STM JOURNALS

Journal of
Computer Technology & Applications

ISSN: 2229-6964 (Online)
ISSN: 2347-7229 (Print)
Volume 16, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoCTA

https://journals.stmjournals.com/jocta

Review JoCTA

A Review of Machine and Deep Learning Techniques for Cyber Security

Yasoda Krishna Reddy Annapureddy[1,*], V. Krishna Reddy[2]

Abstract

Nowadays in the digital landscape, cyber threats and attacks are increasing in an exponential manner, posing server risks to organizations and critical infrastructures. Data breaches often result from sophisticated threat models that exploit vulnerabilities in networks, systems and user behaviors. Cyber solutions are increasingly incorporating machine learning and deep learning to prevent and mitigate these security issues. These technologies have the potential to detect anomalies, classify threats and predict potential solutions. However, the dynamic nature of the threats presents major challenges which are new, and complex threats continue to emerge daily. These increasing threat models must be continually documented and used to retrain which will lead to improvement in the existing prediction models to maintain their accuracy and reliability. A wide range of approaches have already been proposed for threat detection and prediction, each leveraging different algorithms, datasets and evaluation metrics. In this study, the most well-known machine learning and deep learning models for predicting cyber threats are compared. We evaluate these models using key performance indicators such as precision, recall, accuracy, and adaptability to emerging threats, aiming to identify the most effective approaches for real-world scenarios.

Keywords: Cyber security, machine learning, deep learning, threat prediction, threat detection, data analysis, data processing, network security, intrusion detection, malware detection, phishing detection, vulnerability assessment, risk analysis, automation, cyber threat intelligence, critical infrastructure protection

INTRODUCTION

Cyber security is a trending issue in the digital world. As technology usage and the internet evolved exponentially, so with evolving the internet, technology and gadgets, the cyber security threats are also evolving with different forms and faces. In recent times, the realms of machine learning and deep learning have surged in prominence for thwarting and unveiling cyber threats.

***Author for Correspondence**
Yasoda Krishna Reddy Annapureddy
E-mail: yasodaakrishna@gmail.com

[1]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Guntur, Andhra Pradesh, India
[2]Professor & Principal, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Guntur, Andhra Pradesh, India

Received Date: June 06, 2025
Accepted Date: July 05, 2025
Published Date: July 08, 2025

Citation: Yasoda Krishna Reddy Annapureddy, V. Krishna Reddy. A Review of Machine and Deep Learning Techniques for Cyber Security. Journal of Computer Technology & Applications. 2025; 16(3): 1–7p.

This study offers a comprehensive exploration of the latest investigations surrounding the utilization of machine and deep learning methodologies in the sphere of cyber security [1]. It meticulously dissects four pivotal research endeavors, encapsulating their contributions to the cybersecurity domain and illuminating the promise held by machine learning and deep learning in bolstering cyber defenses.

LITERATURE REVIEW

Cyber Security

Cybersecurity is a key term used in the digital world which refers to being safe in the digital electronic systems and networks. The primary

agenda of cyber security is to prevent sensitive information from being stolen or modified using unauthorized access.

Various types of cyber-attacks exist, including viruses, spam emails, trojans, denial-of-service (DoS) attacks, malware, scareware, phishing, financial fraud, brute-force attacks, and others [2]. If a successful attack occurs, the sensitive data will be leaked and organization's operations, reputation and finances will collapse [3]. The recent greatest cyber-attack is ransomware. To prevent these risks, basic cyber security measures such as firewall, intrusion detection systems and antivirus software can help to prevent these attacks.

The Role of Machine Learning in Cybersecurity

Using machine learning for cybersecurity involves applying artificial intelligence techniques to detect, predict, and eliminate potential threats and attacks. This approach capitalizes on the capacity of machine learning algorithms to process big amounts of data, processing the recent threats and making projections based on previous threats. The following methods represent core strategies for integrating machine learning into cybersecurity systems [4].

1. *Detecting irregularities:* Machine learning algorithms can scrutinize network activities, logs and user activities based on the differences than general usage, with compromise of security or doubtful operations.
2. *Identifying malware:* By observing the properties of previously malicious and benign activities. Machine learning models learn to differentiate between the two types based on their distinct features [5]. When new or unobserved software comes into the picture, the machine learning model uses the previous trained model from labeled data to identify and categorize it as either malicious or benign. This process allows to actively detect threats and handle them.
3. *Recognizing phishing attempts:* ML models can be trained to detect phishing emails and sites by assessing various elements such as the email content such as message content and sender details.
4. *Uncovering vulnerabilities:* Machine Learning models can help to detect all possible flaws in the software and network setups by analyzing all the large codebases or network architectures and comparing both to know vulnerabilities [6].
5. *Assessing risks:* Machine Learning models can help in determining the levels of risk and analyze them based on historical data, threat data and setups.
6. *Automating Security:* Machine Learning models can be trained based on the previous data and used to create automation systems capable of identifying threats in real-time, decreasing human errors and response times.
7. *Enhancing cyber threat intelligence:* Machine learning can monitor, analyze and process large amounts of data from various sources, for example we can consider network traffic, social media and dark web forums, to detect threads [7]. This will improve the understanding of the type of thread, and the scale of thread based on the learned model, which will enable organizations to make informed decisions and actively protect their networks and systems from threat [4].
8. *Securing Cyber-Physical Systems:* The art of machine learning can be harnessed to vigilantly oversee and safeguard essential infrastructures like energy grids, transit systems, and production facilities by scrutinizing sensor data and system dynamics to unveil irregularities that might suggest looming cyber onslaughts.

METHODOLOGY

Enhancing the Fortress of Cybersecurity Through the Power of Deep Learning Innovations [7]

This study presents a comprehensive overview of how deep learning and machine learning techniques are applied in a range of cybersecurity domains. Figure 1 shows the workflow structure of deep learning.

Anomaly Detection in a Network

This is the first application discussed where the unsupervised deep learning systems are used to filter the system log data and identify the anomalies in user behavior [8].

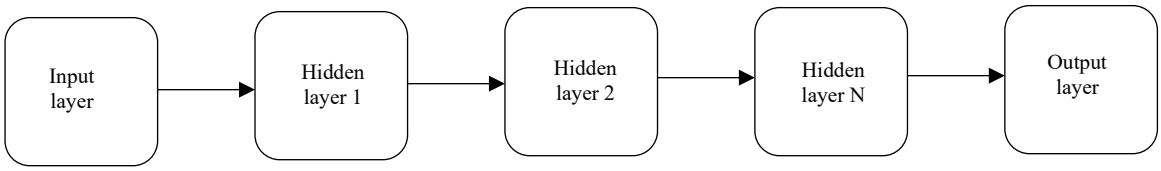

Figure 1. Deep learning.

The system will be trained with previous inputs and then the system is deployed in real time to get time to time logs, if any anomaly is identified in user behavior, then a notification is triggered to admin.

Network Intrusion Detection

This method uses a neural network that uses probabilistic model. In this study, the author mentioned a work that had only one hidden layer with accuracy of 50%; there is another system that uses unsupervised learning for finding the network intrusion [4]. This new system is based on K-means clustering for getting a better accuracy [8]. The accuracy by using K-means clustering is 91.8%.

Breaking the CAPTCHAs

This section analyses different means of breaking the captchas by using a deep learning algorithm:

- Roman characters are mostly used for designing the captcha on more than 50% websites.
- Deep learning techniques can be used can to easily crack the captchas. Deep Learning techniques can either be used to design a secure captcha or to crack the captcha [8].

Phishing Detection

There are multiple ways of phishing like by sending emails or by collecting the secret credentials such as bank username and password [8]. The authors proposed SVM model for finding phishing emails and SVM reported 95% emails correctly.

DDoS Detection

A DDoS attack occurs when a server is overwhelmed by many simultaneous requests, disrupting its normal operations. To address this, an Enhanced Support Vector Machine (ESVM) was used to train the system based on typical user activity. A feature selection mechanism was employed to identify key indicators, enabling the detection of potential attacks [8].

Malware Detection

Malware poses a significant threat as it consists of malicious software written as executable code, often delivered through emails, networks, or external devices. Once executed, a malware attack can be severe, potentially leading to data theft and system compromise [8]. To address this issue, Support Vector Machines (SVM) were employed to detect malware effectively.

A Semantic-Based Machine Learning Framework for Cybersecurity Monitoring

This study outlines a machine learning-based approach that utilizes data from the UCI Machine Learning Repository, which is pre-processed into appropriate input formats for different algorithms [9]. Following pre-processing, feature selection is performed, and the refined data is used to train a machine learning model designed to identify network status. The methodology emphasizes efficient data handling, model training, and performance evaluation using metrics such as accuracy, precision, recall, and confusion matrix. Furthermore, the model is expected to determine the network status within a time frame of less than 5 min.

Methodology

The framework's design comprises a variety of essential components, such as data gathering, data refinement, model creation, performance assessment, and network health detection [9].

Data Collection

Users can select the type of data to be collected and define the duration for data collection. The target device for monitoring can be specified by providing its IP address, allowing the system to gather network data from the designated source [9].

Data Pre-processing

The data needs to be normalized, and any missing values should be removed to stabilize the dataset. The information is subsequently divided into training sets and testing sets. From the amassed information, the suitable algorithm, whether it be a multi-class or single-class classification method, must be selected [9]. The user can input multiple data files to obtain the resulting dataset.

Model Creation and Performance Analysis

Any suitable machine learning algorithm can be applied to the data produced by the pre-processing module [9].

Figure 2 shows the semantic workflow diagram.

Classification Techniques Using Machine and Deep Learning for Cyber-Physical System Security

This study investigates the use of Machine Learning and Deep Learning techniques to strengthen the security of Cyber Physical Systems (CPSs). It begins with an overview of CPSs and explores how ML and DL approaches can be employed to detect and mitigate cyber-attacks on these systems [1].

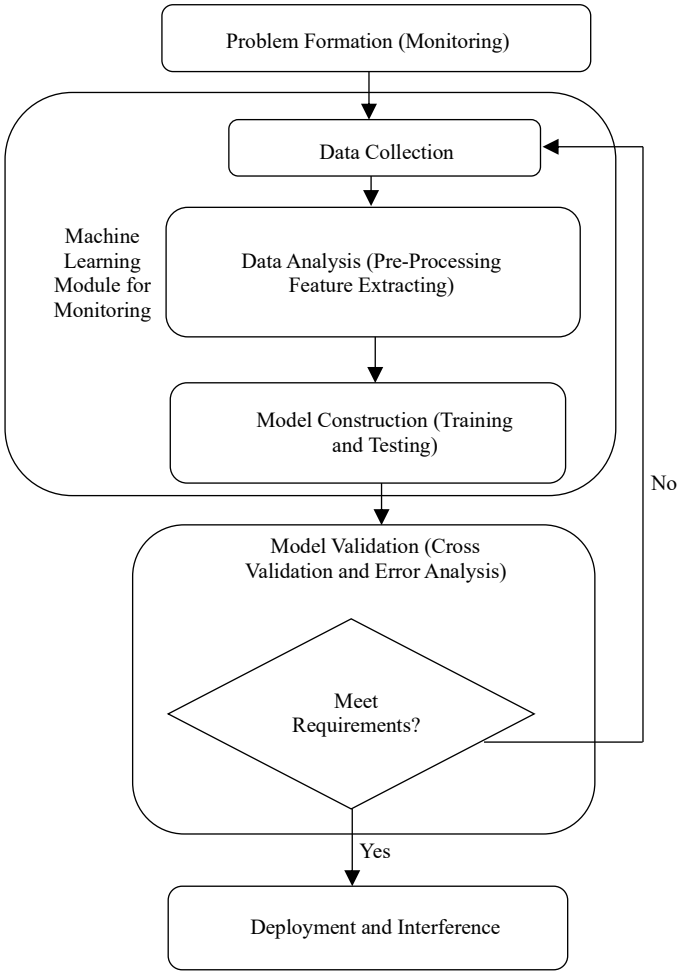

Figure 2. Sematic flow diagram [9].

The study assesses the performance of several classification algorithms, including Decision Trees, Random Forests, Support Vector Machines (SVMs), and Deep Neural Networks (DNNs), in enhancing the security of Cyber-Physical Systems (CPSs) (Figure 3). The authors demonstrate that these techniques significantly improve cyber-attack detection and the overall accuracy of threat intelligence for CPS environments [1].

The proposed cyber-attack detection framework comprises key phases, including data collection, pre-processing, feature extraction, model development, training, and testing [1]. Additionally, ML and DL are shown to enhance the analysis of security events by prioritizing signals and alerts based on their severity and relevance.

The study also addresses a broad range of cyber threats, including viruses, worms, spam, Trojans, denial-of-service (DoS) attacks, malware, scareware, phishing, financial fraud, Distributed Denial-of-Service (DDoS) attacks, Brute-Force attacks, and Man-in-the-Middle attacks [1]. Through a comparative review of multiple research studies, the authors assess which ML/DL models perform best for detecting specific types of threats.

Figure 4 shows the Framework of Cyber-attack detection using learning approach.

Integrating Cyber Threat Intelligence with Machine Learning

This study highlights the increasing significance of incorporating machine learning into cyber threat intelligence in recent times [7]. conveyed needed for organizations to incur advanced technologies to predict, protect against, and eradicate cybercrimes.

Haass started by explaining the flaws of the regular cyber threat intelligence systems, which are not accurate to find the trending threats. He then stated that the machine learning systems can be introduced into the real time systems to analyze large amounts of data and train the models based on the regular user patterns [7], so that it can predict the threats by observing the deviations from the regular patterns. This paper [10] also emphasized that the data used to train the machine learning model should be clean and contain diverse patterns. Additionally, human expertise is essential for evaluating the model using appropriate performance metrics [7].

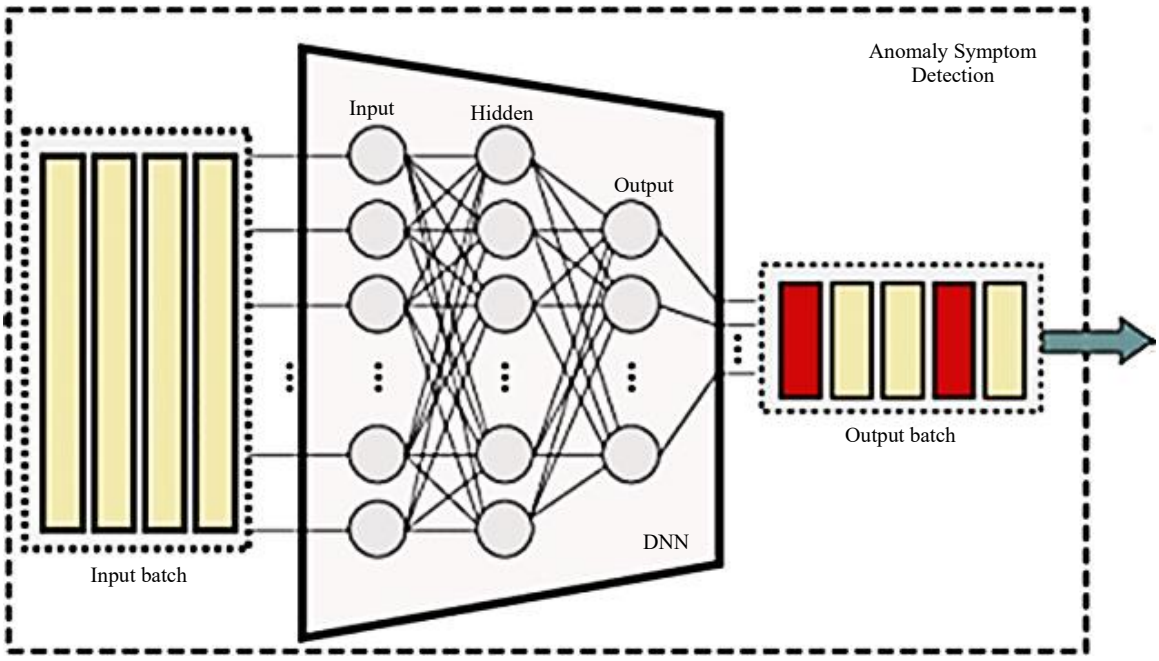

Figure 3. Example of deep neural net (DNN) stage of detection workflow [7].

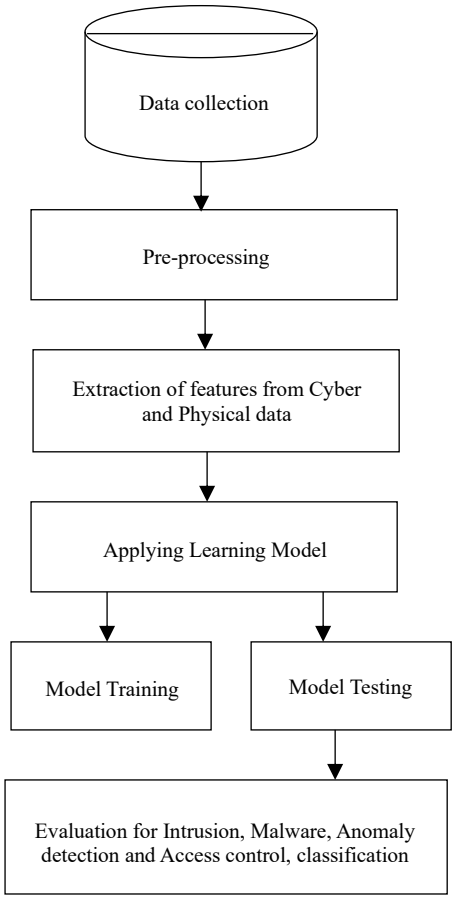

Figure 4. Framework of cyber-attack detection using learning approach [1].

CONCLUSION

The papers reviewed in this study demonstrate the potential of machines and deep learning techniques in enhancing cyber security. These techniques have been shown to be effective in detecting and preventing cyberattacks, improving the accuracy and efficiency of cyber threat intelligence, and enhancing the security of cyber physical systems.

However, these techniques also face significant challenges, including the need for large amounts of training data, the potential for bias and adversarial attacks, and the difficulty in interpreting and explaining the results of deep learning models. Further research is needed to address these challenges and develop more effective and efficient solutions for cyber security.

Overall, the papers reviewed in this study highlight the importance of machine and deep learning techniques in enhancing cyber security and demonstrate the potential of these techniques in improving the security and reliability of our digital infrastructure.

REFERENCES

1. Dhir S, Kumar Y. Study of machine and deep learning classifications in cyber physical system. In 2020 IEEE Third International Conference on Smart Systems and Inventive Technology (ICSSIT). 2020 Aug 20; 333–338.
2. Dastagiraiah C, Reddy VK. Novel machine learning methodology in resource provisioning for forecasting of workload in distributed cloud environment. J Theor Appl Inf Technol. 2022 May 31; 100(10): 3319–3327.

3. Rao KP, Reddy VK, Prasad T, Naresh D. A Cloud Computing Hierarchical Hybrid Intrusion Detection System Using Machine Learning. In: Disruptive technologies in Computing and Communication Systems. CRC Press; Florida, United States. 2024 Jun 24; 92–98.
4. Garigipati N, Reddy DV. An Integrated quantum and biometric key generation based cloud data security framework for structured and unstructured electronic health records. J Theor Appl Inf Technol. 2023 Mar 15; 101(5): 1648–1667.
5. Naga Shirisha VD, Reddy VK. Analysis of complex diseases with different machine learning techniques. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC). 2021 Jul 12.
6. Reddy VK, Reddy LS. Security architecture of cloud computing. Int J Eng Sci Technol. 2011 Sep; 3(9): 7149–55.
7. Haass JC. Cyber Threat Intelligence and Machine Learning. In 2022 IEEE Fourth International Conference on Transdisciplinary AI (TransAI). 2022 Sep 19; 156–159.
8. Sathya K, Premalatha J, Suwathika S. Reinforcing cyber world security with deep learning approaches. In 2020 IEEE international conference on communication and signal processing (ICCSP). 2020 Jul 28; 0766–0769.
9. Goyal Y, Sharma A. A semantic machine learning approach for cyber security monitoring. In 2019 IEEE 3rd International Conference on Computing Methodologies and Communication (ICCMC). 2019 Mar 27; 439–442.
10. Shariff DM, Abhishek H, Akash D. Artificial (or) fake human face generator using generative adversarial network (GAN) machine learning model. In 2021 IEEE fourth international conference on electrical, computer and communication technologies (ICECCT). 2021 Sep 15; 1–5.

