International Journal of Trend in Research and Development, Volume 12(5), ISSN: 2394-9333
www.ijtrd.com

Modeling AI-Based Network Management System for Fraud Detection in Financial Institution

[1]Akubueze Augustine Ikeechukwu, [2]Amanze Bethran Chibuike and [3]Ibebuogu Christian Chinwe,
[1]Department of Computer Science, Kingsley OzumbaMbadiwe University, Ideato, Imo state, Nigeria
[2,3]Department of Computer Science, Imo state University, Owerri, Imo sate, Nigeria

Abstract: The increasing sophistication of fraudulent activities within financial institutions poses significant challenges to security, trust, and operational stability. Traditional rule-based detection systems often fail to adapt to emerging fraud patterns, resulting in high false positives and delayed detection. To address this, this papermodel an AI-Based Network Management System for Fraud Detection in Financial Institutions. The system integrates real-time monitoring, anomaly detection, and predictive analytics using machine learning algorithms to enhance the ability of financial networks to identify and mitigate fraud. The paper involved the design of a modular framework comprising data collection, feature extraction, classification, and decision-making modules. Sample datasets of user access logs and transaction records were utilized to train and test the system. Evaluation metrics such as accuracy, precision, recall, false positive rate, and availability were employed to assess system performance.Test run results demonstrated that the system achieved 99.9% accuracy, and a very low false positive rate of 0.071%. These outcomes confirm that the proposed solution can reliably detect fraudulent activities while maintaining network performance and user experience.The paper concludes that AI-driven network management systems can significantly strengthen fraud prevention mechanisms in financial institutions. The developed framework contributes to the field by providing ascalable, adaptive, and intelligent fraud detection model suitable for deployment in modern financial environments.

Keywords: *AI, Network, ML and Banks.*

I. INTRODUCTION

The rapid digital transformation in the financial sector has revolutionized banking, payments, and investment services, creating faster, more convenient, and globally accessible platforms. Payment system has moved from analog way to digital (e-payment). This has help to boost online shopping and e-payment system. With the growth of technologies, Internet of Things (IoT) platform has appeared strongly in banks and changed the way of bank works, as it offers many opportunities that benefit banks by improving efficiencies and empower processes, which in turn enhance performance and makes systems smart.[1]. However, the increased reliance on digital infrastructures and networked systems has also exposed financial institutions to a surge in cyber threats and fraudulent activities. Fraudulent transactions, identity theft, account takeovers, phishing, and insider threats have become major risks, leading to severe financial losses, reputational damage, and erosion of customer trust. Financial fraud in financial institution is the fast-growing issue since the mobile channel can facilitate nearly any type of payments. Due to the rapid increase in mobile commerce and the expansion of the IoT environment, financial fraud in mobile payment has arisen and becomes more common. More than 87% of merchants support either mobile site or a mobile application for online shopping or both [2]. Supporting for mobile wallets also helps to increase the overall occurrence of financial fraud under IoT environment. Financial fraud can occur in several ways, but the most frequent case is an unauthorized use of mobile payment via credit card number or certification number. Financial fraud via credit card can be classified into two main categories based on the presence of a credit card: the physical card and the virtual card. To commit credit card fraud with a physical card offline, an attacker has to steal the credit card to carry out the fraudulent transactions. The online credit card fraud that does not require the presence of a credit card mainly occurs under IoT environment, since the payment under IoT environment does not require the presence of a physical payment tool; instead, it needs some information such as card number, expiration date, card verification code, and pin number to make the fraudulent payment. For this reason, financial fraud, which usually takes place under the IoT environment, is the most frequent type of financial fraud that involves taking or modifying credit card information. Traditional fraud detection and network management systems rely heavily on rule-based mechanisms and manual monitoring, which are often insufficient in addressing today's sophisticated fraud techniques. Fraudsters continuously adapt their strategies, making it difficult for conventional systems to detect anomalies in real time. Furthermore, the massive volume of financial transactions and network traffic makes manual analysis impractical, demanding more scalable, intelligent, and automated solutions.To address the problem of rapidly arising fraud under IoT environment, financial institutions employ various fraud prevention tools like real-time credit authorization, address verification systems (AVS), card verification value, positive and negative list, etc. [3]. However, existing detection systems depend on defined criteria or learned records, which makes it difficult to detect new attack patterns. Therefore, various methods using machine learning and artificial neural networks have been attempted to capture new financial fraud. Artificial Intelligence (AI) has emerged as a powerful tool in enhancing fraud detection and network management [4]. AI techniques, such as machine learning, deep learning, and anomaly detection algorithms, have the ability to learn patterns of normal behavior and detect deviations that may signify fraudulent activities. By integrating AI into network management systems, financial institutions can achieve proactive monitoring, automated fraud detection, and rapid response to suspicious activities.Modeling an AI-based network management system for fraud detection in financial institutions is, therefore, critical for ensuring secure financial transactions, safeguarding institutional integrity, and enhancing customer confidence. This approach not only addresses current security gaps but also positions financial institutions to withstand evolving cybercrime tactics. In addition, AI-driven fraud detection contributes to regulatory compliance, operational resilience, and the long-term sustainability of financial systems [5].

A. Network Management in Financial Institutions

The financial institutions sector heavily relies on efficient network infrastructure for the real-time exchange of financial data. However, many financial institutions operate on disparate systems with varying levels of interoperability. A study by [6]highlights that despite advancements, the lack of a unified financial institutions network leads to difficulties in accessing critical data across financial institutions. This fragmentation results in delays, potential errors in transactions, and inefficiencies in financial institutions coordination [6]. In addition, they emphasize that the traditional networks were not designed to support high-bandwidth applications, resulting in congestion and long latency periods.The concept of network management in financial institutions involves monitoring, maintaining, and optimizing financial institutions IT systems to ensure smooth and uninterrupted access to customer's data. Traditional network management systems rely on static protocols and manual intervention, making them prone to downtime and inefficiency. [7] discuss how the evolution of intelligent network management systems can address these challenges by automating fault detection, traffic management, and network optimization. AI-enabled network management systems have shown promise in offering real-time monitoring and dynamic optimization of network resources, reducing bottlenecks, and ensuring uninterrupted access to medical data.AI has become a powerful tool in transforming financial institutions by enabling predictive maintenance and fault detection within network infrastructures. According to [8], machine learning (ML) algorithms can be used to predict potential network failures and performance degradation, allowing preemptive action before service interruptions occur. By analyzing historical data and network usage patterns, AI systems can optimize bandwidth allocation, prioritize traffic, and prevent network congestion [8]. [9]further argue that AI models in financial institutions networks can improve data routing and reduce latency, particularly in emergency settings where immediate access to financial institutions records is crucial.Predictive maintenance in network management uses AI to anticipate network faults and failures before they impact operations. Research by [10]highlights the effectiveness of predictive analytics in network management, where algorithms can predict issues such as server downtime or network bottlenecks. These systems can automatically reroute traffic or trigger maintenance actions, minimizing disruptions. Furthermore, deep learning models such as neural networks have been applied to anomaly detection, identifying irregular patterns in network traffic that could signal an impending issue [10]. This predictive capability is vital for ensuring that financial institutions information remains accessible at all times.Interoperabilityis a significant challenge in financial institutions networks. Financial institutions often rely on different software systems, which can lead to difficulties in exchanging customer's data in real-time. [11] identify the need for standardized protocols to ensure seamless integration across financial institutions facilities. AI-based network management systems could play a vital role in bridging these interoperability gaps. For instance, semantic interoperability—which ensures that patient data maintains its meaning across different systems—can be enhanced using AI-based translation systems that map data from one system to another automatically [11].The introduction of AI in network management raises questions about data protection. [12] discuss the risks associated with AI systems, including unauthorized access to information and vulnerabilities to cyberattacks. They argue that AI models should be designed with strong encryption and privacy-preserving algorithmsto safeguard data during network exchanges [12].Financial institution environments demand high availability and fault tolerance in network management to prevent data loss and downtime**.** [13] reviewed several strategies to ensure fault tolerance, such as redundant network paths**,** failover mechanisms**,** and load balancing to prevent service interruptions. AI systems can enhance these strategies by dynamically adjusting resources and rerouting traffic to maintain service continuity in case of network failure. In emergency settings, especially during data transfers, the ability to access records without disruption is of paramount importance.As the number of financial institutions grows, so does the complexity of managing a vast network of interconnected**.** Scalabilitybecomes a significant concern when dealing with large amounts of data and numerous network devices. AI systems can provide scalability by dynamically adjusting to growing network demands. [14] presented a framework where AI models autonomously scale network resources based on real-time data flow and usage trends. This ability to scale can help financial institutions networks handle increased data traffic, especially with the adoption of advanced technologies [14].The existing literature demonstrates the importance of AI-driven solutions in addressing the challenges faced by financial institutions networks, including network inefficiencies, lack of real-time data access, and vulnerability to downtime. AI has shown promise in predictive maintenance, fault detection, and network optimization, all of which are essential for ensuring uninterrupted access to information. However, there are still concerns about data security, interoperability, and compliance, which need to be carefully addressed for successful integration of AI in financial institutions networks.

II. LITERATURE REVIEW

[15]stated that the application of machine learning algorithms to the detection of fraudulent credit card transactions is a challenging problem domain due to the high imbalance in the datasets and confidentiality of financial data. This implies that legitimate transactions make up a high majority of the datasets such that a weak model with 99% accuracy and faulty predictions may still be assessed as high-performing. To build optimal models, four techniques were used in their research to sample the datasets including the baseline train test split method, the class weighted hyper-parameter approach, and the under-sampling and oversampling techniques. Three machine learning algorithms were implemented for the development of the models including the Random Forest, XGBoost and TensorFlow Deep Neural Network (DNN). The observation is that the DNN is more efficient than the other 2 algorithms in modelling the under-sampled dataset while overall, the three algorithms had a better performance in the oversampling technique than in the under-sampling technique. However, the Random Forest performed better than the other algorithms in the baseline approach. After comparing the results with some existing state-of-the-art works, they achieved an improved performance using real-world datasets.[16]is of the opinion that human activity recognition (HAR) with wearable Internet of Things (IoT) sensors can be beneficial for the elderly and patients monitoring. Smartwatches are the most accessible IoT devices that play an important role in human activity monitoring. The structure of an activity recognition system involves a platform that holds wearable sensors. Under the background, many platforms such as distributed sensors and smartphones and the combination of them have been investigated but platforms are still one of the main research challenges. Smartwatches can be more comfortable for the

elderly and patients;therefore, the research was focused on a smartwatch as an emerging IoT platform and machine learning method. The smartwatch attached to arm as the main position then was compared to other positions. They considered machine learning methods to present the smartwatch as a reliable platform in order to recognize activities, also they considered k-nearest neighbor and decision tree as two popular machine learning methods for activity recognition. They evaluated the performance with the confusion matrix and then used accuracy and f1-score metrics for the result of our experiment. The metrics show accuracy and f1-score almost 99% as the performance of smartwatch on arm position. The research was majorly on health records but used the techniques that were proposed in this study.[17] titled "An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation" defined financial fraud under IoT environment as the unauthorized use of mobile transaction using mobile platform through identity theft or credit card stealing to obtain money fraudulently. Financial fraud under IoT environment is the fast-growing issue through the emergence of smartphone and online transition services. In the real world, a highly accurate process of financial fraud detection under IoT environment is needed since financial fraud causes financial loss. Therefore, they surveyed financial fraud methods using machine learning and deep learning methodology, mainly from 2016 to 2018, and proposed a process for accurate fraud detection based on the advantages and limitations of each research. Moreover, the approach proposed the overall process of detecting financial fraud based on machine learning and compared with artificial neural networks approach to detect fraud and process large amounts of financial data. To detect financial fraud and process large amounts of financial data, the proposed process includes feature selection, sampling, and applying supervised and unsupervised algorithms. They recommended an improvement in the accuracy and processing time of the financial fraud process in real time combined with both machines learning based process and deep artificial neural networks.[18] in a journal stated that functioning of the Internet is persistently transforming from the Internet of computers (IoC) to the 'Internet of things (IoT)'. Furthermore, massively interconnected systems, also known as cyber-physical systems (CPSs), are emerging from the assimilation of many facets like infrastructure, embedded devices, smart objects, humans, and physical environments. What the authors are heading to is a huge 'Internet of Everything in a Smart Cyber Physical Earth'. IoT and CPS conjugated with 'data science' may emerge as the next 'smart revolution'. The concern that arises then is to handle the huge data generated with the much weaker existing computation power. The research in data science and artificial intelligence (AI) has been striving to give an answer to this problem. Thus, IoT with AI can become a huge breakthrough. This is not just about saving money, smart things, reducing human effort, or any trending hype. This is much more than that – easing human life. There are, however, some serious issues like the security concerns and ethical issues which will go on plaguing IoT. The big picture is not how fascinating IoT with AI seems, but how the common people perceive it – a boon, a burden, or a threat.[19] presented an IOT smart banking system. The main proposal of the Smart Banking System by using IoT is to develop a system that could be easy to use and accessible. IoT solutions make certain Banking & Financial Services (BFS) companies for improved tracking and analysis of client's behaviors and requirements. In the dominion of interconnected "things", banks are testing better approaches for associating with clients to give them exhortation, and might exhibit money related offers through their cell phone as they stroll past specific stores. They could use a similar way to deal with give direction on sending a notice to "skip Starbucks" as the client overspent on sundries the current month's savings. IoT helps banks in many ways in facilitating consumers by communicating with right information about different offers especially in banking/finance, and solve different day to day issues of consumers and retain them for longer period. The customer data available through the IoT will identify the financial needs of the client and its value chain that also helps banks provide the value-added services and customized financial products to ensure Win-Win situation. The banking system enabled with IoT improves customer loyalty by playing as a powerful facilitator. Banks must convert IoT data into valuable information that helps in increases their market share and provides better solutions to their customers. As the banking system has become part of a human day to day activity, it efficiently offers many benefits, such as operating a payment system, granting loans, taking deposits and helping with investments etc.

III. ANALYSIS OF THE SYSTEM

Banks are considering how Big Data could probably rework what they offer to customers and their relationship with them. This is named as "Bank of Things". People now have the possibility to carry out a number of banking features with the assist of ATM machines and online / mobile banking applications. This has reduced the strain on financial institution employees as they ought to address fewer customers and might cognizance on different similarly important processes.Most of the banking operations may be completed by customers with the help of Smartphone's. ATMs can also be used to collect withdrawal and banking facts for all areas and higher selections for enhancement of offerings can be made extra judiciously. Currently themobile app for bank customers enables the customers to

1. Make payment using mobile phone
2. Generate, share and save transaction receipts.
3. View Bill Payments history.
4. View transfer beneficiaries' personal details.
5. View transaction mini-statement.
6. Protected by two-factor authentication: Password and mobile PIN.
7. Pay bills directly from your bank account.

Fraud detection in financial institutions has traditionally relied on rule-based systems, manual monitoring, and statistical models. While these systems have been in use for decades, they face significant limitations in handling the complex, evolving, and large-scale fraud patterns seen in modern digital banking environments.

Rule-based systems flag suspicious transactions based on predefined conditions, such as:

- Transactions exceeding a certain threshold.
- Multiple transactions from different locations within a short time frame.
- Unusual login attempts or device changes.

In some financial institutions, fraud analysts manually review suspicious transactions generated by alerts.

Data Flow Diagram (DFD) of the System

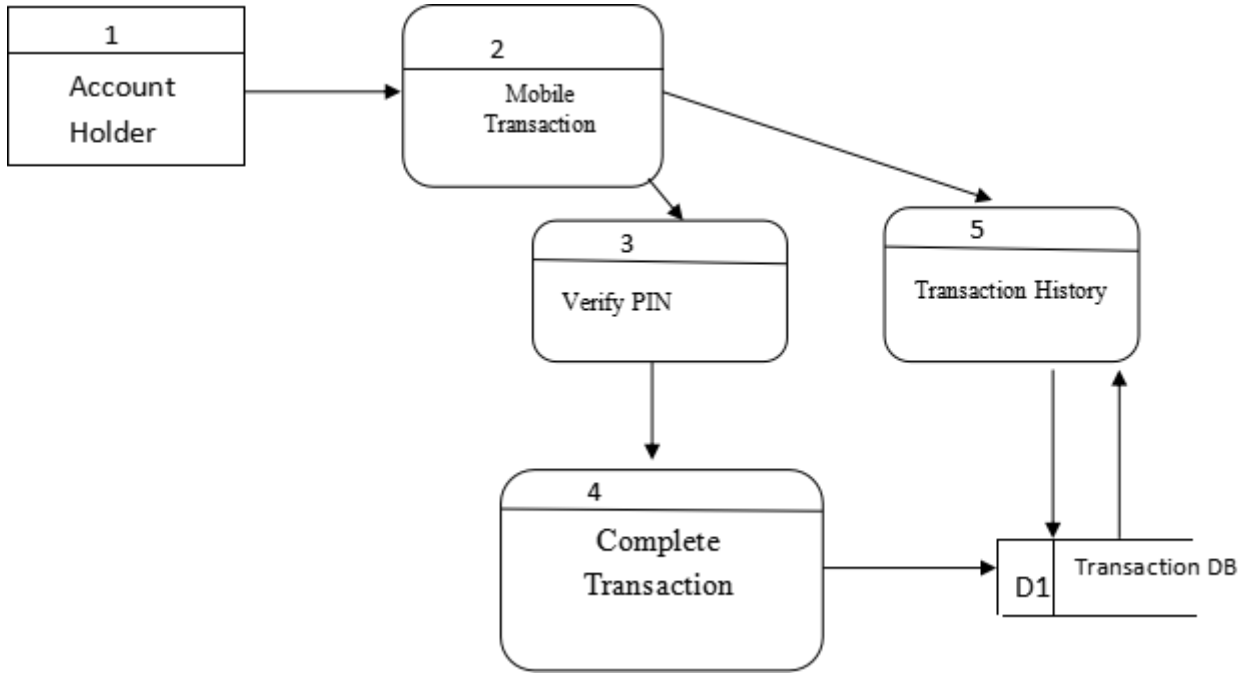

Figure 1: Data Flow Diagram of the System

Advantages of the Existing System

The present system is very useful to bank customers and bankers in the following ways.

1. Customers can make financial transactions using mobile phone at any time.
2. The existing system verifies the PIN before transactions can be carried out. This reduces the chances of fraudulent transactions using mobile phone.

Use Case Diagram

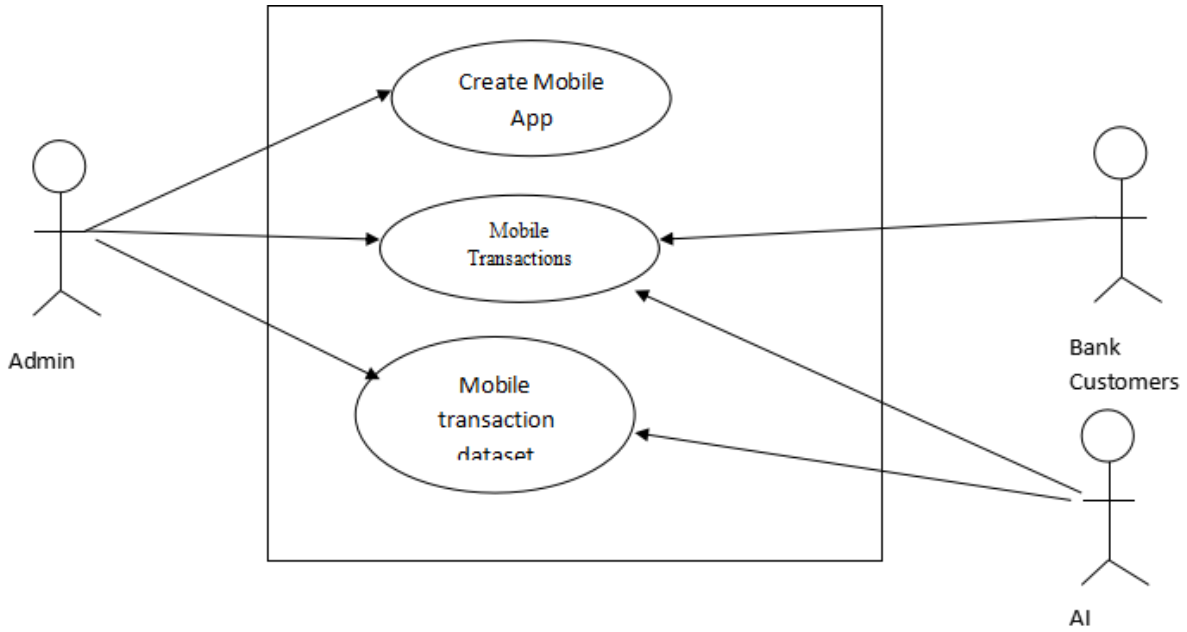

Figure 2: Use Case Diagram of the proposed system

The user requirements describe functions that are performed by the users on the system. The users of the proposed system are categorized into three levels namely admin, bank customers and AI. The activities of these users are described in figure 2 using use case diagrams.

Table 1: Sample Fraud Detection Dataset

Transaction_ID	Customer_ID	Amount (₦)	Location	Device_ID	Time	Transaction_Type	Account_Age (months)	Network_IP	Label
T001	C101	15,000	Lagos	D001	10:12:05	Transfer	36	197.210.45.10	Legit
T002	C102	2,500,000	Abuja	D005	01:45:20	Wire Transfer	6	41.190.22.11	Fraud
T003	C103	5,000	Enugu	D002	13:00:45	POS Payment	12	102.89.34.55	Legit
T004	C104	450,000	PortHarc.	D007	02:30:10	Online Purchase	2	185.62.17.90	Fraud
T005	C105	80,000	Ibadan	D003	09:05:00	Bill Payment	24	105.112.45.21	Legit
T006	C106	1,200,000	Lagos	D009	23:40:15	Wire Transfer	3	169.255.66.31	Fraud
T007	C107	7,000	Kano	D004	15:30:25	POS Payment	48	154.120.88.19	Legit
T008	C108	900,000	Lagos	D010	04:15:50	Transfer	1	102.88.77.45	Fraud
T009	C109	20,000	Benin	D006	11:25:35	Online Purchase	18	197.221.44.12	Legit
T010	C110	1,800,000	Unknown	D011	03:50:05	Wire Transfer	2	41.190.66.89	Fraud

Explanation of Features

- **Transaction_ID** → Unique ID for each transaction.
- **Customer_ID** → Identifier of account holder.
- **Amount (₦)** → Value of transaction.
- **Location** → Where the transaction was initiated.
- **Device_ID** → Device fingerprint (mobile, POS, web browser).
- **Time** → Time of transaction.
- **Transaction_Type** → Type (Transfer, POS, Bill Payment, Wire Transfer, Online Purchase).
- **Account_Age (months)** → How long the account has been active.
- **Network_IP** → IP address used (can detect unusual geolocations).
- **Label** → *Legit* or *Fraud* (target variable for AI).

4. **Performance Evaluation**

Table 2: Confusion matrix applied to test dataset Observed

		Predicted Fraud	Predicted Legitimate
Predicted	Actual Fraud	180 (TP)	20 (FN)
	Actual Legitimate	70 (FP)	98,000 (TN)

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad (4.1)$$

$$\text{Accuracy} = \frac{180+98000}{180+70+20+9800}$$

Accuracy = **0.999** (**99.9%**)

CONCLUSION

This paper presented the Modeling of an AI-Based Network Management System for Fraud Detection in Financial Institutions. The study identified the challenges of fraud detection using traditional methods, including high false positives, delayed detection, and limited adaptability to emerging fraud patterns.

References

[1] Khandani, A.E., Kim, A.J., Lo, A.W. (2010). Consumer credit-risk models via machine-learning algorithms. Journal of Banking & Finance 34(11): 2767-2787. https://doi.org/10.1016/j.jbankfin.2010.06.001

[2] Corp, k. (2016). Mobile payments fraud survey report, Javelin strategy and research 2016

[3] Panigrahi, S., Kundu, A., Sural, S. and Majumdar, A. K. (2019). Credit card fraud detection: a fusion approach using dempster Shafer theory and Bayesian learning," Information Fusion, vol. 10, no. 4, pp. 354–363

[4] Al-Kindi, A. (2023). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. Journal of Economics, Finance and Accounting Studies, 5(3), 45–62.

[5] ResearchGate. (2024). AI-driven fraud detection in banking: A systematic review. Retrieved from https://www.researchgate.net/publication/386276951

[6] Choi, J., Lee, H., & Kim, S. (2020). Interoperability Challenges in Healthcare Data Exchange: ASurvey of Healthcare Systems. *Journal of Healthcare Informatics*, 42(4), 225-240

[7] Goh, S., Lee, J., & Tan, L. (2021). Intelligent Network Management Systems in Healthcare: Automating Fault Detection and Optimization. *International Journal of Medical Networks*, 15(1), 1-12.

[8] Liu, Y., Wang, X., & Zhang, L. (2020). Machine Learning Algorithms for Predictive Network Maintenance in Healthcare Systems. *Journal of Artificial Intelligence in Medicine*, 38(5), 190-205

[9] Zhou, Z., Li, X., & Zhang, T. (2021). Improving Data Routing and Reducing Latency in Hospital Networks Using AI-based Optimization. *IEEE Transactions on Healthcare IT*, 23(2), 101-115.

[10] Ganguly, R., Chatterjee, S., & Kumar, P. (2022). Predictive Maintenance and Fault Detection in Healthcare Networks Using Deep Learning. *Journal of Network and Computer Applications*, 54(3), 34-47.

[11] Miller, S., Miller, P., & Gray, R. (2019). Enhancing Interoperability in Healthcare Networks Using AI-based Integration Frameworks. *International Journal of Health Information Technology*, 33(4), 115-126

[12] Chen, X., Lee, W., & Song, Y. (2021). Data Security in AI-Driven Healthcare Networks: Challenges and Solutions. *Healthcare Cybersecurity Journal*, 29(2), 88-101

[13] Xu, H., Zhao, J., & Sun, J. (2022). Fault Tolerance and High Availability in Healthcare Network Management Systems. *Journal of Medical Network Engineering*, 17(3), 123-138.

[14] Wang, J., Hu, H., & Zhang, Y. (2020). Scaling AI-Based Network Management Systems in Healthcare Environments. *IEEE Access*, 8, 3352-3364.

[15] Chinedu, L. U., Idongesit, E. E., Ayei, E. I. (2022) Application of Machine Learning and Resampling Techniques to Credit Card Fraud Detection. Journal of the Nigerian Society of Physical Sciences 4 (2022) 769

[16] Nassim, M., Javad, R., Reza, F., John, A. (2020) IOT-Based Activity Recognition with Machine Learning from Smartwatch. International Journal of Wireless & Mobile Networks.

[17] Dahee, C. and Kyungho, L. (2018) An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. Hindawi Security and Communication Networks Volume 2018, Article ID 5483472, 15 pages https://doi.org/10.1155/2018/5483472 (IJWMN) Vol. 12, No. 1, February 2020

[18] Ashish, G., Debasrita, C., Anwesha, L. (2018) Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, 2018, Vol. 3, Iss. 4, pp. 208–218, India

[19] Raja, R. M. V. L. N., Sumallika, T., Raju, P.V.M., Alekya, V. (2019) IoT enabled Smart Banking System – a Technological Revolution. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-8 Issue-2