Artificial Intelligence Solutions to Detect Fraud in Healthcare Settings: A Scoping Review

Mohammad Sharique IQBALa, Alaa ABD-ALRAZAQa,b and Mowafa HOUSEHa,1

aDivision of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar

bAI Center for Precision Health, Weill Cornell Medicine-Qatar, Doha, Qatar

Abstract. Over the past decade, Artificial Intelligence (AI) technologies have quickly become implemented in protecting data, including detecting fraud in healthcare organizations. This scoping review aims to explore AI solutions utilized in fraud detection occurring in treatment settings. To find relevant literature, PubMed and Google Scholar were searched. Out of 183 retrieved studies, 31 met all inclusion criteria. This review found that AI has been used to detect different types of fraud such as identity theft and kickbacks in healthcare. Additionally, this review discusses how AI techniques used in network mapping fraud can detect and visualize the hacker’s network. A proper system must be implemented in healthcare settings for successful fraud detection, which may overall improve the healthcare system.

Keywords. Fraud, artificial intelligence, deep learning, machine learning, healthcare settings

1. Introduction

Over the past twenty years, digital crime has rapidly increased. It is challenging and costly to eradicate these issues; it is estimated that more than $86 million is spent by the FBI to combat crime and fraud alike in the United States [1]. This affects large and small businesses alike, as the Association of Certified Fraud Examiners found that fraud costs businesses 5% of their annual turnover [2]. As healthcare organizations more frequently utilize electronic healthcare records and online payment systems, an efficient detection system or model may better assist in detecting and classifying any instances of fraud. As such, to mitigate issues of fraud, several organizations are implementing increasingly sophisticated resources to protect their networks and data. This includes adopting new technologies that utilize Artificial Intelligence (AI). To achieve implementing successful fraud detection, a better understanding of fraud and digital crime prevention strategies is essential to establish a more effective and successful learning strategy.

As big data evolves, detecting fraudulent activities within networks has become increasingly complex. However, AI technology such as deep learning and machine learning approaches can expedite awareness [3]. These approaches draw on data...
techniques to provide a holistic view of interdependencies within a network. Recently, deep learning approaches have made significant contributions to detecting fraudulent activities within healthcare networks. As such, fraud detection experts have recognized them as a solid, reliable, and promising anomaly detection technique [4]. While several studies on AI and fraud detection have been conducted, little research has summarized how novel AI approaches are utilized to mitigate fraud. Studies conducted before the year 2015 do not provide in-depth explorations into AI as the technology was not as developed at this time. To bridge this gap, this review aims to provide an overview of AI solutions used by previous studies to detect fraud in healthcare settings.

2. Methods

This scoping review was conducted in accordance with the PRISMA-ScR (Preferred Reporting Items for Systematic Review and Meta-Analyses-extension for scoping reviews). Two databases were utilized to retrieve relevant studies: Google Scholar and PubMed. We used a combination of 3 groups of search terms related to fraud (e.g., fraud, crime, and forensic), AI (e.g., artificial intelligence, deep learning, and machine learning), and healthcare (e.g., health, medical). We included studies that used AI solutions for detecting fraud in healthcare settings whereas we excluded those that used non-AI solutions and not in healthcare settings. Any studies that were written in a language other than English or published before the year 2015 were not included in the review. Rayyan software was utilized to aid the study selection process. Study selection was conducted in three phases: removing duplicates, reviewing the titles and abstracts of articles, and then reviewing the full articles. The extracted data was then narratively synthesized using an Excel spreadsheet. The study selection, data extraction, and data analysis were carried out by the first author only.

3. Results

A total of 183 citations were retrieved from the two databases. Of these citations, 31 studies were found eligible for this scoping review [1-31]. A flow chart of the study selection process can be found in Appendix 1. Twenty-seven of the included studies were published journal articles, while the remaining 4 studies were papers presented at conferences. The included studies originated from 12 countries, with the largest number of studies published in the United States (n=13). All included articles were published between 2015 and 2020, with the largest number of studies published in 2020 (n=14). More details about the characteristics of the included studies are shown in Appendix 2. The included studies utilized AI for fraud detection (n=17) [1, 2, 6, 8, 14, 17, 18, 19, 21, 22, 23, 24, 26, 27, 28, 30, 31], identifying and classifying detected fraud (n=8) [3, 4, 11, 12, 13, 15, 20, 25], and investigating and analyzing fraudulent data (n=6) [5, 7, 9, 10, 16, 29]. The most common algorithm used in the included studies was Convolutional Neural Network (CNN) (n=13), followed by Artificial Neural Network (ANN) (n=10). The most commonly used validation methods were 5-fold cross validation (n=9) and 10-fold cross validation (n=9). The size of dataset used in the studies ranged from 135 [5] to 4,310 [15]. Only three studies [16, 17, 18] utilized a dataset of 1,000 or less. The most common

2 Appendices are available at GitHub: https://github.com/moiq33909/Research1.
metric used to assess performance of the model was accuracy (n=18), followed by sensitivity (n=15), specificity (n=15), and Area under ROC curve AUC (n=12).

4. Discussion

This review finds that the most utilized AI techniques to detect fraud include both deep learning and other AI detection systems such as Intrusion Detection systems, Neural Networks, and a Defendable Healthcare Networks Environment. Recent research has found that deep learning models can effectively identify patterns and distinguish features in various fraudulent activity more successfully than other techniques. Furthermore, deep learning has become a preferred technique because its algorithms can both more effectively protect medical data as well as prevent devices from being susceptible to malicious activity. Overall, many organizations rely on more traditional methods to protect themselves against cybercrime and fraud; however, these techniques are significantly less effective than those mentioned in this scoping review. This is because various advanced types of attacks and fraud can occur, such as advanced persistent threats (APT) carried out by highly skilled cyber fraud groups.

This review has some limitations. Most studies collected for this review were conducted in the United States, indicating that results were mostly limited to a specific population. This may have inadvertently led to missed information on fraud detection techniques utilized by different countries or cultures. In addition, only two databases, PubMed, and Google Scholar, were searched as other advanced databases (such as Web of Science, ProQuest, and others) were inaccessible. As a result of this limitation, relevant studies may have been missed. Moreover, this review restricted the article search to studies published in English; consequently, this review likely missed many relevant research studies written in other languages. Lastly, deep learning requires a large dataset that have been specifically designated for training and purchasing this data may not be feasible for smaller organizations.

5. Conclusions

This scoping review was performed to explore utilizing AI technology in detecting and identifying fraud and digital crimes occurring in healthcare settings. This review finds that safe, high quality and cost-effective systems must be developed to aid healthcare settings in effectively mitigating fraudulent activity. The applications and other AI techniques are beneficial to treatment settings, but can be challenging to implement and costly to maintain. It is recommended that hybrid technologies be developed to detect fraud alerts quickly and precisely, and that automatically provide alarms and support to designated staff and employees. Ultimately, providing a timely alert and relevant information on fraudulent activity, along with overall better quality of fraud detection, can greatly assist healthcare organizations wherein anonymous fraud may take place.

References


