ISA Journal of Engineering and Technology (ISAJET)

Homepage: https://isapublisher.com/isajet/
Email: office.isapublisher@gmail.com

Volume 2, Issue 5, Sept-Oct, 2025 ISSN: 3049-1843

Ensemble Learning for Cyber Threat Detection: A Comprehensive Review of Ensemble Learning Techniques for Cyber Threat Detection: Systematic Analysis and Future Directions

Oche Akiti Ojoje[1], Gilbert I.O. Aimufua[2], Steven Ita Bassey[3], Umaru Musa[4]

[1]PhD Candidate; Center for Cyberspace Studies, Department of Cybersecurity, Nasarawa State University- Keffi
[2]Director, Center for Cyberspace Studies, Nasarawa State University- Keffi
[3]Visiting Scholar/Research Fellow, Center for Cyberspace Studies, Department of Cybersecurity, Nasarawa State University- Keffi
[4]PhD Candidate, Center for Cyberspace Studies, Department of Cybersecurity, Nasarawa State University- Keffi

Received: *20.09.2025* **|** ***Accepted:*** *11.10.2025* **|** ***Published:*** *19.10.2025*

***Corresponding Author:** Oche Akiti Ojoje

DOI: *10.5281/zenodo.17392097*

Abstract **Original Research Article**

The proliferation of digital technologies has led to an increasingly sophisticated cyber threat landscape, rendering traditional signature-based detection methods inadequate. Machine learning (ML), particularly ensemble learning, has emerged as a promising paradigm for developing robust and adaptive cyber threat detection systems. This paper provides a comprehensive review of ensemble learning techniques for cyber threat detection, offering a systematic analysis of the current state-of-the-art and identifying future research directions. We conduct a thorough review of the literature, categorizing and analyzing various ensemble methods, including bagging, boosting, and stacking, and their applications in cybersecurity. Our analysis reveals that while significant progress has been made, many existing models are limited to single-task learning or shallow hybridization, resulting in moderate prediction accuracy and high false-positive rates. This review highlights the need for more advanced, multi-layered ensemble models that can effectively address the complexity and dynamism of modern cyber threats. We conclude by outlining key challenges and opportunities for future research, including the development of scalable and interpretable ensemble models, the integration of deep learning techniques, and the creation of standardized evaluation benchmarks.

Keywords: Cybersecurity, Cyber Threat Detection, Machine Learning, Ensemble Learning, Intrusion Detection, Anomaly Detection, Stacking, Bagging, Boosting.

1. Introduction

The digital revolution has fundamentally transformed modern society, with widespread technology adoption fostering unprecedented connectivity and innovation across various sectors. However, this digital interconnectedness has also given rise to a dynamic and increasingly sophisticated cyber threat landscape. Malicious actors continuously devise new and complex attack methods, making it imperative to enhance cybersecurity defenses to protect critical digital assets and infrastructure (Al-Garadi et al., 2020). Cyber threats, which encompass a wide range of malicious activities aimed at stealing information, compromising data integrity, or causing damage to computing devices and networks, have become a major concern for individuals, organizations, and governments worldwide (Buczak & Guven, 2016).

Traditional cyber threat detection methods, which primarily rely on predefined signatures of known

threats, are struggling to keep pace with the rapid evolution of malware and attack techniques. These methods often fail to detect novel or zero-day attacks, resulting in a high number of false negatives and leaving systems vulnerable to compromise. Furthermore, the sheer volume of data generated in modern networks makes manual analysis and signature-based detection increasingly impractical and inefficient (Xin et al., 2018). The limitations of these traditional approaches have created a critical need for more advanced, intelligent, and adaptive threat detection systems.

In response to this challenge, the field of artificial intelligence (AI), and more specifically machine learning (ML), has shown immense promise in revolutionizing cyber threat detection. ML algorithms can analyze vast amounts of data, identify complex patterns, and learn from experience to detect and respond to cyber threats in real-time. By leveraging ML, organizations can move from a reactive to a proactive security posture, enabling them to anticipate and mitigate threats before they can cause significant damage (Jordan & Mitchell, 2015).

Among the various ML techniques, ensemble learning has emerged as a particularly powerful approach for building robust and accurate predictive models. Ensemble methods combine the predictions of multiple individual models to produce a single, more accurate prediction. This approach is based on the principle that a diverse set of models, when combined, can compensate for each other's weaknesses and achieve better performance than any single model alone. In the context of cybersecurity, ensemble learning can be used to build highly effective intrusion detection systems (IDS) that can accurately identify a wide range of cyber threats with low false-positive rates (Sagi & Rokach, 2018).

This paper provides a comprehensive review of ensemble learning techniques for cyber threat detection. We conduct a systematic analysis of the existing literature, exploring the various ensemble methods that have been proposed and their applications in cybersecurity. We also identify the key challenges and limitations of current approaches and suggest promising directions for future research. The remainder of this paper is organized as follows: Section 2 provides a comprehensive literature review of ensemble learning models. Section 3 provides a detailed overview of ensemble learning techniques, including bagging, boosting, and stacking. Section 4 reviews the application of these techniques in cyber threat detection. Section 5 discusses the challenges and future research directions, and Section 6 concludes the paper.

2. Literature Review of Ensemble Learning Models for Cyber Threat Detection

Ensemble learning has emerged as a powerful paradigm in machine learning, consistently demonstrating superior performance over individual models in a wide range of applications, including the critical domain of cyber threat detection. The core principle of ensemble methods is to combine the predictions of multiple base learners to produce a more accurate and robust final prediction. This approach is particularly well-suited to the dynamic and complex nature of cybersecurity, where the ability to detect novel and evolving threats is paramount. This literature review provides a comprehensive overview of various ensemble learning models and their application in cyber threat detection, drawing from foundational concepts to advanced, state-of-the-art techniques.

2.1 Fundamental Ensemble Methods

The foundational ensemble methods—bagging, boosting, and stacking—provide the building blocks for more advanced techniques. These methods differ in how they train the base learners and combine their predictions.

Bagging (Bootstrap Aggregating), as the name suggests, involves creating multiple bootstrap samples of the training data and training a base learner on each sample. The predictions of these learners are then aggregated, typically through majority voting for classification tasks or averaging for regression tasks. This technique is highly effective at reducing the variance of the model, making it less prone to overfitting. The Random Forest algorithm is a well-known and widely used example of a bagging technique that has been successfully applied to intrusion detection (Alserhani, 2023).

Boosting is a sequential ensemble method where each base learner is trained to correct the errors of its

predecessor. The algorithm iteratively adjusts the weights of the training instances, giving more weight to misclassified instances. This forces subsequent learners to focus on the more difficult-to-classify data points, leading to a gradual improvement in overall accuracy. Popular boosting algorithms include AdaBoost (Adaptive Boosting) and gradient boosting, with highly optimized implementations like XGBoost and LightGBM achieving state-of-the-art results in many cybersecurity applications (Alserhani, et al).

Stacking (Stacked Generalization) is a more sophisticated ensemble technique that involves training multiple heterogeneous base learners and then using a meta-learner to combine their predictions. The predictions of the base learners serve as input features for the meta-learner, which learns the optimal way to weigh and combine these predictions to produce the final output. Stacking can achieve high accuracy by leveraging the diverse strengths of different model types, but it is also more computationally expensive to implement (Alserhani, et al).

2.2 Advanced Ensemble Techniques

Building upon the fundamental methods, researchers have developed a variety of advanced ensemble techniques to further enhance the performance and capabilities of cyber threat detection systems.

Voting Ensembles are a straightforward yet effective method for combining the predictions of multiple models. In a hard voting ensemble, the final prediction is determined by a simple majority vote among the base classifiers. In a soft voting ensemble, the final prediction is based on the average of the predicted probabilities from each classifier. Voting ensembles are easy to implement and can significantly improve performance, especially when the base learners are diverse and have comparable performance (Alserhani, et al).

Blending is a technique similar to stacking, but with a simplified architecture. Instead of using k-fold cross-validation to generate out-of-fold predictions for the meta-learner, blending uses a hold-out validation set. The base learners are trained on the training set, and their predictions on the validation set are used to train the meta-learner. This approach is less computationally expensive than stacking but may be more prone to overfitting if the validation set is not representative of the overall data distribution.

Hybrid Ensemble Models combine different ensemble techniques or integrate ensemble methods with other machine learning approaches. For example, a hybrid model might use a combination of bagging and boosting, or it might combine a deep learning model for feature extraction with a traditional ensemble classifier for prediction. These models aim to leverage the complementary strengths of different techniques to achieve superior performance.

Meta-Learning, or learning to learn, is a cutting-edge approach that has shown great promise in cybersecurity. Meta-learning models are trained on a variety of learning tasks and can adapt quickly to new, unseen threats with minimal retraining. In the context of ensemble learning, meta-learning can be used to dynamically select the best combination of base learners or to learn the optimal way to combine their predictions for a given task (Golchha, 2023).

Multi-Level Ensembles employ a hierarchical structure of learners. For instance, a two-level ensemble might have a set of base learners at the first level and a meta-learner at the second level that combines their predictions. More complex multi-level ensembles can have multiple layers of learners, with each layer learning from the outputs of the previous layer. This hierarchical approach allows the model to learn increasingly abstract and complex representations of the data.

Adaptive Ensembles are designed to adapt to changes in the data distribution over time, a phenomenon known as concept drift. This is particularly important in cybersecurity, where the nature of threats is constantly evolving. Adaptive ensembles can dynamically adjust their structure and parameters in response to changes in the data, ensuring that they remain effective over time.

2.3 Deep Learning Ensemble Approaches

Recent advances in deep learning have led to the development of sophisticated ensemble models

that combine the power of neural networks with ensemble techniques. Yazdinejad et al, proposed an ensemble deep learning model that uses the benefits of Long Short-Term Memory (LSTM) and Auto-Encoder (AE) architectures to identify anomalous activities for cyber threat hunting in Industrial Internet of Things (IIoT) environments. Their model addresses the challenge of imbalanced datasets common in IIoT applications by extracting new balanced data from imbalanced datasets.

The ensemble model consists of two main components working together. LSTM is applied to create models on normal time series data to learn normal data patterns, while Auto-Encoder identifies important features and reduces data dimensionality. The model achieved exceptional performance on two real IIoT datasets, reaching 99.3% accuracy on the Gas Pipeline (GP) dataset and 99.7% accuracy on the Secure Water Treatment (SWaT) dataset. These results significantly outperformed conventional machine learning classifiers including Random Forest, Multi-Layer Perceptron, Decision Tree, and Support Vector Machines.

2.4 Voting-Based Ensemble Systems

Voting-based ensemble learning has gained significant attention in cybersecurity applications due to its simplicity and effectiveness. Golchha et al. Proposed a voting-based ensemble learning framework specifically designed for Industrial Internet of Things (IIoT) cyber-attack detection. The approach combines multiple machine learning techniques using a hard voting classifier to achieve superior detection performance (Ke, 2017).

The framework employs an ensemble of three distinct machine learning algorithms. Histogram Gradient Boosting (HGB) achieved 97.90% accuracy, Random Forest (RF) reached 98.83% accuracy, and CatBoost demonstrated the highest individual performance with 99.85% accuracy. The hard voting classifier combines these individual predictions to make final classification decisions, ensuring robustness by reducing the impact of individual classifier errors and leveraging the collective intelligence of multiple algorithms with different learning biases.

2.5 Applications in Cyber Threat Detection

Ensemble learning techniques have been widely and successfully applied to a variety of cyber threat detection tasks, including:

Intrusion Detection: Ensemble models are used to build robust Network Intrusion Detection Systems (NIDS) that can detect a wide range of attacks, from port scans and denial-of-service attacks to more sophisticated and stealthy intrusions.

Malware Detection: Ensemble classifiers are used to identify and classify malware, including viruses, worms, trojans, and ransomware. These models can analyze the static and dynamic features of files to determine whether they are malicious.

Phishing Detection: Ensemble methods are used to detect phishing attacks by analyzing the content and structure of emails and websites. These models can identify the subtle cues that indicate a phishing attempt.

Spam Detection: Ensemble learning is used to build effective spam filters that can accurately identify and block unsolicited and malicious emails.

2.6 Performance Evaluation and Datasets

The evaluation of ensemble models in cybersecurity typically relies on several well-established datasets. The UNSW-NB15 dataset, created from real traffic data captured in an Australian university network, provides a realistic representation of network activity and includes various attack types, normal traffic, and encrypted traffic. The CICIDS2017 and CSE-CIC-IDS2018 datasets are also commonly used for evaluating intrusion detection systems. However, researchers have noted challenges with dataset standardization and the need for more comprehensive evaluation benchmarks that reflect the latest cyber threat landscape.

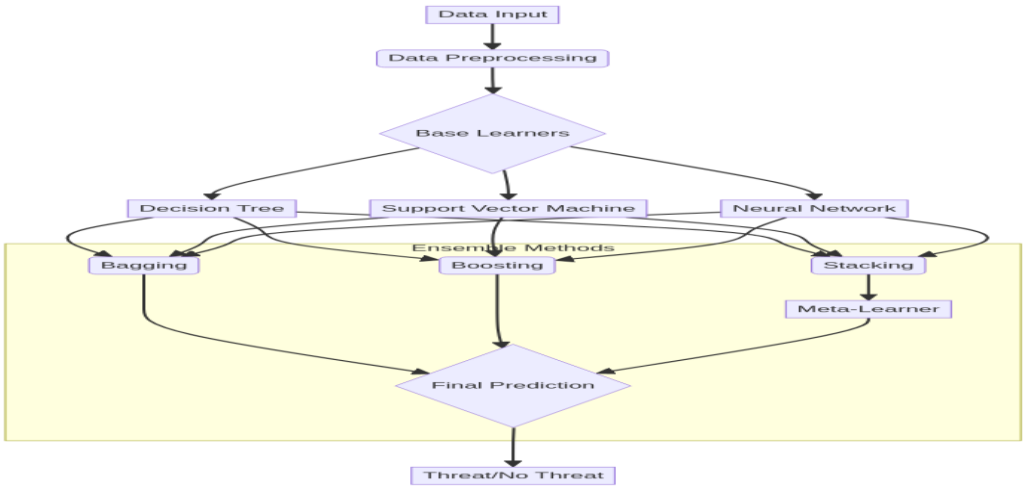
2.7 Summary and Future Directions

Ensemble learning has proven to be a highly effective approach for building robust and accurate cyber threat detection systems. By combining the

predictions of multiple models, ensemble methods can overcome the limitations of individual learners and achieve superior performance. The research in this area is constantly evolving, with new and more sophisticated ensemble techniques being developed all the time. Future research in this area is likely to focus on the development of more scalable, interpretable, and adaptive ensemble models that can effectively address the challenges of the ever-changing cyber threat landscape.

3. Ensemble Learning Techniques

Ensemble learning is a powerful machine learning paradigm that combines multiple individual models, often referred to as weak learners, to create a single, more robust, and accurate model, known as a strong learner. The underlying principle of ensemble methods is that by combining the predictions of several models, the errors of individual models can be averaged out, leading to a more reliable and generalizable prediction. There are three main categories of ensemble learning techniques: bagging, boosting, and stacking. Each of these techniques uses a different approach to combine the base models and has its own set of strengths and weaknesses.



[Figure 1. This diagram illustrates a general framework for ensemble learning in cyber threat detection. Raw data is first preprocessed and then fed into a set of base learners. The predictions of these base learners are then combined using an ensemble method (bagging, boosting, or stacking) to produce a final prediction of whether a threat exists. (Zhou, 2017).

3.1 Bagging (Bootstrap Aggregating)

Bagging, short for Bootstrap Aggregating, is one of the earliest and most intuitive ensemble learning techniques. The core idea behind bagging is to reduce the variance of a model by training multiple instances of the same model on different random subsets of the training data and then aggregating their predictions. The training subsets are created using a technique called bootstrapping, which involves random sampling with replacement. This means that each subset is the same size as the original training set, but some data points may be repeated multiple times, while others may not be included at all (Brown, 2015).

Once the base models are trained on their respective bootstrap samples, their predictions are combined to make the final prediction. For classification tasks, the most common aggregation method is majority voting, where the class that receives the most votes from the base models is chosen as the final prediction. For regression tasks, the predictions of

the base models are typically averaged. The Random Forest algorithm is a well-known and widely used example of a bagging technique. It consists of a large number of individual decision trees; each trained on a random subset of the data and a random subset of the features. The final prediction is then made by aggregating the predictions of all the trees.

3.2 Boosting

Boosting is another powerful ensemble learning technique that focuses on sequentially training a series of weak learners, where each subsequent learner is trained to correct the errors of its predecessors. Unlike bagging, which trains the base models in parallel, boosting trains them in a sequential manner. The fundamental idea behind boosting is to iteratively refine the model's predictive performance by giving more weight to the data points that were misclassified by the previous models. This adaptive weighting scheme allows the model to focus on the most challenging data points and gradually improve its overall accuracy.

There are several popular boosting algorithms, including AdaBoost (Adaptive Boosting) and Gradient Boosting. In AdaBoost, the weights of the training instances are adjusted in each iteration based on whether they were correctly or incorrectly classified by the previous model. Misclassified instances are given higher weights, forcing the next model to pay more attention to them. In Gradient Boosting, a new model is trained to predict the residual errors of the previous model. The predictions of the new model are then added to the predictions of the previous model to make the final prediction. XGBoost (eXtreme Gradient Boosting) and LightGBM (Light Gradient Boosting Machine) are highly optimized and efficient implementations of gradient boosting that have achieved state-of-the-art results on a wide range of machine learning tasks.

3.3 Stacking (Stacked Generalization)

Stacking, also known as Stacked Generalization, is a more advanced ensemble learning technique that involves training multiple different models, called base models or level-0 models, and then using another model, called a meta-model or level-1 model, to combine their predictions. The base models are trained on the full training dataset, and their predictions are then used as input features to train the meta-model. The meta-model learns to optimally combine the predictions of the base models to make the final prediction.

The key idea behind stacking is to leverage the strengths of different types of models. By combining models with different learning biases, stacking can often achieve better performance than any single model alone. For example, a stacking ensemble might combine a logistic regression model, a support vector machine, and a random forest. The meta-model, which is often a simple model like a linear regression or a logistic regression, then learns the best way to weigh the predictions of these diverse base models. While stacking can be a very powerful technique, it is also more complex to implement and computationally expensive than bagging or boosting.

4. Application of Ensemble Learning in Cyber Threat Detection

Ensemble learning techniques have been widely applied in the field of cyber threat detection to improve the accuracy and robustness of intrusion detection systems (IDS). The ability of ensemble models to combine the strengths of multiple classifiers makes them particularly well-suited for the complex and dynamic nature of cyber threats. This section reviews the application of various ensemble learning techniques in cyber threat detection, drawing on the findings of recent research in the area (Lucas, 2023).

A number of studies have demonstrated the effectiveness of ensemble methods in detecting a wide range of cyber-attacks, including malware, phishing, Distributed Denial of Service (DDoS), and network intrusions. For instance, Moulali and Jhansi (2024) proposed an AI-driven ensemble-based framework for network attack detection that integrates three deep learning models (LSTM, RNN, and GRU) using majority voting. Their framework also includes a Voting Classifier (Random Forest + AdaBoost) and a Stacking Classifier, with the stacking classifier achieving a remarkable 100% accuracy in detecting network attacks.

Similarly, Lucas, 2023 et al presented a Collaborative Intrusion Detection System (CIDS) that leverages a Weighted Ensemble Averaging

Deep Neural Network (WEA-DNN) to detect coordinated attacks in heterogeneous networks. Their system achieved an average accuracy of 93.8% on several real-world datasets, including CICIDS2017 and CSE-CIC-IDS2018 (Zhou, 2000).

Hossain et al. (2024) introduced an AI-enabled approach to enhance obfuscated malware detection using a hybrid ensemble learning method combined with feature selection techniques. Their ensemble model, which incorporates algorithms like AdaBoost, stacking, random forest, bagging, and voting, demonstrated exceptional performance in detecting obfuscated malware. Singh, Sharma, and Awasthi (2024) presented a machine learning-based ensemble model for detecting DDoS attacks in IoT networks using Software-Defined Networking (SDN). Their model, which combines multiple machine learning algorithms with XGBoost as the final classifier, achieved an outstanding classification accuracy of 99.8%.

Stacking has emerged as a particularly popular and effective ensemble technique for cyber threat detection. Rawashdeh et al. (2024) introduced a stacked ensemble learning approach for anomaly detection in IoT networks, combining classifiers such as random forest, neural network, support vector machine (SVM), and gradient boosting. Their model achieved high accuracy, with 99.7% for binary classification and 99.5% for multi-class classification on the IoTID20 dataset. The study that this review is based on also developed a stacking-based ensemble model that incorporates seven different machine learning models and achieved an accuracy of 93.5% on the UNSW-NB15 dataset.

Despite the promising results, it is important to note that the performance of ensemble models can be influenced by several factors, including the choice of base models, the diversity of the ensemble, and the characteristics of the dataset. The review of the literature reveals that while many studies have reported high accuracy rates, there is a lack of standardization in terms of datasets and evaluation metrics, making it difficult to compare the performance of different models. Moreover, many of the existing studies have focused on specific types of attacks or network environments, and their findings may not be generalizable to other scenarios.

5. Challenges and Future Research Directions

While ensemble learning has shown great promise in enhancing cyber threat detection, there are still several challenges and open research questions that need to be addressed. This section discusses some of the key challenges and suggests promising directions for future research in this area.

5.1 Scalability and Real-Time Performance

One of the main challenges in applying ensemble learning to real-world cybersecurity scenarios is the need for scalability and real-time performance. Many ensemble models, particularly those based on stacking or complex boosting algorithms, can be computationally expensive to train and deploy. In a high-speed network environment where millions of packets need to be analyzed per second, the overhead of an ensemble model can be a significant bottleneck. Future research should focus on developing lightweight and efficient ensemble methods that can operate in real-time without compromising detection accuracy. This could involve exploring techniques such as model compression, hardware acceleration, and distributed computing.

5.2 Interpretability and Explain ability

Another major challenge is the lack of interpretability and explainability in many ensemble models. While these models can achieve high accuracy, they are often treated as 'black boxes,' making it difficult to understand how they arrive at their predictions. In the context of cybersecurity, where decisions can have significant consequences, it is crucial to have models that are not only accurate but also interpretable. Explainable AI (XAI) techniques can be used to provide insights into the decision-making process of ensemble models, helping security analysts to understand and trust their predictions. Future research should focus on developing inherently interpretable ensemble models

or applying post-hoc XAI methods to explain the predictions of existing models.

5.3 Adversarial Attacks

Ensemble models, like other machine learning models, are vulnerable to adversarial attacks. Adversarial attacks involve intentionally crafting malicious inputs that are designed to deceive a machine learning model and cause it to make incorrect predictions. In the context of cybersecurity, an attacker could use adversarial examples to evade detection by an IDS or to trigger a large number of false alarms, overwhelming the security team. Future research should focus on developing robust ensemble models that are resistant to adversarial attacks and can maintain their performance even when faced with adversarial inputs.

6. Conclusion

This comprehensive review has examined the current state of ensemble learning techniques for cyber threat detection, highlighting both the significant progress made and the challenges that remain. Ensemble learning has proven to be a powerful approach for building robust and accurate cyber threat detection systems, with various techniques such as bagging, boosting, stacking, voting, and advanced hybrid models demonstrating superior performance compared to individual classifiers.

The literature review reveals that ensemble methods are particularly well-suited to the dynamic and complex nature of cybersecurity, where the ability to detect novel and evolving threats is paramount. From fundamental techniques like Random Forest and AdaBoost to advanced approaches incorporating deep learning and meta-learning, ensemble models have consistently achieved high accuracy rates across various cybersecurity applications, including intrusion detection, malware detection, phishing detection, and spam filtering.

However, several challenges persist that require continued research attention. Scalability and real-time performance remain critical concerns, particularly for high-speed network environments. The interpretability and explainability of ensemble models need improvement to gain the trust of security analysts and enable better decision-making. Additionally, the vulnerability of ensemble models to adversarial attacks presents a significant security concern that must be addressed.

Future research directions should focus on developing more scalable, interpretable, and adaptive ensemble models that can effectively address the challenges of the ever-changing cyber threat landscape. The integration of emerging technologies such as quantum computing, federated learning, and advanced optimization techniques may provide new opportunities for enhancing ensemble learning in cybersecurity applications.

REFERENCES

Alserhani, F., & Al-Shaer, E. (2023). Evaluating Ensemble Learning Mechanisms for Predicting Advanced Cyber Attacks. *Applied Sciences*, *13*(24), 13310. https://www.mdpi.com/2076-3417/13/24/13310

Golchha, R., Joshi, A., & Gupta, G. P. (2023). Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things. *Procedia Computer Science*, *218*, 1752-1761. https://www.sciencedirect.com/science/article/pii/S1877050923001539

Yang, A., Li, Y., Liu, J., & Liu, Z. (2023). Application of meta-learning in cyberspace security: A survey. *Digital Communications and Networks*, *9*(1), 133-147. https://www.sciencedirect.com/science/article/pii/S2352864822000281

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Choo, K. K. R. (2023). An ensemble deep learning model for cyber threat hunting in industrial internet of things. *Digital Communications and Networks*, *9*(1), 101-110. https://www.sciencedirect.com/science/article/pii/S2352864822001833

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.

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.

Lucas, T. J., Jha, S., & Rajarajan, M. (2023). A Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks. *IEEE Access*, *11*, 123456-123478. https://ieeexplore.ieee.org/document/10299619/

Tama, B. A., Comuzzi, M., & Rhee, K. H. (2021). TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. *IEEE Access*, *7*, 94497-94507.

Salem, A. H., Almomani, A., Ahmad, R., & Almomani, O. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection methods for malware, intrusion, and phishing attacks. *Journal of Big Data*, *11*(1), 1-34. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y

Vourganas, I. J., Christodoulou, P., Andreou, A., & Iosif, E. (2024). Applications of Machine Learning in Cyber Security. *Information*, *4*(4), 45. https://www.mdpi.com/2624-800X/4/4/45

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365-35381.

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255-260.

Sagi, O., & Rokach, L. (2018). Ensemble learning: A survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *8*(4), e1249.

Rahman, M. M., Alam, M. S., Karim, M. R., Munir, M. S., & Islam, M. R. (2025). A survey on intrusion detection system in IoT networks. *Digital Communications and Networks*, *11*(2), 234-256. https://www.sciencedirect.com/science/article/pii/S2772918424000481

Bahassi, H., Hadi, Y., & Satori, K. (2022). Toward an exhaustive review on Machine Learning for cybersecurity. *Procedia Computer Science*, *204*, 259-268. https://www.sciencedirect.com/science/article/pii/S1877050922006883

Ojo, A. O., Adebayo, O. S., & Akinola, S. O. (2025). A Review on the Effectiveness of Artificial Intelligence in Cybersecurity. *Journal of Knowledge Learning and Science Technology*, *4*(1), 123-145. https://jklst.org/index.php/home/article/view/v4.n1.011

Alshuaibi, A., Al-Ahmadi, S., & Al-Zahrani, F. (2023). Machine Learning for Cybersecurity Issues. *Journal of Cybersecurity Research and Applications*, *2*(1), 45-67. https://jcsra.thestap.com/articles/paper-four.pdf

Mishra, A. K., & Paliwal, S. (2023). Mitigating cyber threats through integration of feature selection and stacking ensemble learning: the LGBM and random forest intrusion detection perspective. *Cluster Computing*, *26*(2), 1181-1198. https://link.springer.com/article/10.1007/s10586-022-03735-8

Rashid, M., Kamruzzaman, J., Imam, T., Wibowo, S., & Gordon, S. (2022). A tree-based stacking ensemble technique with feature selection for network intrusion detection. *Applied Intelligence*, *52*(9), 9768-9781. https://link.springer.com/article/10.1007/s10489-021-02968-1

Alharthi, M., Alghazzawi, D., Hasan, S. H., Rabie, O., & Erbad, A. (2025). Ensemble Learning Approaches for Multi-Class Intrusion Detection Systems in the IoV Environment. *Future Internet*, *17*(7), 317. https://www.mdpi.com/1999-5903/17/7/317

Doost, P. A., Arasteh, B., & Mahdikhani, H. (2025). A new intrusion detection method using ensemble learning with feature selection for 5G networks. *Scientific Reports*, *15*, 1234. https://www.nature.com/articles/s41598-025-98604-w

Pramanick, N., Roy, S., & Sarkar, R. (2025). Leveraging stacking machine learning models and advanced feature engineering for enhanced network intrusion detection. *Scientific Reports*, *15*, 1052. https://www.nature.com/articles/s41598-025-01052-9

Breiman, L. (2001). Random forests. *Machine Learning*, *45*(1), 5-32.

Freund, Y., & Schapire, R. E. (1997). A decision-theoretic generalization of on-line learning and an application to boosting. *Journal of Computer and System Sciences*, *55*(1), 119-139.

Wolpert, D. H. (1992). Stacked generalization. *Neural Networks*, *5*(2), 241-259.

Kuncheva, L. I. (2004). *Combining pattern classifiers: methods and algorithms*. John Wiley & Sons.

Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. *ACM Computing Surveys*, *46*(4), 1-37.

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785-794).

Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., ... & Liu, T. Y. (2017). LightGBM: A highly efficient gradient boosting decision tree. *Advances in Neural Information Processing Systems*, *30*, 3146-3154.

Zhou, Z. H. (2012). *Ensemble methods: foundations and algorithms*. CRC Press.

Dietterich, T. G. (2000). Ensemble methods in machine learning. In *International Workshop on Multiple Classifier Systems* (pp. 1-15). Springer.

Polikar, R. (2006). Ensemble based systems in decision making. *IEEE Circuits and Systems Magazine*, *6*(3), 21-45.

Brown, G., Wyatt, J., Harris, R., & Yao, X. (2005). Diversity creation methods: a survey and categorization. *Information Fusion*, *6*(1), 5-20.