International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 8, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i8.714

Neuromorphic Computing for Real-Time Threat Detection in Banking Networks: A Novel Approach

Giwa Olajumoke Sherifat[1]

Publication Date 2025/08/27

Abstract

This research work looks into the application of Neuromorphic computing for real-time threat detection in banking networks. The emergence of Neuromorphic computing which is inspired by the human brain's neural structure and function offers a more sophisticated and promising solution to the challenges of detecting threat, financial crimes and cyber-attacks. The research also identified limitations of the traditional threat detection approaches in the banking networks and then highlighted the benefits with the introduction of Neuromorphic computing in threat detection and prevention. The Author further explored the key challenges faced in implementing Neuromorphic computing and then recommended potential future directions for research and development in the field. The research finally concluded that Neuromorphic computing has the potential to transform threat detection processes in the banking network and improve financial security generally in financial institutions.

I. INTRODUCTION

The banking sector has been faced with constant challenges in fighting financial crimes resulting from cyber-attacks with increasingly advanced technological criminal strategies. Traditional detection methods have proven inadequate against sophisticated insider threats, who leverage their authorized access and institutional knowledge to circumvent security measures (Akintayo M. A. et al, 2024). However, with the emergence of neuromorphic computing, there is now increased prospect in finding a solution to this problem. By mimicking the neural structure and function of the human brain, neuromorphic computing can process complex data with high efficiency, speed, and low power consumption (Khaled S. A., and Fayroz F. S., 2024).

Neuromorphic computing has the potential to revolutionize real-time threat detection in banking networks by providing a more efficient and adaptive approach to security (Shatson P. F., 2024). Unlike traditional computing architectures, which are limited by processor-memory bottlenecks, neuromorphic computing systems can process simple iterations efficiently, making them well-suited for machine learning applications (Khaled S. A., and Fayroz F. S., 2024). Neuromorphic computing, modeled after the intricate design and processes of the human brain, stands as a notable step forward for the banking industry especially in terms of security. Frankly, traditional threat detection systems are increasingly outpaced by the growing complexity of cyber-attacks and insider threats. As bad actors become more sophisticated, it's clear that conventional security measures struggle to keep up. Neuromorphic systems, by contrast, have the potential to process information in real-time, adaptively identifying anomalies as they occur.

In this article, we will examine the limitations of conventional detection techniques, the advantages offered by neuromorphic computing, and the practical applications this technology may have within banking networks. The aim is to clarify how neuromorphic computing could fundamentally improve real-time threat detection and overall security in the financial sector. By synthesizing insights from diverse technological and academic perspectives, we aim to provide a comprehensive understanding of how neuromorphic computing can be used to improve financial crime prevention strategies in banking (Akintayo M. A. et al, 2024).

II. OVERVIEW OF NEUROMORPHIC COMPUTING AND ITS GOALS

Neuromorphic computing is a type of computing that is inspired by the structure and function of the human brain (Shatson P. F., 2024). It involves the development of artificial neural networks that mimic the behavior of biological neurons and synapses, allowing for efficient and adaptive processing of complex data (Khaled S. A., and Fayroz F. S., 2024). The goal of neuromorphic computing

Sherifat, G. O. (2025). Neuromorphic Computing for Real-Time Threat Detection in Banking Networks: A Novel Approach. *International Journal of Scientific Research and Modern Technology*, *4*(8), 28–31. https://doi.org/10.38124/ijsrmt.v4i8.714

is to create systems that can learn and adapt in real-time, without the need for explicit programming or training (Jubair A. L. et al, 2023).

The development of neuromorphic computing dates back to the 1980s, when Carver Mead, a professor at Caltech, first proposed the concept (Jubair A. L. et al, 2023). Since then, significant advances have been made in the field, with the development of artificial neural networks, synaptic devices, and other neuromorphic systems (Khaled S. A., and Fayroz F. S., 2024).

The primary goal of neuromorphic computing is to create systems that can process information in a way that is similar to the human brain. This involves developing systems that can learn and adapt in real-time, using spiking neural networks and other neuromorphic architectures (Jubair A. L. et al, 2023). By mimicking the brain's neural networks, neuromorphic computing systems can provide efficient and adaptive processing of complex data, making them well-suited for applications such as real-time threat detection in banking networks.

- *Some of the Key Goals of Neuromorphic Computing Include:*

- Developing systems that can learn and adapt in real-time, without the need for explicit programming or training (Jubair A. L. et al, 2023)
- Creating systems that can process complex data with high efficiency, speed, and low power consumption (Shatson P. F., 2024)
- Developing edge AI systems that can operate independently, without the need for centralized processing or cloud connectivity.
- Improving the efficiency and effectiveness of artificial intelligence systems, by leveraging the power of neuromorphic computing.

By achieving these goals, neuromorphic computing has the potential to revolutionize a wide range of applications, from real-time threat detection in banking networks to artificial general intelligence (Khaled S. A., and Fayroz F. S., 2024).

III. NEUROMORPHIC COMPUTING FOR THREAT DETECTION

- *Real-Time Threat Detection in Banking Networks*

Real-time threat detection is a critical component of banking network security, as it enables financial institutions to identify and respond to potential security threats as they emerge. Traditional threat detection systems rely on rule-based approaches, which can be slow to adapt to new threats and may not be effective against sophisticated attacks (Akintayo M. A. et al, 2024). Neuromorphic computing offers a promising solution to this problem, as it can process complex data in real-time and adapt to new threats through machine learning algorithms (Shatson P. F., 2024).

By leveraging neuromorphic computing, banks can improve their ability to detect and prevent financial crimes, such as insider threats and cyber-attacks. Neuromorphic systems can analyze network traffic, system logs, and other data in real-time, identifying potential security threats and alerting bank officials to take action (Akintayo M. A. et al, 2024).

- *Challenges of Real-Time Threat Detection in Banking Networks*

In In the contemporary era where transactions are mostly cashless with most people using banking apps and bank networks to meet their daily transaction needs. The banks are mandated to secure the funds of their clients and in some cases are held liable for loss of funds when cyber-attacks occur. In the midst of the huge transactional traffics in the banking network, it is extremely difficult to identify and crack down criminal elements.

The traditional tools used by the banks often proof inadequate to effectively identify and manage cyber threats when they occur. This is because these criminals are constantly evolving in the tools and strategies, they use in cyber-attacks making it more difficult to track them down.

In-order to address this challenge, the introduction of Neuromorphic computing has been a game-changer in mitigating and reducing the frequent cyber-attacks faced by the banking networks. This technology could proof to be a step towards addressing cyber-attacks in the long run.

- *Requirements for Real-Time Threat Detection Systems*

Certain key requirements must be met for Real-time threat detection systems to be effective. Some of the most important requirements include:

- *Speed and Efficiency:*

Systems must be able to analyze large volumes of data in real-time, without significant latency or performance degradation (Akintayo M. A. et al, 2024).

- *Accuracy and Precision:*

Systems must be able to identify potential security threats with high accuracy and precision, minimizing false positives and false negatives (Akintayo M. A. et al, 2024).

- *Adaptability:*

Systems must be able to adapt to new threats and evolving attack strategies, through machine learning algorithms and other advanced techniques (Shatson P. F., 2024).

- *Scalability:*

Systems must be able to scale to meet the needs of large and complex banking networks, handling high volumes of data and traffic (Akintayo M. A. et al, 2024).

By meeting these requirements, neuromorphic computing systems can provide effective real-time threat detection capabilities for banking networks, improving the security and resilience of financial institutions.

IV. AI AND MACHINE LEARNING APPLICATION

The application of artificial intelligence (AI) and machine learning (ML) in banking networks has revolutionized the way financial institutions detect and prevent financial crimes. Here are some key AI and ML applications in threat detection:

- *Supervised Learning Approaches*

Supervised learning approaches involve training machine learning models on labeled datasets to recognize patterns of fraudulent behavior (Bello O. A. et al, 2023). These models can then be used to identify potential security threats in real-time, by analyzing transaction data and other relevant information (Kute D.V. et al, 2021). Supervised learning approaches have been shown to be effective in detecting insider threats and other types of financial crimes (Manoharan P. 2023).

- *Unsupervised Anomaly Detection*

Unsupervised anomaly detection involves identifying patterns of behavior that are unusual or anomalous, without prior knowledge of the underlying distribution of the data (Goldstein M, and Uchida S. 2016). These can be used to detect and identify unknown threats as well as identifying security risks. Unsupervised anomaly detection is particularly useful in detecting insider threats, where the perpetrator may be operating within their authorized access levels (Manoharan P. 2023).

- *Deep Learning Fraud Detection*

Deep learning fraud detection involves using deep neural networks to identify patterns of fraudulent behavior. These fraud detection models can learn complex data patterns and identify potential security threats with high accuracy. Deep learning models have been shown to be effective in detecting a wide range of financial crimes, including credit card fraud and money laundering (Akintayo M. A. et al, 2024).

- *Real-Time Transaction Monitoring System*

Real-time transaction monitoring refers to the constant check on financial transaction to help detect and identify cases of irregularities in the transaction. With the help of modern advanced machine learning techniques, fraudulent transactions can be easily identified by the monitoring systems of the bank which will enable shift response from the banking personnel. This proactive approach in necessary for the integrity of the bank or financial institutions as it will help in preventing threats and reinforcing confidence from customers. Real-time transaction monitoring systems can help prevent financial crimes by identifying and stopping suspicious transactions before they are processed (Adeyemo K. and Obafemi F. J. 2024).

By leveraging these AI and ML applications, banks can improve their ability to detect and prevent financial crimes, reducing the risk of insider threats and cyber-attacks. Neuromorphic computing essentially represents a significant advancement in threat detection, akin to equipping these systems with a highly adaptive, brain-like architecture. Unlike traditional methods, neuromorphic models don't just follow rigid rules; they can process complex data streams in real time and adjust their responses as new threats emerge. What this means in practice is that banks and other financial institutions gain a continuously learning and dynamic defense mechanism, which gives them the ability to react to cyber risks with increased speed and precision.

V. CHALLENGES OF NEUROMORPHIC COMPUTING

In-spite of the breakthrough experienced by financial institutions with the emergence of Neuromorphic computing, there are some challenges that needs to be addressed. Some of these key challenges include:

- *Hardware Limitations:*

Neuromorphic computing requires specialized hardware that can mimic the behavior of biological neurons and synapses (Jubair A. L. et al, 2023). Developing reliable and efficient hardware for neuromorphic computing is a significant challenge.

- *Scalability:*

Neuromorphic systems need to be scalable to handle large volumes of data and complex networks (Jubair A. L. et al, 2023). Scaling up neuromorphic systems while maintaining their efficiency and accuracy is a significant challenge.

- *Training and Learning:*

Neuromorphic systems require effective training and learning mechanisms to adapt to new threats and evolving attack strategies (Shatson P. F., 2024). Developing these mechanisms is a significant challenge.

- *Integration with Existing Systems:*

Neuromorphic systems need to be integrated with existing security systems and infrastructure. This will involve developing interfaces and protocols which can communicate with traditional security systems (Akintayo M. A. et al, 2024).

VI. FUTURE OF NEUROMORPHIC COMPUTING

Neuromorphic computing offers many opportunities for future research and development. Some potential future directions include:

- *Advances in Hardware and Software:*

Advances in hardware and software for neuromorphic computing could enable more efficient and effective threat detection systems (Jubair A. L. et al, 2023).

- *Integration with Other AI Techniques:*

Integrating neuromorphic computing with other AI techniques, such as deep learning, could enable more effective threat detection systems (Akintayo M. A. et al, 2024).

➢ *Applications Beyond Banking:*

Neuromorphic computing has potential applications beyond banking, including cybersecurity, healthcare, and finance (Khaled S. A., and Fayroz F. S., 2024).

VII. CONCLUSION

In conclusion, neuromorphic computing offers a promising solution for real-time threat detection in banking networks. By imitating the neural structure and function of the human brain, neuromorphic computing can provide efficient and adaptive processing of complex data in real-time (Shatson P. F., 2024). While there are challenges to be addressed as identified in this research, the potential benefits of Neuromorphic computing for threat detection are significant. Further research and development are needed to fully realize the potential of neuromorphic computing for threat detection in banking networks.

REFERENCES

[1]. Adeyemo K. and Obafemi F. J. (2024) *A Survey on the Role of Technological Innovation in Nigerian Deposit Money Bank Fraud Prevention.* South Asian Journal of Social Studies and Economics. 2024 Feb 12;21(3):133-50.

[2]. Akintayo M. A. et al (2024) *Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity*. World Journal of Advanced Research and Reviews, 2024, 24(02), 123–132

[3]. Bello O. A. et al (2023) *Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions.* International Journal of Management Technology. 10(1):85-108.

[4]. Goldstein M, and Uchida S. (2016) *A Comparative evaluation of unsupervised anomaly detection algorithms for multivariate data.* PloS one. 19;11(4): e0152173.

[5]. Jubair A. L. et al (2023) *Introduction to Neuromorphic Computing Systems.* DOI: 10.4018/978-1-6684-6596-7.ch001

[6]. Khaled S. A., and Fayroz F. S. (2024) *Neuromorphic Computing between*

[7]. *Reality and Future Needs.* Intech open journal

[8]. Kute D.V. et al (2021) *Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review.* IEEE access 4; 9:82300-17.

[9]. Manoharan P. (2023) *Supervised Learning for Insider Threat Detection (Doctoral dissertation, Victoria University)*. World Journal of Advanced Research and Reviews, 24(02), 123–132

[10]. Shatson P. F. (2024) *Neuromorphic computing for real-time adaptive penetration testing: analysis of human intuition in AI-dominated work space.* World Journal of Advanced Research and Reviews, 2024, 24(03), 2038-2051