ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

Adaptive Behavioral Analytics for Intrusion Prevention in Ai-Driven Digital Currency and Financial Cyber Defense Systems

Eric Jhessim [1]

[1]Cybersecurity, University of Delaware, Newark, DE, USA.

Publication Date: 2025/07/19

Abstract: Behavioral analytics is a cutting-edge tool in the fight for financial cybersecurity. It uses advanced AI and machine learning to pinpoint dangers that outdated methods might miss. This study examines how well these AI-based tools work and the challenges encountered, especially when trying to mitigate and prevent security breaches in the digital currency world and financial markets. The case study analysis of three large-scale security incidents, namely a cryptocurrency exchange, a banking institution an advanced persistent threat (APT), and a DeFi platform, identified the current state of behavioral analytics implementation. Key findings show that while AI-based solutions can efficiently identify threats that rely on the volume and behavioral patterns of the underlying systems, they struggle with more refined attacks that exploit legitimate features. Consequently, these systems exhibit high false positives and low response times. The cross-case analysis indicates that the behavioral correlations across domains and the threshold off-peak periods are not adequately addressed. The study offers recommendations on better implementation for algorithm development and data integration as well as policy formulation. Therefore, the main contributions are: 1: Common behavioral indicators can be derived from the financial platform. 2: Human-AI cooperation is required to obtain an effective identification process, and 3: The security and operation continuity requirements can be balanced by adjusting the threshold level in real time.

Keywords: *Behavioral Analytics, Financial Cybersecurity, Cyber Defense Systems, Defense Systems, Digital Currency, AI.*

How to Cite: Eric Jhessim; (2025), Adaptive Behavioral Analytics for Intrusion Prevention in Ai-Driven Digital Currency and Financial Cyber Defense Systems. *International Journal of Innovative Science and Research Technology*, 10(7), 1314-1321. https://doi.org/10.38124/ijisrt/25jul835

I. INTRODUCTION

Digital currency and financial cyber defense systems face massive cyber threats as a result of their critical nature and increasing reliance on technology (Darem et al., 2023). The threats include ransomware, data breaches, denial-of-service attacks, and phishing, which target vulnerabilities in financial sectors (Gopalakrishnan, 2025). As cyber threats evolve rapidly, they pose a major challenge for institutions to match the latest technologies and trends. Thus, advanced security measures like multi-factor authentication, AI-driven fraud detection, and encryption are crucial to mitigate the risks (Tripathi, 2024).

Meanwhile, research shows that traditional signature-based intrusion prevention and detection systems are limited, emphasizing the need for adaptive, AI-driven alternatives in cybersecurity. According to (), a novel AI-driven intrusion detection system (IDS) showed high accuracy in different datasets, providing up to 99.99% accuracy in detecting network attacks. In comparison, an AI-powered IDS that combined multiple machine learning (ML) techniques achieved 92.8% accuracy, showing more efficiency than conventional solutions in the detection of known and unknown threats (Alzaylaee, 2025).

Essentially, artificial intelligence (AI) and ML technologies are revolutionizing financial security using advanced pattern recognition and behavioral analytics (Rani, Singh, & Khang, 2025). Based on the evolving nature of cyber threats, there is a need for more proactive cybersecurity measures in digital currency and financial cyber defense systems.

➢ *Aim and Objectives*

This study aims to critically evaluate the effectiveness and implementation challenges regarding adaptive behavioral analytics in AI-driven intrusion prevention systems within digital currency and financial cyber defense ecosystems.

➢ *The Objectives are:*

- To assess the current state of adaptive behavioral analytics systems in detecting and preventing cyber intrusions in different financial platforms.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

- To identify and analyze the key challenges (technical, implementation, organizational) affecting the deployment of AI-driven behavioral analytics in financial cybersecurity systems.
- To compare the performance and adaptability of behavioral analytics systems across different threat scenarios and financial systems.
- To suggest evidence-based recommendations for improving the effectiveness of adaptive behavioral analytics and identify future research directions in AI-driven financial cybersecurity.

➢ *Evolution of Behavioral Analytics in Cybersecurity*

Behavioral analytics in cybersecurity has evolved from rule-based systems to AI-powered techniques. Traditional approaches like signature-based and rule-based systems are limited when it comes to handling sophisticated intrusions (Chen et al., 2024). ML and AI technologies have enhanced threat efficiency, accuracy, and automation (Sarker et al., 2021). For instance, ML thrives in classifying known attacks while deep learning proves effective for the identification of complex patterns like APTs and DDoS (Marison et al., 2025). Likewise, AI-driven systems provide an improved ability to detect anomalies including adaptability and minimal false positives versus conventional approaches. Typically, over the years, AI development in cybersecurity has also shifted from symbolic artificial intelligence to rule-based systems to connectionist frameworks and advanced deep learning networks (Ambani & Rathod, 2025).

This evolution, however, emphasizes the integration of ML and anomaly detection methods. According to Katurde et al. (2024), behavior-based anomaly detection systems (BBADS) exploit advanced behavioral analysis and AI techniques to defend against emerging threats. This is based on network traffic flow data which is combined with ML algorithms such as Random Forest, promising immense benefits in anomaly detection with high accuracy. Likewise, theoretical foundations such as ML algorithms and statistical models guide the design of anomaly detection systems (Rekha et al., 2024). Alasa (2020) wrote that integrating ML models, real-time monitoring, behavioral analytics, and anomaly detection creates a comprehensive framework to address complex threats in dynamic cyber environments.

Integrating behavioral analytics in cybersecurity with financial system architecture is, therefore, critical in addressing emerging cyber threats. AI-driven fraud detection systems are improving financial security using behavioral analytics and advanced pattern recognition (Chilakapati, 2025). In modern enterprises, user behavior analytics (UBA) combined with secure access service edge (SASE) architectures facilitate insider threat detection (Namboodiri, 2024). Also, financial institutions are leveraging data analytics and AI to mitigate cybersecurity risks to enhance their intrusion detection ability and real-time response to threats (Nwafor et al., 2024). Altogether, these advancements provide a multi-dimensional security approach that combines AI-driven insights and human expertise to create resilient defenses against cyber threats in the financial sector (Malatji & Tolah, 2025).

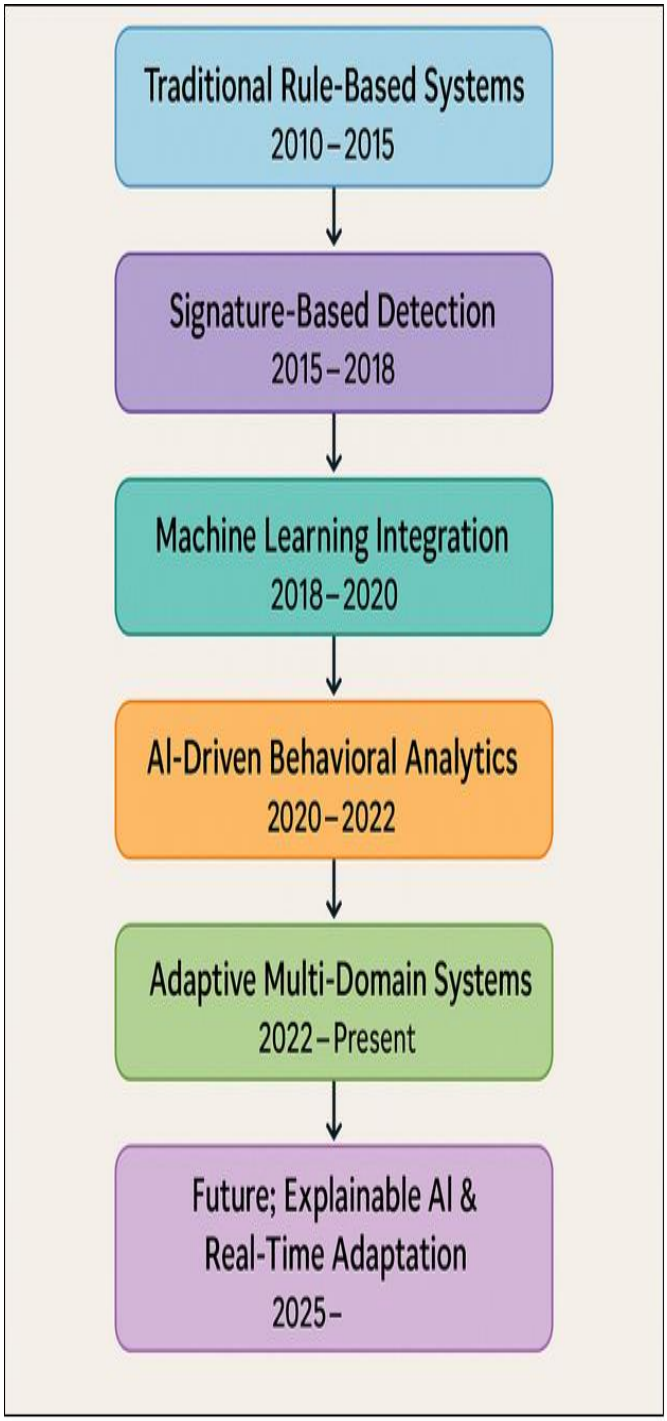

Fig 1 Evolution of Behavioral Analytics in Financial Cybersecurity

➢ *AI-Driven Intrusion Prevention Systems*

Machine learning (ML) algorithms are being adopted as intrusion prevention systems (IPS) to improve cybersecurity. The AI-powered approaches can analyze large data volumes to identify patterns indicating malicious behavior (Bonagiri et al., 2025). Different ML techniques like supervised, unsupervised, and semi-supervised learning are used in IPS including notable algorithms like random forests, support vector machines, and decision trees (Alloghani et al., 2020). Typically, the integration of ML in IPS addresses issues like limited resources, real-time detection in IoT landscapes, and heterogeneity.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

Likewise, it involves the use of pattern recognition algorithms and computational intelligence to handle large datasets and detect intrusions (Das & Nene, 2017). In recent studies, authors have demonstrated that ML-based classification models are effective for highly accurate intrusion detection (Hejleh et al., 2025).

Further, deep learning (DL) has transformed intrusion detection systems (IDS) by improving threat detection and response potential in cybersecurity (Chukwunweike & Shittu, 2024). Many DL architectures like recurrent neural networks (RNNs), convolutional neural networks (CNNs), generative adversarial networks (GANs), and long short-term memory (LSTM) networks have been adopted for analyzing network traffic data and detecting anomalies (Wang et al., 2024). The models particularly excel in identifying patterns while learning from multiple sources to ensure accurate malware detection, insider threats, and phishing attempts (Chukwunweike & Shittu, 2024). Apart from simplifying engineering, the network also maintains performance versus traditional methods such as Random Forest (Getman et al., 2023). Intelligent IDS are developed to capture known attack signatures and unusual behaviors to aim for lower false positives, higher detection rates, and improved resilience (Wasnik & Chavhan, 2023).

Additionally, adaptive and continuous learning mechanisms are developed for real-time data analysis and decision-making. ADAM & RAL stream-based techniques were developed to detect network attacks adapting to concept drifts and minimizing the need for labeled data (Wassermann et al., 2021). A big data platform was also proposed for adaptive learning in network security to achieve quicker computations (Mulinka et al., 2019) while a dynamic learning-driven software landscape for healthcare was presented, using real-time data and machine learning for resource optimization and personalized care (Jacinth et al., 2025). Finally, for reinforcement learning, the use of the Real-Time Actor-Critic (RTAC) algorithm outperformed existing methods in different settings by addressing the limitations of real-world applications of classical Markov Decision Processes (Ramstedt & Pal, 2019). These advancements indicate the ability of real-time adaptive mechanisms and continuous learning frameworks in different domains.

II. CASE STUDY ANALYSIS

- *Case Study 1: Major Cryptocurrency Exchange Breach*

In 2023, the crypto landscape experienced an exchange security incident, exemplifying the sophisticated characteristics of modern cyber threats on digital currency platforms (Mallick & Nath, 2024). The attack emanated through a multiple vector approach which combined supply chain compromise, social engineering, and advanced persistent threat (APT) techniques (Cortes, 2022). Vulnerabilities were identified in the third-party API integrations exchange versus customer service protocols through initial reconnaissance. Also, attackers took advantage of compromised credentials of employees derived from spear-phishing campaigns to establish persistent access to internal systems over many weeks before the primary breach was executed.

The behavioral analytics system of the exchange adopted machine learning (ML) algorithms to monitor patterns of transactions, network traffic anomalies, and user authentication behaviors (Kumari, 2025). However, gaps emerged in the ability to correlate behavioral indicators across platforms. The AI-powered monitoring failed to detect deviations in patterns of administrative access, especially during off-peak hours when legal administrative activities were limited (Al Falasi, 2024). In addition, the threshold settings of the system for detecting anomalies were calibrated to suit variance in normal operations, which misses the progressive escalation of suspicious activities characterizing the attack.

Once detected, the AI system showed strengths and limitations in its adaptive response capabilities as the system successfully spotted unusual transaction volumes and implemented automated protocols to freeze accounts within less than 1 hour of detecting the initial breach. However, the adaptation techniques struggled with the use of legitimate administrative protocols and tools used by the attackers which created false negatives, delaying comprehensive threat isolation. Similarly, the machine learning model of the system required 72 hours to recalibrate and establish new patterns after the incident.

The lessons learned from this include: the post-incident analysis showing the need for enhanced behavioral correlation across domains and enhanced threshold adaptability. Multi-layered behavioral analytics were implemented by the exchange, incorporating user entity behavior analytics (UEBA) alongside network traffic analysis with minimal false positive rates (Brandao, 2025). In addition, system improvements comprised real-time model updating capabilities with improved integration and threat intelligence feeds to enhance and ensure proactive threat detection and response techniques.

- *Case Study 2: Banking Institution's Advanced Persistent Threat*

This involved the use of a sophisticated attach approach. A major international banking institution suffered a sophisticated APT campaign featuring living-off-the-land techniques and extensive evasion mechanisms (Alshamrani et al., 2019). Here, the attackers used fileless malware and system administration to ensure persistence and avoid signature-based detection systems. The attack methodology comprised lateral movement in privileged accounts, exploiting Active Directory vulnerabilities, and exfiltration timing of strategic data to coincide with business operations. The threat agents showed deep knowledge of the internal processes and security protocols of the institution.

The behavioral analytics system of the banking institution faced significant challenges in differentiating malicious activities from administrative functions. The detection mechanisms powered by AI initially categorized the activities of the attackers as normal administration

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

because they mimicked the behaviors of authorized personnel and used standard banking protocols (Ajayi et al., 2024). Complex challenging areas include the identification of subtle deviations in access patterns in the database, recognizing unauthorized access escalation attempts, and detecting behaviors regarding data aggregation which are consistent with routine reporting activities. The baseline model of the system, however, required training to accommodate the attack signatures.

Considering AI-driven detection and response period, detection took place 19 days after the first compromise when the AI system identified some patterns in the database query frequencies and timing of access. The behavioral analytics engine triggered automated alerts while detecting unusual impacts of data access patterns and user privileges. Response automation included enforcement of network segmentation, forensic data collection, and immediate account isolation. However, the response timeline of the AI system was complicated due to requirements of manual validation of alerts to prevent operations disruption which extends the response time to 6 days.

The institution implemented countermeasures like improved behavioral baseline modeling, improved access management, and integration of deception technology and existing AI systems (Raghavendra, 2023). Real-time user behavior analytics, enhanced correlation between network behavioral analytics and endpoint detection, and automated incident response deployment characterized technical improvements while organizational changes were the establishment of dedicated threat-hunting teams with AI detection systems and improved training on security awareness.

- *Case Study 3: DeFi Platform Security Incident*

This case study describes unique challenges in decentralized finance ecosystems. The decentralized finance (DeFi) platform security incident showed distinctive challenges in monitoring financial systems (Parisi & Budorin, 2024). Compared to traditional centralized exchanges, DeFi platforms operate across several blockchain networks with different consensus techniques and security protocols (Xiao et al., 2020). The incident comprised exploitation of bridge vulnerabilities across chains and attacks on flash loans, which creates complex behavioral patterns that are difficult to detect by traditional centralized monitoring systems. The decentralized nature of the platform implied that behavioral analytics systems are required to process data from various blockchain sources concurrently while maintaining detection capabilities.

The behavioral analytics system of the platform faced some challenges in monitoring interactions of smart contracts and spotting malicious patterns in automated market maker (AMM) protocols (Zhu et al., 2024). Certain AI system is required to distinguish between manipulative behaviors tailored to exploit smart contract vulnerabilities and legitimate arbitrage activities. Due to this, behavioral monitoring became more complex as per the composability features of the platform, where users could simultaneously interact with several protocols, creating intricate transaction patterns that challenged the algorithms for detecting anomalies (Wang & Yu, 2025). Besides, the machine learning models of the system required extensive DeFi-based training for behavioral patterns to achieve accuracy levels accepted by the system.

The detection system showed mixed performance when novel DeFi attack vectors were introduced to confront it. Although the system successfully identified unusual volumes of transactions and patterns of timing, it was not effective for sophisticated attacks leveraging legitimate DeFi mechanisms for malicious reasons. The behavioral analytics engine needed 156 hours to adapt to new signatures after the incident, which implied the common challenges of real-time adaptation in rapidly evolving DeFi ecosystems.

Improvements after the incident include part of the development of DeFi-specific behavioral models, integration with several blockchain analytics platforms, and implementation of smart contract monitoring capabilities in the real world (Sah et al., 2024). The platform initialized the use of graph neural networks for analysis of complex DeFi transaction relationships while developing adaptive threshold techniques accounting for high volatility in DeFi markets

Table 1 Comparative Case Study Analysis Table

Aspect/Category	Cryptocurrency Exchange	Banking Institution	DeFi Platform
Detection Time	47 minutes	19 days	156 hours
Attack Vector	Multi-vector APT	Living-off-the-land	Cross-chain exploitation
AI Response	Automated freezing	Manual validation requirement	Mixed performance
Primary Challenge	Cross-platform correlation	Mimicking legitimate tool	Novel DeFi mechanisms
Adaptation Period	72 hours	6 days	156 hours
Estimated Loss Prevented	$50M	$127M	Not applicable

III. COMPARATIVE ANALYSIS AND DISCUSSION

- *Cross-Case Pattern Identification*

The analysis of the case studies shows consistent behavioral indicators beyond platform-based architectures. The incidents demonstrated the characteristics of initial reconnaissance by probing authentication techniques and progressive escalation of access opportunities. Common patterns like temporal patterns of access, especially during off-peak hours, and exploration of system boundaries using legitimate functionality. The analysis also identified the consistent exploitation of attackers on the gap between anomaly detection and normal operational variance, which suggests that existing behavioral analytics systems may not be sufficiently calibrated to identify and spot sophisticated threat agents (actors).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

AI-driven behavioral analytics systems showed considerable strengths in spotting voluminous anomalies and deviations from user behavior patterns. Recurring weaknesses also emerged in the handling of sophisticated attacks leveraging system functionality (Malik, 2024). The three systems in all cases struggled with managing false positives, which required significant manual intervention that delayed response times. In addition, the systems demonstrated limited effectiveness in the correlation of behavioral indicators via many security domains which suggests the need for higher integrated analytical techniques.

Environmental factors influenced the performance of the AI system in all three case studies. Data processing delays and network latency impacted detection capabilities, especially in the DeFi platform where confirmation times in blockchain affected the recognition of behavioral patterns (Hassan, Rehmani, & Chen, 2022). In addition, organizational factors like incident response protocols and security team expertise had a direct influence on the effectiveness of AI-driven recommendations while system performance was impacted by the extent of complexity of the financial ecosystem, as more complex environments required longer adaptation timelines for behavioral analytics systems (Tanikonda et al., 2022).

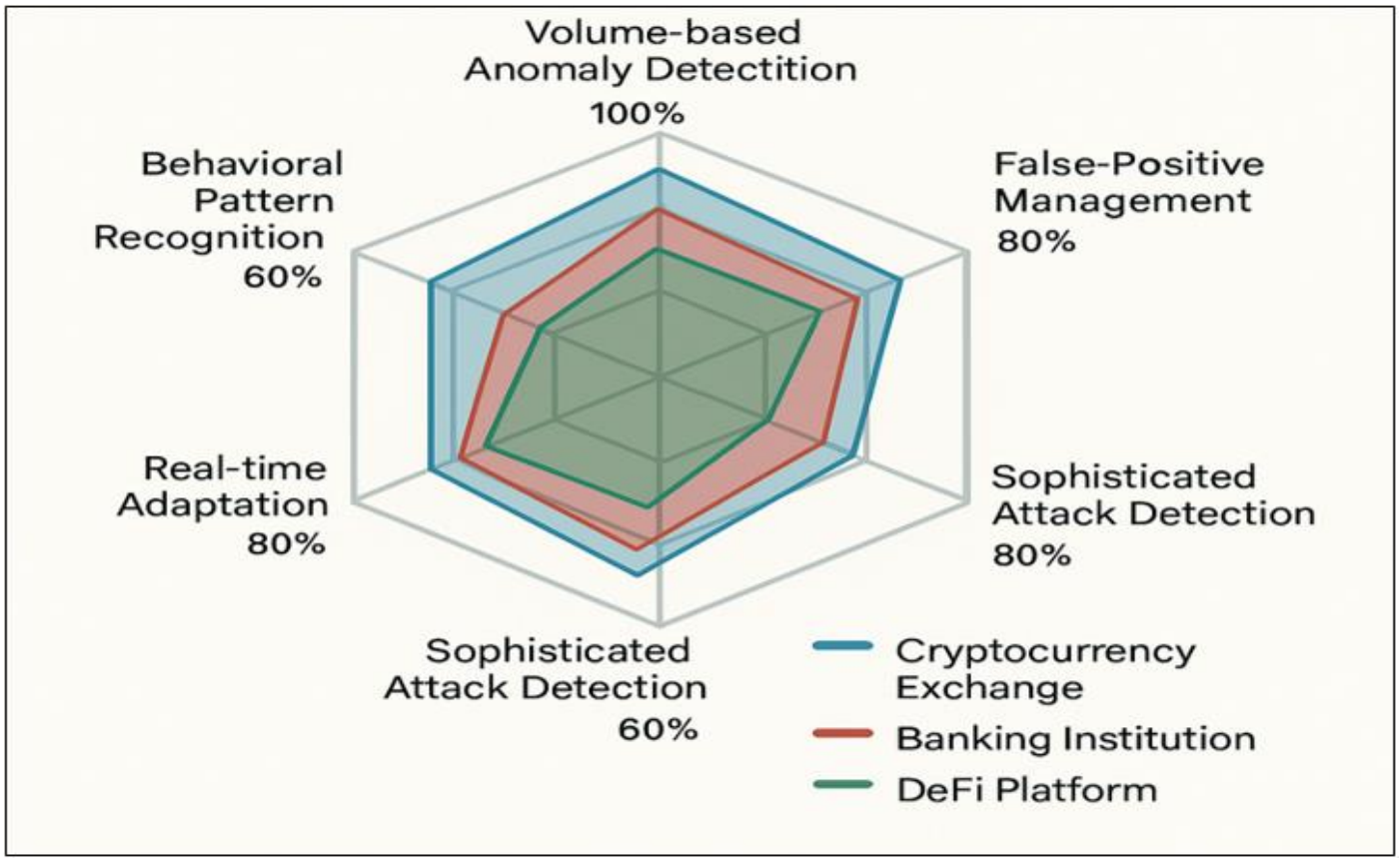

Fig 2 AI System performance in different threat scenarios

➢ *Technological and Operational Implications*

From the case studies, significant challenges exist in integrating behavioral analytics and legacy financial systems. For example, traditional banking infrastructure resisted real-time behavioral monitoring because of performance-related issues and regulatory compliance requirements (Chatterjee & Das, 2024). Integration complexity improved with diversified data sources alongside the need to ensure operational continuity while upgrading systems. The DeFi platform case, however, showed extra challenges regarding the integration of behavioral analytics using blockchain-based systems while managing the overhead of smart contract monitoring.

Moreover, scalability emerged as a major factor impacting the performance of AI systems across different platforms. In the cryptocurrency exchange incident, behavioral analytics systems must be capable of handling large volumes of transactions while maintaining response times in the sub-second (Deepa et al., 2022). In the DeFi environment, processing scalability issues were more prevalent as the system needed to analyze multiple protocol interactions. Overall, the cases indicated that significant computational resources are required for current behavioral analytics systems, which raises concerns about the environmental impact and cost-effectiveness.

Moreover, sophisticated human-AI collaboration frameworks are required for effective threat response in all cases. In the situation at the banking institution, the importance of human validation in the prevention of false positive disruptions was demonstrated while the DeFi platform incident showed the essence of specialized expertise to interpret AI-induced alerts. Meanwhile, success factors exist such as automated evidence collection, clear escalation

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

protocols, and AI-driven recommendations supporting human decision-making.

Overall, the economic analysis depicts that advanced behavioral analytics generate significant value despite the high costs of implementation. For instance, the cryptocurrency exchange case showed potential loss mitigation to the tune of $50 million and the banking institution prevented damages that would have cost $127 million. Nevertheless, operational costs like system maintenance, specialized personnel requirements, and false positive management must be balanced versus security benefits.

IV. RECOMMENDATIONS AND FUTURE DIRECTIONS

- *Technical Recommendations*

Future behavioral analytics systems should focus on developing threshold mechanisms that can adjust to emerging patterns of threat while minimizing false positives. Essentially, the focus should be on the development of hybrid machine learning (ML) models that can integrate supervised learning (for known and identifiable threats) with unsupervised approaches (for new attacks detected). Similarly, graph neural networks that can analyze complex relationship patterns in cryptocurrency platforms and DeFi should be prioritized while algorithm development should emphasize explainable AI techniques offering security teams with clear reasoning behind decision-making regarding threat detection (Rojas-Mayorquin, 2024; Mondol, 2024).

On data integration and improving preprocessing, relevant frameworks should be designed to correlate behavioral indicators in several security domains like user authentication, network traffic, and transaction patterns. Improvements in preprocessing should focus on data normalization techniques capable of handling diverse data sources and maintaining processing speed (G Martin et al., 2021). Edge computing capabilities investment for distributed behavioral analytics processing will be critical for platforms across several blockchain networks or geographic regions (Yang et al., 2019).

In addition, continuous learning systems with the capacity to adapt to new threat signatures must be developed, especially those that do not require retraining the model completely (Arnaldo et al., 2018). The systems should incorporate feedback loops allowing rapid integration of updates regarding threat intelligence while also maintaining performance during adaptation timelines.

- *Strategic and Policy Implications*

Considering regulatory compliance, financial institutions should advocate for frameworks that accommodate the advanced behavioral analytics requirements while maintaining compliance standards and privacy. Likewise, it is expedient that regulatory bodies develop guidelines for AI-driven threat detection systems that integrate and balance effective security with requirements of due process, while cross-border data sharing protocols for behavioral analytics should be developed to enhance the system's threat detection capabilities while respecting privacy laws within the jurisdiction (Rangaraju, 2023; Mbah, 2024).

Moreover, establishing industry-wide behavioral analytics threat intelligence sharing platforms would have a significant impact on improving collective defense capabilities. Therefore, financial institutions should collectively develop standardized behavioral analytics indicators while establishing shared threat signature databases (Ekundayo et al., 2024). In the same vein, public-private partnerships should be developed to fund research on advanced behavioral analytics technologies and create testing ecosystems for new detection algorithms (Rathje & Katila, 2021).

Finally, investment priorities should shift and focus on the development of internal expertise in AI-driven cybersecurity, creating innovation labs to test emerging technologies, and establishing dedicated behavioral analytics teams. Scalable cloud infrastructure that can support real-time behavior analytics processing should be invested in while institutions should prioritize integration capabilities allowing for seamless and viable incorporation of new and emerging security technologies (Vashishth et al., 2024).

V. CONCLUSION

The study offers comprehensive insights into the present and future possibilities of incorporating adaptive behavioral analytics within AI-enhanced financial cybersecurity frameworks. The case study analysis shows that although the behavioral analytics system has an impressive capability to identify traditional anomalies, it still has a critical weakness in identifying sophisticated attacks that utilize legitimate system features. Key findings indicate that the system needs to have better ways of correlating information across different domains, use more advanced methods for setting thresholds, and work well with human analysts to detect threats. This study significantly adds to the existing body of knowledge by identifying common behavioral patterns across various financial platforms and establishing the economic benefits of implementing advanced behavioral analytics, with an estimated loss prevention exceeding $177 million in the studied cases.

However, research limitations include the retrospective nature of case study analysis and the rapidly evolving threat landscape that may affect the long-term applicability of findings. The current methods demand substantial computing power and expert knowledge which is a huge limitation in terms of broader implementation and economic viability. We must pursue ongoing research to refine the real-time adaptation capabilities and advance the methodologies for explainable AI while also pushing for collaborative frameworks on threat intelligence in the industry. Ongoing research into hybrid machine learning models and graph neural networks for interpreting intricate financial interactions is crucial for further enhancing behavioral analytics within the cybersecurity realm

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

REFERENCES

[1]. Aghazadeh Ardebili, A., Hasidi, O., Bendaouia, A., Khalil, A., Khalil, S., Luceri, D., ... & Ficarella, A. (2024). Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review. Energy Informatics, 7(1), 96.

[2]. Agrawal, A. (2020). Approaches for Detecting Anomaly in Real-Time Network.

[3]. Alhashmi, A.A., Alashjaee, A.M., Darem, A.A., Alanazi, A.F., & Effghi, R. (2023). An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures. Engineering, Technology & Applied Science Research, 13(6), 12433-12439.

[4]. Al-Jeshi, S., Tarfa, A., Al-Aswad, H., Elmedany, W., & Balakrishna, C. (2022). A Blockchain-Enabled System for Enhancing Fintech Industry of the Core Banking Systems. 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 209-213.

[5]. Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of Cybersecurity Risks and Threats on Banking and Financial Services. Journal of Internet Services and Information Security, 14(3), 167-190.

[6]. Almazroi, A.A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. IEEE Access, 11, 137188-137203.

[7]. Basheer, M.Y.I., Ali, A.M., Osman, R., Abdul Hamid, N.H., Nordin, S., Ariffin, M.A.M., & Martinez, J.A.I. (2024). Empowering Anomaly Detection Algorithm: A Review. IAES International Journal of Artificial Intelligence (IJ-AI), 13(1), 9–22.

[8]. Bhomia, Y., Sahu, S., & Singh, S.P. (2019). Machine Learning for Anomaly Detection Approaches, Challenges, and Applications. The Pharma Innovation Journal, 8(3), 24–27.

[9]. Botha, R. (2019). The Potential Anti-Money Laundering and Counter-Terrorism Financing Risks and Implications of Virtual Currencies on the Prevailing South African Regulatory and Supervisory Regime (Master's thesis, University of Pretoria, South Africa).

[10]. Bozzetto, C. (2023). Cryptocurrency markets microstructure, with a machine learning application to the Binance bitcoin market.

[11]. Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.

[12]. Chatterjee, P., & Das, A. (2024). AI-Powered Anomaly Detection for Real-Time Performance Monitoring in Cloud Systems. International Journal of Scientific Research in Science and Technology.

[13]. Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity Governance and Digital Finance: Evidence from Sovereign States. Finance Research Letters.

[14]. Chen, J., & Ran, X. (2019). Deep learning with edge computing: A review. Proceedings of the IEEE, 107(8), 1655-1674.

[15]. Devineni, S.K., Kathiriya, S., & Shende, A. (2023). Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity. Journal of Artificial Intelligence & Cloud Computing, 2(2), 1–9.

[16]. Domlur Seetharama, Y. (2021). Anomaly Detection: Enhancing Systems with Machine Learning. International Journal of Science and Research (IJSR).

[17]. Donald, O., Ajala, O.A., Okoye, C.C., Ofodile, O.C., Arinze, C.A., & Daraojimba, O.D. (2024). Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time. Magna Scientia Advanced Research and Reviews.

[18]. Elluri, L., Nagar, A., & Joshi, K. P. (2018, December). An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 1266-1271). IEEE.

[19]. Erondu, C. I., & Erondu, U. I. (2023). The Role of Cyber Security in a Digitalizing Economy: A Development Perspective. International Journal of Research and Innovation in Social Science, 7(11), 1558-1570.

[20]. Falade, P.V. (2023). Decoding the threat landscape: Chatgpt, fraudgpt, and Wormgpt in social engineering attacks. arXiv preprint arXiv:2310.05595.

[21]. Fendt, M., Parsons, M.H., Apfelbach, R., Carthey, A.J., Dickman, C.R., Endres, T., ... & Blumstein, D.T. (2020). Context and trade-offs characterize real-world threat detection systems: a review and comprehensive framework to improve research practice and resolve the translational crisis. Neuroscience & Biobehavioral Reviews, 115, 25–33.

[22]. Galavis, J. (2018). Blame it on the blockchain: cryptocurrencies boom amidst global regulations. U. Miami Int'l & Comp. L. Rev., 26, 561.

[23]. Gandhi, H., Tandon, K., Gite, S., Pradhan, B., & Alamri, A. (2024). Navigating the complexity of money laundering: anti-money laundering advancements with AI/ML insights. International Journal on Smart Sensing and Intelligent Systems.

[24]. Gracy, M., Jeyavadhanam, B.R., Babu, P.K., Karthick, S., & Chandru, R. (2023). Growing Threats Of Cyber Security: Protecting Yourself In A Digital World. 2023 International Conference on Networking and Communications (ICNWC), 1–5.

[25]. Gray, G.L. (2024). An Exploration of the Money Laundering Associated with the Bitfinex Bitcoin Hack. Journal of Emerging Technologies in Accounting.

[26]. Harris, L. (2024). The Role of Artificial Intelligence in Advancing Blockchain Technology.

[27]. Immadisetty, A. (2024). Machine Learning for Real-Time Anomaly Detection. International Journal For Multidisciplinary Research.

[28]. Ivleva, E.S., Makarov, M.Y., & Bobrov, A.G. (2024). Development of the circulation of digital financial assets in the world in the context of digital transformation. Economics and Management.

[29]. Jankov, D., Sikdar, S., Mukherjee, R., Teymourian, K., & Jermaine, C. (2017, June). Real-time high-performance anomaly detection over data streams:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25jul835

Grand challenge. In Proceedings of the 11th ACM International Conference on distributed and event-based systems (pp. 292–297).

[30]. Jidiga, G.R., & Sammulal, P. (2014). Anomaly detection using machine learning with a case study. 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 1060–1065.

[31]. Kumar, R., Swarnkar, M., Singal, G., & Kumar, N. (2021). IoT network traffic classification using machine learning algorithms: An experimental analysis. IEEE Internet of Things Journal, 9(2), 989-1008.

[32]. Kumar, S., Datta, S., Singh, V., Datta, D., Singh, S.K., & Sharma, R. (2024). Applications, challenges, and future directions of human-in-the-loop learning. IEEE Access.

[33]. Kummari, D.N. (2020). Machine Learning Applications in Regulatory Compliance Monitoring for Industrial Operations. Global Research Development (GRD), 5(12), 75–95.

[34]. Lenart, K. (2024). Comparison of Machine Learning and Statistical Approaches of Detecting Anomalies Using a Simulation Study. Econometrics.

[35]. Mestre, A. (2024, May). Towards a Hybrid Intelligence Paradigm: Systematic Integration of Human and Artificial Capabilities. In International Conference on Research Challenges in Information Science (pp. 149–156). Cham: Springer Nature Switzerland.

[36]. Naha, R.T., & Zhang, K. (2024, December). Cryptocurrencies Forensics With Real-Time Intelligence and Graph Database: A Comprehensive Review. In 2024 IEEE International Conference on Big Data (BigData) (pp. 1–12). IEEE.

[37]. Olaniyi, O.O., Omogoroye, O.O., Olaniyi, F.G., Alao, A.I., & Oladoyinbo, T.O. (2024). CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. Journal of Engineering Research and Reports, 26(6), 31–49.

[38]. Palaiokrassas, G., Scherrer, S., Ofeidis, I., & Tassiulas, L. (2023). Leveraging Machine Learning For Multichain DeFi Fraud Detection. 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 678–680.

[39]. Pham, T., & Lee, S. (2016). Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods. arXiv:1611.03941.

[40]. Raj, A., & Sharma, S. (2024). A Comprehensive Study on Anomaly Detection Methods Using Traditional and Machine Learning Approaches. International Journal of High School Research.

[41]. Sabidi, M.L., & Zolkipli, M.F. (2024). The Role of Risk Management in Cybersecurity Protocols. Borneo International Journal, 7(2), 77–81.

[42]. Song, A., Seo, E., & Kim, H. (2023). Anomaly VAE-Transformer: A Deep Learning Approach for Anomaly Detection in Decentralized Finance. IEEE Access, 11, 98115–98131.

[43]. Vassilev, V., Donchev, D., & Tonchev, D. (2021). Impact of false positives and false negatives on security risks in transactions under threat.

[44]. Xu, B., Wang, Y., Liao, X., & Wang, K. (2023). Efficient fraud detection using deep boosting decision trees. Decision Support Systems, 175, 114037.

[45]. Xu, T. (2024). Leveraging Blockchain Empowered Machine Learning Architectures for Advanced Financial Risk Mitigation and Anomaly Detection.

[46]. Youvan, D.C. (2024). Anatomy of a Financial Collapse: The Role of Technical Glitches in Modern Financial Systems.