ARTIFICIAL INTELLIGENCE CRIME:AN OVERVIEW OF MALICIOUS USE AND ABUSE OF AI

M Ram Kumar[1], R C Kalanjali[2], S Lava Kumar[2], E Nithish Kumar[2], G Kiran Kumar[2], D Divakar[2]

[1] *Assistant Professor, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India*
[2] *Research Scholar, Department of Computer Science & Information Technology, Siddharth Institute of Engineering & Technology, Andhra Pradesh, India*

ABSTRACT

This project provides a comprehensive overview of the growing concerns surrounding the malicious use and abuse of Artificial Intelligence (AI) in criminal activities. As AI technologies rapidly evolve and integrate into various sectors, they also become susceptible to exploitation for harmful purposes. Drawing on relevant literature, reports, and representative incidents, this study constructs a typology that delineates the multifaceted ways in which AI capabilities are manipulated for malicious ends. The primary objective is to shed light on the diverse activities associated with AI-related crime and the corresponding risks. The analysis begins by identifying vulnerabilities in AI models, offering insights into potential points of exploitation by malicious actors. Subsequently, the exploration extends to AI-enabled and AI-enhanced attacks, presenting a nuanced perspective on the risks without aiming for a conclusive and exhaustive classification. Specifically, the study proposes four types of malicious AI abuse, including integrity attacks, unintended AI outcomes, algorithmic trading, and membership inference attacks. Additionally, it highlights four categories of malicious AI use: social engineering, misinformation/fake news dissemination, hacking, and the deployment of autonomous weapon systems. This abstract concludes with a call for increased awareness, collaborative governance strategies, and policy development to minimize risks and mitigate the harmful consequences of AI-related crime. The interdisciplinary nature of addressing these challenges emphasizes the importance of collaboration among governments, industries, and civil society to enhance preparedness and resilience against the malicious use and abuse of AI.

Keyword: - *Artificial intelligence, artificial intelligence typology, computer crime, malicious artificial intelligence, security, social implications of technology*

1. INTRODUCTION

The impact of systems using Artificial Intelligence (AI) is at the center of numerous academic studies [1]–[3], political debates [4], and reports of civil society organizations [5]. The development of AI has become the subject of praise due to unprecedented technological capabilities, such as enhanced possibilities for automated image recognition (e.g., detection of cancer in the field of medicine [6], [7]). However, it has also been criticized - even feared - due to aspects such as the uncertain consequences of automation for the labor market (e.g., concerns of mass unemployment [8, pp. 26–27]). This duality of positive vs negative aspects of the technology can also be identified in the context of cybersecurity and cybercrime. Governments use AI to enhance their capabilities, whereas the same technology can be used for attacks against them [9]. While the recent surge in AI development has been fueled by the private sector and applications in customer-oriented applications, sectors such as defense might use similar capabilities in their operations [10]. At the same time, it is increasingly difficult to distinguish between the actions of state and non-state actors. This has recently been demonstrated by a wave of ransomware attacks targeting public infrastructure in many countries, such as the Colonial Pipeline in the United States in May 2021 [11, pp. 127–128]. Additionally, programs and applications developed for non-malicious purposes can also be implemented or modified for malicious intent and potentially cause harm. The dual-use aspect of technology is not an entirely new problem when it comes to

cybercrime1 or (cyber-)security. Nevertheless, how AI can be leveraged for malicious use and abuse constitutes novel vulnerabilities. Permanent assessment of the threat landscape is crucial to create and adapt governance mechanisms, develop proactive measures, and enhance (cyber-)resilience. To build on previous work [14]–[16] and expand the understanding of how AI broadens the potential for malicious activities online, this article evaluates the main categories of use and abuse of AI in a criminal context. We provide several salient examples that allow us to illustrate the challenges at hand. Based on these examples, we present a typology that catalogs the main harmful AI-based activities. Developing knowledge and understanding about the potential malicious use and abuse of AI enables cybersecurity organizations and governmental agencies to anticipate such incidents and increase their preparedness against attacks. Furthermore, a typology is greatly useful in structuring research efforts and identifying gaps in knowledge in areas where more research is warranted.

2. LITERATURE SURVEY

[1] LETHAL ARTIFICIAL INTELLIGENCE AND CHANGE: THE FUTURE OF INTERNATIONAL PEACE AND SECURITY

The development artificial intelligence and its uses for lethal purposes in war will fundamentally change the nature of warfare as well as law-enforcement and thus pose fundamental problems for the stability of the international system. To cope with such changes, states should adopt preventive security governance frameworks based upon the precautionary principle of international law, and upon previous cases where prevention brought stability to all countries. Such new global governance frameworks should be innovative as current models will not suffice. The World Economic Forum has advanced that the two areas that will bring most benefits but also biggest dangers to the future are robotics and artificial intelligence. Additionally, they are also the areas in most urgent need for innovative global governance. Leading scientists working on artificial intelligence have argued that the militarization and use of lethal artificial intelligence would be a highly destabilizing.

[2] CONTRIBUTIONSAND RISKS OF ARTIFICIAL INTELLIGENCE (AI) IN BUILDING SMARTER CITIES: INSIGHTSFROM A SYSTEMATIC REVIEW OF THE LITERATURE

Artificial intelligence (AI) is one of the most disruptive technologies of our time. Interest in the use of AI for urban innovation continues to grow. Particularly, the rise of smart cities—urban locations that are enabled by community, technology, and policy to deliver productivity, innovation, livability, wellbeing, sustainability, accessibility, good governance, and good planning—has increased the demand for AI-enabled innovations. There is, nevertheless, no scholarly work that provides a comprehensive review on the topic. This paper generates insights into how AI can contribute to the development of smarter cities. A systematic review of the literature is selected as the methodologic approach. Results are categorized under the main smart city development dimensions, i.e., economy, society, environment, and governance.

[3] IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CANCER DETECTION

Artificial intelligence has aided in the advancement of healthcare research. The availability of open-source healthcare statistics has prompted researchers to create applications that aid cancer detection and prognosis. Deep learning and machine learning models provide a reliable, rapid, and effective solution to deal with such challenging diseases in these circumstances. PRISMA guidelines had been used to select the articles published on the web of science, EBSCO, and EMBASE between 2009 and 2021. In this study, we performed an efficient search and included the research articles that employed AI-based learning approaches for cancer prediction. A total of 185 papers are considered impactful for cancer prediction using conventional machine and deep learning-based classifications. In addition, the survey also deliberated the work done by the different researchers and highlighted the limitations of the existing literature, and performed the comparison using various parameters such as prediction rate, accuracy, sensitivity, specificity, dice score, detection rate, area undercover, precision, recall, and F1-score. Five investigations have been designed, and solutions to those were explored. Although multiple techniques recommended in the literature have achieved great prediction results, still cancer mortality has not been reduced. Thus, more extensive research to deal with the challenges in the area of cancer prediction is required.

[4] DETECTION OF BREAST CANCER WITH MAMMOGRAPHY: EFFECT OF AN ARTIFICIAL INTELLIGENCE SUPPORT SYSTEM

An enriched retrospective, fully crossed, multireader, multicase, HIPAA-compliant study was performed. Screening digital mammographic examinations from 240 women (median age, 62 years; range, 39–89 years) performed between 2013 and 2017 were included. The 240 examinations (100 showing cancers, 40 leading to false-positive recalls, 100 normal) were interpreted by 14 Mammography Quality Standards Act–qualified radiologists, once with and once without AI support. The readers provided a Breast Imaging Reporting and Data System score and probability of malignancy. AI support provided radiologists with interactive decision support (clicking on a breast region yields a local cancer likelihood score), traditional lesion markers for computer-detected abnormalities, and an examination-

based cancer likelihood score. The area under the receiver operating characteristic curve (AUC), specificity and sensitivity, and reading time were compared between conditions by using mixed-models analysis dof variance and generalized linear models for multiple repeated measurements.

[5] INFORMATION HAZARDS: A TYPOLOGY OF POTENTIAL HARMS FROM KNOWLEDGE

Information hazards are risks that arise from the dissemination or the potential dissemination of true information that may cause harm or enable some agent to cause harm. Such hazards are often subtler than direct physical threats, and, as a consequence, are easily overlooked. They can, however, be important. This paper surveys the terrain and proposes a taxonomy.

3. METHODOLOGY

3.1 EXISTING SYSTEM

In Existing system, To build on previous work and expand the understanding of how AI broadens the potential for malicious activities online, this article evaluates the main categories of use and abuse of AI in a criminal context.We provide several salient examples that allow us to illustrate the challenges at hand. Based on these examples, we present a typology that catalogs the main harmful AI-based activities.

3.1.1 DISADVANTAGES OF EXISTING SYSTEM

- An existing methodology not proposed the term ``AI-Crime'' to describe the situation in which AI technologies are re-oriented to facilitate criminal activity.
- An existing system doesn't implement for Malicious Abuse of AI And Vulnerabilities of AI Models which makes existing system infeasible.

3.2 PROPOSED METHODOLOGY

- Add to the emerging body of knowledge that maps types of malicious use and abuse of AI systems.
- To understand the main concepts, threat scenarios, and possibilities is necessary to develop much-needed preventive measures and proactive responses to such attacks.
- Help in establishing a shared language among and across different disciplines, especially between STEM disciplines and legal practitioners, as well as policymakers. Interdisciplinary research on the topic can reduce confusion caused by excessively technical or monodisciplinary language and aid in bridging existing gaps.
- Propose mitigation strategies, as well as demonstrating that a collective effort among government, academia, and industry is needed.

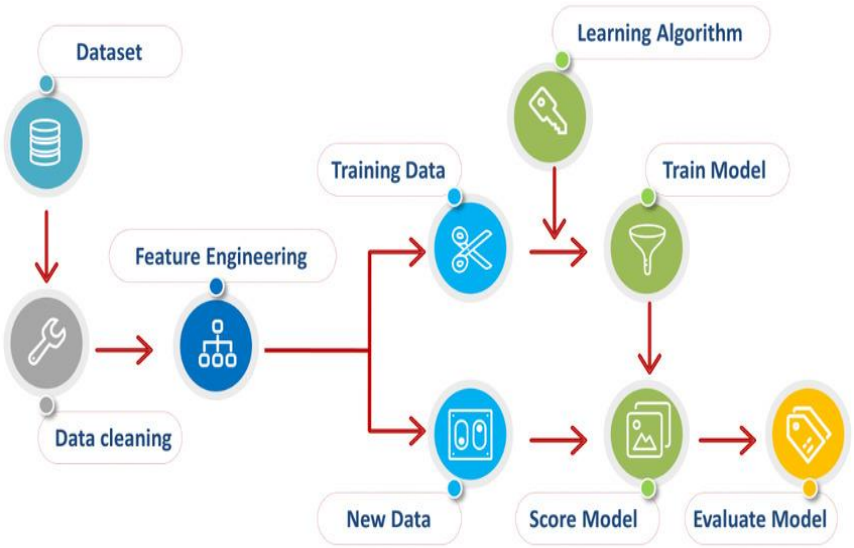
3.2.1 ADVANTAGES OF PROPOSED SYSTEM

- The system aims to propose a typology of the malicious use and abuse of AI based on empirical evidence and contemporary discourse, analyzing how AI systems are used to compromise confidentiality, integrity, and data availability.
- Objectives are limited to identifying essential elements of the malicious use and abuse of AI, and to collect evidence of their use in practice.
- The compiled data enable further analysis of the possible ways in which AI systems can be exploited for criminal activities.

4. SYSTEM DESIGN

It is a process of planning a new business system or replacing an existing system by defining its components or modules to satisfy the specific requirements. Before planning, you need to understand the old system thoroughly and determine how computers can best be used in order to operate efficiently.

4.1 ARCHITECTURE



4.2 MODULES

In this Proposed System, There are three Modules. They are:

1. Data Analytic Manager
2. Remote User
3. Dataset Administration

4.2.1 DATA ANALYTIC MANAGER

This system should provide the Data Analytic manager with the convenience of providing training and testing of dataset

- Login
- Browse Data sets & train & Test
- View Trained & tested Accuracy in Bar chart
- View Trained & Tested Accuracy results
- View crime type ratio
- Download crimetype predicted data sets
- View crime type ratio results
- View all Remote Users
- Logout

4.2.2 REMOTE USER

This system should help the user by registering with his basic details that can be stored in the database and it provides the following such as

- Register
- Login
- Prediction of Crimetype
- Logout

4.2.3 DATASET ADMINISTRATION

This system should provide the Data Set Administration with the convenience of providing training and testing of dataset

- Process Data set
- Manage Data Set

5. RESULTS AND PERFORMANCE

EXECUTION PROCEDURE

The Execution procedure is as follows:

1. In this research work with data with attributes are observable and then all of them are floating data. And there's a decision class/class variable. This data was collected from Kaggle machine learning repository.
2. In this research 70% data use for train model and 30% data use for testing purpose.
3. Decision Tree is used as Classifier.
4. In the classification report we were able to find out the desired result
5. In this analysis the result depends on some part of this research. However, which algorithm gives the best true positive, false positive, true negative, and false negative are the best algorithms in this analysis.

Fig-1 HOME PAGE

Fig-2 LOGIN PAGE

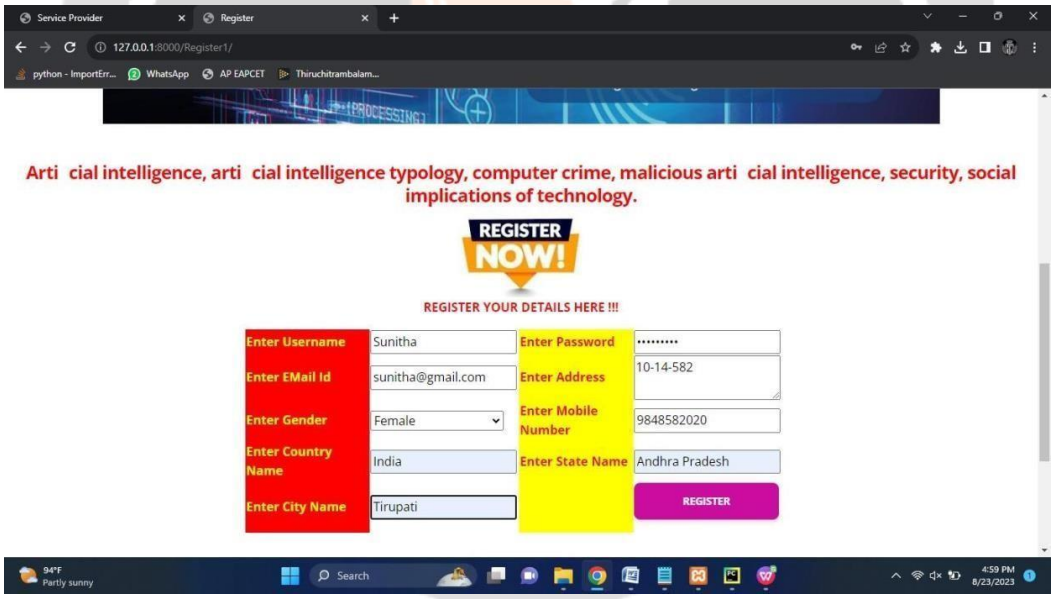


Fig-3 USER REGISTERATION

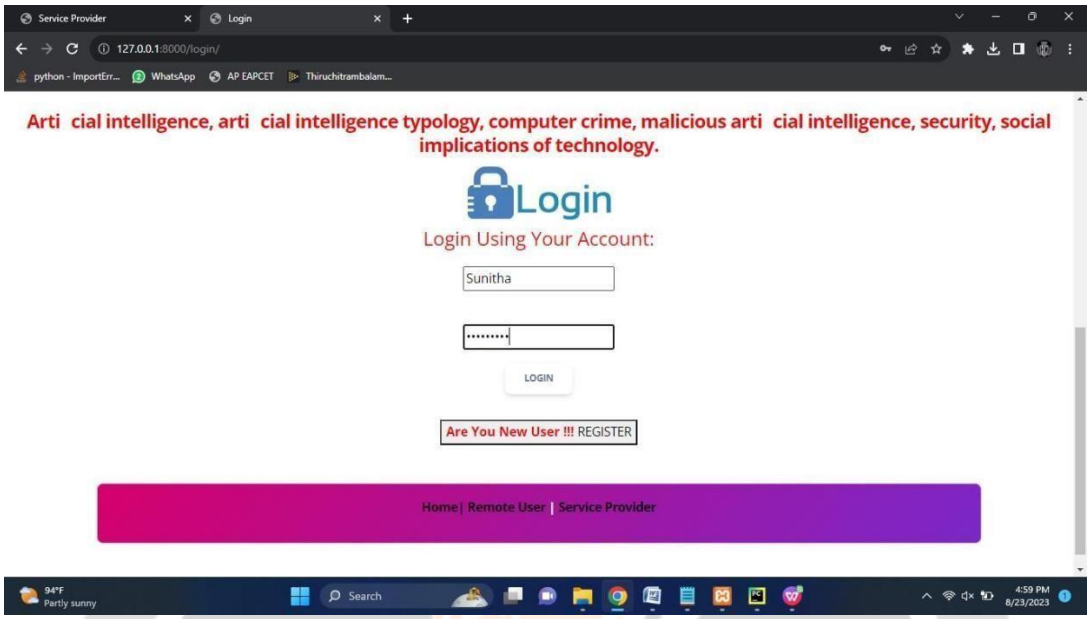


Fig-4 USER LOGIN

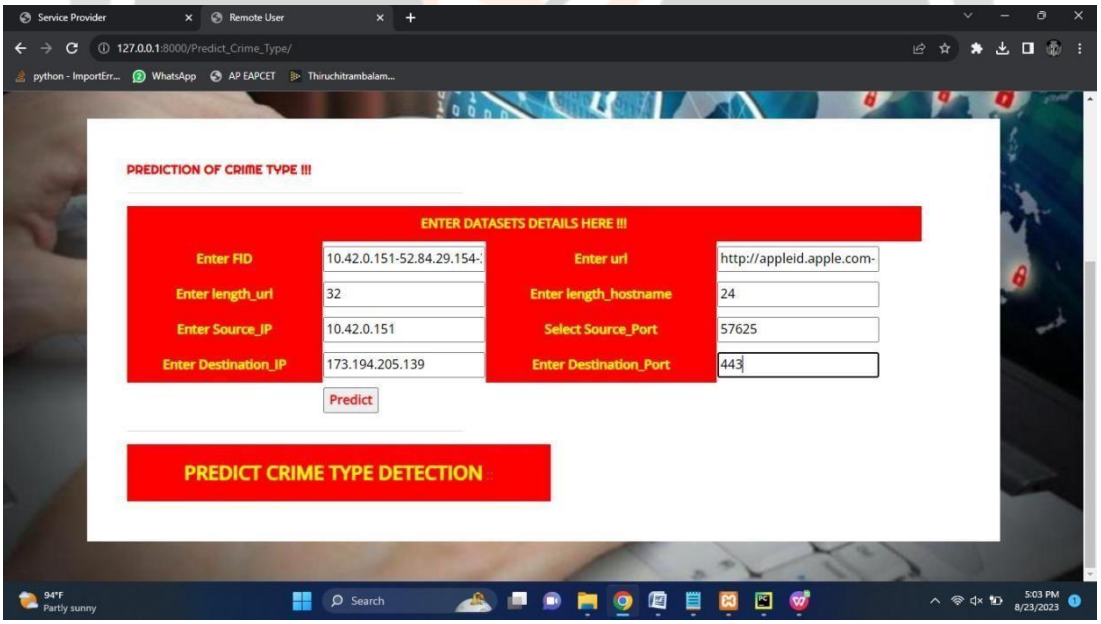


Fig-5 ENTER VALUE OF PREDICTION

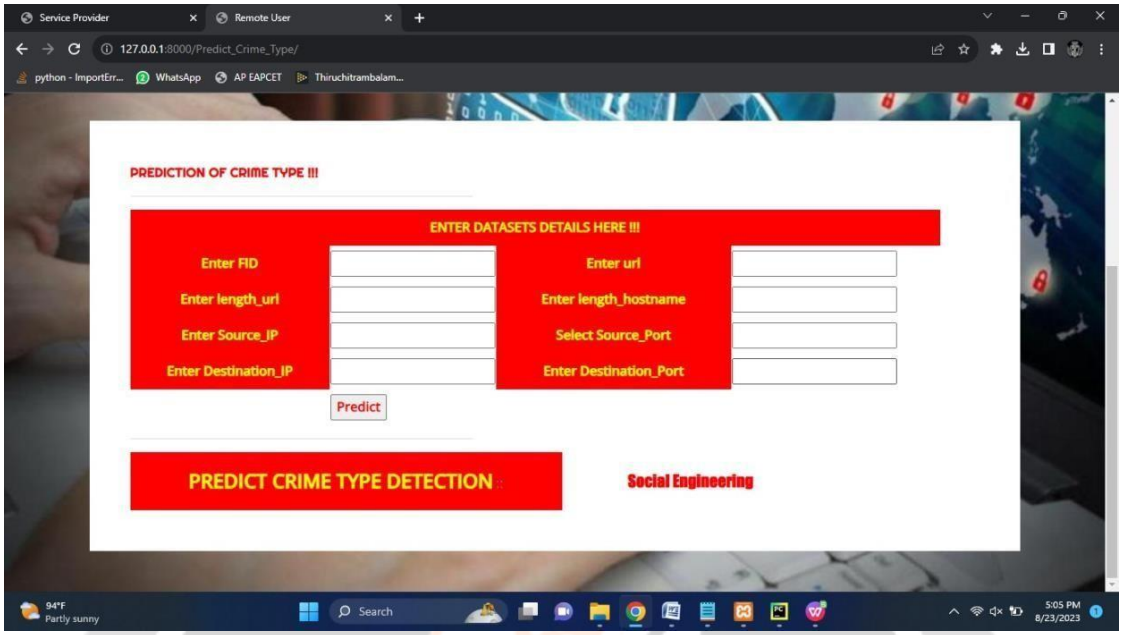


Fig-6 PREDICTION RESULT

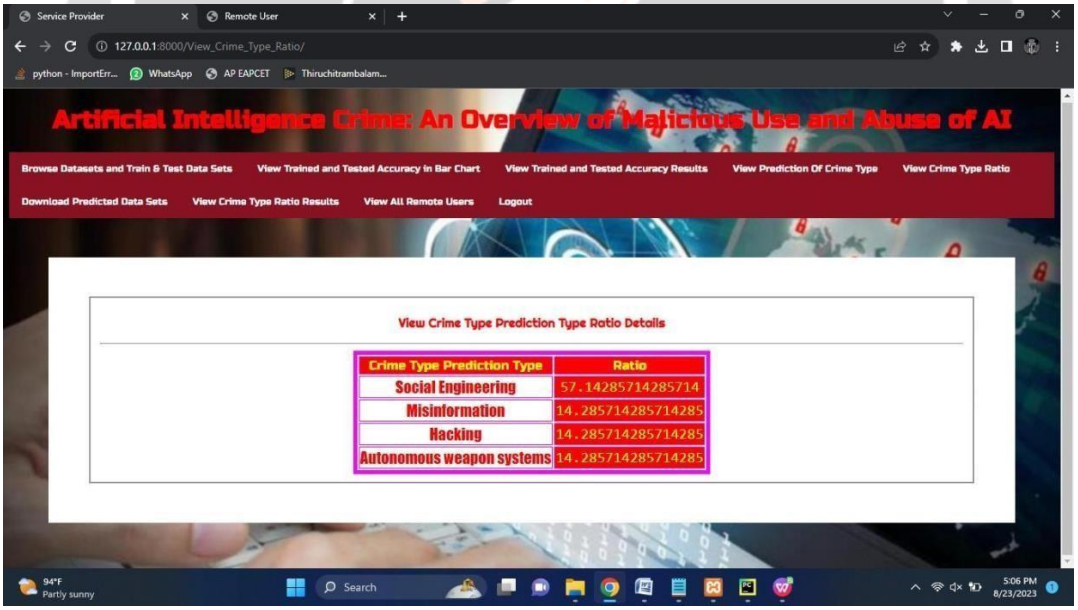


Fig-7 CRIME TYPE RATIO RESULTS

6. CONCLUSION

The threats posed by the use and abuse of AI systems must be well understood to create mechanisms that protect society and critical infrastructures from attacks. Based on the available literature, reports, and previous incidents, we focused on creating a classification of how AI systems can be used or abused by malicious actors.We also outlined attacks that, to the best of ourknowledge, have only been demonstrated through ``proof of concept'', such as IBM's

DeepLocker.In response to the risks presented in this project, we have also explored some possible mitigation strategies. Industries, governments, civil society, and individuals should cooperate in developing knowledge and raising awareness while developing technical and operational systems and procedures to address the challenges.

7. REFERENCE

[1] K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs ofArti_cial Intelligence*. London, U.K.: Yale Univ. Press, 2021.

[2] D. Garcia, ``Lethal arti_cial intelligence and change: The future of internationalpeace and security," *Int. Stud. Rev.*, vol. 20, no. 2, pp. 334_341,Jun. 2018, doi: 10.1093/isr/viy029.

[3] T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, ``Contributionsand risks of arti_cial intelligence (AI) in building smarter cities: Insightsfrom a systematic review of the literature," *Energies*, vol. 13, no. 6,p. 1473, Mar. 2020, doi: 10.3390/en13061473.

[4] I. van Engelshoven. (Oct. 18, 2019). *Speech by Minister Van Engelshovenon Arti_cial Intelligence at UNESCO, on October the 18th in Paris*.Government of The Netherlands. Accessed: Apr. 15, 2021. [Online].Available: https://www.government.nl/documents/speeches/2019/10/18/speech-by-minister-vanengelshoven-on-arti_cial-intelligence-atunesco

[5] O. Osoba andW.Welser IV, *The Risks of Arti_cial Intelligence to Securityand the Future of Work*. Santa Monica, CA, USA: RAND Corporation,2017, doi: 10.7249/PE237.

[6] D. Patel, Y. Shah, N. Thakkar, K. Shah, and M. Shah, ``Implementation ofarti_cial intelligence techniques for cancer detection," *Augmented Hum.Res.*, vol. 5, no. 1, Dec. 2020, doi: 10.1007/s41133-019-0024-3.

[7] A. Rodríguez-Ruiz, E. Krupinski, J.-J. Mordang, K. Schilling,S. H. Heywang-Köbrunner, I. Sechopoulos, and R. M. Mann, ``Detectionof breast cancer with mammography: Effect of an arti_cial intelligencesupport system," *Radiology*, vol. 290, no. 2, pp. 305_314, Feb. 2019, doi: 10.1148/radiol.2018181371.

[8] J. Furman and R. Seamans, ``AI and the economy," Nat. Bur. Econ. Res.,NBER, Cambridge, MA, USA,Work. Paper, 2018, doi: 10.3386/w24689.