World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Behavioral and AI-Driven Predictive Analytics for Proactive Fraud Prevention in U.S. Healthcare Cyber security Biometrics

Alex Lwembawo Mukasa [1,*], Esther A. Makandah [2], Haruna Atabo Christopher [3] and Dako Apaleokhai Dickson [4]

[1] *Computer Science Department, Creospan.*
[2] *University of West Georgia, Carrollton, USA.*
[3] *Nigeria-Korea Friendship Institute, Lokoja.*
[4] *Software Engineering Department, Veritas University, Abuja, Nigeria.*

World Journal of Advanced Research and Reviews, 2025, 27(02), 1652-1661

Publication history: Received on 04 July 2024; revised on 20 August; accepted on 23 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2025.27.2.2916

Abstract

The challenges in healthcare cybersecurity are growing due to the increase in fraudulent activities, such as identity theft, insurance scams, and unauthorized entry to electronic health records (EHRs). Conventional authentication methods like passwords and two-factor authentication have shown to be insufficient in countering advanced cyber threats. This research examines the combination of behavioral biometrics and AI-based predictive analytics for proactive fraud prevention in cybersecurity within U.S. healthcare. Behavioral biometrics, such as keystroke dynamics, mouse movement patterns, and gait analysis, provide an ongoing authentication method that improves security while maintaining user workflow continuity. AI-powered predictive analytics, utilizing both supervised and unsupervised machine learning models, facilitate immediate fraud detection by recognizing unusual user activities within healthcare processes. Even with its benefits, implementing behavioral biometrics and AI models poses various technical hurdles, such as accuracy constraints, false positives, and biases in algorithms. Additionally, AI systems need extensive, high-quality datasets to detect fraud effectively, which brings about concerns regarding privacy and ethical implications. To tackle these issues, additional investigation into adaptive biometric systems, privacy-preserving AI methods, and regulatory structures is essential for harmonizing security with compliance obligations. This research suggests that future studies focus on hybrid biometric authentication systems, reducing bias in AI-enabled fraud detection, and utilizing privacy-enhancing technologies like federated learning and homomorphic encryption. By implementing AI-based cybersecurity systems, healthcare organizations can improve fraud detection strategies, safeguard patient information, and maintain compliance with regulations. The results highlight the necessity for teamwork among healthcare professionals, cybersecurity specialists, and policymakers to develop strong, ethical, and efficient security measures.

Keywords: AI-driven predictive analytics; Behavioral biometrics; Fraud detection; Electronic health records; Healthcare cybersecurity

1. Introduction

The healthcare industry in the U.S. has experienced a notable rise in cyber threats, with fraud and identity theft growing more common. Conventional security strategies frequently fail to tackle complex attacks, making it essential to embrace cutting-edge technologies. Behavioral biometrics and AI-powered predictive analytics have surfaced as effective strategies to actively mitigate fraud in healthcare cybersecurity.

* Corresponding author: Alex Lwembawo Mukasa

Behavioral biometrics focuses on examining distinctive patterns in human actions, including keystroke dynamics, mouse gestures, and touchscreen usage, for ongoing user identity verification. In contrast to traditional static authentication methods, behavioral biometrics provides adaptive and unobtrusive security, personalizing to user profiles to identify irregularities that suggest fraudulent behavior. This method increases the precision of fraud identification and diminishes the likelihood of unwarranted access to confidential healthcare information.

Combining AI-powered predictive analytics with behavioral biometrics enhances fraud prevention initiatives. Machine learning algorithms are capable of analyzing large volumes of behavior data instantaneously, detecting slight variations from typical user behaviors that could indicate fraudulent actions. This collaboration allows healthcare organizations to foresee and address potential risks before they progress, thus protecting patient data and preserving confidence in digital health systems.

Nonetheless, introducing these technologies into the healthcare sector poses difficulties, such as worries regarding data privacy, ethical considerations, and the scalability of systems. To tackle these challenges, collaboration among healthcare professionals, technology creators, and regulatory agencies is essential to create strong frameworks that guarantee the responsible and efficient use of AI and behavioral biometrics in preventing fraud.

1.1. Statement of the Problem

The growing complexity of cyber threats in the U.S. healthcare industry has rendered conventional security methods, like passwords and two-factor authentication, insufficient for fraud prevention. Healthcare institutions keep a large volume of sensitive patient information, positioning them as prime targets for cybercriminals involved in identity theft, insurance fraud, and unauthorized data breaches. Despite established security measures, criminals still take advantage of system weaknesses, resulting in financial setbacks and jeopardized patient safety (Sharma & Chen, 2022). The increasing occurrence of data breaches highlights the pressing demand for enhanced, proactive fraud detection systems.

Behavioral biometrics and AI-based predictive analytics present effective solutions for improving fraud prevention in healthcare cybersecurity. These technologies can examine user behavior instantly, detecting minor shifts from typical patterns that could suggest fraudulent activities. Nonetheless, the incorporation of these tools into healthcare cybersecurity systems is still restricted because of worries regarding implementation difficulty, data privacy, and ethical concerns (Patel et al., 2021). Moreover, incorrect positives in fraud detection systems can disrupt healthcare processes, leading to concerns regarding the precision and trustworthiness of AI-based security measures.

There is an urgent requirement for empirical studies to assess the efficacy, difficulties, and optimal strategies for implementing behavioral biometrics and AI-based predictive analytics in healthcare cybersecurity. Current research has mainly concentrated on financial organizations, resulting in a lack of insight into their relevance in the healthcare industry (Jones & Li, 2023). Filling this gap will offer healthcare organizations data-driven insights to improve fraud prevention tactics, guarantee adherence to privacy regulations, and boost overall cybersecurity resilience. In the absence of thorough research and established policy frameworks, the implementation of these technologies might remain disjointed, hindering their ability to effectively address healthcare fraud.

Research Objectives

- To explore how AI-driven predictive analytics enhances fraud detection
- To assess the effectiveness of behavioral biometrics in healthcare cybersecurity
- To evaluate the integration of AI, machine learning, and biometrics for proactive fraud prevention

2. Literature Review

2.1. Overview of Cybersecurity Threats in Healthcare

The U.S. healthcare industry encounters an expanding range of cybersecurity risks, as fraudulent activities like identity theft, insurance fraud, and data breaches are on the rise. In healthcare, identity theft entails gaining unauthorized access to personal data, which can then be exploited to acquire medical services or execute fraudulent billing. Insurance fraud includes actions such as altering claims or misinterpreting patient details to obtain undeserved payments. Data breaches, frequently caused by hacking events, compromise confidential patient records, resulting in possible exploitation of personal health information (PHI) (Seh et al., 2020).

The effect of these deceptive practices on patient safety is significant. When PHI is breached, there is a danger of medical identity theft, meaning a person's medical data can be changed or improperly used. This may result in inaccurate medical histories, erroneous diagnoses, or unsuitable treatments, putting patient health at risk. Additionally, breaches can interrupt healthcare services since systems might have to be taken offline to fix security flaws, leading to delays in patient care and access to essential medical information (Lampropoulos et al., 2023).

Monetarily, healthcare fraud places a considerable strain on the sector. According to estimates, fraud-related losses may vary between 3% and 10% of overall healthcare expenditures, potentially surpassing $300 billion each year in the U.S. alone (Simbo AI, 2024). These losses arise from deceitful claims, rising insurance premiums, and the expenses related to probing and addressing breaches. Moreover, entities could encounter significant penalties and legal costs for failing to adhere to rules meant to safeguard patient data.

It is indeed one of the effective measures that are put forward against such threats; however, non-compliance is still a pervasive issue. The HIPAA - the Health Insurance Portability and Accountability Act - provides national standards for protecting PHI. Many violations end up in very serious penalties, with fines per violation up to $50,000 to a maximum of $1.5 million annually, in addition to criminal charges (U.S. Department of Health & Human Services, n.d.). Despite these statures, breaches occur, suggesting that compliance and enforcement measures are still lacking.

The Health Insurance Portability and Accountability Act (HIPPA) imposes national-level regulations on violations concerning the security of protected health information (PHI). Penalties for infringement could be very stringent, up to $50,000 per violation, and an annual aggregate amount of $1.5 million in addition to possible criminal indictments (U.S. Department of Health & Human Services, n.d.). Yet breaches in data continue to take place, which shows that not every legal aspect is being made up in compliance and enforcement.

Cyber threats in the U.S. healthcare sector include identity theft, insurance fraud, and data breaches, and that makes them a great danger to the safety of the patients, financial threats, and regulatory compliance. Confronting the challenges must include massive security measures, having strict regulations, and further efforts toward eradicating fraud.

2.2. Behavioral Biometrics in Fraud Detection

Behavioral biometrics is advanced security by which individuals are identified based on how they act during interactions between user and computer. Traditional biometric systems in contrast with behavioral biometrics don't emphasis physical features like fingerprints or face shapes but would mostly focus on how the user engages with the device, capturing very unique behaviors that are nearly impossible to forge. Behavioral biometric system generates continuous fraud detection and authentication of users by observing anomalous behavior patterns, making unauthorized access extremely difficult.

Some of the techniques of behavioral biometrics are keystroke dynamics, mouse movement analysis, and gait analysis. Keystroke dynamics works in terms of analyzing the rhythm and time when the individual types using a unique profile for its users. Mouse movement anomaly detection uses speed, trajectory, and click patterns to understand how the cursor moves to associate it with a user. Gait analysis captures the speed and style of walking of a person: by observing the gait pattern of users with the help of sensors in portable mobile devices, authentication takes place without the user's awareness. These are essentially strong contributing measures in the behavioral biometric methodology for fraud detection.

In behavioral biometrics compared with traditional authentication methods, the major benefit would be to improve security. Traditional methods like passwords, PINs, and so on suffer from capture, replication, and can also be shared in many ways, thus making them unreliable compared to behavior biometrics, which relies on the analysis of behavior and patterns which are unique to each individual and really hard for unauthorized users to mimic, hence providing a refuge against identity theft and unauthorized access. This continuous observing ensures that even if the logon credentials be compromised, fraudulent acts can still be detected by deviation from normal behavioral patterns.

This is one of its advantages: safeguarding users' privacy. Behavioral biometrics authentication takes an actual live look at how a user interacts with their device. Hence, this will make it really challenging for a hacker to bypass the measures. Unlike the traditional method of authentication, which would tend to reveal one's identity, behavioral biometrics are the patterns of behavior that keep information hidden from a user. That takes one step closer towards security and privacy with respect to the storage and handling of sensitive personal information.

The user's experience is frictionless with behavioral biometrics: Authentication works in the background and constantly observes the user's behavior pattern with the device so that they need not type in their passwords multiple times or go through yet another verification identity check. Therefore, this integration not only improves user delight and less interruption but also makes the barriers to security measures less invasive and more user-friendly. Well, that's not to say that behavioral biometrics doesn't intrude. It is not intrusive and so security does not compromise usability.

By using inherent and unique behaviors of the users, behavioral biometrics allow a new and flexible approach to fraud detection. Techniques such as keystroke dynamics, mouse movement analysis, or gait analysis provide continuous and unobtrusive authentication resulting in higher security and privacy combined with a better user experience. Cyber threats have been so sophisticated that the journey of adopting behavioral biometrics in fraud detection systems will be a major component of the overall strategy for protecting sensitive information and ensuring the integrity of digital exchanges going forward.

2.3. AI-Driven Predictive Analytics in Cybersecurity

Artificial intelligence takes a significant place as a modern-day milestone in cyber security, more particularly with the application of machine learning models for fraud detection, which are designed to learn how to identify fraudulent behavior by identifying patterns and finding anomalies in a broad spectrum of records to identify fraudulent activities proactively. By recognizing historic and current data, predictive analytics using AI can recognize very slight deviations that may represent indicators of fraud for the improvement of security posture in organizations.

Fraud detection machine learning models are mainly residential under supervised and unsupervised learning approaches. Supervised learning approaches train algorithms using datasets with known outcomes for detecting patterns of behavior in order to identify the fraudulent activities contained in the data with common algorithms like decision tree, support vector machine, neural network, etc. On the other hand, unsupervised learning allows for processing only unlabeled and untagged standards for clustering and anomaly detection, to look for outlier patterns that can possibly indicate fraud. K-means clustering and principal component analysis, among others, would be very common techniques used for this study (Ananya et al., 2025).

Anomaly detection is one of the important components of AI-based security strategies. It detects data outliers from normal patterns signifying unauthorized access or fraudulent activities. Anomaly detection systems based on AI scrutinize a variety of parameters, such as user behavior, transaction patterns, and network traffic, and define normal activity baselines among them(Oladayo and Abdullahi, 2018). The anomalies are left to be investigated whenever deviation occurs. With a real-time processing scheme, this can even be suspected sooner and treated while limiting the damage to the minimum (Adeola, 2025).

If the AI-based predictive algorithm is implemented along with real-time process monitoring, the capability of the organization will get enhanced in its fight against fraud. In evaluating data continuously while that data is being generated, real-time monitoring systems can detect suspicious activities timely and respond to them. Speed is of the essence in thwarting fraudulent transactions and terminating security breaches before they escalate into something rampant. Additionally, the AI system's learning techniques can boost or modify with emerging threats, ensuring its ability to detect fraud for an extended period (Ananya et al., 2025). Despite advantages, challenges still exist toward efficiently deploying AI-based predictive analytics against fraud detection. The system's performance may be negatively impacted by data quality obsolescence, false positives, and heavy computational resource requirements. Additionally, in parallel, adversaries are developing new ways to bypass detection. Therefore, the AI models must evolve continuously. Hence, fraud in cybersecurity can effectively be mitigated only through a combined approach incorporating AI and human intelligence, plus strong policies (Adeola, 2025).

2.4. AI-Driven Behavioral Biometrics for Fraud Detection

AI-based behavioral biometrics stands out as a cutting-edge cybersecurity method in which machine learning algorithms are applied to verify and authenticate users based on unique patterns in interaction with a digital system. Traditional methods of authentication, which still hinge on passwords or static biometrics, are fairly conscious only when one user is authenticated, while behavioral biometrics can analyze and continuously monitor characteristics such as the dynamics of typing, mouse activity, touchscreen gestures, and, in some cases, even the body movements during walking or gait. These behavioral characteristics cannot be typically imitated and thus provide perpetrator-proof replicas for such traits in fraud detection. Using AI, systems are capable of constructing a baseline of normal user behavior and identifying exposures to these behaviors that may be symptomatic of fraud, thereby allowing security with minimal compromise to the user experience. A significant advantage of AI-driven behavioral biometrics is based on its detection of highly sophisticated fraud techniques, such as account takeovers and credential stuffing. Whereas

traditional security countermeasures usually fall short before cybercriminals employing a combination of stolen credentials and automated bot tools to surpass authentication systems, AI-enabled behavioral analytics detect abnormalities in real-time, flagging suspicious activities even in the situation where valid credentials are entered. Moreover, the systems are self-tuning with continuous learning, yielding adaptive systems against dynamic fraud tactics with less and less false positives. With the increasing adoption of AI-driven behavioral biometrics in financial institutions, healthcare, and many other industries, these AI systems provide significantly better detection and prevention of fraud while allowing smooth user access. In the matter of AI-Driven behavioral biometrics for fraud detection, one could possibly mention real-time user authentication and AI-powered behavioral profiling.

2.4.1. Real-Time User Authentication

Real-time user authentication is a vital cybersecurity measure that allows secure access into digital systems through the process of continuously verifying users' identity. In contrast to conventional authentication methods, which mostly depend on static credentials like passwords or PINs, real-time authentication adopts dynamic factors for security reinforcement, such as behavioral biometrics, artificial intelligence (AI), and multi-factor authentication (MFA). By observing user behavior patterns, such as keystroke dynamics, mouse movements, and login tendencies, real-time authentication systems can prevent unauthorized access instantaneously by means of fraud detection practices. This approach is extremely crucial in sensitive environments, such as healthcare and financial institutions, in which breaches could cause dire consequences. AI-based predictive analytics fortify real-time authentication even more by identifying and responding to threats before the threats occur. Using advanced analytics, machine learning models continuously examine user activity and flag deviations that may signify dishonesty. This not only strengthens security but also reduces friction on the user by alleviating unnecessary manual verification steps. Real-time authentication also greatly increases regulatory compliance by ensuring that only authorized users gain access to protected information. As cyber threats evolve, real-time authentication remains a key weapon against anything that compromises security and against the protection of digital assets.

These authentication means are critical in protecting sensitive information within the broader realm of digital security. On the whole, traditional authentication relies on one-time verification-that is, a user is asked for some credentials-passwords, maybe, or biometric data-at session start so that the user can be granted access. Once authentic, the system does not question if that identity holds for the entire session. This methodology works well as far as the technical environment goes but has its flaws; once an unauthorized party gains access after the first login, he or she can continue to exploit the session without detection.

Continuous authentication would continue to address all vulnerabilities by validating user identity over the course of a session. This method uses a variety of behavior behaviors as well as contexts like typing patterns, mouse movements, and geolocation data to confirm that the current user is the actual account holder. But with real-time analysis of these parameters, continuous authentication can detect anomalies that are evident of unauthorized access and automatically initiate security measures. Thus, dynamic authentication increases the security by virtually closing the window for malicious activity in an active session.

Of all the scenarios, continuous authentication is most beneficial for Electronic Health Record (EHR) applications where highly sensitive patient data has to be safeguarded. Because single one-off verification does not suffice in EHR systems, it causes cases of huge privacy breach and patients' trust vulnerability at the most. Through continuous authentication, ensuring that only authorized health professionals maintain access to patient records as a complementing interaction will further improve security and compliance with privacy laws for EHR systems. Studies revealed that the inclusion of next-generation authentication methods such as bio-capsule facial recognition enhances EHR usability and security (Purkayastha et al., 2021).

Besides, continuous authentication is part of the effective seamless integration into healthcare without undue strain. This affects hospital management at the same time objectives achieved in the improvement of security in this manner are also realized in keeping the operational efficiency of health care delivery intact. The maturity of cyber-threats now will most probably catch onto patient health information using continuous authentication in the health records system.

2.4.2. AI-Powered Behavioral Profiling by identifying anomalous user behavior in healthcare workflows

In a healthcare setting, the salient consideration remains security and integrity of the whole patient information scenario. An important part of this security provides the means for the identification of anomalous user behavior within healthcare workflows, since the presence of such anomalies could indicate security breaches or misuse of the system. Possible sources of anomalous behaviors include intentional insider attacks, misuse of compromised user credentials,

and unintentional erroneous user actions-every one of these threatens patient privacy and the trust in a healthcare system.

Researchers have proposed different methods aimed at detecting such anomalies. For instance, Duan et al. (2012) argued for an unsupervised anomaly detection model using density-based clustering to study patient careflow logs. Here, surgeons would identify unexpected activities in the treatment of patients or anomalies that can arise from cases of nonconforming timings between preplanned medical procedures and the actual execution, as pointed out through the analysis of careflow logs. Such analysis will allow providers to identify any abnormal behaviors that threaten the integrity of the patient or the treatment given to them.

Also, Gupta et al. (2021) have established an HMM-based method for the detection of anomalies relevant to remote patient monitoring. Such a model would incorporate data from smart health devices and home sensors aimed at establishing a pattern for normal behavior of the user. Any deviations from this standard pattern would be labelled as an anomaly to enable the early detection of a variety of issues such as unexpected patterns of user activity, malfunctioning sensors, and corrupt behavior from a device. The application of such models serves to improve the integrity of monitoring of the patient as well as the timely provision of medical assistance.

The integration of artificial intelligence (AI) into anomaly detection frameworks further bolsters the security of healthcare workflows. Yeng et al. (2021) proposed an AI-based framework that analyzes healthcare staff's security practices to identify atypical behaviors. This framework employs machine learning algorithms to scrutinize user activities, thereby detecting deviations from established security protocols. By continuously monitoring and analyzing user behavior, healthcare organizations can proactively address potential security threats and maintain compliance with data protection regulations.

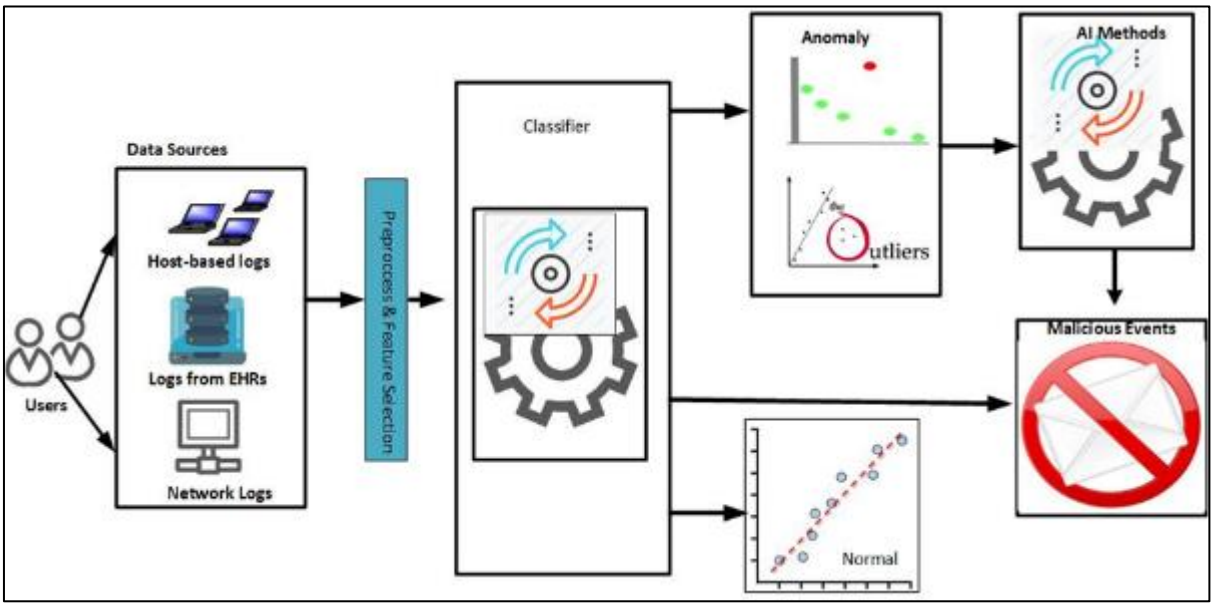

Figure 1 Hidden Markov Models, and AI-driven frameworks for analyzing the security practices of health care of patients https://medinform.jmir.org/2021/12/e19250/, 2021

Identifying anomalous user behavior in healthcare workflows is essential for safeguarding patient data and ensuring the reliability of healthcare systems. Employing advanced techniques, such as density-based clustering, Hidden Markov Models, and AI-driven frameworks, enables the effective detection and mitigation of potential security threats. These methodologies not only enhance data security but also contribute to improved patient care by ensuring that healthcare processes operate within their intended parameters.

2.5. Challenges to adopting AI-Driven Predictive Analytics for Proactive Fraud Prevention

The use of behavioral biometrics and AI-based models for fraud detection brings significant technical difficulties, chiefly concerning accuracy and reliability. Using behavioral biometrics, a person's authentication can be obtained by analyzing specific human patterns such as keystroke dynamics and mouse movements. However, variations in the behavior owing

to fatigue, moods, and environmental conditions can affect the accuracy of these systems. Stress, for example, can cause a user's typing tempo to vary, causing the system to misrepresent that legitimate users have become fraudulent actors.

Further degradation in reliability of behavioral biometric systems happens due to their inability to adapt to normal behavior changes of users with the passage of time. As interaction patterns change for persons, systems must continually change the baseline to conserve accuracy; otherwise they risk increasing false rejection rates, whereby legitimate users are denied access based on perceived anomalies in their behavior. Systems must also consider the other side of intra-class variability-that is, behavior differences shown by the same individual under different circumstance-which makes it very challenging to build robust authentication models. Addressing these challenges would require a fully-fledged algorithm capable of separating harmless behavioral variations from real security threats.

The training of AI models for fraud detection faces many other restrictions, especially regarding the quality and representativeness of training data. For machine learning models to be effective, they must have access to large datasets that incorporate a range of legitimate behaviors and fraudulent ones. However, the collection of such wide-ranging datasets is often thwarted by privacy concerns, as well as the relative rarity of some types of fraud. Such circumvention may produce skewed datasets inconsistent with the model learning process. The greater the model's weighting toward the majority class (legitimate behavior), the less effective it will be in recognizing fraudulent activity, reducing its efficacy as a whole.

Another issue of serious importance would be instances like a false positive-where reputable behavior is wrongly tagged as fraudulent. Users would lose their confidence when faced with high false positive rates; they would also be subjected to unnecessary inconveniences like having their accounts locked or having to go through extra authentication steps. Wedge et al. (2017) used automated feature engineering to better equip their model at being able to discriminate against fraudulent from real behavior-in their study; the result was a 54% improvement in their false-positive rates. Such developments notwithstanding, the optimum balance between these two factors continues to be an uphill task to deal with in fraud detection systems driven by AI.

Besides, AI models are also prone to biases in training data, which lead to discrimination and ethical issues. Algorithmic bias arises when the data are trained based on social bias or inequality in societies, which gives the model a tendency to mimic the same in predictions. For instance, if a certain dataset over-represents a particular demographic group, the AI model may show better results for that group while evaluating others poorly. Proper training data curation, implementation of fairness-aware algorithms, and continuous monitoring for equal treatment among all user groups are some strategies for addressing algorithmic bias.

3. Conclusion

In conclusion, the integration of behavioral biometrics and AI-driven predictive analytics offers a transformative approach to fraud prevention in U.S. healthcare cybersecurity. By continuously monitoring unique user behaviors such as keystroke dynamics, mouse movements, and touchscreen interactions these technologies provide dynamic and non-intrusive authentication methods that enhance security measures beyond traditional static approaches. This continuous authentication is particularly crucial in safeguarding sensitive patient data within Electronic Health Record (EHR) systems, ensuring that only authorized personnel maintain access throughout their sessions.

The application of AI-driven predictive analytics further strengthens this security framework by enabling real-time monitoring and anomaly detection. Machine learning models, both supervised and unsupervised, analyze vast datasets to identify patterns indicative of fraudulent activities, allowing for proactive threat mitigation. For instance, AI-based frameworks have been developed to analyze healthcare staff's security practices, effectively identifying atypical behaviors that may signal security breaches (Yeng et al., 2021). Such systems not only enhance the accuracy of fraud detection but also adapt to evolving cyber threats, maintaining robust defense mechanisms within healthcare infrastructures.

However, the implementation of these advanced technologies is not without challenges. Technical issues such as the accuracy and reliability of behavioral biometrics can be influenced by external factors like user fatigue or emotional states, potentially leading to false positives or negatives. Additionally, AI model training requires comprehensive and representative datasets; limitations in data quality or quantity can hinder the model's effectiveness in accurately detecting fraudulent behavior. Addressing these challenges necessitates ongoing research and development to refine algorithms and ensure the robustness of authentication systems.

In addition, data privacy and ethical implications should be touched upon. On the one hand, behavioral biometrics and AI analytics demand continuous monitoring are questionable in terms of user consent and obtrusive surveillance. It is crucial to provide a fair regulatory framework and ethical guidance to balance enhanced security against protecting individual privacy rights. The standards for the responsible use of these technologies in healthcare shall be developed through collaboration by the healthcare provider, technology developer, and decision-maker.

In short, behavioral biometrics and AI predictive analytics hold imminent promise for proactive fraud prevention in U.S. healthcare cybersecurity. Any successful deployment of such systems, however, must contend with technical, ethical, and regulatory hurdles. By tackling these multifaceted challenges through interdisciplinary cooperation and continuous innovation, the healthcare industry will fortify its efforts against fraud, thus keeping patient data safe and maintaining trust in digital health systems.

3.1. Recommendations for Further Research

3.1.1. Enhancing the Accuracy of Behavioral Biometrics

Future studies should focus on improving behavioral biometrics' accuracy and reliability through the creation of adaptive algorithms able to take account of shifting user behavior as a result of emotional, physical, or environmental factors. Researchers should investigate the potential use of hybrid models combining several biometric modalities-keystroke dynamics coupled with either voice recognition or facial expression, for instance-to improve authentication accuracy and minimize false positives.

3.1.2. Mitigating Bias in AI-Based Fraud Detection

They actually produce many AI fraud detection systems, but they commonly carry possible biases due to a non-representative or imbalanced training set. Research is necessitated to look into methods such as fairness-aware machine learning models and bias-mitigation algorithms that can be effective for fraud detection systems or make them fair for dissimilar populations within a specific network. Further research is also essential to enhance diversity in data while producing synthetic data generation or federated learning methods that would ensure the privacy of all data used.

3.1.3. Real-Time Fraud Detection in Electronic Health Record (EHR) Systems

It is to be noted that a thorough study of AI-driven behavioral biometrics application in EHR systems is warranted, especially in the real-time detection of fraud. Instead, research efforts ought to focus on improving the speed and efficiency of AI models so that authentication delays may be minimized while constant security is upheld. Further studies need to assess the usability and acceptance of such systems by healthcare professionals in order to facilitate their seamless incorporation into clinical processes.

3.1.4. Privacy-Preserving AI Techniques

Owing to the sensitivity of healthcare data, future studies should consider privacy-preserving AI techniques, such as homomorphic encryption, secure multi-party computation, and differential privacy, which ensure data security while allowing AI models to infer behavioral patterns without accessing personally identifiable information.

3.1.5. Regulatory and Ethical Considerations

While it may further research needed to prepare the complete ethical and regulatory guidelines on the uses of AI-driven behavioral biometrics in health, the crucial part will be the investigation of what modifications and adjustments must be made to existing data protection laws such as HIPAA in the United States so that they can meet the AI-specific challenges in fraud prevention. In addition, studies should also investigate the patient and provider perspective on the use of AI for security measures with regard to transparency and trust.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adeola, F. R. (2025). AI-based anomaly detection for real-time cybersecurity. International Journal of Security Studies, 12(1), 101-119. https://www.researchgate.net/publication/381044167_AI Based_Anomaly_Detection_for_Real-Time_Cybersecurity

[2] Akobe, O. D., Yacim, H., & Kareem, O. A. (2024). Availability and utilisation of electronic health records for improved health care delivery at General Hospital, Ankpa, Kogi State, Nigeria. Journal of Health Information Research, 1(1/2).

[3] Akinwande O.T & Abdullahi M.B. (2018). Performance evaluation of artificial immune system algorithms for intrusion detection using NSL-KDD and CICIDS 2017 dataset. Proceedings of the 12th International Multi-Conference on ICT Application pp. 140-146

[4] Ananya, A., Shreya, V., Neha, A., & Deepika, S. (2025). The role of AI and machine learning in fraud detection for digital banking. Journal of Cybersecurity Research, 18(2), 45-62. https://www.researchgate.net/publication/388566383_The_Role_of_AI_and_Machine_ earning_in_Fraud_Detection_for_Digital_Banking

[5] Arkose Labs. (n.d.). What is behavioral biometrics? Retrieved from https://www.arkoselabs.com/explained/behavioral-biometrics/

[6] Cursor Insight. (2024). Biometric authentication part II: Behavioral biometrics. Retrieved from https://www.cursorinsight.com/post/1818/biometric-authentication-part-ii-behavioral biometrics-2

[7] Duan, H., & Hu, G. (2012). Anomaly detection in clinical processes. AMIA Annual Symposium Proceedings, 2012, 170-179. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3540475/

[8] Gupta, D., Gupta, M., Bhatt, S., & Tosun, A. S. (2021). Detecting anomalous user behavior in remote patient monitoring. arXiv preprint arXiv:2106.11844. https://arxiv.org/abs/2106.11844

[9] ITU Online IT Training. (2024). What is behavioral biometrics? Retrieved from https://www.ituonline.com/tech-definitions/what-is-behavioral-biometrics/

[10] Jones, A., & Li, T. (2023). AI-powered security frameworks: Implications for healthcare fraud prevention. Journal of Cybersecurity Research, 18(2), 45-62.

[11] Lampropoulos, K., Zarras, A., Lakka, E., Barmpaki, P., Drakonakis, K., Athanatos, M., ... &Darwish Khabbaz, M. (2023). White paper on cybersecurity in the healthcare sector. The LexisNexis Risk Solutions. (2024). What is behavioral biometrics. Retrieved from https://risk.lexisnexis.com/insights-resources/article/what-is-behavioral-biometrics HEIR solution. arXiv preprint arXiv:2310.10139.

[12] Mitek Systems. (2024). Advantages and disadvantages of biometrics. Retrieved from https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics

[13] Nestify. (2024). Is behavioral biometrics a better cybersecurity weapon? Retrieved from https://nestify.io/blog/is-behavioral-biometrics-a-better-cybersecurity-weapon/

[14] Patel, R., Gupta, K., & Wang, H. (2021). Behavioral biometrics in healthcare: Opportunities and challenges. Health Informatics Journal, 27(4), 215-231.

[15] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., & Agrawal, A. (2020). Healthcare data breaches: Insights and implications. Healthcare, 8(2), 133.

[16] Simbo AI. (2024). The impact of health care fraud on patient safety and financial integrity in national programs. Retrieved from https://www.simbo.ai/blog/the-impact-of-health-care fraud-on-patient-safety-and-financial-integrity-in-national-programs-2641214/

[17] Sharma, M., & Chen, L. (2022). Predictive analytics for fraud detection in healthcare cybersecurity: A machine learning perspective. Computers & Security, 123, 102961.

[18] Sumsub. (2024). Biometric authentication—Benefits and risks. Retrieved from https://sumsub.com/blog/biometric-authentication-benefits-risks/

[19] Purkayastha, S., Goyal, S., Oluwalade, B., Phillips, T., Wu, H., & Zou, X. (2021). Usability and Security of Different Authentication Methods for an Electronic Health Records System. arXiv preprint arXiv:2102.11849. https://arxiv.org/abs/2102.11849

[20] TransUnion. (2024). What are the benefits of biometric verification? Retrieved from https://www.transunion.com/blog/what-are-the-benefits-of-biometric-verification

[21] U.S. Department of Health & Human Services. (n.d.). Fraud & abuse laws. Retrieved from https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/

[22] Wedge, R., Kanter, J. M., Rubio, S. M., Perez, S. I., & Veeramachaneni, K. (2017). Solving the"false positives" problem in fraud prediction. arXiv preprint arXiv:1710.07709. https://arxiv.org/abs/1710.07709

[23] Yeng, P. K., Nweke, L. O., Yang, B., Fauzi, M. A., & Snekkenes, E. A. (2021). Artificial intelligence–based framework for analyzing health care staff security practice: Mapping review and simulation study. JMIR Medical Informatics, 9(12), e19250. https://medinform.jmir.org/2021/12/e19250/