A Survey of Threats to Research Literature-dependent Medical AI Solutions

SHALINI SAINI and NITESH SAXENA, Texas A&M University, USA

Medical Artificial Intelligence (MedAI) harnesses the power of medical research through AI algorithms and vast data to address healthcare challenges. The security, integrity, and credibility of MedAI tools are paramount, because human lives are at stake. Predatory research, in a culture of "publish or perish," is exploiting the "pay for publish" model to infiltrate he research literature repositories. Although, it is challenging to measure the actual predatory research induced data pollution and patient harm, our work shows that the breached integrity of MedAI inputs is a serious threat to trust the MedAI output. We review a wide range of research literature discussing the threats of data pollution in the research literature, feasible attacks impacting MedAI solutions, research literature-based tools, and influence on healthcare. Our contribution lies in presenting a comprehensive literature review, addressing the gap of predatory research vulnerabilities affecting MedAI solutions, and helping to develop robust MedAI solutions in the future.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Computing methodologies** → *Logical and relational learning*; *Knowledge representation and reasoning*; *Information extraction*; • **Applied computing** → **Health care information systems**; • **Security and privacy** → **Information accountability and usage control**; • **Social and professional topics** → *Medical technologies;*

Additional Key Words and Phrases: Predatory science, research literature, NLP, Knowledge Graph, semantic analysis, data pollution, data integrity, Medical Artificial Intelligence, trustworthy medical technologies

ACM Reference format:
Shalini Saini and Nitesh Saxena. 2023. A Survey of Threats to Research Literature-dependent Medical AI Solutions. *ACM Comput. Surv.* 55, 14s, Article 315 (July 2023), 26 pages.
https://doi.org/10.1145/3592597

1 INTRODUCTION

Medical Artificial Intelligence (MedAI) for finding a correct diagnosis, treatments, and drug development represents the new age of healthcare. MedAI can assist precision medicine and personalized medicine on diagnosis and treatment guidance based on enormous data to assist in decision making, primarily to provide otherwise unknown connections among cause, symptom, gene, drug, and environment [105]. There is compelling evidence that MedAI can be vital in enhancing and complementing the "medical intelligence" of the future clinician [50, 73].

How Biomedical Research Is Critical in Healthcare: Rare, unknown, or life-threatening diseases have been a great motivation for academic and industrial research for improving patient-centered solutions in research and clinical settings [1, 5]. Many clinical and non-clinical MedAI

Authors' address: S. Saini and N. Saxena, Texas A&M University, 435 Nagle St, College Station, TX, USA; emails: {s.saini, nsaxena}@tamu.edu.

0360-0300/2023/07-ART315 $15.00
https://doi.org/10.1145/3592597

solutions rely upon scientific research publications in medicine as the primary data source for automated decision-making. *PubMed* [2], maintained by the **National Library of Medicine (NLM)**, is one of the largest medical research literature repositories, comprising more than 30 million citations for biomedical literature. PubMed ID is a unique identifier assigned to each article on PubMed. PubMed-derived database SemMedDB, consisting of 96.3 million predications extracted from all MEDLINE citations, integrating PubMed and **Unified Medical Language System (UMLS)**, is an indispensable input to MedAI systems [10, 41, 52, 68, 72, 81, 98, 107]. MedAI solutions harness the power of research through analytical algorithms spanning heuristics, neural networks, **Natural Language Processing (NLP)**, fuzzy logic, semantic snalysis, **Knowledge Graphs (KGs)**, and **Machine Learning (ML)** to integrate and interpret the complex biomedical and healthcare data [52, 68, 81, 107].

How Research Gets Manipulated and Can Impact the MedAI and Future Research: Undoubtedly, research literature adds enormous value to accelerate innovations in clinical care and drug discovery. However, research literature repositories can be prone to data abuse through undetected fraudulent research. As research publications serve as a core component of MedAI, it draws attention to research literature and any derived database as a potential attack surface. Invalidated or manipulated academic or industrial research commonly referred to as *Predatory Science* [22]. In recent years, there has been an unprecedented rise in predatory science publications interfering with the genuine research [13, 22, 28, 37, 75, 77]. There may even be a possibility of affecting actual patient care based on such fraudulent predatory research [18, 34]. Such unreliable data then can be further abused by malicious actors through exploratory or adversarial attacks to compromise the credibility of MedAI solutions [26, 27, 62, 108]. If the inputs are untrustworthy, irrespective of the efficiency of the applied algorithm, then the output of such a system cannot be considered as trustworthy [100, 105, 106]. Especially in the case of rare diseases where research is limited, any unreliable output will be distracting the service providers, increasing cost and effort. It may likely be leading to the treatments that may be detrimental to the patient care and thus wholly undermining the MedAI's purpose.

Motivation: No comprehensive literature review exists to study the potential threat of predatory science impacting these research information-based **artificial intelligence (AI)** solutions and how it can impact AI usage in modern medical research and clinical practices. Our work is motivated by the increasing significance of research literature-based medical AI solutions in modern healthcare settings and by the increasing presence of predatory research in trusted research literature repositories. We address this gap to analyze the collective threat to research literature-based medical AI decision-making.

Objectives of the Survey: The aim of this survey is to provide a comprehensive study of impact of predatory research on AI-based medical solutions to help developers, researchers, data-curators, and clinicians. Though cost analysis is out of scope of this survey, any influenced misdiagnosis and incorrect treatment can impact the financial burden for the healthcare provider and the patient as well.

- First, we establish a background and identify published works that have investigated or evaluated the threat of predatory science undermining the credibility of genuine research in medicine [13, 20, 22, 23, 28, 31, 37, 54, 57, 60, 61, 69, 75, 77, 84, 87, 90, 92, 93].
- Second, we identify a wide range of existing clinical and non-clinical knowledge-extraction, decision-making solutions, and derived databases utilizing the most trustworthy NIH research literature repository PubMed [9, 10, 29, 41, 52, 68, 72, 81, 98, 99, 102–104, 107].
- Third, we provide a comprehensive study of the direct and indirect impact of predatory science on medicine practices [12, 18, 25, 34, 39, 74, 88, 89]. We study the criticality of potential

security, integrity, and safety issues induced by predatory science in clinical and non-clinical MedAI solutions [11, 16, 24, 26, 27, 30, 35, 43, 44, 47, 53, 56, 62–64, 67, 71, 80, 82, 83, 91, 93, 96, 106, 108].

Contributions of the Survey: The results of this survey guide future research in the area, including developing any defensive measures assuming these attacks indeed turn out to be a significant practical concern. This survey serves researchers and medical practitioners who are interested to know the direct and indirect impact of predatory research on healthcare decisions. To summarize, the key contributions of this survey are as follows:

- Identifying the rising threat of the predatory research and data poisoning in reputable research repositories needs immediate attention of research and medical community to develop practical strategies to minimize the inclusion of predatory research in reputable research repositories.
- Presenting that NIH research literature repository PubMed and PubMed-derived databases as inputs to the state-of-the-art MedAI solutions will allow researchers, developers, and research repository administration to find mitigating strategies.
- Identifying the threat of predatory publications impacting new-age medical AI solutions will allow the development of more secure and robust MedAI solutions at both the data and the algorithm levels.
- Mitigating the threat of data poisoning into trusted resources will encourage the practical adaptation of research-backed decision-making in clinical settings for improved healthcare.

2 TAXONOMY AND RELATED WORK

Taxonomy: We examine and compare a wide range of existing works based on their scope and relevance. Each of these categories presents the significance of the area and its relevance under the scope of our work. A deeper analysis further reveals that a common goal is addressing a particular problem of predatory research impacting medical AI integrity and security. Hence, we develop our taxonomy by structuring the related work and expanding our analysis in these categories.

(1) *Predatory Research* can be classified as a combination or stand-alone variation of bogus, duplicate, manipulated, incorrect, and research frauds. If predatory research is mixed with genuine research, then overall confidence in the research literature repositories is diminished.
(2) *Research literature-based MedAI solutions* use information extracted from the medical research literature repositories like *PubMed*. The MedAI solution is the implementation of AI in medicine to improve overall healthcare. Advanced technological innovations can gather, analyze, synthesize, and infer meaningful information to reduce the time, effort, and cost involved in complex healthcare solutions. MedAI solutions provide a comprehensive and current knowledge dataset for efficient healthcare decision-making.
(3) *The impact of compromised MedAI solutions on medical research and practices* can mislead future medical research and healthcare practices, which can be critical in finely targeted scenarios of precision medicine and can influence public health negatively for a prolonged period.

We analyze the existing work on the threat of predatory research, AI in medicine, vulnerabilities of AI-based solutions, and the impact of research and predatory research on medical practices and prospective medical research.

How Do We Collect the Papers? We used Google Scholar and PubMed as primary search for papers involving medical AI, threats to medical AI, medical AI solutions based on research literature, and the problem of predatory research. In addition, we also utilized the iris.ai search

tool to find a pool of related research papers. We employed Google search to find the major medical AI milestones, incidents of research fraud, the impact of predatory research on public health, and recent work and news regarding medical AI and trends in predatory research. The primary keywords and phrases are *predatory research*, *medical fraud*, *medical AI*, *threats to medical AI*, and *research literature-based medical information extraction tools*.

Related Work: With regard to predatory research, a review from Dinis-Oliveira discusses the main characteristics of predatory journals and the impact of predatory research in the context of forensic and legal medicine research and advocates the critical need for education on the threat of predatory research [23]. Mills et al. found that more than half of the predatory publications studied are from the nature/biomedical field. Their work focuses on the aspects of shaping publishing motives, decisions, and experiences in predatory publishing [61]. Mertkan et al. found that the highest percentage of their studied predatory journals belong to medicine (around 39%) [60].

A survey by Ji et al. on KGs discusses graph convolutional networks, adversarial training, reinforcement learning, deep residual learning, and transfer learning and how MYCIN-like systems apply knowledge-based decisions in medicine [44]. The NIH Translational project focuses on providing unified, standard KGs to accelerate knowledge-based medical decision-making tools. Therefore, KGs are expected to play a critical role in new MedAI solutions [101, 107]. Secinaro et al. discuss the increasing role of AI in predictive medicine, clinical decision-making, patient data, and diagnostics and making a difference using AI in healthcare management [82]. Srinivasu et al. emphasize the importance of explainable AI in the medical decision-support paradigm to be robust and precise as it deals with human survival [91].

Alshehri and Muhammad discuss the literature in the field of IoMT, AI, medical signal use and fusion, edge and cloud computing, privacy, and security in the smart healthcare domain. Their work covers sensors' interoperability, device and information management barriers, and using AI efficiently. However, building more robust solutions against privacy and security attacks is challenging yet essential [11]. The survey by Zhang et al. covers attacks and defenses on textual deep-learning, presenting how manipulated input data can alter AI output, exploiting training and influencing output with or without the knowledge of the Model [108]. Their work has close relevance to information extraction from the research literature as a key pre-processing step before feeding medical information to MedAI.

What Is the difference between This Survey and the Former Ones? There is no broad and precise literature review systematizing all those security and integrity aspects involving predatory research effects on MedAI solutions. Our work investigates the security, integrity, and credibility of MedAI solutions that rely upon research literature repositories as critical data sources. More specifically, we consider the possibility that research literature repositories may contain predatory content. Our observation is that MedAI solutions incorporate predatory publications found in research literature repositories, which undermines the trust in these solutions. Table 1 shows a brief comparison of the scope of our work with other recent relevant work. We identify a gap in covering all aspects of predatory research, information extraction tools, applied AI methods in healthcare, and associated threats. Identifying hidden and non-obvious threats, vulnerabilities, and misuses is essential in designing better defense strategies to protect the integrity and security of current and future MedAI solutions.

3 BACKGROUND

Back in 1956, AI was introduced as an idea to develop machines replicating human intelligence. Medicine has been cautious about adopting AI in day-to-day clinical practices because of the involved complexity of integrating technology with medical, financial, legal, and ethical liabilities [86]. Despite enormous challenges, the rewards of using MedAI are undeniable, and there has

Table 1. Comparison of Recent Relevant Work in Medical AI, Threats, Tools, and Predatory Research

Reference	MedAI and AI threats	MedAI Tools	Predatory Research in Medicine	Predatory Research affecting MedAI Tools
Alshehri and Muhammad [11], 2020, Survey	✓	✗	✗	✗
Zhang et al. [108], 2020, Survey	✓	✗	✗	✗
Dinis-Oliveira [23], 2021, Article	✗	✗	✓	✗
Ji et al. [44], 2021, Survey	✗	✓	✗	✗
Mills et al. [61], 2021, Review	✗	✗	✓	✗
Mertkan et al. [60], 2021, Systematic Review	✗	✗	✓	✗
Secinaro et al. [82], 2021, Literature Review	✓	✗	✗	✗
Srinivasu et al. [91], 2022, Case Studies	✓	✓	✗	✗
Our work, Survey	✓	✓	✓	✓

been increasing use of MedAI in robotic procedures, diagnosis, statistics, and human biology, including *omics* [38]. MedAI has opened a new dimension for medicine to harvest the abundance of knowledge scattered in the medical research literature and isolated silos of diseases, drugs, and patient data. Computational technological advancements can better handle the limitations on data collection, storage, and processing needed for precision medicine [7]. Thus, the research-data-AI trio became more equipped than ever to help modern medicine find the probable cause and the possible treatment in a decent time frame with reasonable trust. The cost of unreliable output from such MedAI solutions is too high to ignore the vulnerabilities and threats associated with research misconduct, data flaws, and exploitable algorithms. An unreliable MedAI output can be fatal in patient care, and flawed results can misalign the overall cycle of future research and healthcare solutions in a harmful direction.

3.1 MedAI Methodologies and Biomedical Knowledge Representation

MedAI Methodologies: Bayesian methodologies are basic standards for acceptable uncertainty in research data and are widely accepted in the medical research community and regulatory agencies [5]. Semi-supervised and unsupervised machine-learning techniques are more applicable to developing transformative machine intelligence-based systems for diagnosing and recommending treatments for a range of diseases and health conditions [1]. Artificial Neural networks and fuzzy logic can be combined as a hybrid intelligent system to accommodate common sense, extract knowledge from raw data, and use humanlike reasoning mechanisms [73]. A PubMed-based study shows that more than 70% of AI methods applied in medical research are neural networks and Support Vector Machines for imaging and genetics [45]. At the same time, NLP is a crucial method to extract information from unstructured data such as research literature, clinical notes, patient reports, and so on [45]. **Deep Learning (DL)** and NLP are widely employed to extract meaningful information from the research literature. The intersection of data science, analytics, and precision medicine optimizes the tools and information used to deliver improved patient outcomes [33].

Biomedical Knowledge Representation: *Syntactic Analysis* and *Semantic Analysis* are two core operations of NLP used to obtain the structure and the intent of the given text. Semantic analysis is closest to understanding and interpreting information in the right context to mimic human intelligence. Semantic analysis is a multilayered process including filtering, segmenting, encoding, defining, and identifying relationships between objects, linguistic perception, syntactic analysis, pattern classification, data classification, feedback, cognitive reasoning, and data understanding.

The UMLS provides semantic knowledge to extract unique associations among diseases, genes, and drugs. Each concept is defined in UMLS by a **Concept Unique Identifier (CUI)** [17]. Two concepts can be connected with one or more semantic relationships known as predicates. A triplet of object-concept, subject-concept, and relationship carries concise and useful information. For example, drug x (object-concept) treats (relationship-predicate) disease Y (subject-concept). Semantic analysis has been a key component of ML to extract relationships among disease, diagnosis, and treatments from the research literature [66].

Resource Description Framework (RDF) is a standard language for representing information about resources in the World Wide Web. RDF provides a way to describe resources using a set of triples, which consist of a subject, a predicate, and an object. It is used in applications, such as data integration, knowledge representation, and semantic web technologies [78].

Knowledge Graphs in Medical Domain: Knowledge Graphs contain a large amount of prior knowledge and are widely used for decision-making systems, search engines, or recommendations [109]. Knowledge Graphs are highly applicable in the medical domain and research. Medical knowledge graphs applying knowledge reasoning can help providers and researchers find known and unknown relationships among diagnostics, diseases, and treatments. Logical inference and probabilistic refinements can develop intelligent systems to suggest treatment options. Knowledge reasoning can derive new relationships among the entities and further enriches the knowledge graphs [21].

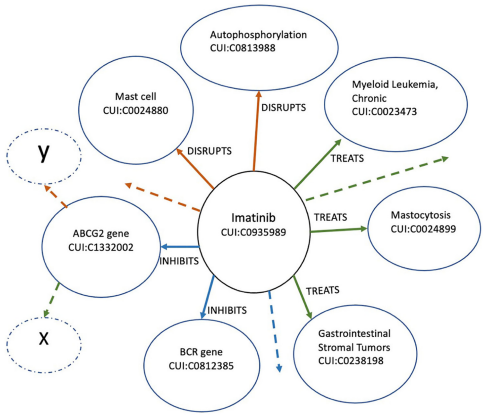

Fig. 1. SemMedDB extracted knowledge graph-nodes (concepts with unique UMLS CUIs); edges(Predicates).

Figure 1 shows a visual presentation of knowledge queried from SemMedDB for a drug *Imatinib* to show how it is associated with genes and diseases through different predicates. Nodes represent the concepts, and edges represent predicates. RTX-KG2, a recently developed *knowledge provider*, is a biomedical knowledge graph to integrate 70 knowledge sources following the standard Biolink model to maximize interoperability [101, 107]. Such advancements can help provide standardized biomedical data to a diverse set of medical applications and reduce the cost of cross-verification and synthesizing among heterogeneous data sources. However, that makes it even more critical to ensure the integrity of the data.

3.2 Security and Integrity of MedAI Solutions

Since 2010, about 40% of 200 new businesses have directed health interventions or predictive capabilities. It is estimated to help with a reduced healthcare spending of around $450 billion if scaled up to mainstream use [48]. However, it also increases the risk of utilizing promising AI methodologies that can be exploited to alter inputs and output through exploratory and adversarial attacks. If the manipulated research publications get included in a reputable research literature repository, then this predatory research poses a potential threat to the data integrity of the data source. However, MedAI aims to bring all the relevant information together and filter out irrelevant information without skipping more challenging instances. This requirement may make MedAI vulnerable to predatory research. It is crucial to include that one single paper on the latest finding that can

alter the life of some patient(s), and it is even more important to validate whether that paper is predatory.

Data pollution and targeted or untargeted data poisoning can mislead the MedAI algorithm [26]. Even without exploiting the MedAI algorithm, undetected bad inputs can traverse the MedAI output. Thus, it is important to identify the threat surface and find solutions to mitigate the threat to the minimum possible level. Misclassification in neural networks is a well-known adversarial attack that is more common to image-based MedAI solutions. However, text-based adversarial attacks are feasible and can damage the confidence in MedAI output [26, 49, 62]. Szegedy et al. showed that adversarial inputs need not appear unusual or pathological, and even slight perturbation can change the outcome completely [97]. An attacker can potentially perturb it in a direction that aligns well with the weights of the MedAI algorithm and thus amplify its effect on the output [35]. The potential for algorithmic bias may violate beneficence and non-malfeasance medical principles affecting a specific population through incorrect or absent diagnosis and treatment [51]. As NLP is a core process to extract intelligent information from the research literature for MedAI, it is critical to have a defense against adversarial attacks [108].

This work focuses on the threats to MedAI solutions using research literature as a primary data source. We primarily study the infiltration of predatory publications impacting MedAI solutions' integrity and security. With all potential benefits, AI can also have profound health effects due to data bias and insufficient sample size and can produce incorrect results. AI may need to be more trustworthy to completely replace humans, especially in more human-dependent settings of therapy sessions. On the one hand, AI can significantly reduce costs and allow easy access to healthcare in rural areas. Patients may prefer to disclose sensitive information to AI than a fellow human. On the other hand, any health-related digital records can pose considerable risk to patient confidentiality, and any manipulation or induced biases can be a severe problem harming the patient.

4 PREDATORY SCIENCE UNDERMINING SCIENTIFIC INTEGRITY

Medical research has been revolutionary in the past few years, and there is an apparent increase in the number of publications each year. However, innovation is not the only reason for soaring numbers. The "publish or perish" culture and **Open Access (OA)** journals are great contributors to an unprecedented increase in research publications. The pressure to publish may influence researchers to bypass rigorous review of their work, which allows journals to follow non-standard and questionable publishing processes. These journals are categorized as predatory journals and promote predatory publications with unintended or intended consequences regarding the data. Research misconduct cases increase the data manipulation probability. We take a close look at the publishing methods and motivations to analyze the reasons supporting the rapid increase of predatory publications. We study the research literature regarding predatory research, available at Google Scholar and PubMed, and extract a summary of the definition, motivations, actors, and impact of predatory research.

Before the dawn of OA journals around 2000, medicine research publications were under traditional journals where the reader pays for access [58]. The traditional model supports a highly ethical, comprehensive, and robust peer-review system to publish trustworthy and valuable research. Over time, many found the traditional approach too strenuous and limiting to disseminate the research timely, almost delaying the actual benefit and impact of the research findings. A multilayered, tedious, mostly yearlong, and complex peer-reviewed process and pay-to-access model pushed researchers to look for alternatives.

Without a robust review process, there is the probability of unauthentic research getting published with flawed findings and conclusions. Such predatory publications can pollute the research

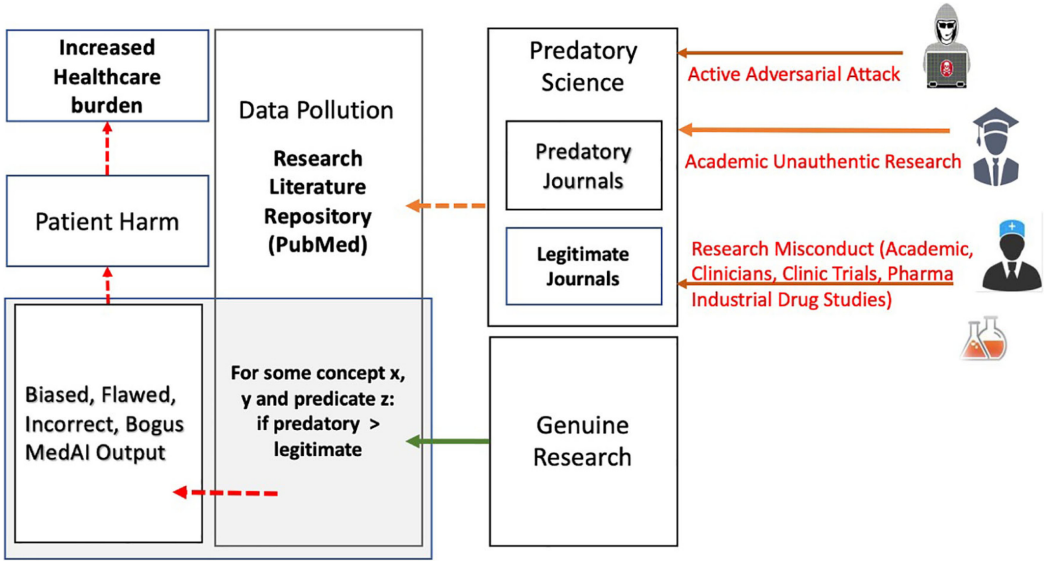

Fig. 2. High-level overview of predatory science impacting MedAI and healthcare.

literature repository. Figure 2 illustrates a high-level overview showing that predatory science can induce biases and influences through data pollution and data poisoning. Polluted data input can cause an intentional or inadvertent failure of real-world MedAI systems. Open Access journals assist researchers with presenting their work quickly, with much shorter publication times and free online access to the research community. The **Article Processing Charge (APC)** may sound necessary to maintain the OA journal's operations, but that pushed prioritizing pay-to-publish over scientific integrity [14]. The OA model is here to stay, so the focus has to shift more to what can be done to restore and maintain research integrity rather than discrediting OA journals altogether. As per the **Directory of Open Access Journals (DOAJ)**, there are 15,954 journals from 124 countries in 80 languages [4]. There is a debate about both the publication systems' pros and cons. However, maintaining the scientific integrity of all research publications is critical, as the consequences of allowing pollution are devastating to science and medicine.

Research misconduct is another critical component of predatory research. As per the U.S. Office of Research Integrity, research misconduct is as follows: (a) *Fabrication is making up data or results and recording or reporting them; (b) Falsification is manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record; (c) Plagiarism is the appropriation of another person's ideas, processes, results, or words without giving appropriate credit; and (d) Research misconduct does not include honest error or differences of opinion* [3]. Research misconduct is a less reported, largely undetected problem with a possible long-term impact because of misleading directions based on fraudulent research [30].

Medical journals are 40% of the 171 journals we studied, with the highest percentage of one or more predatory publications [60]. Reputable journals are also affected by research misconduct during the COVID-19 pandemic due to panic of finding the solution through rapid research [23, 59]. As we study the scholars addressing the problem of predatory science, including factors, actors, and defense strategies, we see the following trends:

- *What is predatory science?* Predatory journals, publishers with questionable practices, and publications involved with research misconduct [13, 22, 69, 77, 84].

Table 2. A Summary of Features of Predatory Journals/Publications

Predatory Journals/Publications Key Features	Citations
Plagiarism, bias, errors and frauds	[31, 37, 54, 57, 77, 92, 93]
Absent or minimal peer review process	[13, 20, 57, 77, 90]
Distorted editorial and publications practices	[20, 37, 84, 90]
Piracy	[54, 57, 77]
Pay-to-publish, Drain Money	[20, 77, 84]
Aggressive indiscriminate solicitation	[37, 77]
Abuse of trust, Concealed conflict of interests	[77, 87]
Low quality writing and images	[20, 84]
More predatory publications once indexed in reputable repositories	[57, 77]
Other: Human activity, Non-relevant scope of interest	[84, 87]

- *What is a predatory journal?* These are mostly OA journals of low quality and ethics [57] with no or minimal peer-review [13, 20, 69, 77, 84]; this is a pay-to-publish model with questionable editorial practices [20, 57, 77, 90]. Table 2 summarizes key features of predatory journals and publications and shows that plagiarism, bias, errors, and fraud are the most discussed issues in studied literature, which can influence MedAI output.
- *What are the reasons and motives?* The most common factors are the importance of quantity over quality [20, 54], a critical component for hiring, promoting, funding, and recognizing authors [13, 20, 31, 57, 69, 77], including the "publish or perish" model [54, 75]. Financial gain, career progression, and finding novelty at all costs are primary motives for researchers, clinicians, and pharma industries for predatory research.
- *Who are the actors?* Global issues include world leaders in research and developing countries, greedy publishers, novice researchers (because of pressure to produce, desperation after multiple rejections, ignorance, and lack of supervision), and experienced researchers who strive for financial gain and fame or are under pressure to produce.
- *What is the damage?* All are agreed that undermining scientific integrity is the most critical danger of allowing predatory science getting mixed with genuine research. A waste of resources, money, and talent are other major concerns [37, 54, 69, 90]. Unverified conclusions may harm patients if physicians are unaware of the bad data [77].
- *What is the extent to harm patients?* Patient harm is not discussed by all papers studied with a focus on predatory journals but is more discussed in retracted research and research misconduct papers. The retracted research may already have done the damage for the period it went undetected, and even after retraction, it may affect physicians and people's perception for a much more extended period [20, 31, 93].
- *What is the defense strategy?* The strategy is to define the standard measurable features [22, 37, 77, 84], promote awareness and education on identifying predatory journals and publishers [54, 77, 84], and conduct data quality checks [31].

There is some indication of the presence of predatory science in reputable databases and how it encourages the publication of more predatory journals once that journal is part of the reputable databases [69]. Citations of such unreliable research in reputable journals is another concern, as there were 389 citations made in WoS-listed journals from 3,427 potentially predatory papers published between 2010 and 2015 [8]. A more recent work highlights that, in general, current and future African neurosurgery physicians are unaware of predatory journals and not equipped to identify them [46]. Table 3 highlights the significance of predatory science undermining scientific integrity, as mentioned by almost all of the studied literature work.

Table 3. Major Impacts of Predatory Science

Key Impact of Predatory Science	Citations
Damaging Scientific Integrity	[13, 20, 37, 54, 57, 77, 84, 87, 90, 93]
Impact patient care and corrode public health	[20, 31, 37, 77, 84, 93]
Pollution in reputable databases	[57, 69]
Waste of money, manpower, and resources	[37, 69]
Reflecting inadequacies in self-regulation	[54]

From the above-discussed literature, there is no standard definition established so far that is acceptable to the global research community. It is challenging to avoid predatory journals without knowing what can or cannot be predatory. Most of these journals do not conduct proper peer-review processes and follow questionable practices, including charging a substantial publication fee known as APC. In addition to reviewed papers, we explored a few major predatory journal sites. They charge APC between $300 and $3500 with a processing time of 9 days to a couple of weeks, which is much shorter than traditional journals. Without a proper review system, unverified research does not have much credibility. As this kind of published work may have plagiarized, incorrect, unverified, or fake data and manipulated results, "predatory journals" are increasingly interfering with genuine research [42]. Retracted research and undetected publications with research misconduct make the probability of bad data higher and a more significant threat to scientific integrity [6, 65]. By 2015, there were estimated to be as many as 10,000 predatory journals worldwide. The ultimate risk is the altered results of synthesized knowledge because of rapidly increasing numbers of such predatory publications [13, 22, 37]. We observe that many research publications point out that predatory research can impact patient care and can corrode public health [20, 31, 37, 77, 84, 93]. However, there is no specific way to measure the actual patient harm caused by predatory research or medical AI. A cost analysis may provide insights into the net benefits or losses of research investments by NIH [1].

In 2013, John Bohannon's investigative fake medical paper was submitted to many publishers and got accepted by 60% of journals, including Elsevier [42]. A 2015 "Dr Fraud" experiment exposed the untrustworthy process of hiring editors and reviewers for predatory journals, as a fictitious scientist was offered the position by 40 journals and by 8 DOAJ [89]. The cancer journal *Tumor Biology* suffered a retraction of 107 papers after their fake peer review process was exposed [6]. More recently, 15 papers from *Tumor Biology* were retracted in 2021 for problems related to image manipulation or misuse [65]. A long-standing issue is becoming even more significant, undermining scientific integrity, and it needs immediate attention from all involved in genuine research efforts [90]. In general, academic institutes have some guidelines to avoid predatory journals, but that did not slow down the growth of predatory journals and predatory publications. There are more suspected predatory journals (10,406) than legitimate journals (10,077) in Cabell's list [37], which indicates the genuine concern of predatory literature polluting research literature repositories.

4.1 Predatory Science Infiltration in Trusted Resources

There are a couple of outstanding academic databases for biomedical research, medicine, and healthcare to provide credited references. The question is how much these credited resources are already infected by predatory publications. The concern is real, as predatory journals are already becoming part of PubMed [57, 69], which is serving as a source to develop other intermediate resources like NIH SemMedDB and Translational KGs to feed MedAI solutions. More specifically, Figure 2 demonstrate the threat of possible patient harm and increasing the overall healthcare burden, which defeats the purpose of utilizing AI in medicine. Figure 3 highlights the threat of

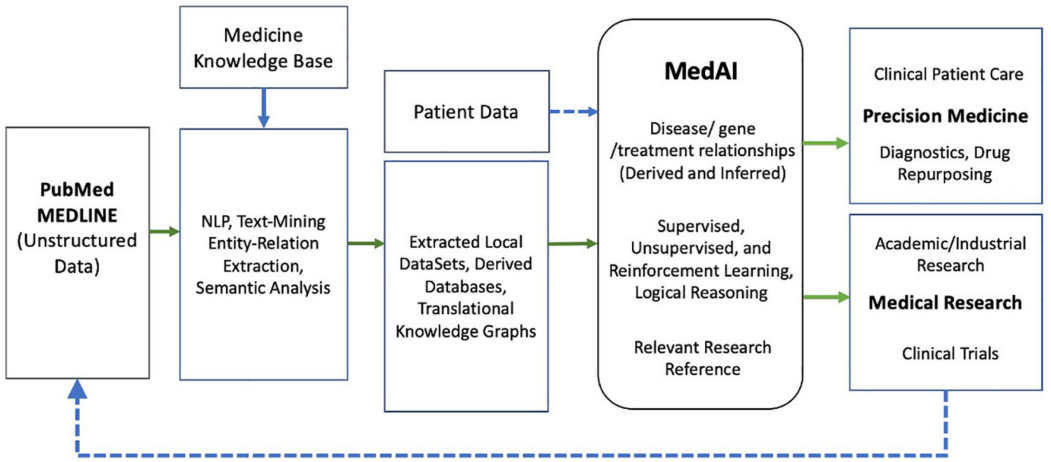

Fig. 3. Information flow among research literature, medicine knowledge base, and MedAI.

predatory research impacting MedAI solutions and patient care as well as influencing future research that will continue the cycle with an increased probability of larger data pollution in research literature repositories, further diminishing the confidence in MedAI output. Flawed or bogus conclusions may go undetected for an extended period and affect clinical practices before being retracted. It is challenging to maintain the integrity and security of research data to use as the basis of MedAI to employ in precision medicine and not to let it be predatory medicine.

5 MEDAI SOLUTIONS DERIVED FROM BIOMEDICAL LITERATURE

Most biomedical research is conducted and documented in natural language, adding ambiguity, context, synonyms, and variants to the recorded information. Exponentially growing biomedical information, adding over a million publications every year to PubMed, is challenging for manual curation. MedAI can tap the potential of research information in data-centric precision medicine. However, it is necessary to develop methods and tools to comprehend vast biomedical text and extract knowledge in machine-readable form to process and present synthesized and inferred information. PubMed has been a reference point in the research literature repositories. Hence, an apparent primary source input for many tools to address the automated curation of biomedical literature [55].

Figure 3 demonstrates the basic flow of information extraction from the research repository and how it can impact MedAI, clinical implementation, patient care, and future research. Text mining through NLP is one core process in extracting knowledge that varies in applied methods, datasets, and user interfaces dependent on the tool's goals. Automated curation utilizes various intermediate tools and datasets. Different components add functionality and cross-verification; it also increases the threat surface to protect and maintain the integrity of these solutions. We searched Google Scholar and PubMed for *biomedical literature-based medical decision-making*, with variations of *medical AI, medical tools, medical solutions, PubMed information extraction tools,* and *PubMed based medical AI solutions*. We searched for biomedical research literature-based tools developed since the mid-2000s to see how these solutions use the diverse technological developments to apply for information extraction, analysis, and knowledge presentation. We focus more on the adopted AI methods, data sources, scope of usage, and limitations with the current possibilities in the field to expand on. Table 4 presents a quick view of methods, data sources, components utilized, and accessibility of studied tools.

Table 4. Comparison of Clinical and Non-clinical Research Literature based MedAI Solutions

Tool	Year	Methods	Scope of Usage	Intermediate Source, Process or Supporting Tool	Availability
PICO [81]	2007	Text-mining, NLP, ML	Researchers, Clinicians	EBM-Evidence Based Medicine, UMLS, MetaMap, SemRep	Public
Semantic MEDLINE [79]	2011	Text mining, NLP, Semantic Analysis	Researchers, Clinicians	D2R Server, SPARQL, UMLS, SemRep, RDF graphs, SemMedDB	Free license for UMLS
GeneView [99]	2012	ML, NLP, text mining, relation extraction	Researchers	ChemIDPlus, NCBI Taxonomy, DrugBank/PharmGKB, Entrez Gene, Kegg, MeSH, dbSNP, Brno nomenclature, OMIM	Public
tmVar [102]	2013	CRF based ML, Entity recognition, tokenization, mutation identification (CRF) and regular expression patterns	Researchers, data curators	Tokenization, mutation identification, post-processing- regular expression for matching irregular and rare mention	Public
PubTator [103]	2013	Text mining, Entity recognition, Dictionary lookup, Annotation, ML	Researchers, data curators	tmVar, GeneTuKit, GenNorm, SR4GN, Dnorm	Public
Literome [72]	2014	NLP, Text mining, ML	Researchers, data curators	MS SPLAT-Statistical Parsing and Linguistic Analysis Toolkit -Taggers and parsers, sentiment analysis	Public
tmVar 2.0 [104]	2017	Text-mining, Pattern matching, dictionary lookup	Researchers	GNormPlus, dbSNP, clinvar	Public
LitVar [10]	2018	ML, Text-mining, Entity recognition	Researchers	tmVar, PubTator, TaggerOne, GNormPlus, SR4GN	Public
Iris.ai [41]	2018	Classification, word-usage frequencies, ranking algorithm on relevance	Researchers	Document Grouping, Core, Arxiv	Free Basic, Paid-Commercial
PubTerm [29]	2019	Co-occurrence and statistics of occurrences, annotation	Researchers, data curators	PubTator, DataTables,	Public
CancerMine [52]	2019	NLP, ML, Logistic Regression classifier, supervised learning algorithm, text mining- genotype-phenotype relationship, word frequencies, and semantic features	Researchers, Clinicians	Kindred relation classifier, PubTator, GNormPlus, tmVar, Dnorm	Public
mediKanren [68]	2020	Logical Reasoning, heuristics, indexing	Researchers, Clinicians	miniKanren, Racket, Knowledge graphs, SemMedDB, Precision Medicine	Public- on Github, proof of concept
LitSuggest [9]	2021	NLP, ML, Ridge classifier, elastic net classifier, Logistic Regression Classifier	Researchers, Curators	Pubmed, PubTator	Public, NIH Web-based tool
RTX-KG2 [107]	2022	Extract-Transform-Load approach, Biolink [101] Schema	Researchers, Clinicians	UMLS, SemMedDB, ChEMBL, DrugBank, Reactome, SMPDB, and 64 other knowledge sources	Public, code on Github, API

SEMANTIC MEDLINE [79] is a web-based application that integrates document retrieval, advanced NLP, automatic summarization, and visualization. RDF graphs are used in network-based bioinformatics analysis to (1) prioritize the candidate disease genes, (2) propose novel drug targets, (3) discover enriched biological functions/processes in disease-related genes, and (4) identify potential disease relationships within the context of the whole knowledge.

D2R Server is a tool for publishing relational databases on the Semantic Web. It enables RDF and HTML browsers to navigate the content of the database and allows us to query the database using the SPARQL semantic query language. Semantic MEDLINE web app shows the relationship between concepts and predicates, including references to the PubMed publication.

PICO provides ubiquitous access to clinical information and knowledge-based resources to answer clinical questions for evidence-based medicine. The PICO representation mainly relies on inherent semantic relationships between concepts to connect different elements. For example, with etiology questions, the connection between interventions and problems is assumed to be causal. Thus, the PICO frame is ill suited to questions that challenge these implicit relations [40, 81].

GeneView is a fast and powerful tool for navigating biomedical literature for keeping pace with the latest research results. The most important features of GeneView include the possibility to search for articles describing a specific biological entity, flexible ranking of results according to users' needs using optimized ranking algorithms, and intuitive visualization of semantically annotated texts. GeneView can considerably reduce the necessary effort for searching, reading, understanding, and annotating biomedical articles [99].

tmVar is a text-mining tool based on a conditional random field for extracting a wide range of sequence variants described at protein, DNA, and RNA levels. tmVar 2.0 implements the future direction from original tmVar research to improve the clinical relevance of dbSNP reference variants by text-mining PubMed [102, 104]. PubTator is a web-based text mining tool for assisting biocuration, providing automatic annotations of biomedical concepts such as genes and mutations

in PubMed abstracts and PMC full-text articles [103]. PubTerm is a simple system to acquire, curate, annotate, and categorize not only abstracts but also genes, diseases, species, drugs, sequence variants, journal, and author-related information [29].

The Iris.ai tool suite is explicitly aimed at researchers in the early phase of a new project [41]. They are especially suitable for interdisciplinary projects where the combination of knowledge from various research fields will be vital to the project's success. Iris.ai searches from a paper of the user's choice or a self-written problem statement. Iris.ai search is based on machine-extracted keywords, contextual synonyms, and hypernyms against more than 200 million Open Access papers, patents, and even EU-funded research projects.

Literome provides a cloud-based knowledge base for genomic medicine, featuring knowledge automatically curated from PubMed abstracts by an NLP system. It offers powerful search and exploration capabilities and a feedback mechanism to improve annotation and extraction continuously. Literome focuses on entities and relations most pertinent to genomic medicine. Users can browse and search the resulting knowledge base through the Literome website, which gets updated as new abstracts become available [72].

Litvar is a novel web-based tool that combines robust and advanced text mining with data integrating from PubMed, dbSNP, and ClinVar for an accurate search of variants and related gene, disease, and drug information. In addition, variants are often asserted with different names in publications; thus, a search in PubMed using only one name usually cannot retrieve all relevant articles [10]. LitVar uses tmVar, a high-performance variant name disambiguation engine, to normalize different forms of the same variant into a unique and standardized name so that all matching articles can be returned regardless of the use of a specific variant in the query. LitVar leverages the state-of-the-art literature annotation tool, PubTator, to provide critical biological relations among variations, drugs, genes, and diseases. LitVar supports searches by variant or variant with a gene found in the title, abstract, and full texts, including supplementary materials. For relation extraction, LitVar currently relies on sentence co-occurrence, and results may include false positives.

CancerMine is an automated approach using text-mining of the database of drivers, oncogenes, and tumor suppressors in different types of cancer [52]. CancerMine is using an ML approach logistic regression classifier on word frequencies and semantic features. A known relationship between genes and their role in a certain kind of cancer can help with early diagnosis and timely treatment. CancerMine can reduce manual effort and save time and cost to extract this information from the research literature.

mediKanren is a MedAI employing reasoning over the NIH SemMedDB knowledge base, using logical reasoning, heuristics, and indexing [68, 85]. mediKanren is a combination of miniKanren (Logic Programming Language), Racket (General-purpose Programming Language), a database SemMedDB, Knowledge Graphs, and a **graphical user interface (GUI)** to simplify data exploration for drug repurposing to assist precision medicine.

A more recent NIH tool, LitSuggest, can find and rank publications from research conducted in the Computational Biology Branch, NCBI/NLM, using advanced machine learning and information retrieval techniques. LitSuggest can automatically scan the literature weekly for new publications relevant to a user-specified topic [9].

RTX-KG2 is presented as the first open source knowledge graph that integrates UMLS, SemMedDB, ChEMBL, DrugBank, SMPDB, and 65 additional knowledge sources within a knowledge graph that conforms to the Biolink standard for its semantic layer and schema at the intersections of these databases. The current version of RTX-KG2 contains 6.4 M nodes and 39.3 M edges with a hierarchy of 77 relationship types from Biolink [101, 107].

5.1 Comparative Analysis of Tools Based on Biomedical Literature

We performed a manual analysis to compare methods, scope of usage, nature of tool (as source, process, intermediate or supporting tool), and availability. We compare these tools based on their objectives and scope, type of input data source and the data format, their limitations, and challenges and if they consider predatory research in source data or during the information extraction/presentation process. From the review of these tools, it is evident that there is an undeniable need to efficiently curate the abundant knowledge from the research literature to enhance decision-making in research and clinical settings. It also clarifies that NLP and text-mining algorithms are basic yet critical components in data curation to make it machine readable for any further utilization. It is interesting to observe that over the years, basic tools developed for information extraction [103, 104] have been being used by more complex data curation with targeted approach [10, 29, 52]. Many such tools utilize entity and relation extraction to assist automatic biocuration [10, 52, 99, 102–104]. Most of the tools use machine learning for data training and predictions, while mediKanren [68] uses logical reasoning, heuristics, and indexing. Supervised machine learning is the most commonly applied AI method using classifiers on keywords, co-occurrence, pattern matching, and dictionary lookup to extract and normalize entities and relationships. Few of these tools utilize similar intermediate systems like UMLS, GNormPlus, ClinVar, DNorm, and dbSNP for more efficient and comprehensive knowledge extraction from the bio-literature. GNormPlus is an end-to-end system that handles gene/protein name and identifier detection in biomedical literature, including gene/protein mentions, family names, and domain names. ClinVar aggregates information about genomic variation and its relationship to human health. dbSNP contains human single nucleotide variations, micro-satellites, and small-scale insertions and deletions along with publication, population frequency, molecular consequence, and genomic. The UMLS integrates and distributes key terminology, classification and coding standards, and associated resources to promote the creation of more effective and interoperable biomedical information systems and services. A recent development with integrating datasets to develop more consistent inputs is prone to the same threat of predatory data-induced data pollution if any component dataset is already exposed to such a threat. For example, RTX-KG2 is based on 70 databases with SemMedDB as a primary source. The most significant contributing knowledge source for RTX-KG2.7.3pre is SemMedDB, which has 19.3 M edges, about one-third of the total edges. SemMedDB is PubMed derived database, and PubMed is vulnerable to predatory research [57, 107]. We compare these MedAI solutions, broadly on their objectives and scope, their data sources, and data formats. We also discuss the limitations and challenges of these tools that can affect the efficiency and integrity of these solutions.

5.1.1 Objectives and Scope. Some tools are more focused on providing ready support to clinicians based on derived or inferred relationships between diseases, genes, and drugs [52, 68, 79, 81] while others are primarily for data curation [29, 102–104]. The Iris.ai tool is explicitly aimed at researchers to provide relevant research literature based on research problem formulation, especially for interdisciplinary projects where the combination of knowledge from multiple research fields can be vital [41]. LitSuggest can help with the biomedical literature recommendations and curation [9]. These tools can be used independently, and more advanced systems utilize the work done through modular tools as subsystems.

5.1.2 Input Data Sources and Data Formats. PubMed as a primary data source was the key criterion to study these tools, but this is worth noting that these tools work with different data formats. For example, many of them extract information from PubMed directly and incorporate other curated domain-specific datasets for genetics, diseases, and drugs to present known and inferred

knowledge. Semantic MEDLINE and mediKanren utilize PubMed-derived SemMedDB and Knowledge Graphs. Some other tools employ other databases in combination with PubMed data. Most of these tools are web-based, with regular updates to the data with growing biomedical literature. mediKanren is still evolving but currently can operate on a moderately advanced laptop with a local GUI interface with local datasets on disk to assist physicians in real-life clinic scenarios [85]. RTX-KG2 is using the largest set of KGs among current solutions and NIH translational data project is expected to be a common uniform standard dataset for future MedAI solutions [101, 107]. LitSuggests is directly extracting information from PubMed, and it can have a direct impact on increasing predatory publications [9].

5.1.3 Limitations and Challenges. Though all tools acknowledge the significance of research literature and data curation, many of these tools face the challenges and limitations of data and algorithms used in the process. The sheer volume of the medical literature and the high cost of expert curation forces current curated variant information in existing databases to be incomplete and out of date [104]. Many of the studied tools work with only titles and abstracts to extract the information. However, more information exists in full text, and these tools may have incomplete or missing information. These tools are also bound to the accuracy of the applied text mining algorithms, which are known to be imperfect in both entity recognition, and relation extraction [10]. As tools are primarily trained on abstracts for entity tagging, their full-text results may be inferior due to their structure and complexity. Another common limitation to using these tools is the domain knowledge, especially with PICO and Iris.ai; results are dependent on how well the problem is formed. Other tools' outputs may also be more valuable to the researchers and clinicians well versed with background knowledge to know what to look for even if the information exists.

All these data-driven knowledge extraction tools heavily depend on the integrity of the research publications hosted by PubMed. Possible pollution in terms of bogus, invalid, manipulated research either through predatory journals or research misconduct cases may cripple the chain of trust, and results cannot be trusted. Any vulnerabilities in lower-level tools may impact the functioning of complex tools using these tools in the process.

This review of research literature-based tools clarifies that none of the studied literature on tools discusses the possibility of data pollution in PubMed or any other intermediate data sources. As there is no current consideration of input data pollution, that confirms the potential threat that predatory research mixed with genuine research in a research repository may impact the output of these tools. To build more robust MedAI tools, it is important to acknowledge the threat and then build the defense to mitigate the threat of predatory research-induced data pollution.

6 ATTACKS AND IMPACT OF PREDATORY SCIENCE ON MEDICINE

On April 11, 2018, the first AI computer vision diagnostic system without a human clinician was approved by the U.S. **Food and Drug Administration (FDA)** [70], and the FDA approved 29 AI-based medical systems between 2016 and early 2020. There has been an immense interest in MedAI since 2010 with a 20-fold increase in AI/ML-based research publications from 2010 to 2019 [15]. On the one hand, this acknowledged the significance of AI in future medicine; on the other hand, it raised the known concerns of adversarial examples even higher, especially in the absence of clear ethical and legal consequences when a machine fails.

We present a basic understanding of the most common threats and attacks that can impact MedAI solutions, and then we compare the studied works, based on their scope, AI method(s), attack type, and key impact. Studied papers are either specific to healthcare or generalized but can be highly damaging in healthcare [24, 26].

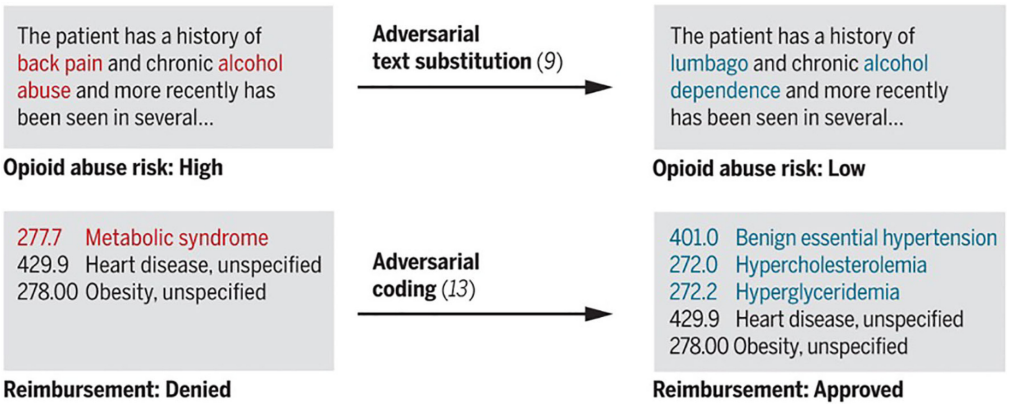

Fig. 4. Text-based adversarial attack to manipulate MedAI output [26].

6.1 Vulnerabilities and Threats to MedAI Solutions

Adversarial examples are known threats, especially in computer vision to alter the output with unsuspecting minor pixels manipulations [35], and a similar approach is expandable in text-based AI algorithms and systems. This somewhat new threat has not been mapped yet to the depth of the possible destruction it may cause when applied to the medical research literature. Appropriate peer review is essential in validating and approving medical diagnostics research, which may require public access to the architecture and methods to maintain transparency but that provides an opportunity for more targeted adversarial attacks [26]. Medical staff may not have advanced knowledge to build secure systems, but internal medical staff may develop applications to keep usability simple with no inbuilt defense mechanism. It is vital to know how model deployment can enable end-users to submit data into a running ML algorithm to subtly influence its behavior without ever knowing or accessing the model or the hosting IT environment [26].

While image-based adversarial attacks are well discussed in the literature, now more studies are finding vulnerabilities to exploit in text-based adversarial attacks. Our understanding is that if the input is polluted but undetected, it is difficult to identify the possible attacks and the defense. Figure 4 shows how text manipulation can turn a high-risk observation into a low-risk event, which will hamper the needed attention to the patient [26]. Especially in the case of opioid abuse, it can be life-threatening in the absence of proper medication assistance. The other scenario presents a motivation to get the reimbursement approved, which can be achieved through adversarial adding of similar yet different medical codes as those are interpreted differently by the AI [26].

It is difficult to define perturbations in symbolic and discrete research literature texts. If an attacker can map the discrete to continuous data, then attacks from computer vision may be applicable to the text. The unperceivable textual adversaries are complex as even minor changes may be noticeable. Also, they can be tracked or detected through many languages reviewing tools through spelling-check or grammar-check. The semantics of a word or sentence may be changed in context and sentiment even by small text changes that are not preferred for designing adversarial attacks. Due to these differences, current state-of-the-art textual attackers either carefully adjust the known computer vision-based methods by enforcing additional constraints or propose novel methods using different techniques. Subtle, undetected, and unsuspected input pollution is necessary for the success of an adversarial attack [76].

Figure 5 shows how Deep Neural Network–based text interpretation using NLP can be manipulated by evasive, minimal yet well-crafted adversarial examples to get completely different output

Task: Sentiment Analysis. ***Classifier:*** Amazon AWS. ***Original label:*** 100% Negative. ***Adversarial label:*** 89% Positive.

Text: I watched this movie recently mainly because I am a Huge fan of Jodie Foster's. I saw this movie was made right between her 2 Oscar award winning performances, so my expectations were fairly high. ~~Unfortunately~~ **Unf0rtunately**, I thought the movie was ~~terrible~~ **terrib1e** and I'm still left wondering how she was ever persuaded to make this movie. The script is really ~~weak~~ **wea k**.

Fig. 5. Change of 100% negative reviews to 89% positive in sentiment analysis [53].

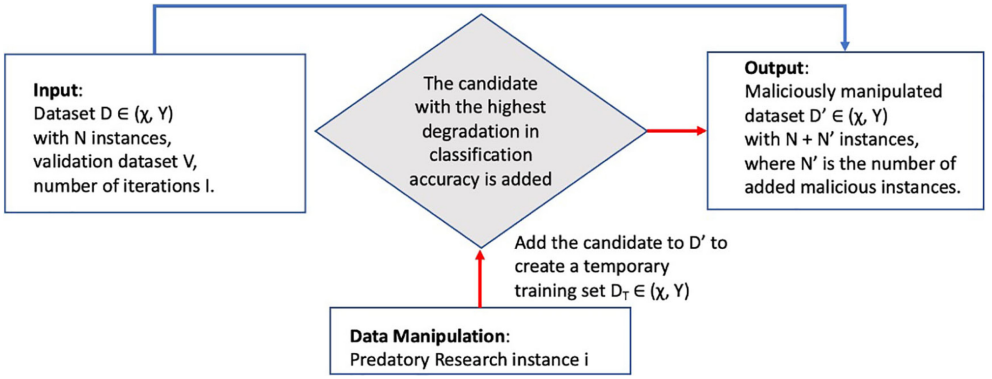

Fig. 6. Algorithm-independent predatory research induced data manipulation attack [62].

from the sentiment analysis. The changes look like typos, with less suspicion, changing only a digit or letter strategically. However, these changes replace a 100% negative result with a 89% positive one [53, 108].

6.2 Type of Attacks Impacting MedAI Solutions

An AI pipeline generally consists of data collection, data pre-processing, model training, model inference, and system integration [95]. Each phase of the AI pipeline can be vulnerable to various security threats. In this survey, we are focusing only on data collection and data preprocessing phases to study if it can impact the MedAI output. The major security risks in the data collection phase include data biases, manipulated data, and data breaches. In terms of research repositories, data collection represents the published research articles and data presented in these publications. Every time a predatory publication is added to a reputable research repository, data pollution may have a larger influence to impact overall conclusions based on data extracted from these research repositories. The data pre-processing phase covers any derived datasets from research repositories to use as MedAI input.

Figure 6 is adopted from Algorithm 1 of Mozaffari et al. and simplified to demonstrate the threat of algorithm-independent attack through input data manipulation [62]. The original dataset D belongs to (X, Y) with N instances, where X represents an instance's attributes and Y is the class label. The attack adds N' malicious instances to the original dataset to develop a manipulated dataset D' belongs to (X, Y) with $N + N'$ instances. For each candidate, the algorithm evaluates its classification accuracy on the validation set. The candidate with the highest degradation in classification accuracy is selected and added to the dataset. This generic and algorithm-independent attack can be applied to a wide range of medical datasets and AI algorithms. The robust and modified algorithm may defeat algorithm-specific attacks, but algorithm-independent attacks pose a larger threat. An attacker may not need to know any specifics of the applied algorithm. However, knowledge of the algorithm can increase the efficacy of such attacks [62]. NIH-developed translational databases are

to provide extracted medical research information in a standard machine-readable format so that more applications can utilize available information without redoing the extraction process each time separately [101]. In this case, if information extracted from predatory publications is part of such intermediate datasets, then it has an even larger scope to impact MedAI solutions.

Adversarial attacks can be categorized based on methodology, application, algorithm, and data. Major methodological categories of attack methods are black-box and white-box. We briefly discuss the attack categories more specifically toward text based as applicable to extract information from research literature and how predatory science can exploit these methods to impact research and clinical MedAI systems.

Poisoning Attacks/Training Phase Attacks/Causative Attacks: During the training, an adversary carefully manipulates the training data to compromise the learning process. An adversary can change the value of the input data to a certain threshold using data injection, modification, and logic corruption methods to manipulate the training data. Data injection pollutes the training data, while the modification is poisoning the data before the training, and logic corruption can temper the model itself. This way, an adversary can bias the overall learning process of the ML model applied to MedAI to misdiagnose the test data to mislead the suggested treatment, which may harm the patient [63].

Evasion Attacks/Testing Phase Attacks/Exploratory Attacks: In an evasion attack, the adversary tries to deceive the MedAI by enforcing adversarial samples during the testing phase. An adversary does not influence the training data but can access the ML model to obtain sufficient information. As a result, it attacks the ML model and manipulates it to misclassify the patient status in a MedAI [96]. White-box attacks and black-box attacks are two major categories of evasion attacks.

White-box attack requires access to the model's complete information, including architecture, parameters, loss functions, activation functions, input, and output data. White-box attacks typically approximate the worst-case attack for a particular model and input, incorporating a set of perturbations. *Logical attack* is a white-box attack corrupting the algorithm itself for generating malfunctioned output. White-box adversary strategy is often very effective as it can exploit the known inputs, training processes, and algorithms. ML models used in different medical applications can be vulnerable to white-box attacks impacting accuracy drop and attack success rate [63].

Black-box attack does not require the details of the algorithm, but it can access the input and output. This type of attack often relies on heuristics to generate adversarial examples. Concatenation, edit, paraphrased-based, GAN-based, substitution, and reprogramming adversaries can be applied to target character, word, sentence, or API to impact different models [108]. It is more practical as in many real-world applications, the detail of the system is a black box to the attacker. Black-box methods are further classified as machine reading comprehension; question answering; visual question answering; dialogue generation; text classification; machine translation; sentiment analysis; natural language inference; textual entailment; malware detection. Each of these black-box attacks can impact MedAI input data, and information extracted in the process, and has the potential to influence the MedAI output.

In an active adversarial attack scenario, predatory publications with a targeted approach can be produced automatically in bulk through next-gen NLP text-generator tools like GPT-3 [19, 36]. The MIT "SCIgen" project verifies a similar threat in the computer science field, where users could generate a paper, and it got accepted in multiple conferences [94]. A targeted adversarial attack on a rare disease can make it look valid while injecting fake data and findings with alternative conclusions. The attacker can approach multiple predatory research publishing venues to publish much work validating these new findings. Based on the current exploratory threat, this active attack is viable and capable of shifting the weight on the concept understood by the MedAI algorithm. Once the algorithm is fed onto these new data, the output can be compromised to support

Table 5. A Summary of Attack Types, Affected AI Methods, Applications, and Key Impacts

Work	Application	AI Method(s)	Attack Type	Key Impact
Mozaffari-Kermani et al. [62], 2015	Healthcare, Biomedicine	Naive Bayes decision tree, Nearest-neighbor classifier, Multilayer Perception	Poisoning Attack	Distrust in MedAI, Patient distress.
Papernot et al. [67], 2018	Clinical data, Network Intrusion, Autonomous vehicles	SVM, Random Forest Classifier	Exploratory attacks, injection, modification, input poisoning	Confidentiality, Integrity, and Availability
Biggio et al. [16], 2018	Computer Vision and Cyber Security	ML, Deep Learning	Evasion attack, Poisoning Attack	Integrity, Availability, Privacy/Confidentiality
Duddu [24], 2018	Cyber Warfare	Supervised, Unsupervised, and Reinforcement Learning	Evasion attacks, Poisoning Attacks, black-box attacks	integrity, availability, and privacy
Finlayson et al. [26], 2018	Computer vision and medical imaging	Deep Learning, Neural Networks	Projected Gradient Descent, black-box, white box	Misclassification by accurate classifiers with or without knowing model
Sun et al. [96], 2018	Health Informatics	Deep Learning, Predictive Modeling	Iterative attacks, optimization-based attacks, FGSM	Misclassification from alive to deceased
Finlayson et al. [27], 2019	Medical Diagnostics and Decision Support	Deep Learning	Evasion attack, Poisoning Attack	Insurance Frauds, Biased drug trials
Ngiam et al. [64], 2019	Big Data and ML in clinical healthcare delivery	Deep Learning, Deep Neural Networks	Neural Networks, Supervised ML	Data privacy and security, Fear of replacing humans

predatory publications on the subject. This approach is hazardous for rare and unknown diseases, as not much data or information can cross-validate.

As we study the different attacks and vulnerabilities of MedAI solutions, we selected diverse yet relevant research under the scope of our work. Table 5 provides a summary of the literature studied on attack types that can impact the integrity and security of AI-based solutions, especially, applicable in healthcare. Mozaffari-Kermani et al. and Sun et al. presented how different attack types can affect multiple AI algorithms causing distrust in MedAI solutions and patient distress [62, 96]. Finlayson et al. demonstrated that medical diagnostics and decision support using Deep Learning is vulnerable to poisoning, evasion, black-box, and white-box attacks causing insurance frauds and biased drug trials [26, 27]. Vulnerability to exploratory, injection and input poisoning attacks threatens the integrity, privacy, availability, and security of MedAI solutions using a range of AI algorithms and methods, including supervised, unsupervised, reinforcement learning, ML, and DL [16, 24, 64, 67].

The most common adversarial attack is on classification algorithms to mislead the system to misclassify by polluted inputs, corrupted predictive models, or exploiting the algorithm's vulnerabilities. Other primary application text-specific categories are machine translation, machine comprehension, text summarization, text entailment, POS tagging, relation extraction, and dialogue system. To adopt the most effective strategy for target data, model, and algorithm, the adversary can fine-tune the attacks by *Iterative attacks* or *Optimization-based attacks* by generating specific adversarial examples for focused attacks on predictive models [96]. In the case of a research literature-based MedAI system, even subtle pollution can be critical in the era of precision medicine with a very targeted approach. The risks of having any possibility of manipulated biased results can be devastating in actual patient care. The following section discusses some compelling cases highlighting predatory science's short- and long-term impact on medical practices.

7 IMPACT OF PREDATORY SCIENCE ON MEDICINE PRACTICES

It is worth looking at some high-profile frauds in medicine to get a sense of how technological advances and manipulation of such systems can impact medical practices and how critical it is to ensure the integrity of MedAI solutions and defining liabilities.

Impact on Clinical Research and Research Repositories: A study shows that over a decade, 9,189 patients were treated in 180 retracted primary studies. Not only were these patients put at risk, but these studies influenced other secondary trials to recruit more patients [92]. The annually increasing number of predatory publications increases the probability of data pollution in trusted research repositories. It is also observed that once a predatory venue is part of the reputable research repository, it publishes more papers, which allows predatory research to slip through with minimal or no review and get mixed in with genuine research [57]. This trend puts a damaging distrust in research literature repositories, as it is unknown how much fraudulent research literature exists from legitimate or predatory journals.

Impact on Advanced MedAI solutions: We observe that various medical AI tools use PubMed as a primary data source directly or as an intermediate resource. When such a trusted source gets infiltrated with unreliable data, it is necessary to evaluate the impact of data pollution on MedAI functioning. Apparently, without having awareness and acknowledgment of predatory science, MedAI may not have any defense mechanism. In the absence of any defense against predatory science, the integrity of MedAI is questioned to provide reliable output.

Impact on Healthcare Decision-Making: It is interesting that the motivation in research fraud is irrespective of the attacking method, like performing unnecessary dermatological surgeries for money, which is image based but can also be applied as text based [80]. For example, a research paper from a predatory journal claims that some rare skin cancer can be treated by the drug "d." If a paper is predatory but exists in a trusted repository like PubMed, it could be crawled through PubMed Central, tagged by MEDLINE, and moved to an intermediate database such as SemMedDB or translational database mapping. However, including such a paper in the input of a MedAI system could potentially pollute the output and reduce the accuracy of the solution. If there is no cross-validation, then it is a high probability that the system will choose the reference. Being desperate for any health aid, a patient may trust this new possible intervention to give it a try.

Impact on Clinical Care and Public Health: There are many known cases where a drug was promoted to cure some disease but not outliers in the trials were not disclosed or false claims were made through fraudulent clinical trials [30, 43]. Anesthesiologist Scott Reuben and family medicine physician Anne Kirkman Campbell are two among many others to commit such fraud for money, fame, and position, causing direct harm to patients, including loss of lives [18, 83]. Misleading conclusions can deprive the community of needed preventive care, which can have a long-term impact on public health. Multiple studies about certain vaccines causing disorders in children baffled the medical community, as well as the general public for more than a decade [56, 74].

8 DISCUSSION AND FUTURE DIRECTIONS

In medicine, ground truth is often ambiguous, and patient care is still primarily provider dependent and often subjective even after all the assisting tools, including MedAI solutions. In such trust-based settings, mistrust can damage the patient and provider relationship and affect patient care. We understand that utilizing AI to tame the scientific knowledge for precision medicine can work against it entirely if the medical and computer science community is not proactive in acknowledging and developing a robust defense against predatory science invasion in the research literature. Medical AI systems are vulnerable to adversarial attacks because of sensitive and complex healthcare data from heterogeneous medical and technical sources.

As discussed in this work, predatory science is on the rise, and that can make the infiltration even higher in PubMed-like repositories. Higher data pollution will pose a higher probability of impacting MedAI tools using the research literature. It is challenging to keep up with the marking or removal of predatory research from trusted repositories.With other technological advancements like Fog Computing and Edge Computing, there are newer open challenges to utilize the power of these solutions specific to medical data handling in real time [32]. However, these solutions are still in development, and in the future, an analysis of applications and security analysis would be relevant to identify solution-specific threats.

There is an apparent fear of relying more on machines and ignoring the value of the human component. However, even with all the advancements, MedAI solutions have a long way to establishing the needed trust and addressing financial, ethical, and legal aspects. On the positive side, the contribution of MedAI is getting well acknowledged and providing an exciting opportunity for physicians, researchers, and computer scientists to work together, unwinding new possibilities in healthcare. It is essential to establish trust in MedAI, especially the research literature data source, as no algorithm can extract the trusted output if inputs are polluted and not trustworthy [106].

We plan to look at other security vulnerabilities to develop a better defense mechanism against data pollution in the era of a plethora of information. Studying how predatory research information is navigating through publication channels and MedAI solutions and eventually altering the clinical decisions affecting patient care will be the focus of our future work. MedAI solutions need to take advantage of all available information, especially open-access research and social media. However, in handling such information platforms, future trustworthy information extraction will have greater challenges and higher stakes. From a broader perspective, the survey indicates the possible failure of any state-of-the-art MedAI logic to deliver the intended output if the inputs are polluted and left unidentified.

9 CONCLUSIONS AND SUMMARY

We address the research gap in identifying the impact of predatory science on MedAI solutions and patient care. Though it may be challenging to measure the extent of actual patient harm as a direct impact of predatory science, it is intended to demonstrate the possible damage undermining trust in MedAI solutions and their practical adaptation in clinical care. A few key findings from this survey are as follows:

- In the absence of a defined strategy to avoid predatory or retracted research publications, numbers are on the rise, and so they serve to pollute MedAI inputs.
- No existing standard guidelines to mitigate the threat of predatory research for extracting information or preparing intermediate research databases, which are being utilized by a wide range of MedAI solutions.
- Most of the work discussing security and integrity talks more about the possibility of exploiting vulnerabilities to fool AI algorithms into misclassifying, but none of the tools or attacking studies discuss the possibility of data pollution in research literature data sources.
- Medical practices and trends are highly influenced by medical research, and undetected predatory research can harm public health for a prolonged period.

We summarize the contributions of our work as follows:

- **Contribution to the Theory:** We create greater awareness of predatory research–induced data pollution in a trusted research repository. We believe that our work provides a good base reference to study the problem, its significance, and the potential threat.
- **Contribution to the Practice:** We explain how medical research influences medical practices, and how medical AI is necessary for modern medical practices. We present that if the

core data input get manipulated, then it can impact the medical AI performance, medical AI adaptation, and future research and overall influence medical practices.

- **Contribution to the community:** If the threat is not mitigated, then targeted attacks can turn into severe threats, putting patients' lives at risk. Once trust is diminished in research literature-based medical AI solutions, that will hinder the adaptation of these solutions in practical settings and thus diminish the intended service to the community. More robust future MedAI can provide great assistance to modern medicine and the community.

From our analysis of the literature on the predatory science, medical AI tools based on research repositories, and AI vulnerabilities, we can see how technological advances help medical research, curating knowledge, and then using this knowledge to advance further in medical decision-making. However, the rising threat of predatory research can pollute these trustworthy research literature repositories and that can potentially impact all those medical AI solutions that are using PubMed as a critical and trusted data source. Our work raises awareness about missing defense against predatory research-induced data pollution, and we expect that our work will initiate the difficult discussion at a larger level and help to develop feasible defense strategies. We are confident that verifying the threats of any sort early in the process will only help develop a more robust MedAI solution for taking precision medicine to the next level in broader settings.

REFERENCES

[1] 2021. NIH-Artificial Intelligence—Machine Learning, and Deep Learning. Retrieved from https://www.nibib.nih.gov/research-funding/machine-learning.

[2] 2021. PubMed. Retrieved from https://pubmed.ncbi.nlm.nih.gov/.

[3] 2023. Definition of Research Misconduct. Retrieved March 2, 2023 from https://ori.hhs.gov/definition-misconduct.

[4] 2023. Directory of Open Access Journals (DOAJ). Retrieved March 2, 2021 from https://doaj.org/.

[5] 2023. National Human Genome Research Institute. Retrieved March 2, 2023 from https://www.genome.gov/dna-day/15-ways/rare-genetic-diseases.

[6] Enago Academy. 2021. Fake Peer Review Leads to Massive Retractions. Retrieved from https://www.enago.com/academy/fake-peer-review-leads-to-massive-retractions/.

[7] Muhammad Afzal, S. M. Riazul Islam, Maqbool Hussain, and Sungyoung Lee. 2020. Precision medicine informatics: Principles, prospects, and challenges. *IEEE Access* 8 (2020), 13593–13612.

[8] Sümeyye Akça and Müge Akbulut. 2021. Are predatory journals contaminating science? An analysis on the Cabells' Predatory Report. *J. Acad. Libr.* 47, 4 (2021), 102366.

[9] Alexis Allot, Kyubum Lee, Qingyu Chen, Ling Luo, and Zhiyong Lu. 2021. LitSuggest: A web-based system for literature recommendation and curation using machine learning. *Nucl. Acids Res.* 49, W1 (2021), W352–W358.

[10] Alexis Allot, Yifan Peng, Chih-Hsuan Wei, Kyubum Lee, Lon Phan, and Zhiyong Lu. 2018. LitVar: A semantic search engine for linking genomic variant data in PubMed and PMC. *Nucl. Acids Res.* 46, W1 (2018), W530–W536.

[11] Fatima Alshehri and Ghulam Muhammad. 2020. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access* 9 (2020), 3660–3678.

[12] Gokhan Bakal, Preetham Talari, Elijah V. Kakani, and Ramakanth Kavuluru. 2018. Exploiting semantic patterns over biomedical knowledge graphs for predicting treatment and causative relations. *J. Biomed. Inf.* 82 (2018), 189–199.

[13] Robert E. Bartholomew. 2014. Science for sale: The rise of predatory journals. *J. Roy. Soc. Med.* 107, 10 (2014), 384.

[14] Jeffrey Beall. 2012. Predatory publishers are corrupting open access. *Nature* 489, 7415 (2012), 179–179.

[15] Stan Benjamens, Pranavsingh Dhunnoo, and Bertalan Meskó. 2020. The state of artificial intelligence-based FDA-approved medical devices and algorithms: An online database. *NPJ Digit. Med.* 3, 1 (2020), 1–8.

[16] Battista Biggio and Fabio Roli. 2018. Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recogn.* 84 (2018), 317–331.

[17] Olivier Bodenreider. 2004. The unified medical language system (UMLS): Integrating biomedical terminology. *Nucl. Acids Res.* 32, suppl_1 (2004), D267–D270.

[18] Brendan Borrell. 2009. A Medical Madoff: Anesthesiologist Faked Data in 21 Studies. Retrieved from https://www.scientificamerican.com/article/a-medical-madoff-anesthestesiologist-faked-data/.

[19] Tom Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared D. Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell and others. 2020. Language models are few-shot learners. *Advances in Neural Information Processing Systems* 33 (2020), 1877–1901.

[20] Arthur L. Caplan. 2015. The problem of publication-pollution denialism. In *Mayo Clinic Proceedings*, Vol. 90. Elsevier, 565–566.
[21] Xiaojun Chen, Shengbin Jia, and Yang Xiang. 2020. A review: Knowledge reasoning over knowledge graph. *Expert Syst. Appl.* 141 (2020), 112948.
[22] Kelly D. Cobey, Manoj M. Lalu, Becky Skidmore, Nadera Ahmadzai, Agnes Grudniewicz, and David Moher. 2018. What is a predatory journal? A scoping review. *F1000Research* 7 (2018).
[23] Ricardo Jorge Dinis-Oliveira. 2021. Predatory journals and meetings in forensic sciences: What every expert needs to know about this "parasitic" publishing model. *Forens. Sci. Res.* 6, 4 (2021), 303–309.
[24] Vasisht Duddu. 2018. A survey of adversarial machine learning in cyber warfare. *Def. Sci. J.* 68, 4 (2018), 356.
[25] J. C. Dufour, J. Mancini, and M. Fieschi. 2009. Searching for evidence-based data. *J. Chir.* 146, 4 (2009), 355–367.
[26] Samuel G. Finlayson, Hyung Won Chung, Isaac S. Kohane, and Andrew L. Beam. 2018. Adversarial attacks against medical deep learning systems. arXiv:1804.05296. Retrieved from https://arxiv.org/abs/1804.05296.
[27] Samuel G. Finlayson, Hyung Won Chung, Isaac S. Kohane, and Andrew L. Beam. 2019. Adversarial Attacks on Medical Machine Learning. Retrieved from https://science.sciencemag.org/content/363/6433/1287.full.
[28] Tove Faber Frandsen. 2017. Are predatory journals undermining the credibility of science? A bibliometric analysis of citers. *Scientometrics* 113, 3 (2017), 1513–1528.
[29] José Garcia-Pelaez, David Rodriguez, Roberto Medina-Molina, Gerardo Garcia-Rivas, Carlos Jerjes-Sánchez, and Victor Trevino. 2019. PubTerm: A web tool for organizing, annotating and curating genes, diseases, molecules and other concepts from PubMed records. *Database: J. Biol. Datab. Curat.* 2019 (2019).
[30] Charles S. Garver R. [n. d.]. FDA Lets Drugs Approved on Fraudulent Research Stay on the Market. Retrieved March 19, 2021 from https://www.scientificamerican.com/article/fda-let-drugs-approved-on-fraudulent-research-stay-on-market/.
[31] Stephen L. George and Marc Buyse. 2015. Data fraud in clinical trials. *Clin. Invest.* 5, 2 (2015), 161.
[32] Sukhpal Singh Gill, Minxian Xu, Carlo Ottaviani, Panos Patros, Rami Bahsoon, Arash Shaghaghi, Muhammed Golec, Vlado Stankovski, Huaming Wu, Ajith Abraham, et al. 2022. AI for next generation computing: Emerging trends and future directions. *Internet Things* 19 (2022), 100514.
[33] Geoffrey S. Ginsburg and Kathryn A. Phillips. 2018. Precision medicine: From science to value. *Health Affairs* 37, 5 (2018), 694–701.
[34] Fiona Godlee, Jane Smith, and Harvey Marcovitch. 2011. Wakefield's Article Linking MMR Vaccine and Autism Was Fraudulent. Retrieved from https://www.bmj.com/content/342/bmj.c7452/.
[35] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. 2014. Explaining and harnessing adversarial examples. arXiv:1412.6572. Retrieved from https://arxiv.org/abs/1412.6572.
[36] GPT3. [n. d.]. Text-generating Algorithm from OpenAI. Retrieved from https://www.digitaltrends.com/features/openai-gpt-3-text-generation-ai/.
[37] Agnes Grudniewicz, David Moher, Kelly D. Cobey, Gregory L. Bryson, Samantha Cukier, Kristiann Allen, Clare Ardern, Lesley Balcom, Tiago Barros, Monica Berger, et al. 2019. Predatory Journals: No Definition, No Defence. Retrieved from https://www.nature.com/articles/d41586-019-03759-y?sf225811500=1.
[38] Pavel Hamet and Johanne Tremblay. 2017. Artificial intelligence in medicine. *Metabolism* 69 (2017), S36–S40.
[39] Arjen Hoogendam, Anton F. H. Stalenhoef, Pieter F. de Vries Robbé, and A. John P. M. Overbeke. 2008. Analysis of queries sent to PubMed at the point of care: Observation of search behaviour in a medical teaching hospital. *BioMed Centr. Med. Inf. Decis. Mak.* 8, 1 (2008), 1–10.
[40] Xiaoli Huang, Jimmy Lin, and Dina Demner-Fushman. 2006. Evaluation of PICO as a knowledge representation for clinical questions. In *AMIA Annual Symposium Proceedings*, Vol. 2006. American Medical Informatics Association, 359.
[41] IRIS.AI. [n. d.]. Retrieved February 24, 2021 from https://iris.ai/.
[42] Oransky Ivan. 2013. Science Reporter Spoofs Hundreds of Open Access Journals with Fake Papers. Retrieved February 24, 2021 from https://retractionwatch.com/2013/10/03/science-reporter-spoofs-hundreds-of-journals-with-a-fake-paper/.
[43] Usman Jaffer and Alan E. P. Cameron. 2006. Deceit and fraud in medical research. *Int. J. Surg.* 4, 2 (2006), 122–126.
[44] Shaoxiong Ji, Shirui Pan, Erik Cambria, Pekka Marttinen, and S. Yu Philip. 2021. A survey on knowledge graphs: Representation, acquisition, and applications. *IEEE Trans. Neural Netw. Learn. Syst.* 33, 2 (2021), 494–514.
[45] Fei Jiang, Yong Jiang, Hui Zhi, Yi Dong, Hao Li, Sufeng Ma, Yilong Wang, Qiang Dong, Haipeng Shen, and Yongjun Wang. 2017. Artificial intelligence in healthcare: Past, present and future. *Stroke Vascul. Neurol.* 2, 4 (2017).
[46] Kantenga Dieu Merci Kabulo, Ulrick Sidney Kanmounye, Sarah Mutomb Ntshindj, Kingombe Yengayenga, Berjo Dongmo Takoutsing, Patrice Ntenga, Luxwell Jokonya, Jeff Ntalaja, Ignatius Esene, Aaron Musara, et al. 2022. Vulnerability of African neurosurgery to predatory journals: An electronic survey of aspiring neurosurgeons, residents, and consultants. *World Neurosurg.* 161 (2022), e508–e513.

[47] Sara Kaviani, Ki Jin Han, and Insoo Sohn. 2022. Adversarial attacks and defenses on AI in medical imaging informatics: A survey. *Expert Syst. Appl.* (2022), 116815.
[48] Steve Van Kuiken, Basel Kayyali, and David Knott. 2013. The Big-data Revolution in US Health Care: Accelerating Value and Innovation. Retrieved from https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care.
[49] Jai Kotia, Adit Kotwal, and Rishika Bharti. 2019. Risk susceptibility of brain tumor classification to adversarial attacks. In *International Conference on Man–Machine Interactions*. Springer, 181–187.
[50] C. Krittanawong. 2018. The rise of artificial intelligence and the uncertain future for physicians. *Eur. J. Intern. Med.* 48 (2018), e13–e14.
[51] Shinjini Kundu. 2021. AI in medicine must be explainable. *Nat. Med.* 27, 8 (2021), 1328–1328.
[52] Jake Lever, Eric Y. Zhao, Jasleen Grewal, Martin R. Jones, and Steven J. M. Jones. 2019. CancerMine: A literature-mined resource for drivers, oncogenes and tumor suppressors in cancer. *Nat. Methods* 16, 6 (2019), 505–507.
[53] Jinfeng Li, Shouling Ji, Tianyu Du, Bo Li, and Ting Wang. 2018. Textbugger: Generating adversarial text against real-world applications. arXiv:1812.05271. Retrieved from https://arxiv.org/abs/1812.05271.
[54] Stephen Lock. 1988. Fraud in medicine. *Br. Med. J.* 296, 6619 (1988), 376.
[55] Zhiyong Lu. 2011. PubMed and beyond: A survey of web tools for searching biomedical literature. *Database* 2011 (2011).
[56] Herve Maisonneuve and Daniel Floret. 2012. Wakefield's affair: 12 years of uncertainty whereas no link between autism and MMR vaccine has been proved. *Press. Med. (Paris, France: 1983)* 41, 9 Pt 1 (2012), 827–834.
[57] Andrea Manca, David Moher, Lucia Cugusi, Zeevi Dvir, and Franca Deriu. 2018. How predatory journals leak into PubMed. *Can. Med. Assoc. J.* 190, 35 (2018), E1042–E1045.
[58] Yondell B. Masten and Alyce S. Ashcraft. 2016. The dark side of dissemination: Traditional and open access versus predatory journals. *Nurs. Educ. Perspect.* 37, 5 (2016), 275.
[59] Mandeep R. Mehra, Sapan S. Desai, Frank Ruschitzka, and Amit N. Patel. 2020. RETRACTED: Hydroxychloroquine or Chloroquine with or without a Macrolide for Treatment of COVID-19: A Multinational Registry Analysis.
[60] Sefika Mertkan, Gulen Onurkan Aliusta, and Nilgun Suphi. 2021. Knowledge production on predatory publishing: A systematic review. *Learn. Publ.* 34, 3 (2021), 407–413.
[61] David Mills and Kelsey Inouye. 2021. Problematizing 'predatory publishing': A systematic review of factors shaping publishing motives, decisions, and experiences. *Learn. Publ.* 34, 2 (2021), 89–104.
[62] Mehran Mozaffari-Kermani, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K. Jha. 2014. Systematic poisoning attacks on and defenses for machine learning in healthcare. *IEEE J. Biomed. Health Inf.* 19, 6 (2014), 1893–1905.
[63] A. K. M. Newaz, Nur Imtiazul Haque, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A. Selcuk Uluagac. 2020. Adversarial attacks to machine learning-based smart healthcare systems. arXiv:2010.03671. Retrieved from https://arxiv.org/abs/2010.03671.
[64] Kee Yuan Ngiam and Wei Khor. 2019. Big data and machine learning algorithms for health-care delivery. *Lancet Oncol.* 20, 5 (2019), e262–e273.
[65] PubMed Notification. 2021. Retraction Notice Regarding Several Articles Published in Tumor Biology. Retrieved from https://pubmed.ncbi.nlm.nih.gov/34957978/.
[66] Lidia Ogiela and Marek R. Ogiela. 2012. Fundamentals of cognitive informatics. In *Advances in Cognitive Information Systems*. Springer, 19–49.
[67] Nicolas Papernot, Patrick McDaniel, Arunesh Sinha, and Michael P. Wellman. 2018. Sok: Security and privacy in machine learning. In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P'18)*. IEEE, 399–414.
[68] Patton. 2020. mediKanren: A System for Bio-medical Reasoning. Retrieved from http://minikanren.org/workshop/2020/minikanren-2020-paper10.pdf.
[69] Marcelo S. Perlin, Takeyoshi Imasato, and Denis Borenstein. 2018. Is predatory publishing a real threat? Evidence from a large database study. *Scientometrics* 116, 1 (2018), 255–273.
[70] 2018. FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems. Retrieved from https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-based-device-detect-certain-diabetes-related-eye.
[71] Filippo Pesapane, Marina Codari, and Francesco Sardanelli. 2018. Artificial intelligence in medical imaging: Threat or opportunity? Radiologists again at the forefront of innovation in medicine. *Eur. Radiol. Exp.* 2, 1 (2018), 1–10.
[72] Hoifung Poon, Chris Quirk, Charlie DeZiel, and David Heckerman. 2014. Literome: PubMed-scale genomic knowledge base in the cloud. *Bioinformatics* 30, 19 (2014), 2840–2842.
[73] A. N. Ramesh, Chandra Kambhampati, John R. T. Monson, and P. J. Drew. 2004. Artificial intelligence in medicine. *Ann. Roy. Coll. Surg. Engl.* 86, 5 (2004), 334.

[74] T. S. Sathyanarayana Rao and Chittaranjan Andrade. 2011. The MMR vaccine and autism: Sensation, refutation, retraction, and fraud. *Ind. J. Psychiatr.* 53, 2 (2011), 95.
[75] Seema Rawat and Sanjay Meena. 2014. Publish or perish: Where are we heading? *J. Res. Med. Sci.* 19, 2 (2014), 87.
[76] Shuhuai Ren, Yihe Deng, Kun He, and Wanxiang Che. 2019. Generating natural language adversarial examples through probability weighted word saliency. In *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*. 1085–1097.
[77] G. Richtig, M. Berger, B. Lange-Asschenfeldt, W. Aberer, and E. Richtig. 2018. Problems and challenges of predatory journals. *J. Eur. Acad. Dermatol. Venereol.* 32, 9 (2018), 1441–1449.
[78] Thomas C. Rindflesch and Marcelo Fiszman. 2003. The interaction of domain knowledge and linguistic structure in natural language processing: Interpreting hypernymic propositions in biomedical text. *J. Biomed. Inf.* 36, 6 (2003), 462–477.
[79] Thomas C. Rindflesch, Halil Kilicoglu, Marcelo Fiszman, Graciela Rosemblat, and Dongwook Shin. 2011. Semantic MEDLINE: An advanced information management application for biomedicine. *Inf. Serv. Use* 31, 1-2 (2011), 15–21.
[80] William J. Rudman, John S. Eberhardt, William Pierce, and Susan Hart-Hester. 2009. Healthcare fraud and abuse. *Perspect. Health Inf. Manage.* 6, Fall (2009).
[81] Connie Schardt, Martha B. Adams, Thomas Owens, Sheri Keitz, and Paul Fontelo. 2007. Utilization of the PICO framework to improve searching PubMed for clinical questions. *BioMed Centr. Med. Inf. Decis. Mak.* 7, 1 (2007), 16.
[82] Silvana Secinaro, Davide Calandra, Aurelio Secinaro, Vivek Muthurangu, and Paolo Biancone. 2021. The role of artificial intelligence in healthcare: A structured literature review. *BMC Med. Inf. Decis. Mak.* 21, 1 (2021), 1–23.
[83] Charles Seife. 2015. Research misconduct identified by the US Food and Drug Administration: Out of sight, out of mind, out of the peer-reviewed literature. *JAMA Intern. Med.* 175, 4 (2015), 567–577.
[84] Larissa Shamseer, David Moher, Onyi Maduekwe, Lucy Turner, Virginia Barbour, Rebecca Burch, Jocalyn Clark, James Galipeau, Jason Roberts, and Beverley J. Shea. 2017. Potential predatory and legitimate biomedical journals: Can you tell the difference? A cross-sectional comparison. *BMC Med.* 15, 1 (2017), 1–14.
[85] Bob Shepard. 2019. Diagnosis in 2.127 Seconds: Solving a Years-long Vomiting Mystery using AI, Research and Brain Power. Retrieved from https://www.uab.edu/news/health/item/10703-diagnosis-in-2-127-seconds-solving-a-years-long-vomiting-mystery-using-ai-research-and-brain-power.
[86] Rishi P. Singh, Grant L. Hom, Michael D. Abramoff, J. Peter Campbell, Michael F. Chiang, et al. 2020. Current challenges and barriers to real-world artificial intelligence adoption for the healthcare system, provider, and the patient. *Transl. Vis. Sci. Technol.* 9, 2 (2020), 45–45.
[87] Richard Smith. 2006. Research misconduct: The poisoning of the well. *J. Roy. Soc. Med.* 99, 5 (2006), 232–237.
[88] A. Sood, A. K. Ghosh, et al. 2006. Literature search using PubMed: An essential tool for practicing evidence-based medicine. *J. Assoc. Phys. Ind.* 54, R (2006), 303.
[89] Agnieszka Sorokowska, Katarzyna Pisanski, Piotr Sorokowski, and Emanuel Kulczycki. 2017. Predatory Journals Recruit Fake Editor. Retrieved February 24, 2021 from https://www.nature.com/news/predatory-journals-recruit-fake-editor-1.21662.
[90] David Moher, Larissa Shamseer, Kelly D. Cobey, Manoj M. Lalu, James Galipeau, Marc T. Avey, Nadera Ahmadzai, Mostafa Alabousi, Pauline Barbeau, Andrew Beck, and others. 2017. Stop this waste of people, animals and money. *Nature* 549, 7670 (2017), 23–25.
[91] Parvathaneni Naga Srinivasu, N. Sandhya, Rutvij H. Jhaveri, and Roshani Raut. 2022. From blackbox to explainable ai in healthcare: Existing tools and case studies. *Mobile Inf. Syst.* 2022 (2022).
[92] R. Grant Steen. 2011. Retractions in the medical literature: How many patients are put at risk by flawed research? *J. Med. Ethics* 37, 11 (2011), 688–692.
[93] R. Grant Steen. 2011. Retractions in the scientific literature: Is the incidence of research fraud increasing? *J. Med. Ethics* 37, 4 (2011), 249–253.
[94] Jeremy Stribling, Max Krohn, and Dan Aguayo. 2005. Scigen-an Automatic cs Paper Generator. Retrieved March 19, 2021 from https://pdos.csail.mit.edu/archive/scigen/.
[95] Stefan Studer, Thanh Binh Bui, Christian Drescher, Alexander Hanuschkin, Ludwig Winkler, Steven Peters, and Klaus-Robert Müller. 2021. Towards CRISP-ML (Q): A machine learning process model with quality assurance methodology. *Mach. Learn. Knowl. Extract.* 3, 2 (2021), 392–413.
[96] Mengying Sun, Fengyi Tang, Jinfeng Yi, Fei Wang, and Jiayu Zhou. 2018. Identify susceptible locations in medical records via adversarial attacks on deep predictive models. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*. 793–801.
[97] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2013. Intriguing properties of neural networks. arXiv:1312.6199. Retrieved from https://arxiv.org/abs/1312.6199.
[98] Cui Tao, Yuji Zhang, Guoqian Jiang, Matt-Mouley Bouamrane, and Christopher G. Chute. 2012. Optimizing semantic MEDLINE for translational science studies using semantic web technologies. In *Proceedings of the 2nd International Workshop on Managing Interoperability and Complexity in Health Systems*. ACM, 53–58.

[99] Philippe Thomas, Johannes Starlinger, Alexander Vowinkel, Sebastian Arzt, and Ulf Leser. 2012. GeneView: A comprehensive semantic search engine for PubMed. *Nucl. Acids Res.* 40, W1 (2012), W585–W591.

[100] Eric J. Topol. 2019. High-performance medicine: The convergence of human and artificial intelligence. *Nat. Med.* 25, 1 (2019), 44–56.

[101] Deepak R. Unni, Sierra A. T. Moxon, Michael Bada, Matthew Brush, Richard Bruskiewich, J. Harry Caufield, Paul A. Clemons, Vlado Dancik, Michel Dumontier, Karamarie Fecho, et al. 2022. Biolink model: A universal schema for knowledge graphs in clinical, biomedical, and translational science. *Clin. Transl. Sci.* (2022).

[102] Chih-Hsuan Wei, Bethany R. Harris, Hung-Yu Kao, and Zhiyong Lu. 2013. tmVar: A text mining approach for extracting sequence variants in biomedical literature. *Bioinformatics* 29, 11 (2013), 1433–1439.

[103] Chih-Hsuan Wei, Hung-Yu Kao, and Zhiyong Lu. 2013. PubTator: A web-based text mining tool for assisting biocuration. *Nucl. Acids Res.* 41, W1 (2013), W518–W522.

[104] Chih-Hsuan Wei, Lon Phan, Juliana Feltz, Rama Maiti, Tim Hefferon, and Zhiyong Lu. 2018. tmVar 2.0: Integrating genomic variant information from literature with dbSNP and ClinVar for precision medicine. *Bioinformatics* 34, 1 (2018), 80–87.

[105] Anna Marie Williams, Yong Liu, Kevin R. Regner, Fabrice Jotterand, Pengyuan Liu, and Mingyu Liang. 2018. Artificial intelligence, physiological genomics, and precision medicine. *Physiol. Genom.* 50, 4 (2018), 237–243.

[106] Todd Winey. 2017. Garbage in, Garbage Out: Avoiding the Common Pitfalls of AI in Healthcare. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/garbage-in-garbage-out-avoiding-the-common-pitfalls-of-ai-in-healthcare.html.

[107] E. C. Wood, Amy K. Glen, Lindsey G. Kvarfordt, Finn Womack, Liliana Acevedo, Timothy S. Yoon, Chunyu Ma, Veronica Flores, Meghamala Sinha, Yodsawalai Chodpathumwan, et al. 2022. RTX-KG2: A system for building a semantically standardized knowledge graph for translational biomedicine. *BMC Bioinf.* 23, 1 (2022), 1–33.

[108] Wei Emma Zhang, Quan Z. Sheng, Ahoud Alhazmi, and Chenliang Li. 2020. Adversarial attacks on deep-learning models in natural language processing: A survey. *ACM Trans. Intell. Syst. Technol.* 11, 3 (2020), 1–41.

[109] Sijin Zhou, Xinyi Dai, Haokun Chen, Weinan Zhang, Kan Ren, Ruiming Tang, Xiuqiang He, and Yong Yu. 2020. Interactive recommender system via knowledge graph-enhanced reinforcement learning. In *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*. 179–188.

Received 21 December 2021; revised 16 March 2023; accepted 2 April 2023