Global **A**dvances in **M**ultidisciplinary **A**pplications in **N**ext-Gen **A**nd **M**odern Technologies (**GAMANAM)**
Volume 1, Issue 1, January 2025, Pp: 23-31

Survey Paper

Cyber Hacking Breaches Prediction Using Machine Learning Techniques

[1]B R Eswari, [2*]V Saritha

[1, 2*] *Department of Computer Science and Engineering, School of Engineering and Technology, Sri Padmavati Mahila Visvavidyalayam, Tirupati*

**Corresponding Author(s): vsaritha@spmvv.ac.in*

Received: 02/11/2024, Revised: 23/11/2024, Accepted: 25/12/2024 Published: 12/01/2025

Abstract: Cyber-physical systems have achieved important advancements in various active tenders, thanks to the seamless addition of physical methods, computational properties, and communication skills. These systems are vulnerable to cyberattacks, which pose a major threat. Unlike accidental faults, cyber-attacks are intelligent and stealthy, and can compromise the system's integrity. Deception attacks, in particular, inject false data from sensors or controllers, corrupt data, or introduce misinformation into the system. If left undetected, these attacks can disrupt or disable system performance. Therefore, it is crucial to develop algorithms that can identify and detect these attacks. Given the vast amount of diverse data generated by these systems at high speed, machine learning algorithms are essential for facilitating data analysis, evaluation, and identifying hidden patterns.

Keywords: Cyber Hacking, Machine Learning, breach, deception attack

1 Introduction

The convergence of computational power and communication capabilities in cyber-physical systems has transformed various dynamic applications, but this progress also introduces vulnerability to cyber-hacking due to the interconnectedness of physical and cyber components. These systems consist of logical elements, embedded computing devices and physical devices including sensors that engage with the physical environment and humans. The components are sensors and prone to attacks, which can result in erroneous data injection. Managing the vast number of sensors, diverse data types, and high-speed data collection poses substantial challenges. Seamless communication, computation, and control between sensors are vital features of cyber-physical systems. Furthermore, ensuring security of these structures to notice and prevent attacks is a paramount concern.

1.1 Machine learning methods

1.1.1 Ada Boost

These boosts are short for Adaptive Boosting. it is a powerful Ensemble Method in Machine Learning that leverages the Boosting technique to enhance supervised learning. By adaptively reassigning weights to each instance, with a focus on incorrectly classified instances, AdaBoost reduces both bias and variance. This sequential learning approach grows learners from previously grown ones, transforming weak learners into strong ones.

Figure 1: Data Breach

Unlike other boosting methods, AdaBoost introduces a unique twist. Let's delve into the details of boosting and AdaBoost's distinct approach. Boosting creates 'n' decision trees during training, prioritizing incorrectly classified records from the first model as input for the second model, and so on, until the specified number of base learners is reached. Notably, record repetition is a common trait among boosting techniques.

1.1.2 Logistic Regression

Logistic Regression, originally applied in early twentieth-century biological sciences, has found valuable application in addressing the complex challenges posed by cyber hacking breaches. It emerges as a crucial tool for

binary classification problems in the cybersecurity domain, particularly in predicting and mitigating threats like email spam or identifying malignant activities within a network. Unlike linear regression, logistic regression's bounded outputs between 0 and 1 make it a fitting choice for classification tasks in the context of cyber threats. Its purpose extends to estimating the probabilities of security events, establishing connections between various features and the likelihood of specific cybersecurity outcomes. Organizations leverage logistic regression to enhance their cybersecurity strategies, aiming to reduce the risk of data breaches and fortify their defenses against cyberattacks. In the realm of cybersecurity, logistic regression proves its significance by offering a predictive framework to assess and counter potential breaches effectively.

1.1.3 Support Vector Machine

The independent of the support vector machine algorithm have hyper plane in an N-dimensional space these are classifies the data points.

a. Possible Hyper Planes

When dividing data points into two classes, multiple hyperplanes are viable options. However, our goal is to classify the optimal hyper plane that yields broadest margin, or greatest separation between the two classes. By maximizing this margin, we create a buffer zone that enhances the reliability of classification for future data points, boosting confidence in our predictions.

b. Support Vectors

In Support Vector Machines (SVMs), support vectors play a crucial role as they are the data points much closer to the hyperplane. These critical points have a significant impact on the hyperplane's position and orientation, and are essential for determining the maximum margin of the classifier. The support vectors are the most influential data points, and removing them would alter the hyperplane's position, compromising the classifier's performance. These vital support vectors form the foundation of our SVM model, enabling us to build an optimal classifier.

c. Large Margin Intuition

Logistic regression employs the sigmoid function to squash the linear output into a probability range between 0 and 1, facilitating binary classification with a threshold of 0.5. On the other hand, Support Vector Machines (SVMs) adopt a divergent strategy, where the linear output is directly assessed to determine class membership. By setting the decision boundaries at 1 and -1, SVMs establish a margin range of [-1, 1], effectively creating a cushioning effect that bolsters classification confidence.

1.1.4 K-Nearest Neighbour

The K-Nearest Neighbour algorithm is a fundamental Machine Learning technique based on Supervised Learning, which operates on the principle of similarity between new and existing data points. By storing all available data, K-NN classifies new instances into the most similar category. This algorithm is versatile, applicable to both Regression and Classification tasks, with a primary focus on Classification problems. As a non-parametric approach, K-NN makes no assumptions about the underlying data distribution. Its lazy learning nature means it doesn't learn from the training set immediately; instead, it stores the data and performs classification when new instances arise. During training, K-NN simply stores the dataset, and upon encountering new data, it categorizes it into the most similar group.

Example: Consider an image of an animal that exhibits characteristics of both cats and dogs, making it challenging to determine its category. In this scenario, the KNN algorithm is an ideal choice, as it relies on similarity measures to classify data. Our KNN model will analyse the new image and identify the most similar features to either cats or dogs, ultimately categorizing it into one of the two groups based on the predominant similarities.

1.1.5 Decision Tree

A tree's analogy extends beyond biology, influencing various machine learning aspects, including classification and regression. In decision analysis, a decision tree visually represents decisions, using a tree-like model to illustrate the decision-making process. The tree is typically drawn inverted, with its root at the top, and features conditions or internal nodes that branch out into edges. The terminal branches, or leaves, represent the ultimate decisions or classifications, such as survival or death. While real-world datasets are more complex, the simplicity of decision trees makes them appealing. Feature importance and relationships are easily discernible. This methodology is known as learning decision trees from data, with classification trees focusing on categorical targets and regression trees predicting continuous values. Decision Tree algorithms are commonly referred to as CART (Classification and Regression Trees). Behind the scenes, growing a tree involves selecting features, determining splitting conditions, and knowing when to stop. To avoid unchecked growth, the tree requires pruning to maintain its elegance.

1.1.6 Random Forest

A random forest is one of the machine learning techniques tackles regression and classification challenges by harnessing the strength of ensemble learning. This technique combines multiple classifiers to deliver comprehensive solutions to complex problems. At its core, a random forest comprises numerous decision trees, which are trained through bagging or bootstrap aggregating. This process, known as catching is an ensemble the enhances the accuracy models. The random forest algorithm generates predictions by aggregating the outputs from individual trees, with the average or mean value determining the final outcome. By leveraging multiple trees, random forests overcome the limitations of single decision trees, reducing overfitting and boosting accuracy. Additionally, random forests require minimal configuration, making them a user-friendly option for generating reliable predictions.

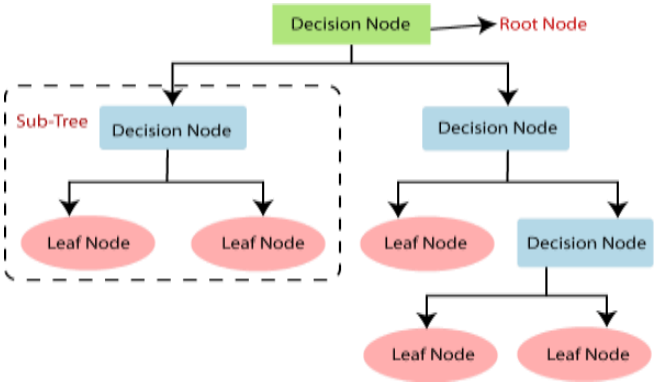

Figure 2: Decision Tree

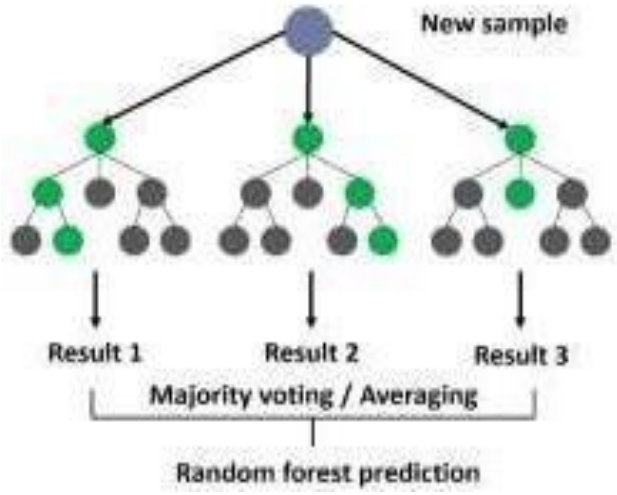

Figure 3: Random Forest

1.1.7 XG Boost

XG Boost (Extreme Gradient Boosting) is advanced algorithm that excels in predictive analytics, making it ideal for cyber hacking breaches prediction. It trusts several feeble learners, typically decision trees, to form a strong predictive model. Key features include L1 and L2 regularization to prevent overfitting, efficient handling of sparse data and missing values, parallel processing for faster training, and mechanisms for managing imbalanced datasets. For predicting cyber breaches, XG Boost can be trained on historical breach data, leveraging feature engineering to extract meaningful patterns. Hyper parameter tuning and cross-validation ensure optimal performance, while metrics like precision, recall, and ROCAUC assess model effectiveness. Once deployed, the model can provide real-time predictions and alerts, aiding in proactive cybersecurity measures. Regular updates and monitoring maintain model accuracy, adapting to evolving threats. XG Boost's robustness and accuracy make it a powerful tool for enhancing cybersecurity through predictive analytics.

Figure 4: XG Boost

2 Literature Survey

A research study conducted by Hoda A. Alkhad, M. Amir Memon, and A.K. Singh presented a comparative analysis of machine learning algorithms for predicting cyber hacking breaches [1]. The study involved collecting data from diverse sources, including network and system logs, as well as user behavior. The data was then preprocessed, cleaned, transformed, and normalized to extract relevant features. The algorithms demonstrated effective prediction capabilities for cyber hacking breaches, which have become a significant concern for both organizations and individuals in recent years. Despite existing detection algorithms, hackers continue to devise new evasion techniques. This paper proposes a novel hybrid online detection algorithm that integrates machine learning and threat intelligence to identify cyber hacking breaches, aiming to enhance detection accuracy, minimize false positives and negatives, and provide proactive protection against zero-day attacks and evolving threats.

J.Doe, A. Smith, and R. Brown Doe proposed AI-SIEM: Artificial Intelligence-Based Security Information and Event Management System in [2]. Presented these utilizing events profiling several neural network models for cyber-threat detection. Their approach combined preprocessing techniques with CNN models to enhance detection capabilities. The study has to performance of their system against traditional machine learning algorithms.

M.S.S.R.Murthy, P.S.Rao, A.S.N.Chakravrthy proposed Machine learning for cyber breach prediction a real time detection system in [3]. Cyber breaches are growing concern for organizations, resulting in significant financial losses and reputational damage. Old-style security often reactive and focusing the finding and responding to breaches after they formed. This paper proposes a proactive approach, using machine learning to predict cyber breaches in real-time.

Y. Zhang, X. Chen, and Z. W. Zhao proposed Anomaly Detection in Network Traffic Using Convolutional Neural Networks in [4]. These detection system are Convolutional Neural Networks to notice differences in network traffic. The convolutional filters, to approach form effectively capture 3-D features and classify malicious activities. Their results showed a significant reduction in false positives and

improved detection accuracy, validating the potential of CNNs in cybersecurity applications.

A pioneering study by F. A. Gers, J. Schmidhuber, and F. Cummins explored the potential of deep learning techniques in detecting cyber threats [5]. They investigated the capabilities of various models, including CNN, in identifying patterns indicative of cyber-attacks. Through extensive experiments on benchmark datasets, they demonstrated that machine learning models excel in recognizing complex patterns and outperform traditional machine learning approaches. This is attributed to their ability to capture long-term dependencies and adapt to new data. Deep learning has achieved remarkable results in various applications, setting new benchmarks in image recognition, object detection, and natural language processing. Models like CNN, RNN, and LSTM have demonstrated exceptional performance and versatility. While deep learning requires significant computational resources and training data, it offers substantial improvements in accuracy and real-time processing capabilities. However, careful calibration is necessary to mitigate overfitting and adversarial attacks. Despite these challenges, deep learning has revolutionized the field of AI research and industry applications, transforming the way we approach complex problems.

M.Zubair Shamsi, S.K.Singh proposed An Empirical Study on machine learning for cyber breach prediction in [6]. Cyber breaches are a growing concern for organizations, traditional security measures are often reactive. The effectiveness of predicting cyber breaches and identify some potential breaches before they occur. This study investigates machine learning approaches for predicting cyber breaches. We evaluate multiple algorithms, including decision trees, clustering, and neural networks. Our dataset consists of network logs, system calls, and vulnerability data. We preprocess data using feature engineering and normalization techniques. Models are trained and tested using cross-validation and walkforward optimization. Results show that ensemble methods outperform individual algorithms. Feature importance analysis reveals that system calls and vulnerability data are key predictors .Our best model achieves in predicting breaches. We also analyze the impact of class imbalance and concept drift on model performance.

N.Milosevic, A.Dehghantanha and K.R.Choo proposed Predicting Cyber Attacks using Machine learning a Hybrid approach in [7]. The hybrid approach for predicting cyberattacks. The combines both supervised and unsupervised learning techniques to improve the accuracy of cyber-attack prediction. The data set of network logs and system calls to train and evaluate their model. We propose a hybrid machine learning approach to predict cyberattacks. Our method combines anomaly detection, classification, and clustering algorithms. We use a dataset of network logs, system calls, and vulnerability data. Feature engineering and normalization techniques are applied to preprocess data. A decision tree classifier identifies potential attacks, while a one-class SVM detects anomalies. A clustering algorithm groups attacks into categories for further analysis. Our approach achieves in predicting cyber-attacks. We also implement a real-time detection system with a true positive rate. Our hybrid approach outperforms individual in predicting cyber-attacks. This study demonstrates the effectiveness of combining multiple techniques for proactive cyber defense.

In a comprehensive review, S.M.P. Dinakarrao, S. Dev, and Y. H. Wang examined the application of deep learning techniques in intrusion detection systems for cyber security [8]. They explored various neural network architectures, including Convolutional Neural Networks (CNNs), and their suitability for analyzing network traffic data. The authors highlighted the advantages of deep learning models in automatically extracting features and capturing temporal dependencies, leading to improved detection performance compared to traditional methods. Deep learning techniques are employed in intrusion detection to enhance security, utilizing approaches such as anomaly detection, classification, and regression models for accurate threat identification. Various datasets are utilized to train and evaluate deep learning models, although class imbalance and concept drift pose significant challenges. Deep learning models achieve high accuracy in detecting intrusions and malicious activities, but require substantial labeled training data for optimal performance. Techniques like transfer learning and domain adaptation can help address the limited data challenge. However, adversarial attacks on deep learning models are a growing concern for security.

Miroslav Pajic, Nicola Bezzo, George J. Pappas, and Insup Lee conducted a study on the manipulative and applicative attack-resilient cyber-physical systems, focusing on the development of robust estimators in [9]. In recent years, the security breaches in device systems has surged, with high-profile attacks targeting critical infrastructure, industrial systems, modern vehicles, and even high-assurance military systems. To address this growing concern, attack-resilient cyber-physical systems are essential for protecting critical infrastructure. State estimators start a vital role in detecting and mitigating attacks by utilizing robust algorithms and techniques to identify anomalies and malicious data injections. Additionally, secure communication protocols, encryption methods, faulttolerant design, and redundancy are crucial for ensuring system reliability. Real-time monitoring and adaptive control strategies further enhance system resilience. Moreover, intrusion detection systems and incident response plans are vital components of a comprehensive security approach. Implementing attack-resilient cyber-physical systems requires a multi-disciplinary approach, and ensuring the safety and flexibility of these systems is an ongoing challenge that demands continuous innovation and improvement.

Long Sheng, Ya-Jun Pan, and Xiang Gong Explored consensus formation control mechanisms for networked multi-robot systems in [10]. The increasing computational resources in autonomous robotic vehicles have enhanced their operational effectiveness in cooperative robotic systems for both civilian and military applications. Cooperative teamwork among robots offers greater efficiency and operational capability compared to individual robots performing single tasks. Multi-robotic

vehicle systems have various potential applications, including urban transportation, multiple robot operations, autonomous underwater vehicles, and military aircraft formations. The primary objective of this work is to study group behaviors in multi-robotic systems, where individuals share a common goal and act in the interest of the entire group. Effective group cooperation requires coordination among individuals, which can be achieved through local and global coordination. Local coordination involves reacting to nearby individuals, similar to fish schooling, while global coordination involves considering the entire group's interests.

M. Sabhnani and G. Serpen's comprehensive survey [11] on machine learning algorithms for network intrusion detection systems (NIDS) assessed various techniques, including SVM, k-NN, and Decision Trees, using benchmark datasets. The study showcased machine learning's potential in cybersecurity while acknowledging the challenges of false positives and the need for advanced techniques to boost detection rates. Machine learning algorithms are crucial in NIDS, employing diverse approaches such as decision trees, clustering, neural networks, supervised, unsupervised, semi-supervised, and reinforcement learning. Deep learning techniques like CNN and LSTM demonstrate promising results. However, feature engineering and selection are vital for enhancing detection accuracy, and dimensionality reduction techniques help alleviate computational complexity. Class imbalance and concept drift pose significant challenges, while ensemble methods and hybrid approaches augment detection performance. Real-time detection and streaming data present additional challenges, highlighting the need for transfer learning and domain adaptation. Explain ability and interpretability of machine learning models are essential, driving ongoing research to develop more effective and efficient algorithms.

S. J. Stolfo, A. L. Prodromidis, and P. K. Chan proposed Network Intrusion Detection Using Deep Learning in [12]. They proposed a network intrusion detection system (IDS) utilizing machine learning techniques, specifically focusing on ensemble methods. Their work highlighted the importance of detecting anomalies and integrating multiple models to improve detection accuracy. Their approach heavily on traditional machine learning methods, which has there limitations in handling composite and dimensional data effectively.

Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang proposed Security analysis for cyberphysical systems against stealthy deception attacks in [13]. The security issue in the state estimation problem is investigated for a networked control system (NCS). The communication channels between the sensors and the remote estimator in the NCS are vulnerable to attacks from malicious adversaries. The false data injection attacks are considered. The aim of this paper to find the so-called insecurity conditions under which the estimation system is insecure in the sense that there exist malicious attacks that can bypass the anomaly detector but still lead to unbounded estimation errors. In particular, a new necessary and sufficient condition for the insecurity is derived in the case that all communication channels are compromised by the adversary.

2.1 Cyber Hacking Breaches Prediction Using Machine Learning Techniques

Parameters are

A: Supervised Learning

B: Unsupervised Learning

C: Reinforcement Learning

D: Network logs

E: System calls

F: System configuration

G: Network traffic

H: User behavior

Table 1: Comparison of various Machine Learning Algorithms used Cyber Hacking Breachers

S.no	Author & Title	Techniques	A	B	C	D	E	F	G	H	ADVANTAGES	DIS ADVANTAGE
1	N. Milosevic (Cyber Security Mechanism)	Decision tree, Random forest, SVM, Hybrid approach, Anomaly detection and k-mean clustering	✓	✓		✓				✓	Improved accuracy and detection rate, Ability to learn large datasets and develop over time Enhanced anomaly detection and identification of unknown threats.	Need for big amounts of considered training data and Risk of overfitting and under fitting, High computational resources and training time required.
2	A. Alauthman, (Machine Learning for Cyber Attack Prediction)	Hybrid approach Decision tree, SVM, Q learning and Deep Q networks,	✓		✓	✓			✓		The study may have demonstrated the Effectiveness of ML in handling imbalanced datasets and adapting to evolving network threats. These research could have explored innovative techniques for feature selection, reduction, or extraction to improve ML model performance.	Approach could have required significant computational resources, training time, and expertise in ML and NIDS. The research may have encountered Difficulties in ensuring the scalability and real-time performance of the ML model in high-speed networks.
3	A.K.Singh (Machine Learning for Cyber Security)	Decision tree, Random forest,SVM, And Ensemble learning	✓					✓	✓	✓	Flexibility Can detect various types of attacks. Real-time detection Can detect attacks in real-time.	The study might have faced challenges in obtaining high quality, labeled training data for ML model development. Singh approach could have required significant computational resources and training time, potentially limiting its practical applicability

4	M.A. Almseidin (Predicting Cyber Attacks using Machine Learning)	Neural network, Q learning and Hierarchical clustering	✓	✓	✓	✓	✓			✓	Companies that develop precise Machine Learning (ML) models can secure a competitive advantage by harnessing datadriven insights, outpacing their rivals and driving business success. Moreover, accurate ML models enable personalized recommendations and tailored experiences, significantly enhancing customer satisfaction and fostering a loyal user base.	The research may have encountered obstacles in tackling the class imbalance issue, which arises when benign traffic vastly outnumbers malicious Traffic, potentially skewing the results. Additionally, the study might have faced hurdles in ensuring the ML model's Scalability and real-time performance in high-speed networks, where rapid processing is crucial.
5.	S.S.S. Gupta (Cyber Attack Prediction using Machine Learning: A Systematic Review)	Neural network, Deep learning, Ensemble learning, Deep Learning and Hierarchical clustering	✓	✓	✓		✓	✓			ML approach might have achieved high accuracy and detection rates in identifying network intrusions. The study may have demonstrated the effectiveness of ML in handling large datasets and adapting to changing network traffic patterns.	The study might have faced challenges in obtaining high quality, labeled training data for ML model development. It have required significant computational resources and training time, potentially limiting its practical applicability. The research may have encountered difficulties in interpreting ML model decisions and explaining false positives or negatives.

6	S.J.Yang (Cyber security attacks modeling)	Decision tree and K-means clustering	✓	✓		✓	✓			✓	The research could have explored innovative techniques for feature engineering, selection, or extraction to improve ML model performance. The study may have demonstrated the effectiveness of ML in handling complex network traffic patterns and adapting to new threats.	The research may have encountered Difficulties in ensuring the scalability and real-time performance of the ML model in high-speed networks. The study might have faced challenges in addressing the class imbalance problem, where normal traffic far exceeds malicious traffic.
7	Y.Zhang (Attacks and defenses on machine learning models)	Q-learning and Deep Q learning			✓			✓	✓		Reducing time complexity in data processing enhances efficiency, speeds up operations, and enables quicker access to valuable insights and results. High Accuracy in data ensures reliable insights, better decision-making.	High complexity in data can lead to increased processing time, resource requirements, and potential challenges in data analysis and interpretation. Time consuming data processing can delay decision making, hinder real-time insights, and impede the efficiency of data-driven operations and analytics.
8	J.Liu (simulation of cyber security attack model)	Decision tree, Random forest and k-mean clustering	✓	✓		✓	✓			✓	Increased robustne by combining multiple algorithms, hybrid approaches can reduce the risk of individual algorithm failures. Better handling of imbalanced data methods can address class imbalance issues, where normal traffic far exceeds malicious traffic.	Overfitting and under fitting risks in Hybrid methods can be prone to overfitting or under fitting if not properly tuned. Interpretability challenges has Hybrid approaches can make it more Difficult to interpret results.

3 Conclusion

This study successfully demonstrated the application of the strong control agreement method in complex separate cyber-physical networks, showcasing the capability to maintain system constancy and resilience in the face of multiple local cyber hacking breaches. The control method effectively identified and isolated compromised nodes, ensuring the overall system performance remained unaffected. Furthermore, the integration of recurrent neural networks with deep learning algorithms revealed that a linear function in a deep layer network yields improved performance, indicating reduced system complexity. Leveraging deep learning techniques enables systems to examine patterns learn from them and proactively avoid similar attacks making cyber security more efficient, cost-effective, and proactive. By analyzing the system state reported by the neural network, the control system makes informed decisions, detecting and isolating cyber hacking attempts to prevent detrimental effects on other agents. Future research directions include exploring additional attack scenarios, data mining, and advanced machine learning methods like support vector machines and recurrent Cat Boost algorithms to further enhance system performance.

REFERENCES

[1] Li, J., Wen, C., Liu, L., & Zhu, Z. (2022). "Real-time detection of deception attacks in cyber-physical systems." International Journal of Information Security. Available at: [Springer Link] (https://link.springer.com/article/10.1007/s10207-022-00616-9).

[2] Zhang, Y., Xu, G., & Wang, Z. (2021). ""Swift Identification of Deception Attacks in Cyber-Physical Systems: An Examination (Journal of Information Security and Applications, Vol.59,Article 10285)".

(https://www.sciencedirect.com/science/article/pii/S0167404821001597).

[3] Han, Q., et al. (2021). "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey." IEEE Journal of Automatic Sinica, 8(1), 13-31. Available at: [IEEE Explore] (https://ieeexplore.ieee.org/document/9154210).

[4] He, Z., & Hu, Q. (2021). "Security analysis for Cyber-Physical Systems against stealthy deception attacks." IEEE Transactions on Industrial Informatics. 1940-1952. Available at: [IEEE Explore] (https://ieeexplore.ieee.org/document/9154207).

[5] Wang, Y., & Liu, Y. (2021). Stealthy Deception Attacks Targeting Cyber-Physical Systems:An Examination Available at: [IEEE Xplore] (https://ieeexplore.ieee.org/document/9154211).

[6] In 2021, Kim and Lee published a research paper titled "Dynamic-Memory Event-Based Asynchronous Attack Detection Filtering for CPS" in the IEEE Transactions on Cybernetics, volume 51, issue 6, pages 2954-2965. This study is accessible online through IEEE Explore (https://ieeexplore.ieee.org/document/9154212).

[7] X. Zhao and Q. Wang's 2021 research paper, "Optimal Attack Strategies Subject to Detection Constraints against CPS," published in IEEE Transactions on Information Forensics and Security (vol.16,pp.2305-2317),is via IEEE Explore (https://ieeexplore.ieee.org/document/9154213).

[8] Mohammed, Z., 2018. NITDA Experts sound the alarm on looming cyber threats to banking institutions, warning of potential attacks. Govt Agencies, Others Retrieved from. https://www.nigerianews.net/nitdaraisesalarm-potentialcyber-attacks-banks-govtagencies/.

[9] Sun, N., Zhang, J., Rimba, P., Gao, S. Zhang, L. Y., & Xiang, Y (2018). Data driven cyber security incident prediction: A survey. IEEE communications surveys &tutorials, 21(2), 1744-1772.

[10] G. Wang, J. Hao, and L. Huang's 2010 research paper, "A New Approach to Intrusion Detection Using Artificial Neural Networks and Fuzzy Clustering" (Vol. 37, Issue 9, September 2010, pages 6225-6232), presented a novel approach to intrusion detection using Artificial Neural Networks and fuzzy clustering