دور الذكاء الاصطناعي في كشف ومنع الجرائم الإلكترونية

The Function of Artificial Intelligence in the Detection and Prevention of Cybercrime

نبراس يوسف محمد
كلية الطب – جامعة القادسية
nibras.yousif@qu.edu.iq

بورخا فرناندیز غوان
جامعة اقليم الباسك –اسبانيا
borja.fernandez@ehu.eus

علي جاسب ثعبان
وزارة الداخلية – العراق
alijasib2018@gmail.com

الملخص:

تتطور الجرائم الإلكترونية بسرعة غير مسبوقة، مما يُشكل تهديدات جسيمة للأفراد والشركات والمؤسسات العامة حول العالم. تفحص الدراسة مدى تطور الذكاء الاصطناعي للكشف عن الجرائم الإلكترونية ومنعها، بالاستفادة من تقنيات التعلم الآلي والتعلم العميق ومعالجة اللغات الطبيعية. تُسهّل حلول الأمن السيبراني المُدارة بالذكاء الاصطناعي الكشف عن الجرائم وأتمتتها، وتُسهّل المراقبة الآنية، مما يُحسّن فعالية التحقيق. جرائم الإلكترونية. ومع ذلك، فإن دمج الذكاء الاصطناعي في الأمن السيبراني يُحسّن أيضًا المخاوف الأخلاقية والقانونية الهامة، بما في ذلك خصوصية البيانات، وتحيز الخوارزميات، وإساءة استخدام تقنيات المراقبة المحتملة. يعتمد هذا البحث على نهج وصفي استقرازي، ويستعرض المقالات والتقارير الفنية ودراسات الحالة التي تُقيّم فعالية نظام الأمن السيبراني المهتم بـ A. تشير الاستنتاجات إلى أنه على الرغم من أن الذكاء الاصطناعي يوفر فوائد كبيرة من خلال تحديد التهديدات السيبرانية والحد منها، إلا أن موقعه الأخلاقي يتطلب هيكلًا تنظيميًا صارمًا لضمان الانفتاح والمسؤولية والعدالة. بناءً على نتائج الدراسات السابقة، يهدف هذا البحث إلى تقديم نموذج يعكس الاستخدام الأخلاقي للذكاء الاصطناعي في الأمن السيبراني، والذي يركز على تطوير استراتيجيات فعالة لمواجهة التحديات المتعلقة بالخصوصية والتحيز. تطلب الدراسة من الذكاء الاصطناعي استخدام الذكاء الاصطناعي في الأمن السيبراني، لحماية الابتكار بشكل فعال من خلال الأفكار الأخلاقية.

الكلمات المفتاحية: الذكاء الاصطناعي AI، الجريمة الالكترونية، تعلم الالة، اكتشاف التهديدات والاعتبارات الاخلاقية.

Abstract:

Cybercrime develops at a unique speed, creating significant threats for individuals, businesses, and public institutions worldwide. This study examines the transformation role of artificial intelligence (AI) in detecting and preventing cybercrimes by taking advantage of Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP) techniques. AI-operated cyber security solutions automate the detection, automate reactions, and facilitate real-time

monitoring, improving the effectiveness of examining cybercrime. However, integration of AI into cybersecurity also raises significant ethical and legal concerns, including the privacy of data, algorithm bias and potential abuse of surveillance technologies. This research adopts a descriptive-analytic approach, and reviews learned articles, technical reports, and case studies, which assess the effectiveness of the AI-operated cyber security system. Conclusions suggest that although AI provides significant benefits in identifying and reducing cyber threats, its moral placement requires a rigid regulatory structure to ensure transparency, responsibility, and justice. Based on the findings of previous studies, this research wants to provide a The model that shows the ethical use of AI in cyber security, focusing on developing effective strategies to meet challenges related to privacy and prejudice .The study calls for AI's adoption in cyber security, balancing innovation with moral ideas to effectively protect digital ideas.

Keywords: Artificial Intelligence (AI), Cybercrime, Machine Learning, Threat Detection, Ethical Considerations.

1. Introduction

The digital age has witnessed connection and convenience, but it has provided a fruitful reason for cyber-criminal activities simultaneously. Reclaiming threats, including fractures of data, financial fraud, identity theft, and cyber espionage, pose sufficient risk to individuals, companies, and authorities globally. Since these cyber hazards continue to grow in complexity and scale, traditional security measures are struggling to maintain speed and require innovative and adaptive defense mechanisms. In response, artificial intelligence (AI) has appeared as a transformational strength in cyber security, utilization of Machine Learning (ML), Deep Learning (DL), and Natural Language *Processing* treatment(NLP). AI-driven cybersecurity solutions not only improve the efficiency of investigative units but also offer predictive insights that help mitigate potential cyber risks before they escalate into large-scale security breaches [1] . While AI presents a revolutionary approach to detect and prevent cybercrime, its integration into the security structure is not without challenges. While AI presents a revolutionary approach to detecting and preventing cybercrime, its integration into the security structure is not without challenges. The extensive collection and analysis of massive data sets raises significant ethical concerns regarding privacy, algorithmic bias, and potential misuse of surveillance technologies [2] . According to a study [1] for [Mamoun Alazab, Soman KP, Sriram Srinivasan] on October 30, 2023 comprehensive and integrated study of deep learning technologies past, present, and future,

including next-generation cybersecurity details [1]. This letter aims to provide a broad and intensive review of the development and architecture of Deep Learning (DL) over time, focusing on its applications on Cybercrime. It also examines various scenarios related to intelligent automation, the Internet of Things (IoT), Big Data (BD), Block chain, and Cloud and Edge Computing Techniques. A study [2] by (Selma Dilek, Hüseyin Çakır, and Mustafa Aydın) indicates that AI enhances cybersecurity efficiency by significantly improving the accuracy of threat detection and reducing human errors through automation of security processes. Besides, We conclude from previous studies, such as [3] in 2023, that AI technologies have increased the effectiveness of cyber threat detection by up to 93%, which reinforces the importance of this research in revealing how to apply these technologies ethically and effectively. In addition, the absence of integrated rules that control the distribution of AI in cyber security makes it more than using it and gives a need for legal and moral inspection. In addition, previous research indicates that the application of artificial intelligence in search of fraud requires criminal classification and a approach that supports the integration of innovation with accountability in cybersecurity operations, In addition, the integration of AI into cyber security systems requires a strong structure that addresses questions such as openness, responsibility, and moral ideas. The lack of extensive rules that control AI distribution in the prevention of fraud increases these challenges. The purpose of this research is to detect online crime and to implement AI for the prevention of innovation and double dimensions of morality. By examining recent developments, case studies, and moral frameworks, while the previous research provides valuable insight into the effectiveness of AI in cyber security, this study wants to provide extensive analysis that balances innovation with moral challenges. In light of the findings of previous studies on the effectiveness of artificial intelligence in increasing cyber security, this research wants to provide an extensive analysis that balances innovation and moral challenges associated with the use of these technologies. While the previous research indicates the important benefits of using AI in the detection of online crime, the purpose of this research is to provide practical recommendations to ensure the responsible use of these technologies. Based on the findings of previous studies, the purpose of this research is to propose innovative solutions that increase the effectiveness of AI in cyber security care for moral and legal issues.

2. Related Work

This section provides intensive examination of current research on the role of artificial intelligence (AI) to increase cyber security and fight cybercrimes. The purpose of literature review is to synthesize today's knowledge, identify holes and find out future research directions.

The rapid growth of technology has increased cyber threats rapidly, making AI an important cyber security tool. This review emphasizes the importance of AI in dealing with these challenges. So the researcher sees the Artificial intelligence (AI) to increase cyber security and fight cybercrimes. The purpose of literature review is to synthesize today's knowledge, identify holes and find out future research directions. In [1] it proposed a hybrid model based on DL with multiple layers of privacy to learn what malware and legitimate activities are more accurately, and urged its development to detect and prevent advanced attacks .In the study [2] The study examines the legal and ethical implications of using AI in automated crowd analysis, the impact of laws and ethics on this field. It focuses specifically on the European perspective, the laws and legislation applicable in Europe regarding crowd analysis using AI. The study also delves into remaining concerns after the legislation is enacted, i.e., the issues that have not been fully resolved even after the implementation of these laws.. Combination of the speed of AI with unique cognition, perception and reasoning of human brain can make access to justice more open and efficient, prevent discrimination and injustice, and considerably improve the current state of legal practice, making it both less stressful for legal professionals and more affordable, effective and beneficial for clients , this is what the study is about [3].The study [4] show transparency in AI plays a very important role in the overall strive to develop more trustworthy. In addition, we see that Alkhazraji , Mohammad Ahmad said in their research [5] that the role of law enforcement strategies and emerging technologies as countermeasures to the growing threat of e-crime and international cooperation, proved efficient for different cybercrimes. Finally, study [6] show the integration of AI into investor relations within development finance institutions raises other ethical considerations. When investor relations models are rolled out across development finance institutions and companies, they automatically gain access to the personal data of individuals subject to scrutiny. We are utilizing findings from various studies to clarify the significant role of artificial intelligence technology in reducing and preventing cybercrime.

3. Methodology

The purpose of this research is to investigate the transformative role of artificial intelligence in the detection and prevention of online crime through extensive analysis of existing literature and technical reports published in the field. The study adopts a descriptive analysis to synthesize and interpret data from previous literature and provides new insights into the effectiveness of AI use in cyber security. The study depends on various sources, including academic studies published in scientific magazines reviewed by colleagues, technical reports published by authorities and private institutions and non-profit organizations, as well as, case studies, white articles, and scientific and technical conferences and seminars. Data collection will include a comprehensive search of highly respected and reliable scientific databases such as IEEE, ACM Digital Library, Scopus, and Web of Science, using relevant keywords such as “artificial intelligence,” “cybersecurity,” “cybercrime,” “machine learning,” and “threat detection.”. In addition, the reference lists of the collected studies and reports will be reviewed to further identify relevant sources, and to obtain recommendations for further resources will be contacted experts on cyber security and artificial intelligence. Data analysis will use the key functions of collected sources to shorten and describe descriptive analysis for characteristics, thematic analysis to identify recurrent subjects, compare conclusions in studies, and reverse analysis and significant analysis and significant analysis to assess the quality and validity of reports. The limitations of this study include its dependence on secondary sources and the ability to bias in source selection or interpretation, which will be reduced through a hard-working effort to gather different sources and seriously evaluate them. Research, including scientific integrity, honor of intellectual property, and openness, will be maintained throughout the study. The purpose of this feature is to analyze existing data in previous literature to provide a structured and comprehensive structure to investigate the transformative role of artificial intelligence in cyber security, to provide valuable insight into the effectiveness of AI use in cyber security, identify challenges and opportunities, and recommends to achieve these techniques.

i. The Concept of artificial intelligence

Despite the recent emergence of the concept of artificial intelligence (AI), legal scholars have given several definitions. Some of the most remarkable include: From a technical point of view, AI is defined as a "program that is programmed by a computer that depends on the algorithm and specific procedures to perform special features or features. This device is equipped with automatic inputs and treats them

according to their program to make instructions. According to this definition, it is clear that AI-based devices depend on the computer, receive inputs in the form of code and rules, and operate using specific programming algorithms. One of the most prominent applications of AI can be seen in a wise robot. AI depends on computers that have real knowledge in them. Thus, the core of AI in the representation of this knowledge is through content-based sequencing of this knowledge, and through the exercise of adaptation and modification of this knowledge [7]. Artificial intelligence is also a branch of computer science aimed at designing computer programs that are able to mimic human intelligence methods. This allows computers to make the ability to think, hear, and visual perception, automated speech, and acting assignments, as an alternative to people, as an alternative to people.

John Macarthur has defined it this way: "Science and design of intelligent machine."

It can be said that artificial intelligence rotates to simulate human mental abilities through computer systems and programs, depending on the complex mathematical algorithms to process and operate the data. Work on developing computer systems has started with intelligent abilities, especially the ability to adapt and learn from past experiences represented by input data. Artificial intelligence (AI) refers to the imitation of human intelligence from machines, basically associated with the concept of human cognitive abilities. Its primary goals include learning, logic, and perception, enabling AI to think, work, and make decisions independently. AI is used in different fields of life and continues to develop with continuous efforts to develop autonomous systems, using advanced algorithms that mimic human flexibility and biological processes. Despite the progress, it lacks a universally accepted definition of AI, as the area is still relatively new and is constantly evolving. Therefore, AI can be defined as software, technologies, or machines that follow human intelligence to perform tasks in the most intelligent, skilled, and accurate way.

ii. Characteristics of artificial intelligence

1. There are many characteristics that characterize artificial intelligence technologies))) and we will discuss them below, As follows:

A) The ability of artificial intelligence to predict and adapt: Artificial intelligence (AI) shows advanced capabilities in prediction and adaptation, making it a powerful tool in different domains. AI can analyze giant data sets and use machine learning techniques to predict natural disasters and increase natural resource management. Big data and the use of predictive analysis to analyze these data have become important practices in many disciplines [8].

b) Monitoring plays a crucial role in harnessing the power of Artificial Intelligence and promoting environmental sustainability. There is an input into decision testing about the world's uncertain states. We show that prophecies allow risky decision-making and that it has an effect on the productivity seen, although it may also increase the variance of the results. We consider the role of human judgment in decision-making as prediction technology improves [9] . We can observe the possibility of artificial intelligence to predict and adapt in many practical examples, such as the ability to fix spelling errors in utilitarian software used in writing programs on your computer or a user type word to predict, as can be seen in the Google Search engine. In addition, AI can provide estimates for traffic movement and travel time or determine the best and shortest passage, as shown in the Google Maps application.

C) Artificial intelligence is capable of motion and perception: Artificial intelligence has the ability to look at the surroundings and make informed decisions, which are fundamental to its movement and interaction skills. Through sensors, cameras, and advanced algorithms, AI can explain visual, auditory, and environmental data to understand and respond to the surroundings. This capacity enables applications such as autonomous vehicles, which safely navigate the roads, and drones that can maneuver through complex areas. The perception of AI is often associated with the decision-making algorithm which allows it to adapt to changing conditions. These features not only increase robotics and its utility in automation but also make it an important player in areas such as healthcare, agriculture, and logistics. As AI continues to develop, its perception and movement properties will further integrate into daily Life simplifies tasks and solves complex challenges. As the study explained [10]. Furthermore, although industrial robots are known to be faster and more accurate than humans, many of the control tasks that humans easily perform in their daily lives are far beyond the efficiency of these robots.

e) Artificial intelligence possesses full autonomy in decision-making without human intervention: Artificial intelligence (AI) has shown autonomous decision-making without human interference in different fields, including health care, marketing, and public administration. This autonomy is achieved through advanced machine learning algorithms and data analysis functions that allow the AI system to process large amounts of information, identify patterns, and determine based on predefined goals. An example of this is in healthcare where AI-based clinical decision support system (CDS) is used quickly in clinical and treatment processes. These systems analyze patient data, medical records, and

even social media to predict health services and recommend autonomous treatment. However, ethical concerns arise regarding the balance between AI autonomy and patient or physician decision-making [11].

f) Cloud computing: Given the huge amounts of data produced every day, it is a major challenge to physically store them. Microsoft Azure is considered one of the most prominent cloud computing programs, as it allows the machine learning model to easily and effectively distribute data stored in the Cloud Server. Smart technologies have many benefits, as they help save time and effort, reduce costs, and improve efficiency and efficiency, as well as their role in protecting workers' lives and safety. However, it also has negative results, which increase the vulnerability of individuals to external hacks and highlight the country's important cyber-attack infrastructure. Therefore, it is necessary to achieve a conscious balance between the benefits of smart technologies and the dangers that result in the resulting dangers. Big data poses challenges to digital transactions, including data storage, transmission, processing, extraction, and service. Cloud computing plays a key role in addressing these challenges through shared computing resources, and the application of these resources has contributed to the remarkable progress in the field of data [12].

iii. The Concept of Cybercrime

Cybercrime patterns have changed technologically since the beginning of the 21st century, particularly with the spread of social media, cloud computing, the Internet of Things, robotics, and cryptocurrencies .This has generated significant cyber threats [13]. The increase in electronic crime has been steady in technology and increasing dependence on the Internet for personal, business, and government operations. As more data is stored online, the possibility of taking advantage of this information for cyber criminals increases. Law enforcement agencies and professionals work on cyber security to deal with electronic crime and to develop strategies and technologies to protect individuals and organizations from the effects. The rise in cybercrime has led to increased awareness and understanding of cybercrime, and understanding its development is crucial for security and political interventions. In research [14]. Cyber threats have emerged since the 1950s, alongside legal issues. This book explores early hacking patterns, antivirus technologies, and the key issues involved. In today's world, information technologies have become an integral part of different aspects of human activity. As a result, the abuse also increases in committing criminal matters. This increasing challenge emphasizes the significant importance of ensuring a strong legal framework to support information

protection, making it an important issue within the spectrum of PR. In a time of information technology, the topic of cyber security attracts global attention. The rapid speed of technological progress has made a significant increase in cybercrimes, which evenly disrupt the operation of states, public institutions, and private companies. These offenses result in adequate financial loss and the normal functioning of organizations and institutions is severely hindered. Cybercrime is a crime committed with the help of or through computer systems, violating the right of information environment subjects to protect information [15]. Using Artificial Intelligence Applications in Devices Police Crime Detection and Prediction: There are many artificial intelligence technologies that have become an essential part of police work, as these techniques have helped to facilitate the process of classifying criminals accurately and fairly. It also helped identify areas and hotspots that cause increased risk and predict a high crime rate there, providing an opportunity to develop active solutions to effectively reduce the risk. Do. In addition, artificial intelligence software has helped forensic experts prove crimes and improve ways of detecting them. So, we explain that This research has two sections, as follows:

g) Employing artificial intelligence applications in investigations and evidence collection: The use of artificial intelligence (AI) in the electronic crime survey and evidence collection changes how law enforcement agencies contact digital forensics and cyber security. AI technologies can automate and improve various aspects of the investigation process, from identifying potential cyber threats to high amounts of digital data to highlighting evidence.

h) AI-powered cyber danger examination: AI-driven cyber threat detection uses advanced algorithms and machine learning techniques to identify and reduce potential safety hazards in real-time. This approach increases the organization's ability to protect against cyber-attacks by analyzing large amounts of data from different sources, including network traffic, user behavior, and system logs. The study [16] . showed that the contemporary digital landscape is characterized by evolving and sophisticated cyber- attacks, the integration of Artificial Intelligence (AI) into cyber security emerges as a pivotal paradigm shift Integration of artificial intelligence (AI) in cybercrime appears as a crucial paradigm shift, In this study showed as follows :

Figure 1: AI and Cyber security

AI can analyze the user behavior and data traffic patterns in the network. When you detect any unusual activity, such as unauthorized access efforts or sudden large data transfer, the system can notify responsible personnel. The study explained [3]. that the application of AI techniques is already being used to assist humans in fighting cybercrimes, as they provide flexibility and learning capabilities to IDPS(Intrusion detection and prevention systems) software. It has become obvious wide knowledge usage in the decision-making process requires intelligent decision support in cyber defense which can be successfully achieved using AI methods.

Predictive analysis is the technology leverages a machine learning algorithm to analyze historical data and identify patterns that may predict a nearby cyber- attack so that this attack can be repelled with preventive measures before it occurs. Prediction markets are extremely important in forecasting crime rates and analyzing criminal policy because the data relevant to decision-makers is so huge, dispersed, and difficult to process efficiently [17].

AI uses deep learning techniques to analyze programs and files, and determine whether they are malicious software based on their signature or behavior. The study [18]. Experimental results demonstrate a 99.54% accuracy in detecting malicious attacks using ensemble machine learning algorithms. The goal is to develop a highly accurate technique for detecting similar malware.AI can analyze a huge amount of data-flowing data from different systems, and help detect hidden threats in this data. Cybercrimes are getting increased with expanding dangers through online fraud and unscrupulous hacking [19].

AI can handle some cyber threats automatically, such as blocking suspected IP addresses or disabled accounts without compromising without the need for human intervention. Cyber-attacks are complex and frequently changing, so human intervention and response are no longer sufficient. The study examines AI-driven automated incident response systems and network security [20].

Natural language treatment models (NLP) can analyze e-posts and text messages to detect phishing efforts or suspected communication.

AI Catboats can be used to collect information from victims or witnesses in case of cyber-attacks and help with the investigation process. The emergence of cybercrime services represents a significant and transformative shift in the field of cybercrime detection. One of the most important research techniques in the field of cybercrime services is how to match supply and demand for their services. In addition to underground marketplaces and dedicated websites, cybercrime forums provide an important channel for cybercrime service providers to attract customers[21] .

iiii. Using artificial intelligence techniques to identify perpetrators

Artificial intelligence technologies used to identify criminals and collect evidence are among the most important modern scientific progress. These techniques have contributed greatly to identifying individuals in airports, ports, roads, and public classes. The study [22] Show that we use facial recognition technology everywhere these days. To understand how to recognize faces, there are three steps: detection, recognition, and verification. First, you must detect any face. Second, you must recognize the face immediately, Finally, It should take some other measures to check if it allows the right person to access. As a result, it has become necessary for a criminal MLA to regulate the use of these techniques by setting up a clear legal structure, conditions, and guidelines for their application in criminal evidence. In this, ensuring recognition of their legal validity by protecting individuals 'rights about individuals' rights against potential abuse of such technologies, is to ensure recognition of their legal validity as acceptable evidence. Consequently, there is a growing need to detect face recognition technologies and the validity of drones in criminal law.

Among the techniques used in this field are Facial Recognition Technology (FRT) that is means, Artificial intelligence has become an important aspect of our daily lives, with face identification technology (face biometry) being one of the most prominent applications. This technique is widely used in safety monitoring and crime prevention, including official documents, border security, airports, ports, and police patrols. It also plays an important role in identifying

criminals by criminals and terrorist acts through the analysis of prison images. In addition, face identification techniques are used to detect suspects by monitoring cameras, enabling considerable distance with accuracy and efficiency and monitoring larger collections from many angles. It is important to point out that traditional criminal investigation methods are ineffective in preventing and responding to crimes because they are very weak. Currently, AI technologies are being applied in various ways, such as video image recognition, crime data mining, and crime prediction before they occur in an attempt to prevent them, thus enhancing police work and criminal investigations [3]. The following diagram illustrates the basic stages of the facial recognition process using artificial intelligence and image processing techniques and algorithms.

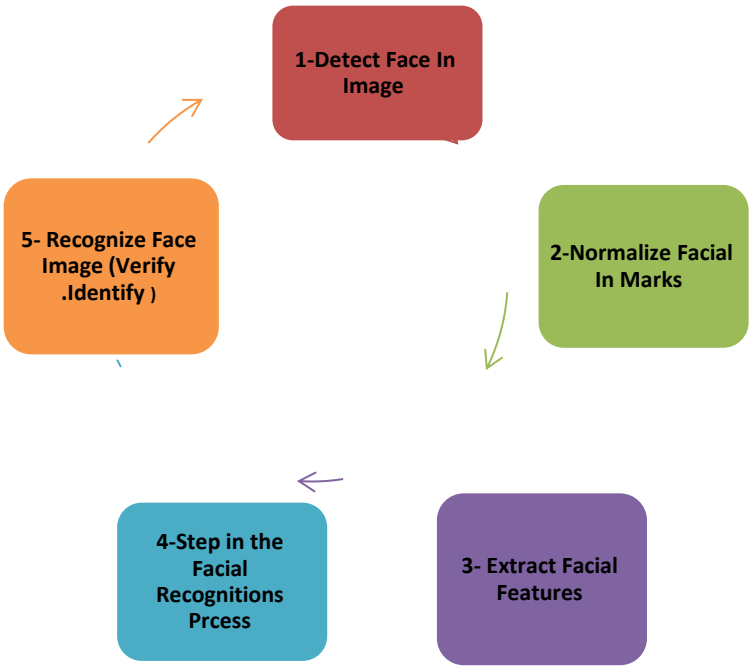

Figure (2): Steps in the Facial Recognition Process

Face Recognition Technology (FRT) is an AI-driven system used to identify or verify individuals by analyzing facial properties. This technique has become increasingly widespread in different applications, including security, law enforcement, and identity confirmation, but it also increases moral concerns about privacy and prejudice. We can explain the steps of facial recognition technology due to its importance in our research, which are represented by the following five stages:

- Detect Face in Image: The system identifies a face location in an image, such as using algorithms such as MTCNN or techniques as the Convolutional Neural Network (CNN).

• Normalize Facial In Marks: After detecting the face, it's far aligned to a healthy widespread sample, making sure proper head orientation and aligning the eyes, nose, and mouth efficiently.

• Extract Facial Features: The system focuses on unique facial features, such as the distance between the eyes, the shape of the nose, and the shape of the jaw, using techniques such as histogram of directed gradients (HOG) or deep learning models like FaceNet and DeepFace.

• Step in the Facial Recognition Process: At this stage, the features that are extracted are compared to a database of facial features using deep learning algorithms or statistical models.

• Recognize Face Image (Verify/Identify):

− If the system (verifies), it compares two faces to determine if they belong to the same person.

− If the system (identifies), it detects a database to find the person matching the founded face.

This is a sequential and cyclical approach to facial recognition technology, which demonstrates that the output at the final stage can be used in a new recognition cycle, thus continuously improving the accuracy and efficiency of the system over time.

In paper [22] , a new model for the performance of face recognition systems in the open-source computer vision field is presented using standardized histograms. It should be noted that face recognition patterns represent a pressing crisis in the field of computer vision. It has received significant attention over the past years due to the numerous demands for it in various fields. Here, we use the Open CV tool for face recognition, which achieves the best results..

Recently, advanced methods have been revealed to bemiring criminals or confirming identity, complementing traditional dependence on the fingers. In these methods, voice imprints and facial recognition have been significantly important in the criminal field, and maintain modern equipment used for accurate identity. These methods depend on the unique and distinctive properties of different parts of the human body, leaving a separate "signature" that separates one person from the other.

A study [23], investigated the ways in which AI-driven facial recognition helps the travel and tourism industry. Using OIPT(Organizational information processing theory), So, Face identification is defined as a technique that uses advanced software that is able to identify facial features from images and distinguish them from other elements within the same image. This technique

compares different facial features to a database that has many images of different individuals. It analyzes the unique properties of the face, such as height and depression that shape the shape of facial properties. These peculiar features act as unique markers used for accurate and effective identity by individuals.

Artificial intelligence technology depends on treating large amounts of data to identify suspicious patterns and behavior. This data may include financial transaction records, network logs, and social media data. The study found [24] concluded that the results obtained by the researcher were collected carefully and cautiously as it was found that 103 research papers out of 2099 acquired effective information sources to address the presented study topics ,Hence, a systematic review of 32 out of 103 research papers in major databases (IEEE Xplore, SAGE, Science Direct, Springer, and MDPIs) was conducted, showing that a large number of them focus on privacy prediction of big data applications using a content-based and hybrid approach, which addresses the main security challenge of big data breach.

Machine learning is used to train models to identify patterns and behaviors associated with online crime. These models can help predict future crimes based on historical data. Predictive police work is the application of analytical techniques - especially quantitative technology - to identify possible goals for police intervention and prevent crime or solve past crimes by making statistical predictions [25] . In the research[26] , machine learning models were used to deal with cybercrime, where Learning models such as Decision Tree (DT), Random Forest (RF), and K- nearest neighbor (KNN) learning models such as Random Forest (RF).

In addition, Smart robots have an important role in investigating crimes, Wise robots have become an integral part of different aspects of human life at the present time, and their adoption is expected to assess situations in the near future and their advanced abilities by determining with minimum miscarratical rates compared to human decisions due to the reason for in the nearest future is expected to increase significantly.

In many countries around the world, there has been a growing dependence on autonomous robots, representing a qualitative leap in safety features. These robots work freely without human intervention and are well suited to handle situations, especially those that induce the risk of human safety. The security assignment has a growing dependence on robots, which recognize specific and very fast, especially in academic fields, and because they are in contact with people and their requests with extensive and accurate information about the

subjects of awareness campaigns. For instance, in 2017, Dubai Police announced the launch of the first artificial intelligence robot in the Arab region, designed to raise awareness about the dangers of drugs in an innovative manner [27]. Similarly, China has initiated experimental projects in the field of robotic policing, where robots patrol public areas to identify and neutralize threats. Although robotic policing is not yet widely prevalent in most countries, the use of robots by law enforcement authorities has yielded positive results[27] . For example, crime rates dropped by 10% from their usual levels in a Mexican city. The presence of robots serves at the very least as a deterrent to crime and, at most, as witnesses and evidence collectors [27] . In a study four-category classification study of security robots was conducted, through which the latest mobile technologies developed for crime-fighting robots were identified, which deal with critical situations using coping strategies [13].

4. Ethical and Legal Considerations in AI-Driven Cybercrime Detection

The use of artificial intelligence (AI) in online crime detection shows significant moral and legal ideas that must be addressed to ensure justice, openness, and responsibility. Since AI systems are more integrated into law enforcement and cyber security practice, it is important to navigate these challenges to protect personal rights and prevent abuse.

i. Privacy Concerns:

Data collection and monitoring are important components for detecting AI-operated cybercrime, but they increase important moral and legal concerns about privacy and personal rights. A large amount of data is required to effectively train the AI system, which leads to extensive data collection and monitoring practices, which must be carefully controlled to prevent abuse and protect personal information. As computer crimes have become increasingly rampant, it challenges the cyber police seriously in many countries around the world [7]. Data protection is a basic concern when it comes to AI-operated online crime detection, as the efficiency of these systems depends a lot on the integrity, privacy, and availability of the data processed by them. It is necessary to ensure strong data protection measures to protect sensitive information from unauthorized access, fractures, and malicious attacks. Automated incident response systems powered by AI are another critical focus area. These systems leverage AI models to execute real-time containment, mitigation, and remediation processes, reducing response times and minimizing human intervention [8].

ii. Algorithmic Bias:

Fairness and Non-Discrimination: AI algorithms can perpetuate biases present in the data they are trained on, leading to unfair or discriminatory outcomes for certain demographic groups[8]. Data collection, algorithm design, and model evaluation are needed to ensure careful attention to ensure justice. Transparency and clarity: A "Black Box" for many AI algorithms makes it difficult to understand how decisions are made, reducing openness and responsibility. Work on developing AI (XAI) is necessary to ensure that AI-driven decisions can be understood and justified .Besides, showing the importance of the fact that transparency expresses a conceptual metaphor of more general significance, linked to knowledge, brings positive connotations that may have normative effects on organizational discussions [4] .

iii. Accountability and Oversight:

One of the drawbacks of AI algorithms is that they perpetuate biases present in the data they are trained on, leading to unfair or discriminatory outcomes for certain demographic groups.. It requires clear guidelines to determine whether the developers, users, or organization that distributes AI is responsible for errors, prejudices, or immoral activities. AI is important to ensure openness and disability in the decision. Then, given a set of social values, AI systems allow for the invocation of a responsible reasoning component to determine whether to be held accountable for certain outcomes and whether to be held accountable for compliance or violation of certain values and concerns [9]. . Human inspection in AI refers to the active participation of people in monitoring, guidance, and intervention in the AI system to ensure moral, accurate, and safe operation. This lets people make AI decisions, correct errors, and stop unexpected results. This inspection is essential in high-day applications such as health care, law enforcement, and finance, ensuring responsibility and adaptation to human values. The study [10] proposes that Signal Detection Theory (SDT) offers a promising framework for better understanding what affects people's sensitivity (i.e., how well they are able to detect errors) and response bias (i.e., the tendency to report errors given perceived evidence of an error) in detecting errors, and an SDT perspective on the detection of inaccuracies is straightforward.

iiii.Legal and ethical compliance:

The Data Protection Regulations in AI are the legal framework designed by the AI system to ensure responsible collection of personal data, processing, and storage. These rules, such as GDPR, mandate transparency, user consent, minimization of data, and responsibility for the protection of privacy in Europe. They also require organizations to prevent abuse and use measures such as date approval, secure storage, and influence assessment to prevent abuse and ensure ethical AI perfectly.

Article [11] It was revealed that the General Data Protection Regulation (GDPR), which is a European Union regulation, will replace the current Data Protection Directive 95/46/EC on May 25, 2018. The GDPR applies directly to each member state and will also apply to organizations outside the EU that process data relating to EU citizens. The General Data Protection Regulation introduced a number of changes from the old regulation, the most significant of which was a significant increase in the maximum fine that can be imposed for violations of the regulation - the maximum fine for "lesser" violations is €10 million or 2% of the organization's turnover; The maximum fine for serious breaches is double this amount. For example, Talk was fined £400,000 in 2015 for allowing hackers to access its customers' data and information under the General Data Protection Regulation. The legal standard for evidence in AI ensures that the data and insight produced by the AI system are acceptable, reliable, and fair in legal negotiations. These standards require transparency in the AI algorithm, traceability of decision -making and data verification used. To understand how AI is being used in the legal sector, the research paper[12] It presents the results of structured interviews and design sessions with a group of community members, where they were asked whether, how, and why they would use AI technologies equipped with large language models to respond to legal issues such as receiving an eviction notice..

5. Results and Discussion

The study highlights the critical role of artificial intelligence (AI) in detecting and preventing online crime. It discusses advancements such as future analysis tools and facial recognition centers, which have proven effective in identifying suspicious activities and predicting crimes. The findings underscore that the implementation of AI technologies, including future police systems and speech and facial recognition techniques, significantly enhances safety by improving the ability to detect and manage various cybercrimes. However, these discoveries also raise important discussions about the ethical and security challenges associated with these technologies.

Despite the obvious benefits of AI techniques, there are concerns regarding privacy and the potential misuse of data and software. For instance, the inappropriate application of facial recognition technologies may lead to violations of personal rights if strict legal protections are not enforced. Additionally, the study indicates that some of these technologies may suffer from accuracy issues or limitations due to algorithmic bias, which can affect their effectiveness in certain contexts.

Consequently, the study emphasizes the need to establish a comprehensive

legal and ethical framework to ensure the responsible and secure use of AI technologies. This highlights the importance of balancing the technical advantages of these systems with the protection of individuals' fundamental rights. Although AI represents a powerful tool for enhancing cybersecurity , it necessitates careful management of the associated challenges to ensure maximum benefits without compromising ethical values.

These applications can be hacked and exposed to cyber threats and attacks, which cause a threat to National security, the right to privacy, and the right to image if misused.

These findings of our research are consistent with [1], [6], [13] which emphasized the role and importance of artificial intelligence in enhancing cybersecurity but also warned of the potential risks associated with its use. These findings indicate that the correct and reasonable use of AI in combating cybercrime requires a careful balance between leveraging its capabilities and ensuring the protection of fundamental rights and freedoms.

6. Conclusion

This research examined the important role of artificial intelligence (AI) both in detecting and preventing online crime and emphasized the important balance between technological innovation and moral ideas. The study discovered challenges and opportunities presented by AI technologies - including machine learning and natural language treatment - to increase cyber security measures. Conclusions indicate that AI has a significant ability to analyze a huge data set, which can enable potential dangers with an identity and increased speed and accuracy of animal patterns. However, the study also emphasized the moral concerns related to privacy and algorithm bias and emphasized the need for strong legal and regulatory structures to ensure AI's responsible distribution in cyber security. In addition, the research provided measures with the goal of developing special training programs for security agencies to improve mechanisms for online crime, increase organizational data security strategies, and facilitate the effective use of AI technologies. In summary, AI represents a powerful tool for combating cybercrime. However, the implementation requires careful assessment to protect fundamental rights and freedom. By using a comprehensive approach that integrates technology, morality, and legal structure, stakeholders can benefit from AI's ability to achieve a more efficient and morally sound cyber security currency.

Finally, this study confirms that artificial intelligence plays an important role in detecting and preventing cybercrime, through a variety of technologies and methods. However, these technologies raise security, ethical, and legal

concerns that must be considered and addressed effectively. Based on these findings, we recommend the following.

1. To analyze data and applications, use intelligent analytical and future indicative programs within the criminal information system, providing accurate information and data. This will help to monitor national security conditions to resolve complex criminal cases and protect the state's internal security and sovereignty.

2. Emphasize the requirement for procedural criminal justice intervention through artificial intelligence applications and security functions. This includes facial recognition technologies and the distribution of highly intelligent robots in investigative functions, including their role in evidence collection.

3. Use data analysis methods to check user behavior on social media platforms to identify extremist tendencies among internet-based radical elements.

4. In order to promote increased cooperation between the public and private sector institutions in cyber security to facilitate information, expertise, and resources.

5. Develop public awareness and educational programs related to risks related to online crime and methods of self-protection.

References

[1] vinayakumar R *et al.*, "Deep Learning for Cyber Security Applications: A Comprehensive Survey," Oct. 12, 2021. doi: 10.36227/techrxiv.16748161.v1.

[2] E. Veltmeijer and C. Gerritsen, "Legal and ethical implications of AI-based crowd analysis: the AI Act and beyond," *AI Ethics*, Jan. 2025, doi: 10.1007/s43681-024-00644-x.

[3] S. Dilek, H. Cakır, and M. Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," *Int. J. Artif. Intell. Appl.*, vol. 6, no. 1, pp. 21–39, Jan. 2015, doi: 10.5121/ijaia.2015.6102.

[4] S. Larsson and F. Heintz, "Transparency in artificial intelligence," *Internet Policy Rev.*, vol. 9, no. 2, pp. 1–16, May 2020, doi: 10.14763/2020.2.1469.

[5] M. A. Alkhazraji, "RIT Digital Institutional Repository Assessing The Effectiveness of Law Enforcement Strategies in Combating E-Crime Using AI," 2024.

[6] Y. W. Kassa, J. I. James, and E. G. Belay, "Cybercrime Intention Recognition: A Systematic Literature Review," *Inf.*, vol. 15, no. 5, pp. 1–25, 2024, doi: 10.3390/info15050263.

[7] Y. Wu, D. Xiang, J. M. Gao, and Y. Wu, "Research on investigation and evidence collection of cybercrime Cases," in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Mar. 2019. doi: 10.1088/1742-6596/1176/4/042064.

[8] J. Buolamwini, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification *," 2018.

[9] M. Dastani and V. Yazdanpanah, "Responsibility of AI Systems," *AI Soc.*, vol. 38, no. 2, pp. 843–852, Apr. 2023, doi: 10.1007/s00146-022-01481-4.

[10] M. Langer, K. Baum, and N. Schlicker, "Effective Human Oversight of AI-Based Systems: A Signal Detection Perspective on the Detection of Inaccurate and Unfair Outputs," *Minds Mach.*, vol. 35, no. 1, Mar. 2025, doi: 10.1007/s11023-024-09701-0.

[11] J. Kingsto, "Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation," 127AD.

[12] M. Hagan and S. Law School, "Towards Human-Centered Standards for Legal Help AI," 2023. [Online]. Available: https://ssrn.com/abstract=4582745

[13] A. Ezzat, M. Elhaw, D. Hany, and S. Elanany, "The Use of Artificial Intelligence in Investigating, Combating and Predicting Various Crimes through Understanding the Psychology of Perpetrators," 2023. [Online]. Available: https://jrtdd.com

[14] A. K. Agrawal, J. S. Gans, and A. Goldfarb, "Exploring the Impact of Artificial Intelligence: Prediction versus Judgment," 2018. [Online]. Available: http://www.nber.org/papers/w24626

[15] W. L. Perry, B. McInnis, C. C. Price, S. C. Smith, and J. S. Hollywood, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations." [Online]. Available: www.rand.org

[16] M. Beetz, M. Buss, and D. Wollherr, "Cognitive Technical Systems-What Is the Role of Artificial Intelligence?" [Online]. Available: www.cotesys.org

[17] C. Yang, Q. Huang, Z. Li, K. Liu, and F. Hu, "Big Data and cloud computing: innovation opportunities and challenges," Jan. 02, 2017, *Taylor and Francis Ltd.* doi: 10.1080/17538947.2016.1239771.

[18] "Outline of Cybercrime: The Transformation of Crime in the Information Age, 2nd edition." [Online]. Available: https://ssrn.com/abstract=4707509

[19] N. Allahrakha, "Transformation of Crimes (Cybercrimes) in Digital Age," *Int. J. Law Policy*.

[20] T. Batrachenko, I. Lehan, V. Kuchmenko, V. Kovalchuk, and O. Mazurenko, "Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies," 2024, *Malque Publishing*. doi: 10.31893/multiscience.2024ss0212.

[21] V. Varma Vegesna, "Enhancing Cyber Resilience by Integrating AI-Driven Threat Detection and Mitigation Strategies," 2023.

[22] F. Gibelli, G. Maio, and G. Ricci, "Editorial: Healthcare in the age of sapient machines: physician decision-making autonomy faced with artificial intelligence. Ethical, deontological and compensatory aspects," 2024, *Frontiers Media SA*. doi: 10.3389/fmed.2024.1477371.

[23] "Predicting Crime." [Online]. Available: http://ssrn.com/abstract=1118931https://ssrn.com/abstract=1118931Electroniccopyavailableat:https://ssrn.com/abstract=1118931

[24] J. Singh and J. Singh, "Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms," *Inf. Softw. Technol.*, vol. 121, May 2020, doi: 10.1016/j.infsof.2020.106273.

[25] H. A. Rahaman, "A Proposed Model for Cybercrime Detection Algorithm Using A Big Data Analytics," *Int. J. Comput. Sci. Inf. Secur. IJCSIS*, vol. 18, no. 6, pp. 146–153, 2020.

[26] S. Abdul and S. Muhammad, "AI for Cyber Security: Automated Incident Response Systems." [Online]. Available: https://www.researchgate.net/publication/383825151

[27] U. Akyazi, M. Van Eeten, and C. H. Gañán, "Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum." [Online]. Available: https://www.cambridgecybercrime.uk/datasets.html