JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AI-POWERED SECURITY ENHANCEMENTS IN DOCTOR APPOINTMENT BOOKING SYSTEMS

[1]Shubhankar Lokhande, [2]Niranjan Pawar, [3]Saurav Rajput, [4]Mrunal Gaikwad, [5]Dr.Lovenish Sharma

[1]Bachelors of technology, [2]Bachelors of technology, [3] Bachelors of technology, [4] Bachelors of technology, [5]Assistant professor

Ajeenkya DY Patil University, Pune, India

Abstract : The focus of this paper is on detecting fraud through leveraging Artificial Intelligence (AI) to prevent unethical practices and protect patients' other sensitive data in digital doctor appointment systems, which are becoming increasingly in demand. The argument asserts that it is necessary to integrate AI into the system to facilitate secure, reliable, and efficient scheduling of healthcare systems to adhere to the need for the services supplied to grow. Hence, this is what this study deals with: AI-based fraud detection solutions using supervised and unsupervised machine learning, anomaly detection by natural language processing, and real-time data security monitoring tools. This thesis analyzes a variety of key technologies, decision trees, support vector machines, and behavioural analytics, for suitability to use to identify non-human activities, verify patients, and predict appointment no-shows. The work of this thesis is of importance as not only does it provide increased operational efficiency, but also its reliability for compliance with privacy regulation, building patient trust, and establishing a stable, intelligent, and strong appointment management system.

***IndexTerms* - Anomaly Detection, Appointment Booking Systems, Artificial Intelligence, Fraud Prevention, Machine Learning, Patient Authentication**

I. INTRODUCTION

As an important mitigating tool for appointment scheduling systems, Artificial Intelligence (AI) is also growing. Analysis and detection of suspicious activity are done based on the use of a larger dataset of appointment information plus AI-driven models. Identification of outliers and non-human activities in healthcare systems has been successful using techniques such as pattern recognition and classification such as decision trees and support vector machines [1]. Also, the use of AI in booking systems allows for real-time authentication checks, monitoring of physical usage and alerting of impending fraud, preventing hard clinical impact.

Besides the detection of fraud, AI significantly makes data secure and enhances the user verification processes. These techniques, such as Natural Language Processing (NLP) and biometric recognition, are used to confirm patients' identities while smart access controls restrict sensitive appointments and health record access to permitted persons only [2]. Besides that, machine learning models learn from emerging fraud patterns continuously, thus, being evolving defenses without manual updates.

Although there has been considerable progress in this area, most doctor appointment systems are still lacking in integration of data and disconnected architecture, as well as outdated forms of authentication. However, today's platforms put a lot of emphasis on the convenience of users and the design of interfaces at the cost of solid fraud prevention. Proper application of a security-centric framework that includes AI-driven detection, prevention, and response mechanisms is a critical issue in protecting the healthcare ecosystem from rising cyber threats and fraudulent behavior. [3]

The research paper aims to explore and propose AI-based solutions specially tuned toward boosted security of doctor appointment booking systems and their detection of fraud. As such, it explores how data monitoring that includes predictive analytics and machine learning may protect these systems. This study allows building secure, intelligent appointment systems that go beyond improving process efficiency to trust and integrity in digital healthcare infrastructure by focusing on vulnerabilities on both the patient side and the administrative side.

II. LITERATURE REVIEW :

The arrival of computerized doctor appointment systems has already brought about total transformation in healthcare accessibility in the sense that it has made patients embrace convenience and real-time scheduling. But, as is the case with all digital platforms, fraudulent behaviour and security flaws have increased. Using artificial intelligence to integrate into the appointment booking system proves itself to be a promising strategy to mitigate such risks, improve operational efficiency, and keep the confidentiality of patient data.

Improving security needs to be done with AI technologies because they can detect suspicious behaviours, fraudulent entries, and unauthorized access in booking systems. Especially, machine learning models can identify variations such as automated bulk reservations or even the invalid credentials used to try to access the administrative system. In a transaction-heavy environment, system security can be enhanced by fraud detection mechanisms based on decision trees and anomaly detection techniques, for example, in the case of healthcare appointment systems.

Knowing the behaviour pattern of a patient and validating it not only helps in preventing fraud but also signals to the patient the potential time to schedule an appointment. Toker et al. (2024) proposed an AI-based system of behavioural analysis of patients for the prediction of patient no-shows and to increase system reliability. [4] As presented by Dashtban and Li (2022) [5], deep learning models that include stacked autoencoders and classification layers identify anomalous or risky patterns in patient attendance data, which may identify indicia of fraudulently used or proxy-registered accounts.

Hotel management systems are revamped through encrypted communication, real-time monitoring, and secure data workflow by AI. The AI-driven dashboards can check logins, monitor all the threats, and enforce access controls on appointment platforms. Predictive fraud prevention is integrated into the scheduling layer as an added extra and also protects patient data.

A close link exists between patient safety data privacy and trust in healthcare systems. The integration of AI-driven authentication systems coupled with biometric verification and behavioural analytics also adds to trust in the system and deploys the process of making an appointment. It minimizes fraud and increases the rate of satisfied customers as it does not allow fake reservations and the manipulation of the waitlist.

Although AI presents vast potential for fraud prevention in appointment systems, issues with model interpretability, real-time responsiveness, and integration with legacy systems. Large datasets, robust infrastructure, and adherence to healthcare data laws such as HIPAA and GDPR are essential for effective adoption. To address these issues, future studies should focus on a collaborative security framework and explainable AI models.

III. METHODOLOGY:

1. Machine Learning Algorithms

Supervised learning techniques such as Random Forest and Support Vector Machines are utilized to determine whether transactions are genuine or fraudulent based on labeled training data.[6]. In unsupervised Learning, Clustering techniques like K-means and DBSCAN are used to detect anomalies in user behavior, which may suggest possible fraud.[7]

2. Natural Language Processing

Sentimental analysis involves reviewing user feedback, revealing dissatisfaction or complaints that might indicate fraudulent activities[8]. Anomaly detection focuses on examining user interactions and aids in identifying deviations from typical behavior patterns.

3. Anomaly Detection Systems

Utilizing statistical techniques and machine learning algorithms to identify anomalies in user behavior, which could indicate fraudulent actions. [9]

IV. PROPOSED FRAMEWORK

4.1. System Architecture

The proposed framework is composed of multiple interconnected components:

1. The data Input module gathers and preprocesses user data, transaction records, and interaction logs.

2. Fraud Detection Model Uses trained models to recognize and flag potentially fraudulent activities in real-time

3. AI processing Model implements machine learning and NLP techniques to examine incoming data for patterns that indicate fraud.

4. User Notification System alerts the user and administrator about detected fraud and suggests preventive measures.

Continuous Learning Mechanism models are updated with new data through a continuous learning mechanism, allowing them to adjust to changing fraud patterns

4.2. Implementation Steps

1. Data Preprocessing: This process begins with cleaning and normalizing the data to ensure quality and relevance for analysis.

2. Continuous Monitoring and Adjustment: System performance is consistently evaluated, and algorithms are based on feedback and new fraud patterns.[10]

3. Feature Selection: Essential features that influence fraud detection, such as user behaviour patterns and transaction histories. [11]

4. Integration with Existing System: Seamlessly incorporates the AI framework into existing booking systems to enhance functionality without disrupting user experience.

5. Model Training and Validation: User historical data is served to train machine learning models, which are then validated using cross-validation techniques.[12]

V. ACCURACY AND PREDICTION MODEL ANALYSIS

1. Data Handling

1.1. Data structure

A dictionary is established to store patient details such as User ID, Name, Number of Cancellations, and Number of bookings. This dictionary was subsequently transformed into a Pandas Data Frame, which serves as a powerful data structure for data manipulation and analysis.

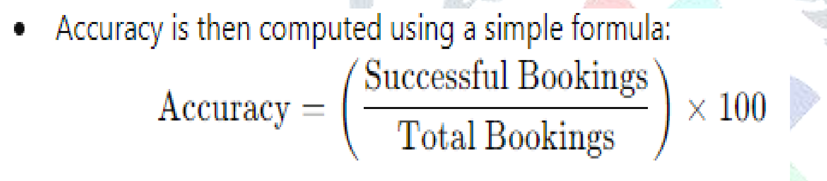
2. Calculations

2.1.Aggregation:

Total Booking is the total count of bookings, calculated by using the sum() method on the Number of Bookings column. Total Cancellations are computed in a similar method, using the same method on the “Number of Bookings” column

2.2.Accuracy Calculation:

To calculate successful bookings, the number of cancellations was subtracted from the total number of bookings. The accuracy rate of 90.59% was determined by dividing the number of successful bookings by the total number of bookings and multiplying by 100. As shown in this figure, most of the bookings are successful (9.41%, not to be precise).



- Accuracy is then computed using a simple formula:

$$\text{Accuracy} = \left(\frac{\text{Successful Bookings}}{\text{Total Bookings}}\right) \times 100$$

Fig.1

2.3.Interpretation:

If the accuracy rate is below 95%, there is a strong reason for questioning why the cancellations are happening. Such areas as how patient satisfaction may affect cancellation, the effect of external approaches on cancellation, or how well appointment reminders work could be investigated.

2.4.Implication:

Accuracy is high-quality work that the healthcare provider needs to perform well, as it helps in operational efficiency, resource allocation, and finally, patient care. This may lead to wasted resources and scheduling problems with low accuracy.

VI. DISCUSSION

Artificial intelligence (AI), when integrated into hospital and overall healthcare management systems has proven their mettle for transformation in multiple operational areas such as appointment scheduling, fraud detection, patient engagement as well as cost optimization. AI technologies have both systemically and increased efficiency and patient-centred care deliverance, which have been shown by numerous studies. Using predictive modelling and personalized scheduling algorithms, Dashtban and Li (2022)[5] showed that powered appointment systems have not shown rates. The deep learning and patient history data-based systems are applied to predict the non-attendance of these systems, which improves resource utilization and reduces the financial burden on the hospitals. In line with these developments, (stressed the importance of a module, independent structure in Artificially Intelligence Hospital Management Systems (HMS). Decision support, and workflow automation with patient data integration, under the guise of continuous operational feedback loops for learning and system enhancement, contribute in an essential way to the system.

In addition, the use of innovative platforms like Medizin and mobile health app development with the aid of AI-based expert systems (for example, iridology-based diagnosis tools) for medication adherence, real-time feedback, as well as access to healthcare in places either poor or remote has been enhanced. For all of that, there is little spoken about in HMS, and yet they are important elements of fraud detection – decision support, workflow automation, and patent data integration – all supported by continuous feedback loops for learning and system enhancement.

Additionally, today we have advanced platforms like Medizin and AI-powered health app development with expert systems like diagnostics tools based on iridology, medication adherence, enhanced immediate feedback and expanded healthcare access in remote and or underserved regions. Although fraud detection, through often neglected in Health Management Systems (HMS), has been explored through machine learning models in the digital transaction system. Khare & Srivastava (2023)[4] illustrated how decision trees and precision-focused classification models can effectively detect financial anomalies, which could be repurposed within healthcare billing and claim systems. Despite these advancements, AI adoption encounters challenges due to data quality issues, the compatibility of existing with new AI technologies, and the adaptation of healthcare providers. Ala & Chen (2022) [13] highlight the ongoing need for standardization in appointment scheduling methods and AI application frameworks.

VII. CONCLUSION

The body of literature reviewed consistently indicates that AI is not merely an enhancement but a crucial component in the advancement of contemporary hospital management systems. The deployment of AI in scheduling, fraud detection, patient engagement, and outpatient optimization offers measurable improvements in operational efficiency, cost-effectiveness, and patient satisfaction. Things like SDAE-based predictive models and AI-based appointment systems have proved that healthcare can move from reactive to proactive where there is no loss of appointments and unnecessary consultation. Moreover, the incorporation of user-friendly mobile applications as well as AI health bots facilitates better connectivity with patients from healthcare providers for more inclusivity in healthcare services. Future studies should concentrate on building hybrid AI models that involve the usage of rule-based systems and neural networks and using larger and anonymized datasets in the training of predictive algorithms. Furthermore, if ethical and technical issues had to be addressed, blockchain for secure data exchange and explainable AI for transparency could be equally incorporated. However, if we are to implement AI in healthcare, we need to take an integral approach — one that does justice to the capabilities of technology and one that lives up to the readiness of organizations, adherence to the rules, and placement of human-centred design at the heart of the matter.

REFERENCES:

[1] Kanksha, Bhaskar, A., Pande, S., Malik, R., & Khamparia, A. (2021). An intelligent unsupervised technique for fraud detection in health care systems. *Intelligent Decision Technologies*, *15*(1), 127-139.

[2] Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. *International Journal of System Assurance Engineering and Management*, *14*(6), 2120-2135.

[3] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105.

[4] Toker, K., Ataş, K., Mayadağlı, A., Görmezoğlu, Z., Tuncay, I., & Kazancıoğlu, R. (2024, October). A Solution to Reduce the Impact of Patients' No-Show Behavior on Hospital Operating Costs: Artificial Intelligence-Based Appointment System. In *Healthcare* (Vol. 12, No. 21, p. 2161). MDPI.

[5] Dashtban, M., & Li, W. (2022). Predicting non-attendance in hospital outpatient appointments using deep learning approach. *Health Systems*, *11*(3), 189-210.

[6] Li, Z., Zhang, H., Masum, M., Shahriar, H., & Haddad, H. (2020, April). Cyber fraud prediction with supervised machine learning techniques. In *Proceedings of the 2020 ACM Southeast Conference* (pp. 176-180).

[7] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2012, August). An effective unsupervised network anomaly detection method. In *Proceedings of the international conference on advances in computing, communications and informatics* (pp. 533-539).

[8] Sharma, S., & Jain, A. (2020). Role of sentiment analysis in social media security and analytics. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(5), e1366.

[9] Shi, Y., Liu, Y., Tong, H., He, J., Yan, G., & Cao, N. (2020). Visual analytics of anomalous user behaviors: A survey. *IEEE Transactions on Big Data*, *8*(2), 377-396.

[10] Mehana, A., & Nuci, K. P. (2020). Fraud Detection using Data-Driven approach. *arXiv preprint arXiv:2009.06365*.

[11] Doreswamy, Hooshmand, M. K., & Gad, I. (2020). Feature selection approach using ensemble learning for network anomaly detection. *CAAI Transactions on Intelligence Technology*, *5*(4), 283-293.

[12] Bin Rafiq, R., Modave, F., Guha, S., & Albert, M. V. (2020, November). Validation methods to promote real-world applicability of machine learning in medicine. In *Proceedings of the 2020 3rd International Conference on Digital Medicine and Image Processing* (pp. 13-19).

[13] Ala, A., & Chen, F. (2022). Appointment scheduling problem in complexity systems of the healthcare services: A comprehensive review. *Journal of Healthcare Engineering*, *2022*(1), 5819813.