ETDT

Emerging Trends in Digital Transformation

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-19***

AI-ENHANCED THREAT IDENTIFICATION FOR CYBERSECURITY IN FINANCIAL INSTITUTIONS USING MACHINE LEARNING MODELS

V.LALITHA[1], B. SAHITHI[2], B.H.S NAGI REDDY[3], J.SURESH[4], A. DHANUSH[5]

[1]Assistant Professor, Dept. of CSE(AI&ML), Sai Spurthi Institute of Technology, Khammam, Telangana, India

[2,3,4,5]B.TechStudents, Dept. of CSE(AI&ML), Sai Spurthi Institute of Technology, Khammam, Telangana, India

ABSTRACT*:* As digital assets become more linked to each other, cyber risks get bigger and more complicated. To find and reduce these threats, financial institutions should spend money on AI-powered solutions. In this case, their money will be safe. Machine learning has become an important tool for looking into threats to financial security that are unpredictable, complicated, and always changing. Tools that use artificial intelligence (AI), like natural language processing, advanced algorithms, and automatic reasoning systems, can help banks find possible threats and make their data more secure. This paper suggests a way for financial companies to use AI and machine learning to find cyber security problems. Machine learning systems are always getting better at finding strange data that could mean there is a security problem. Using specialized models that give useful information about internal and external threats, this approach helps financial organizations find and stop bad behavior.

Keywords*:*insights, internal, external, malicious, advancements.

1. INTRODUCTION

Financial fraud is the unlawful and dishonest acquisition of money. Insurance, banking, corporate finance, and taxes are among the sectors that experience this phenomenon. Financial statement fraud, tax evasion, money laundering, and credit card fraud are among the most hazardous forms of financial fraud. Despite the greatest efforts to prevent it, financial fraud results in annual losses of hundreds of millions of dollars, which have a detrimental impact on both companies and society. People, enterprises, banks, and stores are all impacted by this substantial financial loss. Fraud detection is now more critical than it has ever been due to the recent increase in fraudulent activities.

The income statement, balance sheet, cash flow statement, and explanatory notes are the four fundamental forms of financial statements. The income statement is a financial statement that evaluates a company's net income or profit by analyzing its revenues and expenses over a specific period. The balance sheet provides a real-time representation of a company's assets, liabilities, and stockholder equity. The cash flow statement evaluates the profitability of a company in the interim to account for debt, investments, and operating expenses. The explanatory notes provide additional information regarding the financial statement elements, such as asset depreciation, significant accounting standards, and subsequent events.Financial statement fraud is the act of manipulating financial statements to present a company as more profitable than it actually is, evade taxes, obtain loans, or increase stock prices. The conceptual framework of auditing known as the "fraud triangle" assists in comprehending the underlying causes of fraudulent behavior. It is composed of three components: opportunity, rationalizing, and incentive. The risk of fraudulent behavior is increased when these elements are combined. The fraud triangle is frequently employed by auditing professionals to investigate the rationale behind fraudulent behavior, underscoring the importance of comprehending these dynamics in the battle against financial fraud.

FraudDynamics:

In the context of financial fraud, companies frequently encounter incentives or pressures that may result in dishonest behavior. Additionally, opportunities for fraudulent activities are created by ineffective controls or

DOI : https://doi.org/10.5281/zenodo.16810845

inadequate investigations. In the majority of cases, fraudsters are significantly influenced by external events and circumstances when they validate their actions.

2. LITERATURE SURVEY

Babu, K. S. (2024). This paper examines the potential of artificial intelligence (AI) to improve the cybersecurity practices of the financial industry by focusing on machine learning (ML) algorithms for threat identification. The study demonstrates the effectiveness of AI-driven systems in identifying and preventing cyber attacks in real time by employing sophisticated machine learning models such as deep learning and support vector machines. According to the survey, financial institutions must implement AI-based cyber security solutions to mitigate more intricate risks, such as ransomware, fraud, and phishing. The paper also contrasts the efficacy of artificial intelligence models with conventional cybersecurity strategies, emphasizing the former's superior capacity to identify novel risks and provide prompt responses. The results underscore the significance of conducting routine training sessions for artificial intelligence systems with a variety of datasets to enhance accuracy and reduce the number of false positives.

Zhang, L., & Wang, H. (2024). This paper examines the application of artificial intelligence and machine learning methodologies to identify and mitigate cyber security threats at financial institutions. It offers a variety of AI-powered techniques, such as anomaly detection, pattern recognition, and categorization models, that enable financial institutions to promptly identify potential defects and odd activities.. The authors discuss the integration of artificial intelligence into threat intelligence platforms, with an emphasis on automated incident response and predictive analytics to reduce the necessity for human intervention. The challenges of implementing artificial intelligence, such as the necessity of extensive system training to prevent misidentifications and issues with data privacy, are also discussed. Research suggests that artificial intelligence has the potential to significantly transform the cyber security landscape by facilitating proactive risk management and faster response times to emergent threats.

Hassan, S. I., & Ahmed, R. (2023). The objective of this paper is to examine the potential of artificial intelligence and machine learning to improve the cyber security of the financial sector. The authors present numerous examples of how artificial intelligence (AI) has effectively reduced cyberthreats, such as automated security intrusion response and fraud identification. The paper discusses a variety of machine learning (ML) techniques, such as reinforcement learning and supervised learning, that are employed to improve defensive strategies, anticipate future attacks, and detect antagonistic behavior. It also examines the potential for neural networks and decision trees to enhance the accuracy of security system detection. The paper also addresses issues such as algorithm bias, data integrity, and the necessity of open decision-making processes in artificial intelligence systems that are implemented by financial institutions. In their conclusion, the authors emphasize the necessity of hybrid strategies that combine traditional security measures with artificial intelligence-driven models to enhance security.

Patel, J., & Singh, N. (2023). This article examines the utilization of machine learning techniques to improve the cyber security systems of the financial services industry. The article provides a concise overview of the various machine learning techniques, such as regression analysis, classification, and clustering, and their applications in the detection of financial cybercrimes, such as data breaches, fraud, and insider threats. The authors also examine the potential of AI-driven models to provide predictive threat intelligence. They demonstrate how machine learning models can identify new attack trends by learning from historical data. The paper demonstrates the practical advantages of integrating machine learning with existing cyber security systems through case studies and simulations, thereby offering financial organizations a more adaptable and scalable security strategy. The paper underscores the necessity of feature selection, data preparation, and model modification in order to increase detection rates and reduce false alarms.

Li, W., & Zhang, Q. (2023).This work provides a thorough examination of artificial intelligence and machine learning techniques that are designed to ensure the security of financial transactions. It underscores the importance of real-time fraud detection models and anomaly detection, which are becoming more prevalent in banking systems. The authors explore the potential of convolution neural networks (CNNs), a type of deep learning network, to detect fraudulent transactions and analyze transaction trends. They also examine the potential for the integration of blockchain and artificial intelligence technologies to enhance transaction security

DOI : https://doi.org/10.5281/zenodo.16810845

and reduce the likelihood of cyber attacks. The paper demonstrates the potential for AI-based systems to significantly reduce false positives while concurrently improving the speed and accuracy of fraud detection through the use of experimental data and performance evaluations. The investigation concludes with recommendations for financial institutions regarding the implementation of artificial intelligence to continuously monitor and protect against internet intrusions.

Cheng, M., & Li, J. (2023). This paper underscores the importance of real-time threat detection in institutions through the use of machine learning techniques. Using real-time data processing and machine learning models, such as decision trees, k-nearest neighbors (KNN), and ensemble techniques, the authors explore the potential for institutions to identify threats such as malware, phishing attempts, and unlawful access. The study also examines the development of a cyber security system that is based on machine learning and incorporates data from a variety of sources, including network traffic, user behavior, and transaction records, in order to predict potential threats. In order to guarantee that these systems can adjust to new, evolving cyber security challenges, the paper underscores the necessity of consistent model updates and training exercises. The authors also emphasize the significance of ensuring that the model is interpretable and transparent, particularly for financial institutions that are required to adhere to stringent regulations.

Ibrahim, M., & Hassan, K. (2023). This work investigates the utilization of artificial intelligence and machine learning methodologies to mitigate financial institution fraud. The authors provide a comprehensive examination of a variety of artificial intelligence techniques, such as support vector machines and random forests, as well as supervised learning models that are designed to detect fraudulent activity by identifying trends in financial transactions. They examine both conventional and artificial intelligence-powered fraud detection systems, highlighting the advantages of the latter in terms of accuracy, scalability, and the potential to identify novel fraud schemes. The paper also addresses challenges such as the necessity of an effective method of model deployment and data privacy concerns. Additionally, it presents case studies of successful fraud detection systems that are propelled by artificial intelligence, thereby emphasizing the importance of advancements in fraud prevention and risk management.

Wu, H., & Wang, Y. (2023). This paper examines the potential applications of artificial intelligence technology in the financial industry to address cyber security concerns related to risk management. The authors demonstrate the potential of machine learning algorithms, such as reinforcement learning, to assess and mitigate risks in real time by simulating a variety of intrusion scenarios and offering adaptive responses. The study assesses the ability of numerous artificial intelligence model types to anticipate, identify, and respond to cyberthreats in banking systems, with a particular emphasis on the efficacy of deep learning methods such as recurrent neural networks (RNNs). The investigation also investigates the potential integration of artificial intelligence into conventional risk management systems, thereby providing financial institutions with guidance on their cyber security posture. The writers emphasize two additional significant concerns: the danger of hostile assaults on artificial intelligence models themselves and the complexity of implementing AI systems.

Chen, X., & Zhou, Z. (2022). This paper explores the potential of artificial intelligence to identify and mitigate cyberthreats in the financial sector. The authors examine a variety of artificial intelligence and machine learning methods, such as supervised and unsupervised learning, in order to identify unusual trends in financial transactions and consumer behavior. The report underscores the increasing necessity for financial institutions to implement contemporary artificial intelligence systems, such as support vector machines, neural networks, and clustering algorithms, in order to achieve comprehensive risk identification. The authors also examine the obstacles that financial institutions encounter when implementing artificial intelligence technology, including the complexity of integrating AI into existing systems, the interpretability of models, and data security. The research reveals that while artificial intelligence has the potential to significantly enhance cyber security, its implementation necessitates meticulous planning, qualified professionals, and ongoing model optimization.

Gao, R., & Wang, J. (2022). This document explores the potential of artificial intelligence to assist financial institutions in the monitoring of risks and the regulation of their own operations. The authors demonstrate the potential of machine learning models to investigate vast quantities of data in real time, thereby allowing institutions to promptly identify and resolve security vulnerabilities, by examining the capabilities of AI-driven threat intelligence systems. The paper evaluates the efficacy of specific artificial intelligence algorithms, such as support vector machines, neural networks, and decision trees, in managing a variety of cyberthreats, such as data

DOI : https://doi.org/10.5281/zenodo.16810845

breaches, financial misconduct, and insider attacks. It also addresses the necessity of integrating artificial intelligence with conventional security measures and the necessity of ensuring the confidentiality and integrity of financial data through the implementation of sophisticated data protection strategies. The authors advise financial organizations to invest in cyber security technologies to proactively identify, halt, and react to breaches, driven by artificial intelligence.

Kumar, R., & Singh, M. (2021). investigate the potential of machine learning techniques to improve the cyber security of the financial sector. The authors offer a method for identifying and predicting cyberthreats in banking environments by employing decision trees, logistic regression, and ensemble techniques, among other machine learning models. The paper underscores the importance of selecting the appropriate features and training data to increase the accuracy of the model, reduce false positives, and ensure that the system can adapt to new challenges. The study demonstrates how artificial intelligence can improve traditional cyber security methods by enabling quicker and more precise threat identification by examining the deficiencies of financial companies. Additionally, the paper delivers responses and examines the potential hazards of artificial intelligence, such as antagonistic machine learning attacks.

Singh, D., & Agarwal, S. (2021). This paper examines the practical applications of cyber security solutions in the financial sector that are powered by artificial intelligence. The authors demonstrate the integration of machine learning algorithms into the cyber security architecture of a major banking institution to enhance threat identification and response through a comprehensive case study of the company. The study demonstrates how artificial intelligence can aggressively identify weaknesses and reduce the risks associated with data breaches and fraud by employing predictive modeling techniques. The paper also discusses the integration of artificial intelligence technologies with existing security systems, such as intrusion detection systems, to improve real-time monitoring. It also examines issues such as the necessity of continuous system optimization to remain current with evolving threats and the scalability of AI solutions.

Tan, B., & Li, Y. (2021). This comprehensive literature review elucidates the potential of artificial intelligence (AI) to improve the cyber security of financial institutions. The authors examine a diverse array of AI techniques, such as reinforcement learning, deep learning, and supervised learning, and how they can be implemented to identify insider threats, fraud, and phishing scams. The paper underscores the most recent developments in artificial intelligence algorithms, including support vector machines and neural networks, as well as an assessment of their efficacy in real-world banking environments. The authors also address the potential applications of artificial intelligence in cyber security in the future, such as the potential integration of blockchain technology with AI to improve security. The report's conclusion emphasizes the necessity of additional research to resolve the crucial challenges of algorithm openness and data privacy

Zhao, Y., & Zhang, X. (2020). This is the year 2020. This paper explores the potential application of AI-based detection methods to threat reduction, as well as the evolving danger scenario in financial institutions. The authors investigate the potential of a variety of machine learning models, including random forests, deep neural networks (DNNs), and k-nearest neighbors (KNN), to enhance the detection of cyber security risks, including phishing, DDoS attacks, and financial fraud. The paper demonstrates through experimental analysis that artificial intelligence models outperform conventional rule-based systems in terms of detection accuracy and response speed. The paper also emphasizes the obstacles that financial firms encounter when implementing artificial intelligence, such as the necessity of extensive datasets for model training, the intricacy of integration, and the probability of model biases. It concludes by suggesting potential solutions to these issues, thereby enhancing the overall security posture of financial institutions.

Gupta, R., & Sharma, N. (2020). This is the year 2020. This document examines the potential applications of artificial intelligence and machine learning in the financial services sector to detect cyber attacks. The authors investigate the application of unsupervised machine learning techniques, such as anomaly detection and clusterering, which are particularly beneficial for identifying unknown hazards in financial institutions. The project also examines the potential integration of artificial intelligence into existing security systems to enhance their ability to detect and respond to a diverse array of cyberthreats, such as financial fraud, account usurpation, and identity theft. The paper demonstrates the potential of artificial intelligence to reduce operating expenses, accelerate response times, and improve cyber security safeguards through the use of numerous case studies. Privacy concerns, data security challenges, and the necessity of ongoing surveillance and artificial intelligence

DOI : *https://doi.org/10.5281/zenodo.16810845*

system modifications to align with evolving threats are also addressed.

3. SYSTEM DESIGN

EXISTING SYSTEM:

Falsified financial statements (FFS) occur when financial factors such as income, assets, sales, and profits are overstated while costs, promises, or losses are minimized. Manual auditing and checks are traditional methods for detecting fraudulent claims, but they are costly, inaccurate, and time-consuming. On the other hand, smart procedures have a lot of potential for assisting auditors in properly reviewing large amounts of financial statements.

This paper examines and summarizes the existing research on intelligent fraud detection in firm financial statements. The primary focus will be on approaches such as machine learning and data mining, as well as the many sources of data utilized to detect financial crime. These innovative ways are more accurate and time-efficient than traditional methods, which is why they are so vital in combating financial fraud.

KeyIssues,Gaps,andLimitationsinFraudDetection

The basic challenges, weaknesses, and limitations of detecting financial statement fraud are discussed, as well as potential future research approaches. Most current research focuses on supervised algorithms. Unsupervised approaches, such as clustering, are receiving less attention. Future research should focus on bio-inspired, evolutionary, unsupervised, and semi-supervised heuristic algorithms for detecting fraud more quickly. Future research will focus on adding textual and audio data to datasets. However, while this type of unstructured data introduces new difficulties, it also has the potential to provide useful information for detecting fraud.

Disadvantages:

The results were below expectations.

- Takes a long time.
- Theories have limitations.

PROPOSED SYSTEM

To detect financial statement fraud, we propose using machine learning techniques. The method consists of numerous steps:

DataPreparation:

Bring in the information and review it.

Fill any blank fields with the default figures.

It is critical to document the labels in the dataset.

Separate the data into training and testing sets to forecast fraud or non-fraud events.

AlgorithmSelection:

Three ways for improving prediction accuracy and usefulness:

There are three types of classifiers: Random Forest, Ada Boost, and K-Nearest Neighbors (KNN).

TrainingandPrediction:

Use the chosen algorithms to work with the training data.

Based on the training data, predict what will happen with the test sample.

To measure performance, compare expected and actual test outcomes.

ModelEvaluation:

Examine the model's F1-score, accuracy, precision, memory, and predictability to determine how well it works. When the system trains models, it provides datasets containing both fraud and non-fraud occurrences. The machine learning algorithm can accurately anticipate when fraud will occur and distinguish between occurrences that are likely to be fraudulent and those that are not. This strategy is an easy and effective way to prevent scams and the associated expenditures.

Advantages:

- Effectively manage large datasets. • Improved experimental findings over current systems.
- Less time was lost.
- Provides accurate predictions about what will happen.
- This strategy increases the dependability and effectiveness of fraud detection systems by identifying and reducing potential fraud risks.

DOI : https://doi.org/10.5281/zenodo.16810845

ALGORITHMS USED AND MODEL BUILDING

These machine learning algorithms are well-known for their capacity to detect scams, and it employs them all.

RandomForestAlgorithm:

It can handle very large datasets successfully since it generates numerous decision trees during training and forecasts using the class mode.

K-NearestNeighbors(KNN)Classifier:

An easy-to-understand strategy for categorizing cases based on their similarity to others in the collection.

AdaBoostAlgorithm:

A method of learning in which numerous weak classifiers are combined to form a strong classifier that concentrates on cases that are difficult to define.

4. RESULTS

```
#--------------------Data Selection---------------#
*******************
```

	step	type	amount	...	newbalanceDest	isFraud	isFlaggedFraud
0	1	PAYMENT	NaN	...	0.00	0	0
1	1	PAYMENT	1864.28	...	0.00	0	0
2	1	TRANSFER	NaN	...	0.00	1	0
3	1	CASH_OUT	181.00	...	0.00	1	0
4	1	PAYMENT	11668.14	...	0.00	0	0
5	1	PAYMENT	7817.71	...	0.00	0	0
6	1	PAYMENT	7107.77	...	0.00	0	0
7	1	PAYMENT	7861.64	...	0.00	0	0
8	1	PAYMENT	4024.36	...	0.00	0	0
9	1	DEBIT	5337.77	...	40348.79	0	0
10	1	DEBIT	9644.94	...	157982.12	0	0
11	1	PAYMENT	3099.97	...	0.00	0	0
12	1	PAYMENT	2560.74	...	0.00	0	0
13	1	PAYMENT	11633.76	...	0.00	0	0
14	1	PAYMENT	4098.78	...	0.00	0	0
15	1	CASH_OUT	229133.94	...	51513.44	0	0
16	1	PAYMENT	1563.82	...	0.00	0	0
17	1	PAYMENT	1157.86	...	0.00	0	0
18	1	PAYMENT	671.64	...	0.00	0	0
19	1	TRANSFER	215310.30	...	0.00	0	0

DATAPREPROCESSING

FindMissingValues

```
#--------------------Find missing values---------------#
*******************
step              0
type              0
amount            2
nameOrig          0
oldbalanceOrg     0
newbalanceOrig    0
nameDest          0
oldbalanceDest    0
newbalanceDest    0
isFraud           0
isFlaggedFraud    0
dtype: int64
```


DOI : https://doi.org/10.5281/zenodo.16810845

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-19***

```
#------------------Fill 0 from missing Values--------------#
******************
step            0
type            0
amount          0
nameOrig        0
oldbalanceOrg   0
newbalanceOrig  0
nameDest        0
oldbalanceDest  0
newbalanceDest  0
isFraud         0
isFlaggedFraud  0
dtype: int64
```

HandlingMissingvalues: LabelEncoding:

LABEL ENCODING:

```
#--------------------Before Label Encoding---------------#
******************
    step      type     amount  ... newbalanceDest  isFraud  isFlaggedFraud
0      1   PAYMENT       0.00  ...            0.00        0               0
1      1   PAYMENT    1864.28  ...            0.00        0               0
2      1  TRANSFER       0.00  ...            0.00        1               0
3      1  CASH_OUT     181.00  ...            0.00        1               0
4      1   PAYMENT   11668.14  ...            0.00        0               0
5      1   PAYMENT    7817.71  ...            0.00        0               0
6      1   PAYMENT    7107.77  ...            0.00        0               0
7      1   PAYMENT    7861.64  ...            0.00        0               0
8      1   PAYMENT    4024.36  ...            0.00        0               0
9      1     DEBIT    5337.77  ...        40348.79        0               0
10     1     DEBIT    9644.94  ...       157982.12        0               0
11     1   PAYMENT    3099.97  ...            0.00        0               0
12     1   PAYMENT    2560.74  ...            0.00        0               0
13     1   PAYMENT   11633.76  ...            0.00        0               0
14     1   PAYMENT    4098.78  ...            0.00        0               0
15     1  CASH_OUT  229133.94  ...        51513.44        0               0
16     1   PAYMENT    1563.82  ...            0.00        0               0
17     1   PAYMENT    1157.86  ...            0.00        0               0
18     1   PAYMENT     671.64  ...            0.00        0               0
19     1  TRANSFER  215310.30  ...            0.00        0               0

#--------------------After Label Encoding---------------#
******************
    step  type     amount  ...  newbalanceDest  isFraud  isFlaggedFraud
0      1     3       0.00  ...            0.00        0               0
1      1     3    1864.28  ...            0.00        0               0
2      1     4       0.00  ...            0.00        1               0
3      1     1     181.00  ...            0.00        1               0
4      1     3   11668.14  ...            0.00        0               0
5      1     3    7817.71  ...            0.00        0               0
6      1     3    7107.77  ...            0.00        0               0
7      1     3    7861.64  ...            0.00        0               0
8      1     3    4024.36  ...            0.00        0               0
9      1     2    5337.77  ...        40348.79        0               0
10     1     2    9644.94  ...       157982.12        0               0
11     1     3    3099.97  ...            0.00        0               0
12     1     3    2560.74  ...            0.00        0               0
13     1     3   11633.76  ...            0.00        0               0
14     1     3    4098.78  ...            0.00        0               0
15     1     1  229133.94  ...        51513.44        0               0
16     1     3    1563.82  ...            0.00        0               0
17     1     3    1157.86  ...            0.00        0               0
18     1     3     671.64  ...            0.00        0               0
19     1     4  215310.30  ...            0.00        0               0
```


DOI : https://doi.org/10.5281/zenodo.16810845

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-19***

DATASPLITTING:

```
#--------------------Data Splitting--------------#
*******************
Total no of dataset : (80000, 11)
Training set Without Target (64000, 10)
Training set only Target (64000,)
Testing set Without Target (16000, 10)
Testing set only Target (16000,)
```

5. CONCLUSION

The Random Forest, K-Nearest Neighbors (KNN), and AdaBoost algorithms are utilized in this article to offer a new method for detecting financial statement fraud. This strategy, often known as the "Three Algorithms Approach," works best on files with minimal dimensions. Most of the time, these algorithms' classifiers are more accurate than traditional methods of detecting fraud.

REFERENCES

1. Babu, K. S. (2024). Artificial Intelligence-Based Cyber Security Threat Identification in Financial Institutions Using Machine Learning Approach. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 1473-1490.
2. Zhang, L., & Wang, H. (2024). AI-based Cyber security: Detection and Response Mechanisms in Financial Institutions. Cyber security Research and Applications, 5(2), 22-35.
3. Hassan, S. I., & Ahmed, R. (2023). Enhancing Cyber security in Financial Sectors Using AI and Machine Learning. Journal of Financial Technology, 8(4), 59-73.
4. Patel, J., & Singh, N. (2023). The Role of Machine Learning in Financial Sector Cyber security. Computational Finance, 12(3), 44-58.
5. Li, W., & Zhang, Q. (2023). Secure Financial Transactions with AI Algorithms for Cyber Threat Detection. Journal of Financial Cyber security, 15(1), 102-118.
6. Cheng, M., & Li, J. (2023). Machine Learning Models for Real-Time Cyber Threat Identification in Banks. Financial Technologies and Security, 11(2), 89-105.
7. Ibrahim, M., & Hassan, K. (2023). Fraud Detection and Prevention using AI in Financial Institutions. Journal of Machine Learning in Finance, 7(2), 45-60.
8. Wu, H., & Wang, Y. (2023). An AI Approach to Cyber security Risk Management in Banking. International Journal of Cyber security, 14(3), 27-43.
9. Chen, X., & Zhou, Z. (2022). Leveraging AI for Threat Identification and Prevention in Financial Institutions. Journal of Artificial Intelligence in Financial Systems, 10(1), 101-115.
10. Gao, R., & Wang, J. (2022). Implementing AI for Threat Monitoring and Risk Management in Financial Institutions. Cyber security and Financial Innovation, 8(4), 14-28.
11. Kumar, R., & Singh, M. (2021). Machine Learning Algorithms for Enhancing Cyber security in Financial Sectors. Journal of Cyber Risk Management, 9(2), 50-65.
12. Singh, D., & Agarwal, S. (2021). AI-Driven Solutions for Cyber security in Banks: A Case Research. International Journal of Banking and Finance Technology, 4(1), 91-105.
13. Tan, B., & Li, Y. (2021). Artificial Intelligence in Cyber security for Financial Institutions: A Review and Future Prospects. Financial Security Technology Journal, 17(3), 67-82.
14. Zhao, Y., & Zhang, X. (2020). Cyber security Threats in Financial Institutions and the Role of AI-Based Detection Methods. Journal of Financial Cyber security, 6(4), 118-133.
15. Gupta, R., & Sharma, N. (2020). AI and Machine Learning for Cyber Threat Detection in Financial Services. Journal of Financial Technology and Security, 5(3), 76-88.

DOI : *https://doi.org/10.5281/zenodo.16810845*