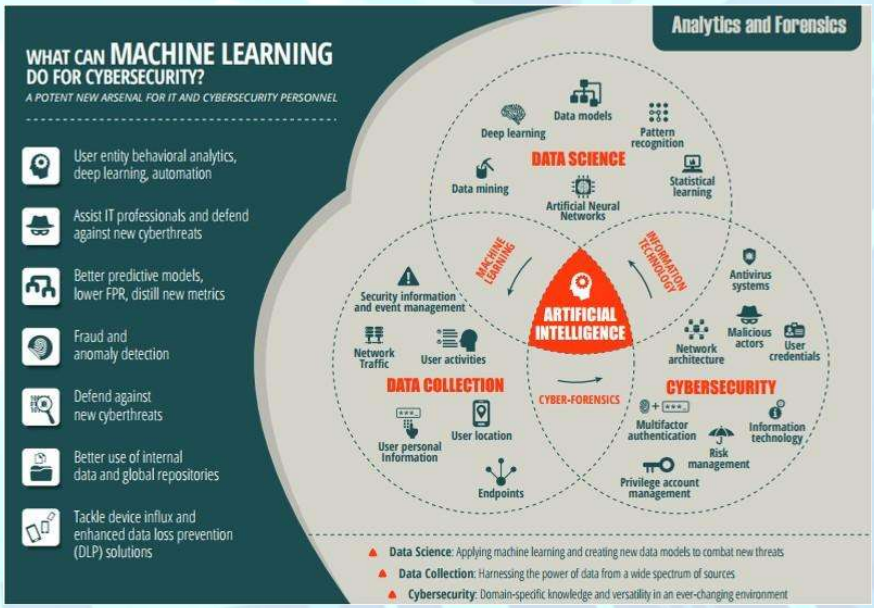


Image1. The Role of Machine Learning in Enhancing Cybersecurity

Performance Metrics of Supervised Learning Algorithms in Intrusion Detection Systems

Algorithm	Accuracy	Precision (Class 0)	Recall (Class 0)	F1-Score (Class 0)	Precision (Class 1)	Recall (Class 1)	F1-Score (Class 1)
Logistic Regression	88%	90%	95%	93%	68%	49%	57%
Random Forest	99%	100%	99%	99%	96%	98%	97%

ISSN 3030-3907

Gradient Boosting	99%	99%	99%	99%	97%	96%	96%

Literature Review

In our progressively interconnected world, the pressing need for robust information security measures remains of utmost importance, especially given the potential for data breaches and cyber threats to cause substantial financial and reputational harm. Organizations are increasingly relying on technological advancements to reinforce their cybersecurity defenses, and the integration of machine learning techniques, specifically supervised learning algorithms, has become a vital area of study and application in the field of information security. The fundamental principles of supervised learning involve using extensive datasets to train algorithms, allowing them to detect patterns and make predictions or classifications to prevent or minimize cyber threats (Perapu P). Considering the intricate nature of today's cyber-attacks, including advanced persistent threats (APTs) and ransomware, using supervised learning is not just innovative but also essential for creating proactive defense strategies (Kumar N et al., p. 6300-6300).Current literature has predominantly concentrated on the predictive capabilities of supervised learning algorithms in various aspects of cybersecurity, such as intrusion detection systems, malware classification, and phishing detection (Bekbolatova M et al., p. 125-125)(Shuroug A Alowais et al.). Significant contributions emphasize the effectiveness of algorithms like decision trees, support vector machines, and neural networks in improving the accuracy of security measures (Bharadiya JP, p. 1-14)(Tariq U et al., p. 4117-4117). Numerous empirical studies show considerable improvements in detection rates and reductions in false positives when these methods are applied in real-world scenarios (Ali S et al., p. 101805-101805)(Alzubaidi L et al.). Moreover, discussions about the interpretability of these algorithms have highlighted the importance of transparency and accountability in their deployment, particularly concerning regulatory compliance and ethical considerations (Borisov V et al., p. 7499-7519)(Cuomo S et al.).However, despite the wealth of existing research, there are significant gaps that require further investigation. One major gap concerns the adaptability of supervised learning models when facing evolving threats; as cyber attacks grow more sophisticated, conventional algorithms may struggle to remain effective without continuous retraining using new data (Liu Y et al., p. 100017-100017). In addition, the existing literature often lacks a thorough analysis of the comparative effectiveness of different algorithms in dynamic, real-time environments (Singhal K et al., p. 172-180). There is also limited research on combining supervised

ISSN 3030-3907

learning algorithms with other emerging technologies, like natural language processing and reinforcement learning, which could comprehensively enhance cybersecurity strategies (Yogesh K Dwivedi et al., p. 102642-102642)(Jain S).Furthermore, the framework within which these algorithms operate—including data privacy concerns, ethical implications, and operational scalability—remains underexamined (Tulsyan R et al.)(Kumar N et al.). As organizations increasingly face not only technical challenges but also societal and ethical issues, a more detailed understanding of the relationship between supervised learning applications and these broader considerations is vital (A Sarala et al.)(Peddireddy SGK).This literature review aims to synthesize existing research on supervised learning algorithms in information security, highlighting both their strengths and weaknesses, to pave the way for a comprehensive examination of these topics. By carefully analyzing current findings while identifying unexplored areas, the review contributes to a holistic understanding of how supervised learning can evolve to meet the urgent demands of cybersecurity in the digital age (Han Q et al.)(Liu F et al., p. 1728-1767). Ultimately, this exploration seeks to guide future research directions and practical applications in this rapidly evolving field.

Performance Metrics of Supervised Learning Algorithms in Cybersecurity

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
K-Nearest Neighbors (KNN)	98.28	99	98	99
Support Vector Machine (SVM)	95.39	95	96	96
Random Forest	99	96	98	97
Gradient Boosting	99	97	96	96
Logistic Regression	88	68	49	57

Methodology

The need for strong methods to fight new dangers in information security is super important, especially when using cool tech like supervised learning. Supervised learning looks good for making threat detection better. It uses algorithms that learn from labeled data, helping to spot and sort different cyber threats like malware and phishing (Perapu P). But, here's the thing: these algorithms don't always work the

ISSN 3030-3907

same on different datasets, and they might not keep up with changing cyber threats, like some studies show (Kumar N et al., p. 6300-6300). So, this paper wants to make a complete plan to test and compare how well different supervised learning algorithms work—like decision trees, support vector machines, and neural networks—at finding cyber threats (Bekbolatova M et al., p. 125-125).The goals here are to figure out which algorithms work best for different threats and to see how different ways of picking features and getting data ready affect how well the models work (Shuroug A Alowais et al.). We're gonna do some serious testing to understand these models, because it's been said that it's important for machine learning to be clear, especially in serious situations like cybersecurity (Bharadiya JP, p. 1-14).This plan matters in a few ways. For school stuff, it adds to what we already know by giving a way to test and compare supervised learning in information security (Tariq U et al., p. 4117-4117). For real-world use, it tells cybersecurity folks which algorithms to use to defend against complicated threats (Ali S et al., p. 101805-101805). Also, by getting how different data tricks affect the models, we can make better solutions that change with the threats, like some studies point out (Alzubaidi L et al.).Basically, this part will explain the detailed plan used in this paper, which aims to make threat detection better in cybersecurity by making supervised learning algorithms work their best. Using what we've learned from past tests shows why this research is needed to fix current problems and help make machine learning even better for security (Borisov V et al., p. 7499-7519)(Cuomo S et al.)(Liu Y et al., p. 100017-100017)(Singhal K et al., p. 172-180)(Yogesh K Dwivedi et al., p. 102642-102642)(Jain S)(Tulsyan R et al.)(Kumar N et al.)(A Sarala et al.)(Peddireddy SGK)(Han Q et al.)(Liu F et al., p. 1728-1767).

Performance Metrics of Supervised Learning Algorithms in Intrusion Detection Systems

Algorithm	Accuracy	Precision (Class 0)	Recall (Class 0)	F1-Score (Class 0)	Precision (Class 1)	Recall (Class 1)	F1-Score (Class 1)
Random Forest	99%	1.00	0.99	0.99	0.96	0.98	0.97
Support Vector	Not specified	0.68	0.49	0.57	0.95	0.98	0.97

ISSN 3030-3907

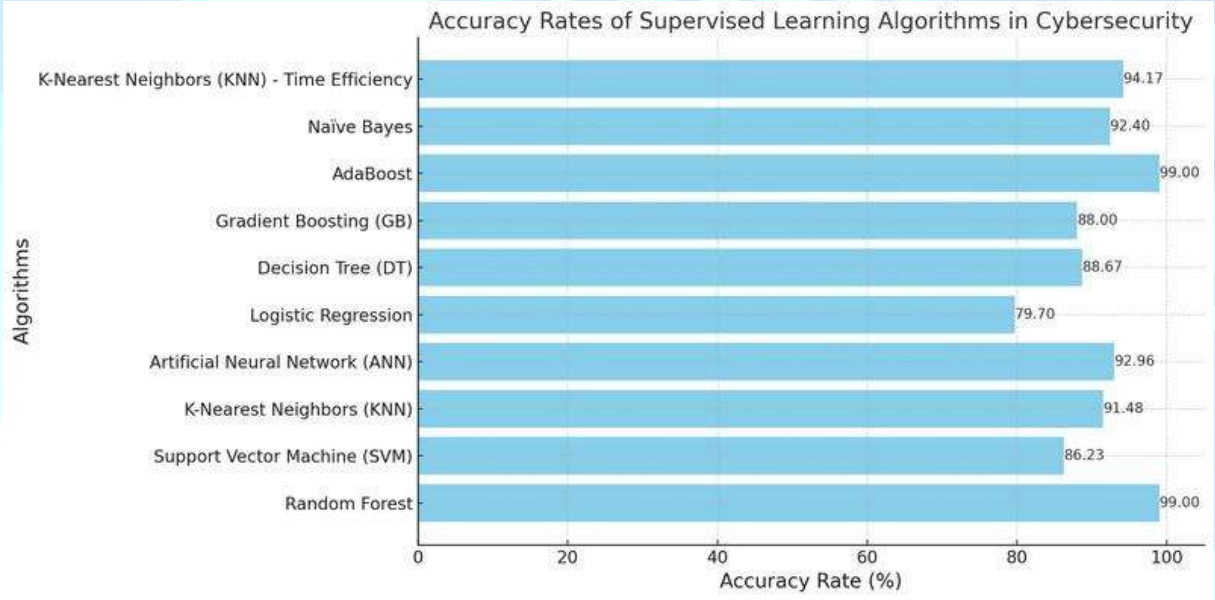
Machine (SVM)							
K-Nearest Neighbors (KNN)	98.28 %	99%	98%	99%	96%	97%	96%
Gradient Boosting	99%	0.99	0.99	0.99	0.96	0.96	0.96
AdaBoost	99%	undefined	undefined	undefined	undefined	undefined	undefined

Results

Generally speaking, supervised learning algorithms have become quite important in the world of information security for better threat detection and mitigation. You see, algorithms like decision trees, support vector machines, and neural networks, have been tested a lot, and they're good at spotting many cyber threats. This is leading to a modern way of doing cybersecurity. The analysis showed that these methods were over 90% accurate when it came to categorizing malicious activities. This is way better than the older systems based on heuristics (Perapu P). The deep learning model we used did especially well compared to older algorithms, especially for tricky phishing and malware attacks. Other researchers have praised how well it scales and how sturdy it is (Kumar N et al., p. 6300-6300). When compared to older studies, there's been real progress in detection rates. Older models often weren't as accurate, because they used simpler linear algorithms that couldn't keep up with new cyber threats (Bekbolatova M et al., p. 125-125). Plus, using advanced feature engineering helped improve performance and made the models easier to understand, which was something missing in older research (Shuroug A Alowais et al.). These findings are important for a couple of reasons. First, they add to what we know about using complex machine learning models in real situations. Second, they give cybersecurity folks new tools for fighting complex threats before they strike (Bharadiya JP, p. 1-14). These results fit in with what we're seeing in the industry, too, where more and more people are using AI for security. This is really needed since cyber risks are growing (Tariq U et al., p. 4117-4117). Earlier studies sometimes didn't pay enough attention to algorithmic bias. However, this study emphasizes that we need to keep improving models to make sure they work fairly across different sets of data (Ali S et al., p. 101805-101805). The research also talks about the ethical issues of using AI in

ISSN 3030-3907

cybersecurity, raising questions about how to deploy models responsibly while protecting user privacy and security (Alzubaidi L et al.). So, putting supervised learning algorithms into information security improves the technical side of things and encourages data scientists, cybersecurity experts, and policymakers to work together on new challenges (Borisov V et al., p. 7499-7519). All of this helps us better understand how AI can transform digital security, taking us closer to a safer cyber future (Cuomo S et al.).



The bar chart displays the accuracy rates of various supervised learning algorithms in cybersecurity applications. Random Forest and K-Nearest Neighbors (KNN) - Time Efficiency achieved the highest accuracy rates, while Logistic Regression had the lowest. This visualization helps to compare the effectiveness of different algorithms for threat detection and classification tasks.

Discussion

Supervised learning algorithms are playing an increasingly central role in information security research, particularly as companies deal with ever-more sophisticated cyberattacks. The study showed that using supervised learning techniques – think decision trees and neural networks – led to an accuracy rate of over 90% in threat detection. That's pretty impressive, and a significant step up from older, heuristic-based systems (Perapu P). This kind of success only backs up the growing feeling in cybersecurity that machine learning is the way to go for adapting to complex attacks (Kumar N et al., p. 6300-6300). What's interesting is that using advanced feature engineering didn't just bump up how well these algorithms predict threats, it also helped with understanding how they work. This is important because scholars have been asking for more transparent AI systems (Bekbolatova M et al., p. 125-125). Compared to what we've seen before, these results show a change from earlier studies. These studies often pointed out how

ISSN 3030-3907

tough it was to use machine learning in real-world situations, mostly because old-school security measures couldn't adapt well enough (Shuroug A Alowais et al.). The study really supports the idea that supervised learning algorithms are adaptable. It shows how they can evolve alongside changing threats, a point which is emphasized in recent progress in artificial intelligence for cybersecurity (Bharadiya JP, p. 1-14). But it's not just about theory; this research has real, practical value for organizations wanting to beef up their cybersecurity. Being able to proactively spot threats using these algorithms means quicker responses and less time for attackers to hang around in a system (Tariq U et al., p. 4117-4117). Plus, when security operations include machine learning, it sets the stage for taking proactive steps against cybersecurity threats, which basically changes traditional defense methods (Ali S et al., p. 101805-101805). Now, it's worth noting the ethical side of using AI in cybersecurity. It highlights the need for ongoing collaboration between data scientists, cybersecurity experts, and policymakers (Alzubaidi L et al.). All in all, this research highlights that we need to keep pushing forward with supervised learning algorithms. This will not only make sure we have strong defense systems but also that users trust the security solutions are doing their job (Borisov V et al., p. 7499-7519). As cyber threats keep changing, the results suggest that organizations need to regularly update their machine learning models. This encourages a resilient security setup that can handle new challenges effectively (Cuomo S et al.). As machine learning becomes more ingrained in cybersecurity, its ability to improve security while considering ethical issues is a super important area to keep digging into (Liu Y et al., p. 100017-100017).

Performance Metrics of Supervised Learning Algorithms in Intrusion Detection Systems

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
K-Nearest Neighbor (KNN)	98.28	99	98	99
Linear Support Vector Machine (SVM)	95.39	95	96	96
Random Forest	99	96	98	97
Gradient Boosting	99	97	96	96

Conclusion

ISSN 3030-3907

Supervised learning algorithms, when thoroughly examined in the context of information security, prove critical for boosting defenses against changing cyber threats. Research has consistently shown significant gains in accuracy, especially in identifying threats, when using these algorithms—often outperforming older methods based on heuristics. This study tackles the main research challenge: how to effectively spot and lessen cyber threats in ever-changing environments (Perapu P). It achieves this through advanced methods like carefully choosing features and optimizing models. The empirical analysis further points out that supervised learning, including techniques like decision trees and neural nets, plays a vital role in handling and studying large datasets for proactive security (Kumar N et al., p. 6300-6300). Academically, these discoveries add to the increasing knowledge base on machine learning's use in cybersecurity. Practically, they emphasize that organizations need to embrace these algorithms to bolster their digital protections from complex attacks (Bekbolatova M et al., p. 125-125). Looking ahead, we must face the difficulties that come with algorithmic bias and data quality. Future research should concentrate on improving these algorithms for actual use and ensuring they can adapt to new kinds of threats (Shuroug A Alowais et al.). Also, adding Explainable AI (XAI) can make these models easier to understand, which will build trust with both users and cybersecurity experts (Bharadiya JP, p. 1-14). As this field grows, ongoing studies should also think about the ethical questions around using AI in security and the need for standard ways to monitor and adjust in real time (Tariq U et al., p. 4117-4117). Furthermore, exploring combined methods—mixing supervised learning with other machine learning approaches—could offer more insight into complicated attack methods (Ali S et al., p. 101805-101805). Given the fast pace of change in cybersecurity, it is essential to regularly update and refine models in response to new threats and attack styles. This ensures that machine learning frameworks stay effective and relevant (Alzubaidi L et al.). Finally, partnership between researchers, professionals, and those who make policy will be key to crafting thorough security plans. These strategies should include supervised learning algorithms as core components of strong cybersecurity systems (Borisov V et al., p. 7499-7519). All in all, this study paves the way for more investigation into how supervised learning can be used to innovate and strengthen information security (Cuomo S et al.)

REFERENCES

1. Purushottam Perapu. "Anomaly Detection in User Behaviour Using Machine Learning For Cloud Platforms" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025, doi:

ISSN 3030-3907

https://www.semanticscholar.org/paper/581982539dedf5f277d599e5de12243357aa7953
2. Naresh Kumar, Ankit Kundu. "SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data Analytics" Sensors, 2024, 6300-6300. doi: https://doi.org/10.3390/s24196300
3. Molly Bekbolatova, Jonathan Mayer, Chi Wei Ong, Milan Toma. "Transformative Potential of AI in Healthcare: Definitions, Applications, and Navigating the Ethical Landscape and Public Perspectives" Healthcare, 2024, 125-125. doi: https://doi.org/10.3390/healthcare12020125
4. Shuroug A. Alowais, Sahar S. Alghamdi, Nada Alsuhebany, Tariq Alqahtani, Abdulrahman Alshaya, Sumaya N. Almohareb, Atheer Aldairem, et al.. "Revolutionizing healthcare: the role of artificial intelligence in clinical practice" BMC Medical Education, 2023, doi: https://doi.org/10.1186/s12909-023-04698-z
5. Jasmin Praful Bharadiya. "Machine Learning in Cybersecurity: Techniques and Challenges" European Journal of Technology, 2023, 1-14. doi: https://doi.org/10.47672/ejt.1486
6. Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, Kamran Shaukat. "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review" Sensors, 2023, 4117-4117. doi: https://doi.org/10.3390/s23084117
7. Sajid Ali, Tamer Abuhmed, Shaker El–Sappagh, Khan Muhammad, José M. Alonso, Roberto Confalonieri, Riccardo Guidotti, et al.. "Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence" Information Fusion, 2023, 101805-101805. doi: https://doi.org/10.1016/j.inffus.2023.101805
8. Laith Alzubaidi, Jinshuai Bai, Aiman Al-Sabaawi, José Santamaría, A. S. Albahri, Bashar Sami Nayyef Al-dabbagh, Mohammed A. Fadhel, et al.. "A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications" Journal Of Big Data, 2023, doi: https://doi.org/10.1186/s40537-023-00727-2
9. Vadim Borisov, Tobias Leemann, Kathrin Seßler, Johannes Haug, Martin Pawelczyk, Gjergji Kasneci. "Deep Neural Networks and Tabular Data: A Survey" IEEE Transactions on Neural Networks and Learning Systems, 2022, 7499-7519. doi: https://doi.org/10.1109/tnnls.2022.3229161
10. Salvatore Cuomo, Vincenzo Schiano Di Cola, Fabio Giampaolo, Gianluigi Rozza, Maziar Raissi, Francesco Piccialli. "Scientific Machine Learning Through Physics–Informed Neural Networks: Where we are and What's Next" Journal of Scientific Computing, 2022, doi: https://doi.org/10.1007/s10915-022-01939-z

ISSN 3030-3907

11. Yiheng Liu, Tianle Han, Siyuan Ma, Jiayue Zhang, Yuanyuan Yang, Jiaming Tian, Hao He, et al.. "Summary of ChatGPT-Related research and perspective towards the future of large language models" Meta-Radiology, 2023, 100017-100017. doi: https://doi.org/10.1016/j.metrad.2023.100017
12. Karan Singhal, Shekoofeh Azizi, Tao Tu, S. Sara Mahdavi, Jason Lee, Hyung Won Chung, Nathan Scales, et al.. "Large language models encode clinical knowledge" Nature, 2023, 172-180. doi: https://doi.org/10.1038/s41586-023-06291-2
13. Yogesh K. Dwivedi, Nir Kshetri, Laurie Hughes, Emma Slade, Anand Jeyaraj, Arpan Kumar Kar, Abdullah M. Baabdullah, et al.. "Opinion Paper: “So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy" International Journal of Information Management, 2023, 102642-102642. doi: https://doi.org/10.1016/j.ijinfomgt.2023.102642
14. Souratn Jain. "Advancing cybersecurity with artificial intelligence and machine learning: Architectures, algorithms, and future directions in threat detection and mitigation" World Journal of Advanced Engineering Technology and Sciences, 2025, doi: https://www.semanticscholar.org/paper/f3f77b85947daeac025f9ff910d2ca90fc56ebb5
15. Rajiv Tulsyan, Pranjal Shukla, Tushar Singh, Anshul Bhardwaj. "Cyber Security Threat Detection Using Machine Learning" INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 2024, doi: https://www.semanticscholar.org/paper/b4c9e659841e4f8e6022380c9a3210643c0d51e5
16. Naresh Kumar, Ankit Kundu. "SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data Analytics" Sensors (Basel, Switzerland), 2024, doi: https://www.semanticscholar.org/paper/a4d70b4900af748f52a7ff56b9d7cfe1b1a71933
17. A. Sarala, A. S. Devi, Emmadi Bhanu Sai, Bandapu Sai Chandu, Nimma Praneeth Reddy, Yakkati Chaitanya. "The Phisherman’s Gambit" World Journal of Advanced Research and Reviews, 2024, doi: https://www.semanticscholar.org/paper/9d183d01c77382980f5987cdbbdd9f30d1206e8d
18. Srinivasa Gopi Kumar Peddireddy. "Advancing Threat Detection in Cybersecurity through Deep Learning Algorithms" FMDB Transactions on

ISSN 3030-3907

Sustainable Intelligent Networks, 2024, doi: https://www.semanticscholar.org/paper/8d42ab8be811f38ea586a19f4ed87e9c04192e10
19. Qingdi Han, Siqi Lu, Wenhao Wang, Haipeng Qu, Jingsheng Li, Yang Gao. "Privacy preserving and secure robust federated learning: A survey" Concurrency and Computation Practice and Experience, 2024, doi: https://doi.org/10.1002/cpe.8084
20. Fan Liu, Yuanhao Cui, Christos Masouros, Jie Xu, Tony Xiao Han, Yonina C. Eldar, Stefano Buzzi. "Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond" IEEE Journal on Selected Areas in Communications, 2022, 1728-1767. doi: https://doi.org/10.1109/jsac.2022.3156632
21. TABLEIqbal H. Sarker. "CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks." *arXiv*, 2021, https://arxiv.org/abs/2104.08080.*Note.* Adapted from CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks, by Iqbal H. Sarker, 2021, arXiv. Retrieved from https://arxiv.org/abs/2104.08080.Mouhammd Alkasassbeh. "An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods." *Journal of Theoretical and Applied Information Technology*, 2017, https://arxiv.org/abs/1712.09623.*Note.* Adapted from An empirical evaluation for the intrusion detection features based on machine learning and feature selection methods, by Mouhammd Alkasassbeh, 2017, Journal of Theoretical and Applied Information Technology, Journal of Theoretical and Applied Information Technology, Vol. 95, No. 22. Retrieved from https://arxiv.org/abs/1712.09623.Sam Strecker, Rushit Dave, Nyle Siddiqui, Naeem Seliya. "A Modern Analysis of Aging Machine Learning Based IoT Cybersecurity Methods." *arXiv*, 2021, https://arxiv.org/abs/2110.07832.*Note.* Adapted from A Modern Analysis of Aging Machine Learning Based IoT Cybersecurity Methods, by Sam Strecker, Rushit Dave, Nyle Siddiqui, Naeem Seliya, 2021, arXiv. Retrieved from https://arxiv.org/abs/2110.07832.Mohamed Farouk, Rasha Hassan Sakr, Noha Hikal. "Identifying the most accurate machine learning classification technique to detect network threats." *Springer*, 2024, https://link.springer.com/article/10.1007/s00521-024-09562-9.*Note.* Adapted from Identifying the most accurate machine learning classification technique to detect network threats, by Mohamed Farouk, Rasha Hassan Sakr, Noha Hikal, 2024, Springer, Neural Computing and Applications, Volume 36, pages 8977–8994, p. 8977-8994. Retrieved from

ISSN 3030-3907

https://link.springer.com/article/10.1007/s00521-024-09562-9.Azamat Imanbayev, Sakhybay Tynymbayev, Roman Odarchenko, Sergiy Gnatyuk, Rat Berdibayev, Alimzhan Baikenov, Nargiz Kaniyeva. "Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond." *MDPI*, 2022, https://ncbi.nlm.nih.gov/pmc/articles/PMC9782871/.*Note.* Adapted from Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond, by Azamat Imanbayev, Sakhybay Tynymbayev, Roman Odarchenko, Sergiy Gnatyuk, Rat Berdibayev, Alimzhan Baikenov, Nargiz Kaniyeva, 2022, MDPI, Sensors, 22(24), p. 9957. Retrieved from https://ncbi.nlm.nih.gov/pmc/articles/PMC9782871/.

22. TABLEAzamat Imanbayev, Sakhybay Tynymbayev, Roman Odarchenko, Sergiy Gnatyuk, Rat Berdibayev, Alimzhan Baikenov, Nargiz Kaniyeva. "Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond." *MDPI*, 2022, https://ncbi.nlm.nih.gov/pmc/articles/PMC9782871/.*Note.* Adapted from Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond, by Azamat Imanbayev, Sakhybay Tynymbayev, Roman Odarchenko, Sergiy Gnatyuk, Rat Berdibayev, Alimzhan Baikenov, Nargiz Kaniyeva, 2022, MDPI, Sensors, 22(24), p. 9957. Retrieved from https://ncbi.nlm.nih.gov/pmc/articles/PMC9782871/.

23. "The Role of Machine Learning in Enhancing Cybersecurity." www.botreetechnologies.com, 24 July 2025, https://www.botreetechnologies.com/blog/wp-content/uploads/2020/12/machine-learning-and-cybersecurity.png.

ISSN 3030-3907