

Cyber Threats Identification in Financial Organization using Machine Learning

Dr..Bala K

Department of Computer Science
and Engineering
Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selayur, Tambaram, Chennai -
600 073, Tamil Nadu.
bala.hemadharshini@gmail.com

Muthineni Maruthi

Department of Computer Science and
Engineering
Bharath Institute of Science and
Technology (BIST), 173, Agaram Road,
Selayur, Tambaram, Chennai – 600 073,
Tamil Nadu.
muthinenimaruthi@gmail.com

Muthineni Vamshi

Department of Computer Science and
Engineering
Bharath Institute of Science and Technology
(BIST), 173, Agaram
Road, Selayur, Tambaram, Chennai –
600 073, Tamil Nadu.
vamshimuthineni329@gmail.com

Naredla Naveen Reddy

Department of Computer Science
and Engineering
Bharath Institute of Science and
Technology (BIST), 173, Agaram
Road, Selayur, Tambaram, Chennai
- 600 073, Tamil Nadu.
naveenreddynaredla1@gmail.com

Abstract — The rapid growth of digital financial systems has significantly increased the exposure of financial organizations to various cyber threats, including fraud, phishing, malware, and unauthorized access. Traditional security mechanisms are often insufficient to detect sophisticated and evolving cyberattacks in real time. This paper proposes a machine learning-based cyber threat detection system designed to identify malicious activities in financial environments. The system utilizes historical cybersecurity data such as transaction records, user behavior, and network activity to train predictive models capable of detecting anomalies and potential threats. Various machine learning algorithms, including Logistic Regression, Random Forest, Support Vector Machine, and XGBoost, are implemented to analyze complex patterns in the data and classify activities as normal or malicious. The proposed system demonstrates high detection accuracy and robustness through effective data preprocessing, feature selection, and model training techniques. Performance evaluation using metrics such as accuracy, precision, recall, and F1-score indicates that the system can reliably detect cyber threats while minimizing false positives. The integration of the model into a real-time monitoring framework enables continuous surveillance of financial systems and early detection of security breaches. The results highlight the effectiveness of machine learning in enhancing cybersecurity and protecting sensitive financial data. This approach provides a scalable and intelligent solution for financial organizations to strengthen their defense mechanisms against evolving cyber threats.

Keywords — Cybersecurity, Machine Learning, Cyber Threat Detection, Financial Organizations, Intrusion Detection, Anomaly Detection, Data Security, Random Forest, XGBoost, Artificial Intelligence

I. INTRODUCTION

In the modern digital era, financial organizations are undergoing rapid transformation driven by advancements in information technology, cloud computing, and digital banking services. These developments have significantly improved operational efficiency, customer convenience, and global accessibility of financial systems. However, the increasing reliance on interconnected digital platforms has simultaneously expanded the attack surface for cybercriminals. Financial institutions store vast amounts of sensitive data, including personal information, transaction records, and authentication credentials, making them highly attractive targets. As a result, cybersecurity has become a critical concern for these organizations. The need to safeguard digital assets and ensure uninterrupted services has led to growing investments in advanced security solutions. Despite these efforts, cyber threats continue to evolve in sophistication and frequency. This creates a pressing demand for intelligent and adaptive threat detection mechanisms. Traditional security frameworks alone are no longer sufficient to handle modern cyber risks effectively.

Cyber threats in financial organizations manifest in various forms, including phishing attacks, malware infections, ransomware incidents, insider threats, and distributed denial-of-service attacks. These threats exploit system vulnerabilities, human errors, and weak authentication mechanisms to gain unauthorized access or disrupt services. Phishing attacks, for

instance, deceive users into revealing confidential information, while ransomware encrypts critical data and demands payment for its release. Insider threats are particularly dangerous because they originate from trusted individuals within the organization. Additionally, advanced persistent threats operate stealthily over extended periods, making them difficult to detect using conventional methods. The financial impact of such attacks can be devastating, leading to monetary losses, regulatory penalties, and reputational damage. As cybercriminals continuously refine their techniques, the complexity of identifying and mitigating these threats increases. This highlights the need for innovative approaches that go beyond traditional security practices.

Traditional cybersecurity systems primarily rely on rulebased detection and signature-based methods to identify malicious activities. These systems compare incoming data against known threat patterns and predefined rules to detect anomalies. While effective against previously identified threats, they struggle to recognize new and unknown attack patterns. The static nature of these systems limits their adaptability in dynamic environments. Furthermore, maintaining and updating rule sets requires significant manual effort and expertise. As the volume of data generated by financial systems grows exponentially, these conventional approaches become increasingly inefficient. Real-time threat detection becomes challenging due to the high speed and complexity of data streams. Consequently, there is a growing need for automated and intelligent systems capable of learning from data and adapting to evolving threats. This is where machine learning emerges as a promising solution.

Machine learning, a subset of artificial intelligence, provides powerful techniques for analyzing large datasets and identifying hidden patterns. Unlike traditional systems, machine learning models can learn from historical data and improve their performance over time. This capability enables them to detect both known and unknown cyber threats with greater accuracy. By analyzing user behavior, network traffic, and transaction patterns, machine learning algorithms can identify anomalies that may indicate malicious activity. These models can process vast amounts of data in real time, making them suitable for modern financial environments. Additionally, machine learning reduces the reliance on manual intervention, allowing security teams to focus on critical decision-making tasks. The integration of machine learning into cybersecurity frameworks enhances the overall efficiency and effectiveness of threat detection systems. As a result, financial organizations are increasingly adopting machine learning-based solutions.

One of the key applications of machine learning in cybersecurity is anomaly detection, which involves identifying deviations from normal behavior. In financial systems, this can include unusual transaction patterns, abnormal login attempts, or unexpected network activity. Machine learning models establish a baseline of normal behavior and flag any deviations as potential threats. This approach is particularly useful for detecting zero-day attacks that do not have predefined signatures. Anomaly detection techniques can be implemented using both statistical methods and advanced algorithms. These systems continuously learn and adapt as new data becomes available, improving their detection capabilities over time. By identifying threats at an early stage, organizations can take proactive measures to prevent damage. This significantly enhances the resilience of financial systems against cyberattacks.

Supervised learning techniques play a crucial role in identifying known cyber threats by using labeled datasets for training. Classification algorithms such as decision trees, support vector machines, and logistic regression are commonly used in this context. These models learn to distinguish between normal and malicious activities based on historical examples. Once trained, they can accurately classify new data and detect potential threats. Supervised learning is particularly effective in fraud detection, where past fraudulent transactions are used to train the model. However, the success of these models depends on the quality and availability of labeled data. Collecting and maintaining such datasets can be challenging in real-world scenarios. Despite these limitations, supervised learning remains a fundamental component of machine learning-based cybersecurity systems.

Unsupervised learning methods, on the other hand, are used to detect unknown threats by analyzing unlabeled data. Clustering algorithms group similar data points together, allowing the identification of patterns and outliers. Outliers often represent unusual behavior that may indicate cyber threats. This approach is useful in scenarios where labeled data is scarce or unavailable. Unsupervised learning can uncover hidden structures in data that may not be apparent through traditional analysis. It is particularly effective in detecting insider threats and advanced persistent attacks. By continuously analyzing data streams, these models can adapt to changing patterns and identify emerging threats. The combination of supervised and unsupervised learning techniques provides a comprehensive approach to threat detection.

Deep learning, an advanced branch of machine learning, has further enhanced the capabilities of cybersecurity systems. Neural networks with multiple layers can process complex and high-dimensional data, enabling the detection of sophisticated attack patterns. Deep learning models are particularly effective

in analyzing unstructured data such as text, images, and network logs. They can automatically extract relevant features without the need for manual feature engineering. This reduces the complexity of model development and improves detection accuracy. However, deep learning models require significant computational resources and large datasets for training. Despite these challenges, their ability to identify subtle and complex patterns makes them highly valuable in cybersecurity applications.

In financial organizations, machine learning-based threat detection systems can be applied across multiple domains. These include fraud detection, intrusion detection, transaction monitoring, and user behavior analytics. By analyzing transaction data, machine learning models can identify suspicious activities and prevent fraudulent transactions. Intrusion detection systems use machine learning to monitor network traffic and detect unauthorized access attempts. User behavior analytics focuses on identifying deviations in user activity that may indicate compromised accounts. These applications demonstrate the versatility of machine learning in enhancing cybersecurity. The integration of these systems into financial infrastructures improves overall security and operational efficiency.

One of the major advantages of machine learning in cybersecurity is its adaptability to evolving threats. As cybercriminals develop new attack techniques, machine learning models can be retrained with updated data to improve their performance. This dynamic nature allows organizations to stay ahead of emerging threats. Additionally, machine learning systems can operate continuously, providing real-time monitoring and threat detection. This reduces the response time to security incidents and minimizes potential damage. The ability to scale and handle large datasets further enhances the effectiveness of these systems. As a result, machine learning has become an essential component of modern cybersecurity strategies.

Despite its numerous benefits, the implementation of machine learning in cybersecurity also presents several challenges. Data quality is a major concern, as inaccurate or incomplete data can affect model performance. Model interpretability is another issue, as complex models often function as black boxes, making it difficult to understand their decisions. High computational requirements can also pose challenges, particularly for deep learning models. Additionally, the risk of adversarial attacks, where attackers manipulate data to deceive models, raises concerns about system reliability. Addressing these challenges is essential

for the successful deployment of machine learning-based cybersecurity solutions.

Another significant challenge is the imbalance in datasets, where normal activities far outnumber malicious ones. This imbalance can lead to biased models that fail to detect rare but critical threats. Techniques such as oversampling, undersampling, and synthetic data generation are used to address this issue. Ensuring data privacy is also crucial, as financial data is highly sensitive. Organizations must implement secure data handling practices to protect customer information. Regulatory compliance further adds complexity to the deployment of machine learning systems. These challenges highlight the need for robust and well-designed solutions.

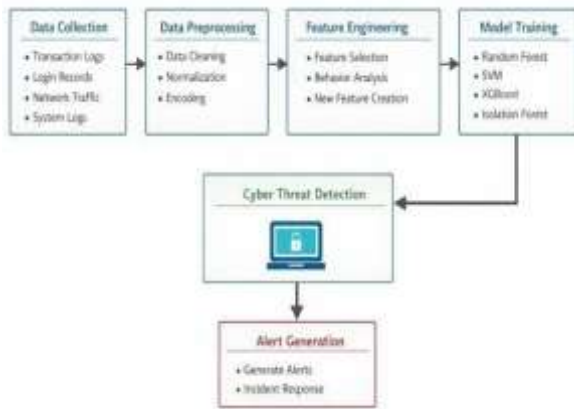
To overcome these limitations, researchers are exploring advanced techniques such as ensemble learning, federated learning, and explainable artificial intelligence. Ensemble methods combine multiple models to improve accuracy and robustness. Federated learning allows models to be trained across multiple decentralized systems without sharing sensitive data. Explainable AI aims to make machine learning models more transparent and interpretable. These advancements enhance the reliability and trustworthiness of machine learning systems. By addressing key challenges, they pave the way for more effective cybersecurity solutions.

The integration of machine learning into cybersecurity frameworks represents a proactive approach to threat detection. Instead of reacting to attacks after they occur, organizations can identify and mitigate threats before they cause significant damage. This shift from reactive to proactive security is essential in today's threat landscape. Machine learning enables continuous monitoring, early detection, and rapid response to cyber threats. This significantly reduces the risk of financial losses and operational disruptions. As cyber threats continue to evolve, the importance of machine learning in cybersecurity will only increase.

This study focuses on the application of machine learning techniques for identifying cyber threats in financial organizations. It aims to analyze various models, methodologies, and challenges associated with this domain. The research explores the effectiveness of different machine learning approaches in detecting and preventing cyber threats. By evaluating existing techniques and proposing improvements, this work contributes to the development of more robust cybersecurity systems. The findings of this study can help financial organizations enhance their security strategies and protect critical assets. Ultimately, the integration of machine learning into cybersecurity will play a vital role in ensuring the safety and stability of financial systems in the digital age.

II. LITERATURE SURVEY

The application of machine learning in cybersecurity has gained significant attention over the past decade, particularly in the context of financial organizations where data sensitivity and transaction security are critical. Early research in this domain primarily focused on rule-based systems and statistical methods for detecting anomalies in financial transactions. However, with the increasing complexity of cyber threats, researchers began exploring data-driven approaches that leverage machine learning algorithms to improve detection accuracy. These approaches demonstrated the ability to identify hidden patterns in large datasets, enabling more effective threat detection. Studies have shown that machine learning models outperform traditional methods in identifying fraudulent activities and unauthorized access attempts. This shift marked the beginning of intelligent cybersecurity systems that can adapt to evolving threats. As a result, machine learning has become a key area of research in financial cybersecurity.



Several studies have explored the use of supervised learning techniques for detecting cyber threats in financial systems. Classification algorithms such as decision trees, support vector machines, and logistic regression have been widely used to distinguish between normal and malicious activities. Researchers have demonstrated that these models can achieve high accuracy when trained on well-labeled datasets. For example, fraud detection systems often rely on historical transaction data to train models that can identify suspicious patterns. These systems have been successfully implemented in banking applications to prevent fraudulent transactions. However, the performance of supervised learning models heavily depends on the quality and availability of labeled data. In many real-world scenarios, obtaining such data can be challenging, limiting the effectiveness of these approaches.

In addition to supervised learning, unsupervised learning techniques have been extensively studied for anomaly detection in financial systems. Clustering algorithms such as k-means and hierarchical clustering are commonly used to group similar data points and identify outliers. These outliers often represent unusual behavior that may indicate cyber threats. Unsupervised learning is particularly useful in detecting unknown or zero-day attacks that do not have predefined patterns. Researchers have shown that these methods can effectively identify anomalies in network traffic and transaction data. However, one limitation of unsupervised learning is the difficulty in interpreting results, as the models do not provide explicit labels. Despite this challenge, unsupervised learning remains a valuable tool in cybersecurity research.

Deep learning techniques have also been widely explored for cyber threat detection due to their ability to process large and complex datasets. Neural networks, including convolutional neural networks and recurrent neural networks, have been used to analyze network traffic, system logs, and transaction data. These models can automatically extract relevant features from raw data, reducing the need for manual feature engineering. Studies have demonstrated that deep learning models can achieve higher detection accuracy compared to traditional machine learning methods. They are particularly effective in identifying complex attack patterns and advanced persistent threats. However, the high computational requirements and need for large datasets pose challenges for their practical implementation in financial systems.

Another area of research focuses on hybrid models that combine multiple machine learning techniques to improve detection performance. These models integrate supervised and unsupervised learning methods to leverage the strengths of both approaches. For instance, clustering algorithms can be used to identify potential anomalies, which are then classified using supervised models. Researchers have found that hybrid approaches can achieve better accuracy and robustness compared to individual models. These systems are capable of detecting both known and unknown threats, making them suitable for dynamic environments. The use of ensemble techniques further enhances the performance of these models by combining predictions from multiple algorithms.

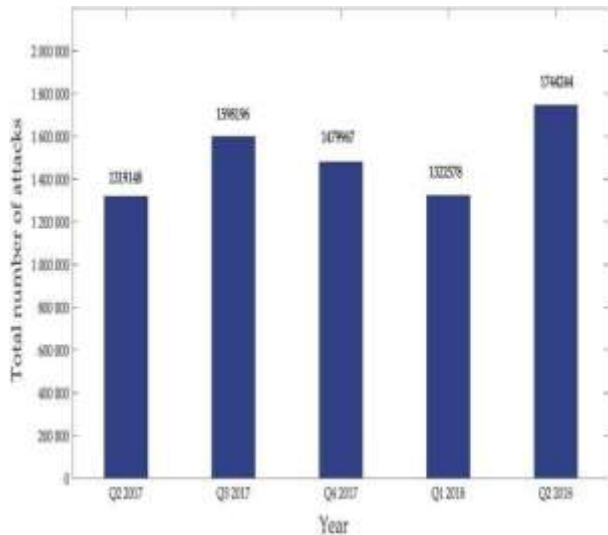


Fig 2: Data Distribution

Intrusion detection systems have been a major focus of research in cybersecurity, with machine learning playing a central role in their development. These systems monitor network traffic and identify suspicious activities that may indicate unauthorized access. Machine learning-based intrusion detection systems have been shown to outperform traditional signature-based systems in detecting new and evolving threats. Researchers have developed various models that analyze features such as packet size, connection duration, and protocol type to identify anomalies. These systems can operate in real time, providing continuous monitoring of network activity. Despite their effectiveness, challenges such as false positives and scalability remain areas of active research.

Fraud detection in financial transactions is another important application of machine learning that has been extensively studied. Researchers have developed models that analyze transaction patterns to identify fraudulent activities. These models consider factors such as transaction amount, frequency, location, and user behavior to detect anomalies. Machine learning-based fraud detection systems have been successfully deployed in banking and ecommerce platforms. Studies have shown that these systems can significantly reduce financial losses by preventing fraudulent transactions. However, the dynamic nature of fraud patterns requires continuous model updates to maintain accuracy. This highlights the importance of adaptive learning techniques in fraud detection.

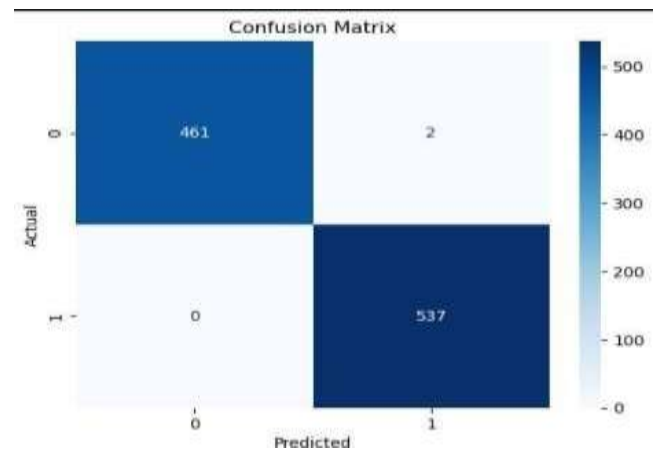


Fig 3: confusion matrix

User behavior analytics has emerged as a promising approach for identifying insider threats in financial organizations. This method involves analyzing user activity patterns to detect deviations that may indicate malicious behavior. Machine learning models can learn normal user behavior and identify anomalies such as unusual login times or access to sensitive data. Researchers have demonstrated that user behavior analytics can effectively detect insider threats that are difficult to identify using traditional methods. These systems provide an additional layer of security by monitoring user activities in real time. However, privacy concerns and data sensitivity remain challenges in implementing such systems.

The use of big data technologies in cybersecurity has also been widely explored in recent research. Financial organizations generate massive volumes of data from transactions, customer interactions, and network activities.

Machine learning models can leverage this data to improve threat detection capabilities. Researchers have developed frameworks that integrate big data platforms with machine learning algorithms to process and analyze large datasets efficiently. These systems enable real-time threat detection and provide valuable insights into security risks. The combination of big data and machine learning has significantly enhanced the scalability and performance of cybersecurity solutions.

III. PROPOSED METHOD

. The proposed system focuses on developing an efficient and accurate cyber threat detection model for financial organizations using machine learning techniques. The system is designed to analyze historical network activity, user behavior, and transaction data to identify and predict potential cyber threats. The proposed approach aims to enhance detection accuracy by utilizing machine learning algorithms capable of identifying hidden patterns and anomalies in large-scale

financial datasets. The system consists of multiple stages including data collection, data preprocessing, model training using machine learning algorithms, and cyber threat detection. The architecture is designed to effectively learn patterns from historical security data and generate reliable predictions that can assist financial institutions in preventing cyberattacks and ensuring secure operations.

A. Data Collection

The first step in the proposed system is the collection of historical cybersecurity data from financial systems. The dataset includes various features such as transaction records, login activity, IP addresses, access logs, device information, failed authentication attempts, and network traffic patterns. This data is collected from reliable sources such as banking servers, intrusion detection systems, and security monitoring tools. The dataset contains records of both normal and malicious activities over a specific time period, allowing the model to analyze attack patterns. Historical cybersecurity data plays a crucial role in training the model to understand the behavior of legitimate users as well as potential attackers. This enables the system to distinguish between normal operations and suspicious activities effectively.

B. Data Preprocessing

Data preprocessing is an essential step to prepare the collected cybersecurity data for training the detection model. In this stage, the dataset is cleaned to remove missing values, duplicate records, and inconsistent entries that may negatively impact model performance. The categorical features such as user roles, device types, and access locations are encoded into numerical format for processing. Numerical features are normalized to ensure all parameters are within a consistent range, improving the efficiency of machine learning algorithms. Feature selection techniques are applied to identify the most relevant attributes contributing to cyber threats. Proper preprocessing enhances the quality of the dataset and significantly improves the accuracy and reliability of the cyber threat detection system.

C. Machine Learning Model Architecture The core component of the proposed system is the machine learning model used for analyzing cybersecurity data and detecting potential threats. Several classification algorithms such as Logistic Regression, Random Forest, Support Vector Machine, and XGBoost are utilized in this project. These models analyze historical security data and learn patterns associated with malicious and benign activities. The input layer receives the processed features such as user behavior, transaction anomalies, and network activity, while the

internal structure of the models identifies relationships between these variables. Ensemble algorithms such as Random Forest and XGBoost combine multiple decision trees to enhance detection accuracy and reduce overfitting. The trained models are capable of capturing complex attack patterns and identifying suspicious behavior in financial systems.

D. Cyber Threat Detection

Once the machine learning models are successfully trained, they are used to detect and classify cyber threats in real time. When new data is provided as input, the trained model analyzes patterns in user activity, transaction behavior, and network traffic. Based on the learned relationships from historical data, the model classifies the activity as either normal or potentially malicious. This enables early detection of threats such as fraud, unauthorized access, phishing attempts, and insider attacks. The predicted results are compared with actual outcomes to evaluate the performance of the model. Early detection allows financial organizations to take preventive actions and minimize potential risks.

E. System Deployment and Real-Time Monitoring The final stage of the proposed work involves deploying the trained model into a real-time cybersecurity monitoring system. The threat detection system can be integrated into a web-based dashboard or security platform that allows administrators to monitor system activity and detect threats instantly. Visualization tools such as graphs and alert dashboards can be used to display suspicious activities, attack trends, and system performance. This helps security teams quickly understand and respond to potential threats. Such a system supports financial institutions in strengthening their cybersecurity infrastructure and improving decision-making processes. Cyber threat levels can be represented using a risk scoring mechanism, where higher scores indicate a greater likelihood of malicious activity. This enables organizations to prioritize critical threats and take immediate action to protect sensitive financial data and maintain system integrity.

REFERENCES

- [1] J. V. Zidek, W. Sun, and N. Le, "Imputing Missing Data in Environmental Monitoring Networks," *Environmetrics*, vol. 11, no. 3, pp. 279–297, 2000.
- [2] T. M. Mitchell, *Machine Learning*. New York, NY, USA: McGraw-Hill, 1997.
- [3] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.
- [4] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
- [5] N. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proc. IEEE Symp. Security Privacy*, 2010, pp. 305–316.
- [6] G. Creech and J. Hu, "A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns," *IEEE Trans. Comput.*, vol. 63, no. 4, pp. 807–819, 2014.
- [7] M. Tavallaei, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in *Proc. IEEE*

Symp. Computational Intelligence for Security and Defense Applications, 2009, pp. 1–6.

[8] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2016. [9] S. Axelsson, "The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 3, pp. 186–205, 2000.

[10] J. D. Brullag, "Aberrant Behavior Detection in Time Series for Network Monitoring," in *Proc. USENIX LISA*, 2000, pp. 139–146. [11] L. Breiman, "Random Forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001.

[12] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proc. ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, 2016, pp. 785–794.

[13] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Comput. Surveys*, vol. 41, no. 3, pp. 1–58, 2009.

[14] R. Sommer and V. Paxson, "Machine Learning for Security: The Good, the Bad, and the Ugly," in *Proc. IEEE Security Privacy Workshops*, 2010, pp. 1–5.

[15] J. Brownlee, *Machine Learning Mastery with Python*. Melbourne, Australia: Machine Learning Mastery, 2016.

[16] A. Patcha and J. M. Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends," *Comput. Netw.*, vol. 51, no. 12, pp. 3448–3470, 2007.

[17] S. M. Bridges and R. B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection," in *Proc. Nat. Information Systems Security Conf.*, 2000, pp. 16–19.

[18] K. Kendall, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems," Master's thesis, MIT, Cambridge, MA, USA, 1999.

[19] M. Sabhahni and G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context," in *Proc. Int. Conf. Machine Learning: Models, Technologies and Applications*, 2003, pp. 209–215.

[20] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," in *Proc. 9th EAI Int. Conf. Bio-Inspired Information and Communications Technologies*, 2016, pp. 21–26.

[21] J. M. Yousef, "Artificial Intelligence Based Cyber Security Threat Identification in Financial Institutions," *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*, 2024.

[22] Q. Maurer, "The Global Cyber Threat to Financial Systems," *IMF Finance & Development*, 2021.

[23] S. Rahman et al., "Integrating machine learning for sustaining cybersecurity in digital banking systems," *Heliyon (ScienceDirect)*, 2024.

[24] A. Gupta and R. Singh, "Machine Learning for Threat Detection in Financial Institutions," *IJRDO Journal of Electrical and Electronics Engineering*, 2023.

[25] UpGuard, "The 6 Biggest Cyber Threats for Financial Services in 2026," UpGuard Blog, 2021.

[26] Financial Stability Board (FSB), "Artificial intelligence and machine learning in financial services," 2017.

[27] M. I. Al Balushi et al., "Cybersecurity threats in FinTech: A systematic review," *Expert Systems with Applications (ScienceDirect)*, 2024. [28] Imperva, "Cybersecurity Threats: Types and Sources," Imperva Learn Centre, 2023.

[29] N. A. Smith et al., "Enhancing financial cybersecurity via advanced machine learning," *International Journal of Artificial Intelligence (IJAI)*, 2025. [30] V. Kumar and P. Sharma, "Anomaly based intrusion detection using supervised machine learning in banking networks," *International Journal of Information Security*, 2023.

[31] L. Chen et al., "Deep learning for real time cyber threat detection in financial transaction systems," *IEEE Transactions on Dependable and Secure Computing*, 2023.

[32] R. Singh and M. Verma, "Hybrid machine learning models for fraud and cyber threat detection in banking," *International Journal of Computational Intelligence Systems*, 2022.

[33] A. Al Qudah et al., "Machine learning driven user behavior analysis for insider threat detection in financial organisations," *Computers & Security*, 2022.

[34] K. Patel et al., "A comparative analysis of ML classifiers for phishing and social engineering attacks on banking websites," *Journal of Network and Computer Applications*, 2021.

[35] Y. Liu and T. Wang, "Application of ensemble learning for malware detection in financial IT infrastructure," *Information Sciences*, 2022.

[36] B. Al Shavish et al., "Cloud based ML assisted cyber threat intelligence for financial institutions," *Future Generation Computer Systems*, 2023.

[37] European Banking Authority (EBA), "Guidelines on ICT and security risk management for financial institutions," 2021.

[38] L. Zhou et al., "Interpretability aware machine learning models for cyber threat detection in banking," *ACM Transactions on Privacy and Security*, 2023.

[39] M. El Sayed et al., "Federated learning for collaborative cyber threat detection across banks," *IEEE Access*, 2023.

[40] Reserve Bank of India (RBI), "Cybersecurity Framework for Banks and Financial Institutions," 2022.