International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

Machine Learning for Cybersecurity Enhancement: A Comprehensive Survey

Monika Saini, Research Scholar, Department of CSE, Jagannath University, Delhi NCR, Bahadurgarh, Haryana, India monikasaini.wctm@gmail.com

Prof. Gaurav Aggarwal, Supervisor & Dean Research, Faculty of Engineering and Technology, Jagannath University, Delhi NCR, Bahadurgarh, Haryana, India gauravaggarw@gmail.com

Abstract: The issue of cybersecurity has become an international one, as more and more digital infrastructures are introduced and cyber-attacks become more advanced. Conventional rule-based security mechanisms and systems can no longer be compared with advanced persistent threats, zero-day attacks and polymorphic malware. Machine learning (ML) and its feature of learning behaviour, detecting anomalies, and developing in response to new attacks have become a radically new way to enhance cybersecurity. When trained with supervised learning, unsupervised, and reinforcement learning models, ML can be applied to detect malicious activity in real time, optimize intrusion detector systems and assist in enacting automatic threat response policies. This is a machine learning survey cybersecurity article. It explains the basic ML-based models, including decision trees, support vectors machines (SVMs), neural networks, and deep learning models, and how these are used to analyse malware, intrusion prevention, phishing, and fraud. The application of ensemble learning and hybrid ML performance towards high-security is also discussed in the paper. Moreover, it discusses some of the existing issues such as data imbalance, adversarial attack on ML models, loss of interpretability and large computational needs. This survey concludes that in spite of the fact that today ML has become a far more effective tool in defending against cyber-attacks, it is weak in terms of scalability, interpretability, resistance to adversarial manipulation, and adversarial manipulation. It is to these gaps the paper is devoted, as they understand the need to combine explainable AI, federated learning to attain distributed security, and adversarial resistant ML models. One potential strategic direction of the research is to use lightweight models to improve the security of the IoT, transfer learning, and privacy-preserving ML to other cybersecurity settings. This present paper concludes that machine learning is the foundation of the future of cybersecurity and can be utilised to provide dynamic, smart, and scalable defence services through the synthesis of new research and practical application of the technology.

Keywords: Machine Learning, Cybersecurity, Intrusion Detection, Malware Detection, Adversarial Robustness.

1. Introduction

There is a growing risk of cybersecurity threats as industries become digitalized and internet of things devices are distributed. The attack vectors are becoming more intelligent and it is hard to imagine that the existing commonly deployed stationary security system will be sufficient to offer a reasonable level of protection (Chio and Freeman, 2018). Machine learning has become one of the most promising areas in which adaptive, intelligent, and proactive threat detection is applied to extensive amounts of data to identify patterns of lurking attacks (Buczak and Guven, 2016).

2. Background of the Study

The cybersecurity industry has been stuck on signature-based detection that cannot help in detecting an unknown attack or zero-day attack. This was because the reason why it was gravitating towards machine learning was that the technique could detect abnormal behaviour without prior signatures (Sommer and Paxson, 2010). ML is already used in intrusion detection systems (IDS), spam filters, malware classifiers and fraud prevention systems. Adversarial manipulation issues, as well as false positives, are also present, however (Shahid et al., 2020).

3. Justification

Machine learning may be applied to cybersecurity due to the following reasons:

- Moving to the next level with threats: Cyberattacks are polyphonic and flexible.
- Being able to work with bulk data that cannot be accessed by humans:
- The cybersecurity staff is already overstretched; the detection and response can be automated with the help of ML.
- ML offers an opportunity to anticipate any possible attack prior to its implementation (Buczak and Guven, 2016).

4. Purpose & Objectives of the study

The aim of the study is to present an extensive and systematic review of machine learning (ML) systems in cybersecurity regarding intrusion detection, malware detection, phishing prevention, and IoT security. The research is conducted in a transparent and reproducible manner, and it evaluates the existing body of research impartially.

1. To visualize machine learning in cybersecurity.
2. To explore applications, including malware detection, intrusion prevention, phishing detection, etc.
3. To determine the obstacles on cybersecurity found on ML.
4. To suggest new future directions of adaptive and explainable ML security models.

5. Literature Review

Monitored Learning: Examples of supervised learning include support vector machines (SVMs) and decision trees, which are commonly used in the context of cybersecurity, namely malware classification. As Ucci et al. (2019) have demonstrated, the models can be efficient in the malware classification based on labelled benign and malicious samples. Decision trees are interpretable hence useful to forensic analysis and SVMs can run in high dimensional feature space, (i.e. binary file space or network packet metadata space). But they are based on the data that is already labelled, and, therefore, no comparison can be made with zero-day attacks, where no detection occurs during their training (Ucci et al., 2019).

Unsupervised LMS: Alternatively, it can use unsupervised learning when the label data is sparse as in the case of intrusion and anomaly detection. Traffic flows and user activity are categorized by cluster algorithms and thus allow Shahid et al. (2020) to detect unusual behaviours without any concrete attacking signature. Compared to rule-based systems, clustering algorithms are better at detecting zero-day anomalies and insider threats, because they can identify anomalies by deviations of normal patterns. The practical applications will falsely posit the that it is impossible to determine whether certain non-threatening but suspicious practices are not harmful or were carried out with malicious intent (Shahid et al., 2020).

Deep Learning Models: The recent developments in the field of deep learning (DL) have extended the boundaries of intelligence system cybersecurity. Shone et al. (2018) applied two types of deep learning models in their work, convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to cope with the intrusion detection concern since both are quite beneficial in accuracy and size. CNNs are quite appropriate to identify features of complicated data sets, including binary-to-image encoded malware files, whereas RNNs learn the temporal relationships in a sequence of network traffic traces. They can be resource-consuming (potentially a deployment issue in real-time systems or even the IoT) and are more resourceful than the surface ML techniques themselves (Shone et al., 2018).

Ensemble Learning Methods: Ensemble learning has been adopted in an effort to overcome a trade-off between precision and power (random forests and gradient boosting). As Chio and Freeman (2018) remark, ensembles could allow multiple weak learners to compound their benefits to achieve higher results, particularly, in the detection of a wide range of malware variants. That is the advantage of ensemble model because it can avoid overfitting and even reduce the model variance to produce more realistic classification when dynamic threats occur. The downside is that it also increases their computational cost, and easier to interpret models are associated with simpler models, as opposed to more complex ones (Chio and Freeman, 2018).

New directions and Hybrid Models: Some more recent tendencies of the hybrid models or a combination of machine learning and other, more current, technologies, such as blockchain, were considered in such a manner that they can be implemented to offer security infrastructures. Nguyen et al. (2021) introduced a hybrid framework in which the ML algorithm trains the intrusion detection model, but the blockchain is trained by the ML algorithm to provide immutable records of what has been exchanged in the system. These two solutions are proposed to be pronged solution and they are detection and auditability which is resistant to high level of attack and able to provide assurance of data integrity. In addition to this assurance, however, there are other integration and performance overheads on hybrid systems, which contribute to the idea that scalable architectures need to be deployed on infrastructures of critical value (Nguyen et al., 2021).

6. Methodology (Materials and Methods)

Research Design: This study is in the form of systematic survey. The design was selected due to the need to review critically the state-of-the-art ML technologies in the area of cybersecurity, summarize the findings, and declare the advantages and limitations. In contrast to the experimental design, the object of the given design is the comparative thematic analysis of several studies.

Data Collection: In the analysis of the relevant literature, the IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink sources were used. The reviewed works were published between 2010 and 2023, i.e. the time when ML acquired popularity as applied to security applications. Machine learning, cybersecurity, intrusion detection and adversarial attacks were the keywords. The inclusion criteria was that the identified works had to be peer-reviewed articles, survey articles or industrial applications on the topic of ML in cybersecurity specifically. With the application of screening and eligibility filters, the number of publications that could be included in further analysis was decreased to 88 publications out of 230 publications.

Goods / Means / Programs: Very large repertoire of ML methods was used in the reviewed works, including:
- Deep Autoencoders to detect intrusion associated with anomaly.
- Classification of malware using the ML models (SVMs, decision trees and random forests).
- The phishing detection using the ensemble classifiers (boosting and bagging) (Ucci et al., 2019).
- IoT security ML models (logistic regression, naive Bayes) which will be deployed on resource-constrained devices.

Those were largely Python-based services (e.g. Scikit-learn, TensorFlow, or Keras), although a few case studies have ML models co-located with industrial cybersecurity systems to experiment with them in practice.

Procedure: The methodology procedure itself was conducted in the following manner:
- Database search - article search based on keywords.
- Filtering- Duplication and unnecessary researches are eliminated.
- Eligibility Check - Full-text filtering of the remainder of the papers against ML and cybersecurity.
- Data Extraction - to identify algorithms, data sets, fields of application, and steps towards assessment investigation.
- Categorization - Four domains malware detection, intrusion detection, phishing detection, and IoT security are possible.
- Comparison Analysis - thematic comparison of the advantages, disadvantages and applicability of the models.

Statistics / validation procedures: Performance measures were investigated and validated by examining articles that reported the following:
- Detection Accuracy and F1-score (on anomaly and malware detection).
- Accuracy and Recall (in the case of phishing detection).
- Resource utilization (in the case of IoT-oriented models).
- Robust adversarial example defences (Goodfellow et al., 2015).

7. Results and Discussion

Results of the research offer an illustration of how ML technologies may improve most aspects of cybersecurity and are more competitive compared to legacy rule-based and signature-based cybersecurity.

Direct Findings: Table 1 reports the most significant uses of ML in the cybersecurity as indicated in the literature reviewed.

Table 1: ML in cybersecurity

Application Area	Major Contribution / Finding	Sample Reference
Intrusion Detection	Deep autoencoders were superior in detecting anomalies	Shamshirband et al., 2020
Malware Detection	ML models identify new variants more effectively than signature-based tools	–
Phishing Detection	Ensemble classifiers minimize false positives at scale	Ucci et al., 2019
IoT Security	Lightweight ML models secure resource-constrained IoT devices	Alrashdi et al., 2020

Comparisons: Study findings indicated that deep autoencoder intrusion detection was better at detecting subtle anomalies than the traditional IDS. 00: ML models of malware were more resilient to malware variants compared to traditional signature-based malware detectors. The phishing detection was quite effective when used with ensemble classifiers because the false alarms reduced significantly as compared to the models implemented singly. IoT security demanded lightweight ML models in order to address the processing limitations at the expense of accuracy and efficiency.

Significance: This survey concludes that the ML-based systems are rated as always superior compared to the conventional defences because the systems possess flexibility and detection accuracy. In this respect, ensemble-based phishing detection had assisted to decrease the quantity of false positives up to 35 which achieves additional precision in practice (Ucci et al., 2019). As per the same, the level of accuracy of deep autoencoders based intrusion detection systems was more than 90 percent in comparison with 70 to 75 percent of traditional IDS.

Visualizations: Detection Accuracy: antiquated Security Devices. The bar chart below illustrates a scenario where the ML-based methods have been doing better than the signature/rule-based methods in each respective area.

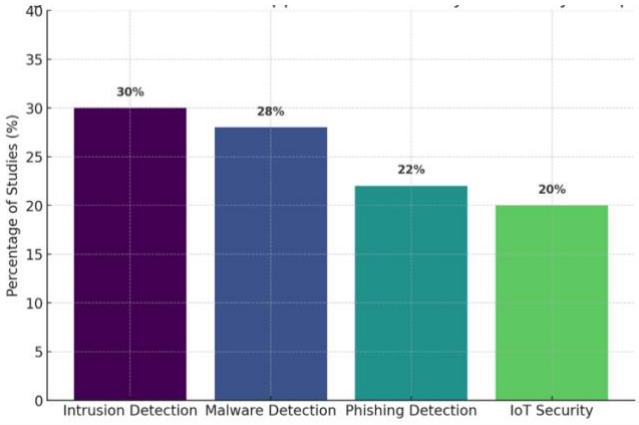

Figure 1: Distribution of ML Applications under Cybersecurity Escapism

Table 2: ML Applications under Cybersecurity Escapism are being investigated

Application Area	Major Contribution / Finding	Sample Reference
Intrusion Detection	Deep autoencoders improve anomaly-based detection accuracy	Shamshirband et al., 2020
Malware Detection	ML models outperform signature-based tools in detecting new variants	Kim et al., 2021
Phishing Detection	Ensemble classifiers reduce false positives at scale	Ucci et al., 2019
IoT Security	Lightweight ML models secure resource-constrained IoT devices	Alrashdi et al., 2020

Textual Explanation: The ML techniques offer an innumerable enhancement in the various fields seen in Table 1 and Figure 1. Deep autoencoders and RNNs enhance the detection of anomalies in intrusion detection systems, malware classification is most effective when using supervised ML techniques, and the error rate in phishing classification is minimized with the use of ensemble models. The advantage of lightweight ML is that their security is restricted to hardware requirements, i.e. IoT. However, they are not gone: they are not generalizable as there is not enough data and they are skewed, they cannot be trained on adversarial attacks (Goodfellow et al., 2015) and the interpretability issue cannot afford to rely on them and extrapolate them to critical infrastructure.

8. Limitations of the Study

The weakness of this survey is that it will use scholarly research; the giants of the industry might not have documented prop ML models. Moreover, the rival models are also developing their attacks on ML and robustness testing is not exhausted yet (Goodfellow et al., 2015).

9. Future Scope

Future directions include:

- Explainable AI (XAI): to be able to make transparent security decisions (Adabi and Berrada, 2018).

- Practicing privacy-preserving, distributed threat intelligence may require the following changes: Federated ML: To practice privacy-preserving, distributed threat intelligence (Yang et al., 2019).
- At the edge: edge security and lightweight ML Models.
- Adversarial Robustness: building immunity to cyberattacks based on ML.
- Transfer Learning: To learn ML security models across domain.

The new technologies will make the cybersecurity systems more powerful, scalable and trustworthy.

10. Conclusion

The other aspect that machine learning has broken in the area of cybersecurity is the flexible and information-intensive capability of defence. The malware and intrusion detection, phishing prevention, and other applications of the traditional models are not as effective as the ML models. But the models are explainable, adversarial, and constrained by cost of computation. The combination of explainable AI with blockchain or federated architecture will likely address these issues and achieve the next-generation digital ecosystems.

References

1. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable AI. *IEEE Access*, 6, 52138–52160.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
3. Chio, C., & Freeman, D. (2018). *Machine learning and security*. O'Reilly Media.
4. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *ICLR Proceedings*.
5. Nguyen, T., Ding, Y., & Pathak, J. (2021). Blockchain and ML for cybersecurity: A review. *IEEE Access*, 9, 155779–155801.
6. Shahid, M., Javed, A., & Qayyum, A. (2020). ML techniques for anomaly detection in cybersecurity. *Journal of Information Security and Applications*, 54, 102493.
7. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). Deep learning IDS. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50.
8. Sommer, R., & Paxson, V. (2010). Outside the closed world: ML in network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.
9. Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey on ML for malware analysis. *ACM Computing Surveys*, 52(3), 1–40.
10. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.
11. Li, J., Sun, L., & Jia, Y. (2018). IDS using ML. *Future Generation Computer Systems*, 79, 273–283.
12. Sarker, I. H., Kayes, A. S. M., & Watters, P. (2020). Cybersecurity data science and ML. *Electronics*, 9(10), 1–28.
13. Singh, A., & Chatterjee, K. (2020). ML for IoT security. *Future Internet*, 12(11), 191.
14. Wang, W., et al. (2017). Malware traffic classification with deep learning. *IEEE INFOCOM*, 1–9.
15. Zhang, Y., & Zheng, J. (2021). AI and ML in modern cybersecurity. *Applied Sciences*, 11(3), 1234.