International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Review on Adaptive Learning Framework for Cyber Financial Thread Detection

Naveen Krishna Yadav

Research Scholar, Department of Computer Science & Engineering, Maharana Pratap College of Technology, Gwalior

Naveenkrishna1812@gmail.com

Richanya Bhadouria

Professor, Department of Computer Science & Engineering, Maharana Pratap College of Technology, Gwalior

Richanyaqwerty@gmail.com

Abstract— As digital financial services (DFS) have grown rapidly, they have become more vulnerable to advanced cyberattacks and require intelligent and adaptive security solutions. This review intends to explore the most recent developments in the Adaptive Learning frameworks for Cyber Financial Threat Detection, focusing on techniques, applications, performance analysis and future research directions. To analyze recent studies on the development of deep learning-based cybersecurity models, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, Transformerbased architectures, and Graph Neural Networks (GNNs) were used in a systematic review approach. The review also covers popular benchmark datasets, evaluation methods and some new technologies like Explainable Artificial Intelligence (XAI) and Federated Learning. The results revealed that adaptive deep learning is effective in detecting fraud, intrusion, malware, phishing and anomaly than traditional rule-based detection methods. Detected studies were found to have high detection accuracy, higher precision and recall rate, lower false-positive rates, and better adaptability to new cyber threats. However, there are still some limitations in the area of computational complexity, small number of labeled data, each model's interpretability, and its deployment in real time. The review underscores the opportunities and challenges of adaptive deep learning to offer scalable, intelligent, and resilient cybersecurity solutions, and suggests research areas that could be fruitful for building a more secure digital financial ecosystem.

Keywords—Adaptive Deep Learning, Cyber Financial Threat Detection, Intrusion Detection, Fraud Detection, Explainable Artificial Intelligence (XAI).

I. Introduction

Financial Services is witnessing a rapid digital transformation, which has greatly enhanced access, speed and efficiency of FS services globally. With the advancement of technology, online banking, digital payment systems, cryptocurrency transactions, mobile wallets, and cloud-based financial platforms are becoming integral to the present economic activities. Despite the technological advancements, there have been opportunities for cybercriminals to find weaknesses in financial systems. Financial threats in the cyber world are becoming more complex, including phishing, ransomware, fraud detection evasion, account takeover, identity theft and high-tech attacks by malicious software. With attackers always changing tactics,

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

financial institutions need intelligent, adaptive and automated security solutions that can adapt to the changing threats in real-time. Many traditional cybersecurity strategies are based on a set of rules, signature-based detection and static machine learning models. These methods work against known attacks, but can have a disadvantage in detecting new or evolving forms of cyberattacks. Financial cyberattacks are constantly new and innovative, and security systems must be able to learn from new data, adapt to new attack patterns, and enhance their ability to detect new attacks without being manually "trained." The demand has prompted the search for new technologies, like Artificial Intelligence (AI) and Deep Learning (DL), as potential solutions for the next generation of cybersecurity solutions [1].

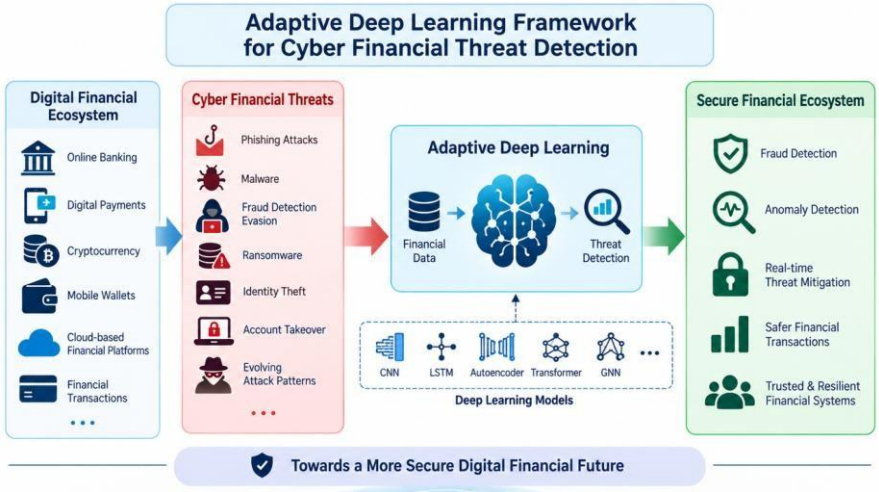


Fig. 1 Adaptive Deep learning Framework for Cyber Financial Threat Detection [1]

Deep Learning has been very successful analyzing vast amounts of complex, multidimensional financial and network data. These models can automatically discover meaningful patterns in large datasets, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Transformer-based architectures. These models have been extensively used in fraud detection, anomaly detection, malware classification, intrusion detection, and transaction behavior analysis [2]. They can discover hidden relationships in structured and unstructured data, allowing them to identify suspicious activities more precisely than conventional machine learning approaches. Deep learning can be trained directly from raw or processed data and learns hierarchical feature representations, thereby diminishing the need for manual feature engineering and enhance detection performance for a wide range of financial security applications.

While deep learning models are impressive, real-world cybersecurity landscapes demand more than just a correct prediction. Financial systems produce vast amounts of live transaction data, authentication logs, network traffic and user behaviour data that needs to be constantly analyzed. Intelligent security systems must be adaptable to offer performance improvements when the attack patterns change over time, as seen in static models. To overcome this problem, Adaptive Deep Learning introduces technologies to allow models to learn continually with better training methods, adaptive feature extraction, hybrid architectures, and learning mechanisms. These features enable detection systems to be more adaptable and resilient to new threats and to remain high-performing in volatile financial climates.

The Adaptive Deep Learning frameworks integrate cutting-edge neural network structures with adaptable learning algorithms to improve cyber financial threat detection. These are able to examine transaction patterns, customer behaviors, network activity and security events in parallel to pinpoint suspicious activities more accurately. They can adapt detection thresholds over time, enhance the ability to detect anomalies, prioritize those events deemed as high risk, and fine-tune security monitoring as new data emerges. In the era of financial institutions moving to the cloud, digital banking, IoT-enabled payment systems, and distributed financial infrastructures, deep learning systems can be adaptive, scalable, and intelligent to defend against the next generation of cyberattacks [3], [4], [5].

There is a considerable amount of recent research that has found adaptive deep learning architectures to be suitable for financial cybersecurity applications which include fraud detection, intrusion detection systems, ransomware prevention, malware detection, phishing identification, network traffic analysis, and intelligent threat monitoring. To boost the detection accuracy and decrease false positives in complex financial settings, researchers have explored several deep learning models, such as CNNs, LSTMs, Autoencoders, Graph Neural Networks (GNNs), and Transformer-based models. Additionally, AI capabilities like explainable AI, federated learning, transfer learning and real-time security analytics have broadened the scope of adaptive cybersecurity solutions, making them increasingly relevant for financial institutions who are dealing with a distributed, cloud-based and data-intensive environment.

This is a comprehensive review paper that provides a detailed description of Adaptive Deep Learning Frameworks for Cyber Financial Threat Detection. It covers the history of AI in cybersecurity, its relevance to financial security, the important techniques, data sources, evaluation methodologies, and areas of application of recent research. Further, this review highlights current problems such as data imbalance, computational complexity, real-time deployment, interpretability, privacy protection, and adversarial attacks, and proposes future research directions on the improvement of more robust and adaptive cyber financial defense system. This review aims to synthesize the latest advances in this dynamic and evolving domain, offering practitioners and researchers a framework to better understand the integration of adaptive deep learning in bolstering cybersecurity and enhancing threat identification in contemporary digital financial landscapes.

Sources of Data: This review is based on the work of recent research studies that have examined adaptive learning models with publicly available cybersecurity data. The most commonly used datasets are CICIDS2017, CSE-CIC-IDS2018, UNSW-NB15, NSL-KDD, CIC-IoT 2023, WUSTL-IIoT-2018, WUSTL-IIoT-2021, and Kaggle benchmark datasets. They consist of network traffic, intrusion records, malware behavior, phishing patterns, and attack scenarios that involve financial cybersecurity, which can be used for comparing the various adaptive learning techniques.

II. Literature Review

Asha & Raja, 2026 et al. To implement an adaptive cyber threat detection, a hybrid AI-based firewall framework was developed, leveraging CNN-LSTM-Autoencoder, Explainable AI (XAI), Federated Learning (FL), and Multi-Agent Reinforcement Learning (MARL).

Evaluation was carried out on benchmark datasets such as CICIDS2017, UNSW-NB15, NSLKDD, CSE-CIC-IDS2018 and the large scale SRM-TFC-2024 with 127 million records.

The accuracy of the performance results ranged from 79–82%, precision was 87–92% and the false positive was only 1–3%. The proposed QX-FedMARL architecture achieved better performance than the traditional firewall and IDS methods, and has the ability to make decisions transparently, share intelligence with privacy, and detect next-generation zero-day attacks effectively [6].

Zahangir & Sultana, 2026 et al. With the assistance Integrated AI Cybersecurity System, LSTM Anomaly Detection, SHA-256 Homomorphic Hashing for Data Integrity, Q-learning Automated Threat Response, and Lattice-based Encryption for Quantum-resistant Security. High anomaly detection accuracy, reliable tamper identification and adaptive response to incidents under various threat situations were seen during evaluation in a simulated IoT environment. The embedded design enhanced the scalability, automation, and security of resource-limited digital infrastructure. Potential was shown in the fields of smart cities, healthcare systems and critical infrastructure and future enhancements focused on adaptability in real time and validation in heterogeneous operational environments [7].

Roopesh 2024 et al. Systematic review of Machine Learning and Deep Learning in cyber security in network, cloud and IoT environments according to PRISMA guidelines. Among the deep learning models, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) outperformed rule-based security techniques in terms of threat detection, anomaly detection, and intrusion prevention. There were a number of challenges in implementing the system, such as adversarial attacks, data privacy issues, and high computation needs. Suggested solutions they discussed were adversarial training, federated learning, and model optimization to enhance security, efficiency, and real-world deployment of intelligent cybersecurity systems [8].

Maureen 2024 et al. Deep Learning greatly improved cybersecurity by enabling automated detection of malware, phishing attacks, and insider threats, as well as real-time threat detection capabilities. Deep Learning helped cybersecurity significantly by enabling automated detection of malware, phishing attacks and insider threats and real-time threat detection capabilities. The convolutional kernel and recurrent neural networks were able to effectively learn such complex patterns from network traffic, user behavior and system logs without requiring much of manual feature engineering. It enabled higher accuracy in detection for various cybersecurity applications. There were key challenges, such as the inability to withstand attacks and the lack of model robustness.

Adversarial training, data augmentation, and incorporating traditional security methods bolstered the overall resilience and adaptability of cyber defense systems [9].

Srinivasan 2022 et al. The thorough study covered the various fields of cyber security such as Intrusion detection, Malware analysis, Phishing detection, Spam filtering, Botnet detection, Insider threat detection, Cryptography, Biometrics, and Network traffic analysis (NTA) within the scope of Deep Learning. Several deep learning architectures outperformed traditional machine learning approaches to complex security applications.

The new applications fields were cloud security, Internet of Things, edge computing, cyberphysical systems, smart cities, and Industry 4.0 environments. Current studies pointed out the necessity of using more sophisticated deep learning structures for maximizing scalability, adaptability and security applications in the future [10].

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Table I. Literature Summary

Author/Year	Method	Dataset	Results	Research Gaps
Lilhore et al. (2025) [11]	SmartTrust using CNN, LSTM, Transformer, RL, Blockchain (ZTA)	CIC-IoT 2023, UNSW-NB15	99.19% insider threat, 98.23% privilege escalation, 99.27% data breach detection; >40% fewer false positives.	High computational complexity limits resourceconstrained deployment.
Radha et al. (2025) [12]	Hybrid GNN + RL	Kaggle benchmark dataset	96.8% accuracy, 95.2% precision, 94.7% recall, 98.3% ROCAUC.	Needs validation on real-world FinTech datasets.
Saeed (2025) [13]	LSTM, SHA-256 hashing, Qlearning, Lattice encryption	Simulated IoT network	High anomaly detection, secure integrity verification, adaptive response.	Requires live heterogeneous environment validation.
Mesadieu et al. (2024) [14]	DRL (Q-Network) for SCADA anomaly detection	WUSTL-IIoT-2018, WUSTL-IIoT-2021	99.36% attack detection accuracy.	Limited evaluation beyond SCADA.
Soltani et al. (2024) [15]	Multi-agent continual anomaly detection with Federated Learning (CNN, LSTM)	CIC-IDS2017, CSE-CIC-IDS2018	CNN >95% detection under concept drift; LSTM detected attacks within first 15 packets.	Needs optimization for large-scale distributed deployment.

III. Adaptive Deep Learning Techniques for Cyber Financial Threat Detection

In the digital age, financial systems are increasingly becoming a target for cyberattacks, and Adaptive Deep Learning is emerging as one of the most promising strategies to improve the cybersecurity of these systems. With the increasing use of digital banking, online payment platforms, mobile applications, cloud computing, and cryptocurrency services by financial institutions, cyber threats are becoming larger and more complex. Attackers continually refine

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

their tactics and tricks to defeat standard defenses, leading to static detection methods becoming progressively less effective. To tackle this problem, Adaptive Deep Learning introduces the ability to continuously improve the model's learning process, adapt their recognition of new attack patterns, and improve the accuracy of the attack recognition process in dynamic financial environments [16], [17], [18], [19].

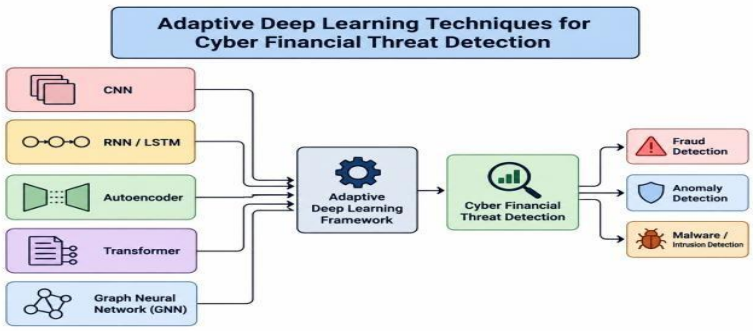


Fig. 2 Adaptive Deep Learning Techniques For Cyber Financial Threat Detection[16] One of the key advantages of adaptive deep learning is its capacity to automatically learn meaningful features from high dimensional and large datasets. Financial cybersecurity requires the analysis of a wide range of data, such as transaction data, user authentication logs, network traffic, device data and user behavior. Deep learning models are more complex than traditional machine learning approaches, which rely on a substantial amount of manual feature engineering, and they learn hierarchy representations directly from the data at hand. By automating the process of identifying patterns, security systems can detect subtle anomalies that could signal fraudulent transactions, phishing, account takeover, or malware activities. Structured financial data and network traffic are being used to identify complex patterns, making Convolutional Neural Networks (CNNs) a widely used approach for cyber threat detection. The layers' structure allows to extract local feature relationships while using pooling operations to remove noise. CNN-based methods have been shown to be successful in malware classification, phishing detection and intrusion detection, especially when dealing with financial security information that can be expressed as feature matrices or converted to imagelike representations for analysis.

Recurrent Neural Networks (RNNs) are crucial in handling sequential financial transactions, where the sequence of events is critical to the ability of threat detection. Financial transactions are made continuously over time and so it is important to have temporal information to recognize suspicious behavior. The Long Short-Term Memory (LSTM) networks are more powerful than the previous recurrent networks as they are able to preserve long-term memory of the inputs by getting rid of the Vanishing Gradient Problem. Learning these relationships across a number of time steps, rather than just one, enables LSTM-based techniques to detect unusual spending behavior, abnormal login sequences, and changing fraud patterns.

An alternative deep learning approach to anomaly detection in financial cybersecurity is the autoencoder. These are unsupervised models that learn compressed representations of typical system behaviour, and then reconstruct the original data with minimal error. Anomaly handling is very important in reconstruction errors; if the abnormal behavior takes place, the system can recognize the unseen threats without labeled attack data. This is why autoencoders have found

great applications in detecting zero-day attacks, insider attacks, and unknown fraud patterns, where labelled data may not be abundant.

Architectures based on transformers have gained significant attention recently for their capability of capturing long-range dependencies in complex financial data. Transformers, in contrast to sequential recurrent models, make use of a self-attention mechanism that considers the relationships between several elements of the data. This feature helps process vast amounts of financial data more efficiently and helps decipher the context of relationships between transactions, user activities, and security events. With the rise of financial institutions producing more and more complex, interconnected data, Transformer models offer more scalability in real-time threat detection.

Financial transactions are naturally part of interconnected network of customers, accounts, devices, merchants and payment channels, which is another reason why Graph Neural Networks (GNNs) have become a crucial development in the field of adaptive cybersecurity. GNNs learn relationships from the structures of the graphs rather than just individual records. This relational learning capability enables the identification of organized fraud rings, money laundering schemes and coordinated cybercrime networks that can't be seen when transactions are analysed one by one.

The key attribute that sets these deep learning methods apart from traditional static models is adaptability. Unlike traditional training methods that use static datasets, adaptive approaches integrate continuous learning techniques, enabling models to adapt as they receive new financial information. Online learning mechanisms make it possible for the models to be updated incrementally without having to start training from scratch, and transfer learning can take what is learned in one cybersecurity application and use it for another, related financial application. These adaptive strategies help to decrease maintenance costs and increase resistance to constantly changing attack methods.

In addition, the hybrid deep learning architectures have emerged as a popular choice as they make use of the best of several models in a single system. CNN-LSTM combinations are an example where CNNs are used for spatial feature extraction and LSTMs are used for temporal sequence analysis. In much the same way, Autoencoder-Transformer hybrids combine anomaly detection and context-aware learning to enhance detection accuracy. These combinations can lead to higher accuracy, better generalization and lower false-positive rates than can single models working alone.

The latest advancements have also extended the capabilities of adaptive deep learning by incorporating other AI technologies to further power the system. Explainable AI (XAI) enhances model transparency by offering explainable explanations behind detection choices and aiding monetary establishments meet regulatory requirements and foster trust in automated security systems. Federated Learning is a method that allows multiple organizations to work together to train deep learning models, while also maintaining the privacy of the customer, which is especially useful for cross-institutional fraud detection. Real-time analytics platforms that are connected to adaptive deep learning platforms also enable continuous monitoring of financial ecosystems without causing significant delays in operations.

Even with these strides, there are still some technical hurdles. While practical implementation remains hindered by the high computational demands, data imbalance between genuine and

fraudulent transactions, limited availability of cybersecurity datasets with labels, adversarial attacks on deep learning systems, and deployment challenges in real-time financial systems, the future of applying deep learning to detect fraud and crime in finance holds promise. The key advantages of adaptive deep learning include automated feature learning, continuous adaptation, and intelligent analysis of complex financial data, making it a powerful tool for cyber financial threat detection while addressing the challenges of scalability and reliability. By overcoming the limitations of scalability and reliability, adaptive deep learning offers a powerful tool for detecting cyber threats in the financial sector. As deep learning models advance, the development of CNNs, LSTMs, Autoencoders, Transformers, Graph Neural Networks and hybrid models shows how these techniques are closing the gap on the evolving nature of cyber threats. In the rapidly evolving landscape of financial cybersecurity, these methods are likely to become a core component of the systems that will be built to safeguard the modern digital financial ecosystem from new attacks in the future.

IV. Applications and Performance Evaluation in Financial Cybersecurity cybersecurity. Financial Cyber Security Application and Performance Evaluation. By examining the vast amounts of transaction, network, and user behavior data, Adaptive Deep Learning has emerged as a major weapon in the financial sector's fight against cybersecurity threats in today's complex financial landscape. These models can be used by financial institutions to identify emerging cyber threats as they happen, and to enhance the accuracy of detection and speed of response. Recent research indicates that adaptive deep learning has been effectively used in a variety of financial security areas, such as in [20], [21], [22].

It has many applications, such as fraud detection, intrusion detection, malware and ransomware identification, phishing detection, anomaly detection, and cloud-based financial security. These models are able to analyse transaction patterns, system logs, network traffic, emails and user activities for any suspicious activity that could suggest unauthorised access, fraudulent transactions or developing cyberattacks. Deep learning is more effective than traditional rulebased security systems in the financial landscape because of its ability to learn and adapt to new patterns of attack.

Standard metrics like Accuracy, Precision, Recall, F1-Score, ROC-AUC, False Positive Rate are widely used to assess the performance of adaptive deep learning models. Such measures can help to measure the ability to detect such fraud and the operational reliability, especially in financial datasets where the incidence of fraudulent transactions is relatively low. Beyond classification accuracy, researchers assess the computational efficiency and response time of models to ensure that they can be applied in real-time financial security applications [23], [24]. While there have been great advances in threat detection, there are still practical challenges in deployment, including high computation needs, lack of labeled data sets, privacy issues, model interpretability, and adversarial attacks. The current research aims at developing lightweight deep learning architectures, explainable AI, federated learning, and real-time analytics to enhance practical implementation. In summary, adaptive deep learning is further bolstering financial cybersecurity, offering flexible, precise, and intelligent solutions that can effectively tackle increasingly complex cyber threats.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

V. Challenges, Research Gaps, and Future Directions A. Challenges

Although there have been numerous advancements, Adaptive Deep Learning has some challenges in financial cybersecurity. Available high-quality, labeled datasets are another key challenge, because financial data is often sensitive and subject to privacy laws. In addition, deep learning models are also resource intensive and can be challenging to deploy in real-time for certain financial systems. Moreover, the issues of false positive, model interpretability and adversarial attacks remain to impact the reliability and trustworthiness of such security systems.

B. Research Gaps

Research conducted to date shows that there are several areas that need to be explored. Previous research has concentrated on a particular type of attack, for example fraud, or phishing, but not on the development of a unified model to detect multiple financial threats at the same time. Very few research works have been performed on light weight deep learning model for resource-limited systems and cross-platform financial systems. In addition, the performance of various models on a study-by-study basis is difficult to compare, due to the lack of uniform datasets and evaluation procedures.

C. Future Directions

Going forward, adaptive, explainable and privacy-preserving deep learning frameworks for financial cybersecurity need to be developed. By leveraging Explainable AI (XAI), Federated Learning, Graph Neural Networks (GNNs), and Transformer-based architectures, detection accuracy and transparency of the models can be enhanced. There is also a need for researchers to develop real-time threat detection algorithms, automated systems for rapid response and scalable cloud-based security solutions to enhance protection against emerging threats in the cyber financial landscape. In the rapidly evolving landscape of financial technologies, adaptive deep learning is poised to become an integral component in shaping robust and resilient digital financial ecosystems.

V. Conclusion

As digital financial services grow more vital for banking, payment, and cloud-based financial systems, cybersecurity becomes a key subject to safeguard the systems from the growing threats in cyberspace. This review evaluates the emerging field of Adaptive Deep Learning as a promising solution to detect and counter advanced attacks, such as fraud, phishing, malware, intrusion, and anomaly attacks. Recent research analysis shows that deep learning architectures like CNNs, LSTMs, Autoencoders, Transformers, and Graph Neural Networks offer much more efficiency in terms of detection accuracy, precision, and adaptability than traditional rulebased security methods. The review also highlights the importance of cutting-edge technologies, such as Explainable Artificial Intelligence (XAI), Federated Learning, and realtime analytics, for improving transparency, data privacy, and collaborative threat detection. While these improvements have been made, there are still some challenges to consider, such as the computational complexity, the lack of labeled datasets, the interpretability of models, and constraints when deployed in real-time. Overcoming these challenges is crucial for creating more effective and scalable cybersecurity solutions. The areas that need further investigation are lightweight adaptive models, uniform assessment frameworks, privacy-enhancing learning algorithms, and automated reaction mechanisms that can cope with rapidly changing attack patterns. In summary, Adaptive Deep Learning offers a promising framework for the

development of future-ready, intelligent, resilient, and secure financial ecosystems to meet evolving cyber threats.

References

[1] E. Walker, S. Mitchell, B. Carter, O. Reynolds, and C. Paul, "Adaptive AI Frameworks for Financial Fraud and Cyber Threat Detection Authors".

[2] A. A. Hammad, S. R. Ahmed, and M. R. Ahmed, *Deep Reinforcement Learning for Adaptive Cyber Defense in Network Security*, vol. 1, no. 1. Association for Computing Machinery. doi: 10.1145/3660853.3660930.

[3] A. Carlo, "Quantum Computing' s Disruption of Cyber Security: Challenges and MLBased Solutions," no. February, 2025, doi: 10.13140/RG.2.2.23148.68482.

[4] E. Oye, "Blockchain-Based Systems For Secure Machine Learning In Cybersecurity," *SSRN Electron. J.*, no. December, 2025, doi: 10.2139/ssrn.5080340.

[5] E. Oye, "Blockchain-Based Systems For Secure Machine Learning In Cybersecurity," *SSRN Electron. J.*, 2025, doi: 10.2139/ssrn.5080340.

[6] V. Asha and S. K. S. Raja, "An Intelligent AI-Driven Firewall Framework for Zero-Day Threat Detection in Mobile and Interactive Network Environments Using Deep Learning and Explainable AI," vol. 2, pp. 630–649, 2026, doi: 10.58346/JOWUA.2026. I2.035.

[7] M. Zahangir and S. Sultana, "An adaptive firewall framework using deep reinforcement learning for threat-aware cyber threat detection and mitigation policy learning," vol. 31, no. July, 2026.

[8] M. Roopesh, N. Nishat, I. Arif, and A. E. Bajwa, "a Comprehensive Review of Machine Learning and Deep Learning Applications in Cybersecurity: an Interdisciplinary Approach," *Acad. J. Sci. Technol. Eng. Math. Educ.*, vol. 4, no. 04, pp. 37–53, 2024, doi: 10.69593/ajsteme. v4i04.118.

[9] Maureen Oluchukwuamaka Okafor, "Deep learning in cybersecurity: Enhancing threat detection and response," *World J. Adv. Res. Rev.*, vol. 24, no. 3, pp. 1116–1132, 2024, doi: 10.30574/wjarr.2024.24.3.3819.

[10] M. Alazab, S. Srinivasan, S. Venkatraman, V. Quoc Pham, V. Ravi, and Q.-V. Pham, "Deep learning for cyber security applications: A comprehensive survey," *Techrxiv.Org*, no. October, pp. 0–34, 2023.

[11] U. K. Lilhore, S. Simaiya, R. Alroobaea, A. M. Baqasah, and M. Alsafyani, *SmartTrust : a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture*. 2025.

[12] M. Radha, Y. Vasa, A. R. Kumbham, P. Vallurupalli, S. A. Kumar, and A. Dhivya, "A Hybrid Graph Neural Network-Based Reinforcement Learning Approach for Adaptive Cybersecurity Risk Management in FinTech," *2025 Int. Conf. Comput. Technol. & Data Commun.*, pp. 1–6, 2025, doi: 10.1109/ICCTDC64446.2025.11158732.

[13] M. M. Saeed, "An AI-Driven Cybersecurity Framework for IoT : Integrating LSTM-Based Anomaly Detection , Reinforcement Learning , and Post-Quantum Encryption," *IEEE Access*, vol. 13, no. June, pp. 104027–104036, 2025, doi: 10.1109/ACCESS.2025.3576506.

[14] F. Mesadieu, D. Torre, and A. Chennamaneni, "Leveraging Deep Reinforcement Learning Technique for Intrusion Detection in SCADA Infrastructure," no. April, 2024.

[15] M. Soltani, K. Khajavi, M. J. Siavoshani, and A. H. Jahangir, "A multi - agent adaptive deep learning framework for online intrusion detection," *Cybersecurity*, 2024, doi: 10.1186/s42400-023-00199-0.

[16] L. Yang and A. Shami, *Towards Autonomous Cybersecurity: An Intelligent AutoML Framework for Autonomous Intrusion Detection*, vol. 1, no. 1. Association for Computing Machinery, 2024. doi: 10.1145/3689933.3690833.

[17] J. K. Manda, "AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations," *SSRN Electron. J.*, vol. 6, no. 2, pp. 333–340, 2024, doi: 10.2139/ssrn.5003638.

[18] G. Sadaram, L. Karaka, … S. M.-M. M., and undefined 2024, "AI-Powered Cyber Threat Detection: Leveraging Machine Learning for Real-Time Anomaly Identification and Threat Mitigation," *Mswmanagementj.Com*, vol. 12, no. 2, pp. 788–803, 2024.

[19] B. Reddy Maddireddy and B. R. Maddireddy, "A Comprehensive Analysis of Machine Learning Algorithms in Intrusion Detection Systems," vol. 01, no. 4, pp. 877–893, 2024.

[20] A. Suparman, E. P. A. Akhmad, and B. M. Dinata, "Leveraging Artificial Intelligence for Enhancing Cybersecurity: A Deep Learning Approach to Real-Time Threat Detection," *J. Acad. Sci.*, vol. 1, no. 7, pp. 835–842, 2024, doi: 10.59613/0yv79c49.

[21] J. Yu, A. V. Shvetsov, and S. Hamood Alsamhi, "Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions," *IEEE Access*, vol. 12, no. September, pp. 159579–159596, 2024, doi: 10.1109/ACCESS.2024.3482987.

[22] S. Srinivas Vellela, P. Bhanu Latha, Y. Manikanta Kalyan, K. Deepu Prabhunadh, S. Pavan Kumar, and D. Kumar, "A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System," *Int. J. Mod. Trends Sci. Technol.*, vol. 2024, no. 02, pp. 110–116, 2024, doi: 10.46501/IJMTST1002015.

[23] A. S. George, "Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis Partners Universal Innovative Research Publication (PUIRP)," *Partners Univers. Innov. Res. Publ.*, vol. 3, no. 9, pp. 15–28, 2024, doi: 10.5281/zenodo.13333202.

[24] T. K. Adenekan, "Data-Driven Cybersecurity: Leveraging Predictive Analytics for Proactive Threat Mitigation," no. November, 2024.