

International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

Artificial Intelligence-Driven Cybersecurity: A Review of Machine Learning Approaches for Threat Detection and Prevention

Aruna Kumari P

Research Scholar, Sabarmati University, Ahmedabad

Dr. Pankaj Khairnar

Research Guide, Sabarmati University, Ahmedabad

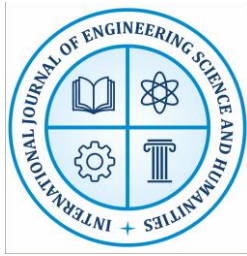
Abstract

Cyber attacks have become more frequent, more automated and more difficult to recognise, and the signature-based tools that have long protected networks struggle to keep pace with new and changing threats. Artificial intelligence (AI), and machine learning (ML) in particular, has therefore attracted wide interest as a way to detect and prevent attacks by learning patterns of malicious behaviour from data. It examines the main families of learning techniques and how they are applied; the use of classical and deep models for network intrusion detection; ML-based detection of malware and phishing; and the benchmark datasets, evaluation practices and open challenges that shape the field. The review finds that ensemble methods and deep architectures such as recurrent networks and auto-encoders generally outperform traditional classifiers on benchmark data, and that hybrid models are increasingly common. However, it also finds recurring weaknesses: dependence on outdated or imbalanced datasets, inconsistent evaluation, high false-alarm rates in practice, limited interpretability and vulnerability to adversarial manipulation. The paper concludes that AI is a powerful complement to, rather than a replacement for, conventional defences, and it outlines future research directions in realistic datasets, explainable and adversarially robust models, continual learning and automated response.

Keywords: artificial intelligence; cybersecurity; machine learning; deep learning; intrusion detection; malware detection; threat prevention

1.1. Introduction

Cybersecurity refers to the technologies, processes and practices that protect computer systems, networks and data from unauthorised access, damage and disruption. As governments, businesses and individuals have moved more of their activities online, the amount of valuable information stored and transmitted digitally has grown enormously, and so has the incentive to attack it. Organisations now face threats ranging from opportunistic malware and phishing campaigns to carefully planned intrusions by well-resourced groups. Traditional defences such as firewalls, access control and antivirus software remain essential, but most of them depend on



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

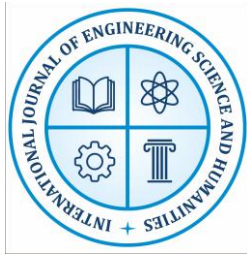
rules or signatures written by human experts. Such tools work well against known threats but are slow to respond to new attack variants, and they can be bypassed by attackers who make small changes to their code or behaviour (Buczak & Guven, 2016; Khraisat et al., 2019).

The threat landscape has changed in scale, speed and complexity. Attack tools are widely available, many attacks are fully automated, and malware authors routinely use packing, encryption and polymorphism to avoid detection. Distributed denial-of-service attacks, botnets, ransomware and credential-stealing phishing sites appear and disappear rapidly, while advanced intrusions may remain hidden for long periods. At the same time, the growth of cloud services, mobile devices and the Internet of Things has enlarged the attack surface and increased the volume of network traffic that must be monitored. Security teams therefore face more events than they can inspect by hand, and many of the alerts they receive are false alarms (Sarker et al., 2020). These conditions have created a strong need for automated, adaptive methods that can separate genuine threats from normal activity with little human effort.

1.2 Artificial Intelligence and Machine Learning in Cybersecurity

AI is a broad field concerned with building systems that perform tasks normally requiring human intelligence. Machine learning, a branch of AI, allows a system to learn patterns from data and to make predictions without being explicitly programmed for each case. In cybersecurity, supervised ML models learn to classify network flows, files, URLs or user actions as benign or malicious from labelled examples; unsupervised models learn what normal behaviour looks like and flag deviations; and deep learning models, built from many layers of artificial neurons, learn useful features directly from raw or lightly processed data (Xin et al., 2018). Because these models generalise from examples, they can recognise new variants of known attacks and, in some cases, previously unseen attacks. Reviews show that ML and DL are now applied to intrusion detection, malware analysis, spam and phishing filtering, fraud detection and user behaviour analytics (Berman et al., 2019; Sarker et al., 2020).

This paper reviews research published between 2014 and 2022 on the use of ML and DL for detecting and preventing cyber threats. It focuses on network intrusion detection, which has the largest body of literature, and also considers malware and phishing detection, which are among the most common threats faced by organisations. The review is organised as follows. Section 2 presents the literature review in four parts: an overview of ML and DL techniques used in cybersecurity; ML-based intrusion detection; ML-based malware and phishing detection; and benchmark datasets, evaluation practices and challenges. Three tables summarise the techniques, representative studies and datasets. Section 3 draws conclusions from the review, and Section 4 outlines directions for future work.



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

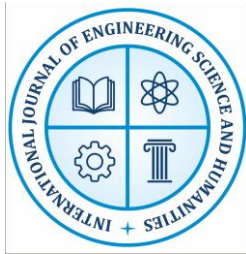
2. Literature Review

2.1 Overview of Machine Learning and Deep Learning Techniques in Cybersecurity

Early surveys established the foundations for applying learning techniques to security problems. Buczak and Guven (2016) reviewed data-mining and ML methods for cyber intrusion detection and grouped them into misuse detection, which matches known attack patterns, and anomaly detection, which models normal behaviour and flags deviations. They examined methods such as artificial neural networks, Bayesian networks, clustering, decision trees, ensemble learning, evolutionary computation, hidden Markov models and support vector machines (SVMs), and they stressed that the choice of method depends on the type of data, the need for interpretability and the cost of training and updating the model. Xin et al. (2018) extended this work to include deep learning and observed that DL methods had begun to outperform shallow learners on several network security tasks, especially when large volumes of data were available.

Deep learning brought new architectures into the field. Berman et al. (2019) surveyed DL methods for cybersecurity, including deep belief networks, auto-encoders, convolutional neural networks (CNNs), recurrent neural networks (RNNs) and generative adversarial networks, and showed how each had been applied to intrusion detection, malware analysis, spam and domain-generation-algorithm detection. Sarker et al. (2020) placed these methods within a broader “cybersecurity data science” framework in which data collection, feature engineering, model building and decision-making are combined to produce intelligent, data-driven security services. Not all evaluations were favourable, however. Apruzzese et al. (2018) tested a range of ML and DL algorithms on intrusion, malware and spam detection and concluded that their performance was not yet sufficient for fully autonomous use: models often produced too many false positives, were sensitive to changes in data and were vulnerable to evasion. Table 1 summarises the main technique families discussed in this literature.

The literature also distinguishes techniques by the kind of supervision they require. Supervised learning is the most common choice because labelled benchmark datasets are widely available, and it usually gives the highest accuracy on attack types seen during training. Its weakness is that labels for real traffic are expensive to obtain and quickly become outdated. Unsupervised and semi-supervised methods reduce the need for labels by modelling normal activity and treating unusual events as suspicious, which makes them attractive for detecting zero-day attacks, although they generally produce more false alarms (Buczak & Guven, 2016; Khraisat et al., 2019). Hybrid designs that use unsupervised learning for feature extraction and supervised learning for classification attempt to combine the benefits of both, and they appear repeatedly in the studies reviewed in the following sections (Liu & Lang, 2019).



International Journal of Engineering, Science and Humanities

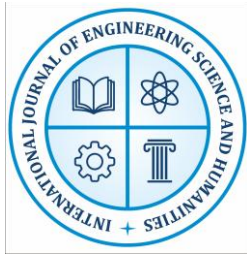
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

Table 1. Main machine learning and deep learning techniques used in cybersecurity

Technique	Learning type	Typical security applications	Strengths	Limitations
Decision tree	Supervised	Intrusion and malware classification	Fast; easy to interpret	Prone to overfitting
Random forest / gradient boosting	Supervised (ensemble)	Intrusion detection; phishing URL classification	High accuracy on tabular data; robust	Less interpretable; larger models
Support vector machine	Supervised	Intrusion detection; spam filtering	Effective in high-dimensional spaces	Slow to train on very large datasets
k-nearest neighbour	Supervised (instance-based)	Anomaly and intrusion detection	Simple; no training phase	Slow prediction; sensitive to scaling
Naïve Bayes	Supervised (probabilistic)	Spam and phishing filtering	Very fast; needs little data	Assumes feature independence
Clustering (e.g. k-means)	Unsupervised	Anomaly detection; grouping malware families	Needs no labels	Higher false-alarm rates
Auto-encoder	Unsupervised / deep	Anomaly-based intrusion detection; feature reduction	Learns normal behaviour without labels	Threshold setting is difficult
Convolutional neural network	Supervised / deep	Malware binary and traffic classification	Learns local patterns automatically	Needs large labelled datasets
Recurrent neural network / LSTM	Supervised / deep	Sequential traffic, logs and system calls	Captures temporal dependencies	Slower training; less interpretable

2.2 Machine Learning for Network Intrusion Detection

Network intrusion detection systems (IDS) monitor traffic to identify malicious activity and are the most widely studied application of ML in cybersecurity. Khraisat et al. (2019) classified IDS into signature-based systems, which are precise but cannot detect zero-day attacks, and anomaly-



International Journal of Engineering, Science and Humanities

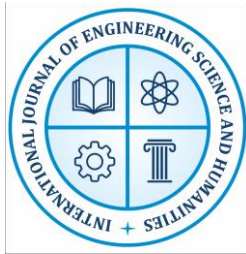
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

based systems, which can detect new attacks but tend to generate more false alarms; they argued that hybrid approaches combining the two offer the best balance. Liu and Lang (2019) proposed a taxonomy of ML and DL intrusion detection methods based on the type of data analysed, such as packets, flows, sessions and logs, and noted that DL models are well suited to raw or sequential data, while shallow models depend heavily on hand-crafted features.

Several studies demonstrated the benefits of deep architectures. Yin et al. (2017) applied an RNN to the NSL-KDD dataset and reported better binary and multi-class accuracy than traditional methods such as J48, artificial neural networks, random forest and SVM. Shone et al. (2018) proposed a non-symmetric deep auto-encoder for unsupervised feature learning, stacked and combined with a random forest classifier, and showed that it achieved strong accuracy on KDD Cup '99 and NSL-KDD while reducing training time compared with a deep belief network. Vinayakumar et al. (2019) evaluated deep neural networks on several public datasets, including KDD Cup '99, NSL-KDD, UNSW-NB15 and CICIDS2017, and proposed a scalable hybrid framework for monitoring network and host-level events in real time. Ferrag et al. (2020) compared seven DL models on the CSE-CIC-IDS2018 and Bot-IoT datasets and found that performance differed considerably by attack type, underlining the need for per-class evaluation.

Classical ML has also continued to improve, particularly through feature selection and ensembles. Kasongo and Sun (2020) used an XGBoost-based feature-selection method on the UNSW-NB15 dataset and showed that a reduced feature set improved the accuracy of several classifiers, including decision trees. For real-time and resource-constrained settings, Mirsky et al. (2018) introduced Kitsune, an online, unsupervised IDS that uses an ensemble of small auto-encoders to detect attacks on local networks and can run efficiently on low-power hardware. Ahmad et al. (2021) systematically reviewed ML and DL intrusion detection studies and concluded that, although DL methods often achieve higher accuracy, many studies rely on old datasets and pay little attention to class imbalance and computational cost. Table 2 summarises representative studies.

Taken together, these studies reveal several trends. Over time, research has shifted from single shallow classifiers towards ensembles and deep or hybrid architectures, and from older datasets such as KDD Cup '99 towards more recent ones such as UNSW-NB15 and CICIDS2017. Feature engineering remains important even for deep models, because removing irrelevant or redundant features reduces training time and can improve accuracy (Kasongo & Sun, 2020). There is also growing interest in practical requirements such as online learning, low computational cost and real-time operation (Mirsky et al., 2018; Vinayakumar et al., 2019). Nevertheless, results reported by different studies are difficult to compare directly, because they use different datasets, data splits, pre-processing steps and metrics, a problem highlighted by several reviewers (Ahmad et al., 2021; Ring et al., 2019).



International Journal of Engineering, Science and Humanities

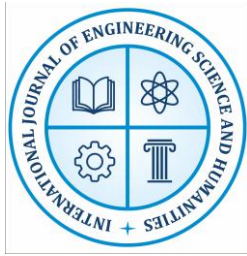
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

Table 2. Summary of representative studies on AI-based threat detection

Study	Approach	Dataset(s)	Main contribution / finding
Saxe & Berlin (2015)	Deep neural network on static binary features	Windows executables	Accurate malware detection at a low false-positive rate without dynamic analysis
Yin et al. (2017)	Recurrent neural network	NSL-KDD	Outperformed traditional classifiers in binary and multi-class detection
Shone et al. (2018)	Non-symmetric deep auto-encoder + random forest	KDD Cup '99, NSL-KDD	High accuracy with reduced training time
Mirsky et al. (2018)	Ensemble of auto-encoders (Kitsune)	Network traffic captures	Online, unsupervised detection suitable for low-power devices
Sahingoz et al. (2019)	Seven classifiers with NLP-based URL features	Phishing and legitimate URLs	Random forest gave the best phishing detection results
Vinayakumar et al. (2019)	Deep neural network; scalable hybrid framework	KDD Cup '99, NSL-KDD, UNSW-NB15, CICIDS2017 and others	DNNs performed well across datasets; real-time monitoring framework
Ferrag et al. (2020)	Seven deep learning models	CSE-CIC-IDS2018, Bot-IoT	Performance varied by attack class; comparative benchmark of DL models
Kasongo & Sun (2020)	XGBoost feature selection + classical classifiers	UNSW-NB15	Reduced feature set improved classifier accuracy

2.3 Machine Learning for Malware and Phishing Detection

Malware detection has traditionally relied on signatures extracted from known samples, an approach easily defeated by code obfuscation. ML offers an alternative by learning from features that describe a file's structure or behaviour. Static analysis examines features such as byte



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

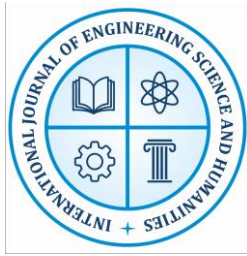
sequences, imported functions and file headers without running the program, while dynamic analysis records behaviour such as system calls and network activity in a controlled environment. Saxe and Berlin (2015) showed that a deep neural network trained on static features extracted from Windows executables could detect malware accurately while keeping false positives low, demonstrating that large-scale, signature-free detection was practical. Berman et al. (2019) reported that CNNs and RNNs have since been widely used to classify malware from binary images, opcode sequences and API call traces, often outperforming methods based on manual feature engineering.

Phishing, which tricks users into revealing credentials or installing malware, is another major target for ML. Because phishing websites are short-lived, blacklists quickly become outdated. Sahingoz et al. (2019) proposed a real-time phishing detection system that analyses URLs using natural language processing features and compared seven classification algorithms; random forest produced the best results, and the system did not depend on third-party services. Other studies reviewed by Sarker et al. (2020) used features from page content, e-mail text and domain information. Across malware and phishing research, a common finding is that ML improves detection of new variants, but models must be retrained frequently because attackers adapt quickly (Apruzzese et al., 2018).

ML has also been applied to other threats that combine features of malware and network intrusion. Botnets, which use networks of compromised machines to send spam or launch denial-of-service attacks, can be identified from the regular communication patterns between infected hosts and their command servers. Ransomware can often be detected from its behaviour, such as rapid file encryption or unusual access to many files, before it completes its attack. Insider threats and compromised accounts can be detected by modelling normal user behaviour and flagging unusual logins or data access (Sarker et al., 2020; Xin et al., 2018). These applications show that the same core learning techniques can be adapted to many security problems, provided that suitable data and features are available, and they suggest that combining network, host and user-level evidence is likely to give stronger protection than any single source (Berman et al., 2019).

2.4 Datasets, Evaluation Practices and Challenges

The quality of ML-based security systems depends heavily on the data used to train and test them. Older datasets such as KDD Cup '99 and its improved version NSL-KDD are still widely used but do not reflect modern traffic. Moustafa and Slay (2015) created UNSW-NB15, which combines realistic normal traffic with nine families of modern attacks. Sharafaldin et al. (2018) produced the CICIDS2017 dataset, which models realistic user behaviour and includes attacks such as brute force, denial of service, web attacks, infiltration and botnets, with flow features extracted by the CICFlowMeter tool. Ring et al. (2019) surveyed a large number of network-



International Journal of Engineering, Science and Humanities

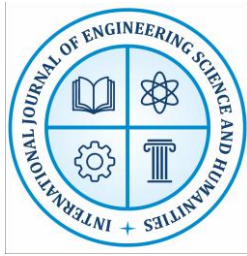
An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

based intrusion detection datasets, compared their properties and recommended that researchers evaluate models on more than one dataset, since each has particular strengths and weaknesses. Table 3 summarises commonly used datasets.

Table 3. Commonly used benchmark datasets for AI-based threat detection

Dataset	Year released	Main attack types	Remarks
KDD Cup '99	1999	DoS, probe, R2L, U2R	Historic benchmark; many duplicate records
NSL-KDD	2009	DoS, probe, R2L, U2R	Duplicates removed; still dated traffic
UNSW-NB15	2015	Nine families, e.g. exploits, fuzzers, backdoors, worms	Modern synthetic attacks with realistic normal traffic (Moustafa & Slay, 2015)
CICIDS2017	2017	Brute force, DoS/DDoS, web attacks, infiltration, botnet	Realistic user profiles; flow-based features (Sharafaldin et al., 2018)
CSE-CIC-IDS2018	2018	Similar to CICIDS2017 at larger scale	Large, cloud-based capture; used by Ferrag et al. (2020)
Bot-IoT	2019	DDoS, DoS, reconnaissance, data theft in IoT	Focus on IoT and botnet traffic; highly imbalanced

Evaluation practices also raise concerns. Many security datasets are highly imbalanced, with normal traffic far outnumbering attacks and some attack types extremely rare. Under these conditions, overall accuracy can be misleading, and the literature increasingly recommends reporting precision, recall, F1-score, false-positive and false-negative rates for each class (Ahmad et al., 2021; Ferrag et al., 2020). Beyond the data, several challenges limit the practical use of AI-based defences. Models trained in the laboratory may perform worse on live networks because traffic patterns change over time, a problem known as concept drift. Many DL models are difficult to interpret, which makes it hard for analysts to trust or explain their decisions. Most importantly, ML models can themselves be attacked. Papernot et al. (2018) systematised the security and privacy threats to ML, including adversarial examples that cause misclassification, poisoning of training data and the extraction of private information from models. In cybersecurity, where adversaries actively try to evade detection, such weaknesses are a serious concern (Apruzzese et al., 2018). Finally, relatively few studies go beyond detection to evaluate



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

automated prevention, such as blocking traffic or isolating hosts, and to measure response time and the cost of false alarms in operation (Khraisat et al., 2019).

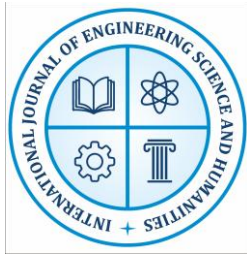
Operational factors add further difficulty. An IDS deployed on a busy network may examine millions of flows every day, so even a false-positive rate of one percent can produce thousands of unnecessary alerts and lead to alert fatigue among analysts. Models must also process traffic quickly enough to support real-time decisions, and many deep models require specialised hardware to do so (Vinayakumar et al., 2019). Privacy and legal constraints limit the sharing of real security data between organisations, which in turn limits the availability of realistic training data. These issues explain why, despite strong results in research papers, AI-based detection is usually deployed alongside rather than instead of signature-based tools, with human analysts reviewing high-impact decisions (Apruzzese et al., 2018; Sarker et al., 2020).

3. Conclusion

This review has examined research from 2014 to 2022 on the use of machine learning and deep learning for detecting and preventing cyber threats. The literature shows clear progress. Classical algorithms such as decision trees, support vector machines and ensemble methods provide fast and often accurate detection, especially when combined with careful feature selection. Deep learning models, including recurrent networks, convolutional networks and auto-encoders, can learn useful features automatically and frequently achieve higher accuracy on benchmark datasets for intrusion, malware and phishing detection. Hybrid models that combine different architectures, or that join deep feature learning with classical classifiers, have become a common and effective design.

The review further shows that the choice of technique should depend on the security task and the operating environment. Ensemble methods such as random forest and gradient boosting offer a strong balance between accuracy, speed and ease of use for structured data such as flow records. Deep models are most useful when large volumes of data are available, when the data are sequential or unstructured, or when hand-crafted features are hard to design. Unsupervised and anomaly-based methods remain important for detecting new attacks, even though they require careful tuning to control false alarms. Benchmark datasets have improved, with UNSW-NB15 and CICIDS2017 offering more realistic traffic than earlier collections, but no single dataset is sufficient for a complete evaluation.

The review also shows that high accuracy on a benchmark does not guarantee strong performance in practice. Many studies rely on outdated or imbalanced datasets, report a narrow set of metrics, and give limited attention to false alarms, processing time and model interpretability. AI-based systems also introduce new risks, since attackers can attempt to evade or poison the models themselves. Overall, AI should be seen as a powerful complement to conventional security controls rather than a replacement for them. Its greatest value lies in



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com ISSN: 2250-3552

helping security teams detect new and changing threats more quickly, reducing the burden of manual analysis, and supporting faster and better-informed responses.

4. Future Scope

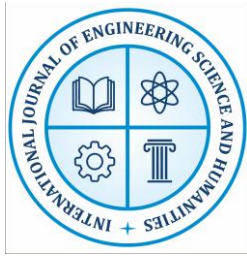
Several directions for future research emerge from this review. First, there is a need for new, realistic and regularly updated datasets that reflect current traffic, cloud and IoT environments, and modern attack techniques, together with shared evaluation protocols that make results comparable across studies. Researchers should evaluate models on several datasets and report per-class results, false-positive and false-negative rates, and processing costs, rather than accuracy alone.

Second, future work should improve the robustness of AI models against adversarial attacks. Techniques such as adversarial training, robust feature design and the combination of several diverse models may make evasion more difficult. Third, explainable AI methods are needed so that security analysts can understand why a model raised an alert, which would increase trust and support faster investigation. Fourth, because both normal behaviour and attacks change over time, continual and online learning methods should be developed so that models can adapt without full retraining, while avoiding the risk of learning from poisoned data.

Finally, more research is needed on moving from detection to prevention. Future studies should design and test automated response mechanisms, such as blocking, rate-limiting and host isolation, that act on model predictions in real time while keeping humans involved in uncertain or high-impact decisions. Lightweight models for edge and IoT devices, privacy-preserving approaches such as federated learning, and closer collaboration between researchers and industry would also help AI-driven cybersecurity move from promising laboratory results to dependable, real-world protection.

References

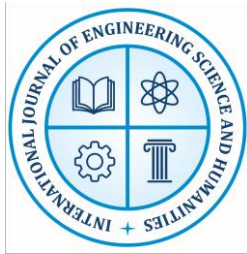
1. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150. <https://doi.org/10.1002/ett.4150>
2. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 371–390). IEEE. <https://doi.org/10.23919/CYCON.2018.8405026>
3. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, 10(4), 122. <https://doi.org/10.3390/info10040122>



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

4. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. <https://doi.org/10.1109/COMST.2015.2494502>
5. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. <https://doi.org/10.1016/j.jisa.2019.102419>
6. Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data*, 7(1), 105. <https://doi.org/10.1186/s40537-020-00379-6>
7. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1), 20. <https://doi.org/10.1186/s42400-019-0038-7>
8. Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9(20), 4396. <https://doi.org/10.3390/app9204396>
9. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2018)*. Internet Society. <https://doi.org/10.14722/ndss.2018.23204>
10. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/MilCIS.2015.7348942>
11. Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. P. (2018). SoK: Security and privacy in machine learning. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 399–414). IEEE. <https://doi.org/10.1109/EuroSP.2018.00035>
12. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, 86, 147–167. <https://doi.org/10.1016/j.cose.2019.06.005>
13. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 117, 345–357. <https://doi.org/10.1016/j.eswa.2018.09.029>
14. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7(1), 41. <https://doi.org/10.1186/s40537-020-00318-5>



International Journal of Engineering, Science and Humanities

An international peer reviewed, refereed, open-access journal
Impact Factor 8.3 www.ijesh.com **ISSN: 2250-3552**

15. Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. In 2015 10th International Conference on Malicious and Unwanted Software (MALWARE) (pp. 11–20). IEEE. <https://doi.org/10.1109/MALWARE.2015.7413680>
16. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018) (pp. 108–116). SciTePress. <https://doi.org/10.5220/0006639801080116>
17. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. <https://doi.org/10.1109/TETCI.2017.2772792>
18. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550. <https://doi.org/10.1109/ACCESS.2019.2895334>
19. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381. <https://doi.org/10.1109/ACCESS.2018.2836950>
20. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961. <https://doi.org/10.1109/ACCESS.2017.2762418>