Pak. j. life soc. Sci. (2024), 22(2): 9519-9535 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.00721

RESEARCH ARTICLE

The Future of Criminal Law in the Age of Electronic Crimes and Artificial Intelligence

Dr. Ahmad Hazim Mustafa

Salahaddin University, College of Law, Erbil, Iraq

ARTICLE INFO

Received: Aug 16, 2024

Accepted: Oct 22, 2024

Keywords

Electronic Crimes

Criminal Law

Artificial Intelligence

***Corresponding Author:**

ABSTRACT

As technological advancements continue to reshape our world, the realm of criminal law faces unprecedented challenges and opportunities. The proliferation of electronic crimes and the rise of artificial intelligence (AI) have generated complex legal, ethical, and practical considerations for criminal justice systems worldwide. This research paper delves into the multifaceted impact of electronic crimes and AI on criminal law, examining how they alter traditional legal paradigms, discussing emerging legal frameworks, and addressing the implications for individual rights and societal norms. By exploring various case studies and analyzing the evolution of legislation, this paper seeks to provide insight into the evolving landscape of criminal law in the age of electronic crimes and artificial intelligence

INTRODUCTION

In the contemporary context of the swiftly progressing digital environment, the issue of information security has arisen as a matter of utmost importance. The advent of the internet and networked gadgets has brought us a period of unparalleled ease, however it has also exposed consumers to the escalating dangers of electronic crimes. The emergence of the virtual realm has led to the emergence of a novel category of weaponry known as digital assaults. These attacks only occur within the domain of cyberspace, yet possess a level of effectiveness that is comparable to conventional physical threats. Among the various types of cyberattacks, those directed on critical infrastructure, such as power grids and military systems, present notably grave risks, since they have the capacity to cause catastrophic failures.

The potential ramifications of these technological offenses can be significant. Cyber attacks has the capability to disrupt computer networks and telecommunications systems, resulting in the inaccessibility of crucial data and jeopardizing the performance of essential services. As the dependence of society on networked technology grows, there is a growing imperative to address the associated hazards.

Significantly, financial and medical organizations have emerged as primary targets for these assaults because to the sensitive nature of the data they manage. The rapid increase of frameworks, data repositories, cloud services, apps, and devices has significantly enlarged the attack surface, hence

providing bad actors with a greater number of possibilities to exploit weaknesses inside the network. In light of this, businesses and organizations are endeavoring to attain a position of superiority in this digital realm by using the capabilities of artificial intelligence (AI) and other emerging technologies.

The utilization of artificial intelligence, characterized by its capacity to do accurate mathematical calculations and complex numerical evaluations, has demonstrated its efficacy as a powerful asset in safeguarding the authenticity and security of the digital domain. Significant applicability has been observed in the detection and mitigation of unforeseen digital assaults across various cyberspaces, encompassing web-based platforms as well as highly fortified websites. One of the main functions of this system is to detect illicit content on government websites and identify cyberattacks in their early phases, enabling the implementation of preventive countermeasures.

Artificial intelligence (AI) serves as a pivotal component in ensuring online security, therefore instigating a significant transformation in the domain of criminal law. The utilization of computational reasoning techniques presents novel opportunities for enhancing cybersecurity measures in response to the increasing challenges faced by electronic criminal activities. Artificial intelligence (AI) systems has the capability to rapidly analyze extensive quantities of data, enabling them to identify patterns that may signify hostile activity. Consequently, these systems can promptly react to counteract such threats. Nevertheless, the integration of artificial intelligence (AI) inside the criminal law framework presents a distinct array of obstacles. The legal framework should be modified to effectively address the complexities of electronic offenses and the dynamic strategies adopted by those engaging in cybercriminal activities. Achieving an optimal equilibrium between upholding individual privacy rights and facilitating the implementation of efficient AI-based security measures is a nuanced undertaking that needs meticulous deliberation.

Problem Statement

The subject of criminal law has been confronted with new issues and complications due to the fast progress of technology, namely in the areas of electronic communication and artificial intelligence. The increasing interconnectivity and dependence on digital systems inside society have led to a significant rise in electronic crimes, necessitating the adaptation and evolution of legal systems. In addition, the incorporation of artificial intelligence (AI) into many aspects of everyday existence gives rise to significant inquiries on legal responsibility, privacy, and the limits of criminal culpability.

The objective of this issue statement is to tackle the complex difficulties presented by electronic crimes and artificial intelligence within the framework of criminal law. The primary aims of this study are to comprehend, evaluate, and provide resolutions for the subsequent significant concerns:

The present discourse aims to delineate and classify electronic crimes, encompassing activities such as hacking, identity theft, online fraud, and cyberbullying. It is evident that the exponential growth of these offenses has beyond the capacity of the legal framework to effectively address them. The precise definition and categorization of these offences are of utmost importance in ensuring efficient law enforcement and equitable judicial proceedings.

The issue of jurisdiction and international cooperation is particularly salient in the context of electronic crimes, since these offenses frequently transcend national boundaries, hence presenting intricate issues in terms of determining legal authority. The establishment of mechanisms for international collaboration in the investigation and prosecution of these crimes is imperative in order to guarantee the accountability of offenders, irrespective of their geographic whereabouts.

The incorporation of artificial intelligence (AI) across several domains, such as law enforcement, gives rise to concerns regarding the legal and ethical ramifications of choices made by AI systems. The difficulty of ascertaining the allocation of legal culpability in circumstances involving acts or choices created by artificial intelligence is of considerable importance.

The utilization of electronic surveillance techniques and artificial intelligence algorithms in the context of predictive policing raises significant concerns regarding the potential violation of individual privacy rights. The delicate task of reconciling the need of safeguarding public safety with the imperative of upholding civil freedoms necessitates meticulous legal analysis.

The problem lies in guaranteeing the admissibility and accuracy of digital evidence during judicial proceedings. The necessity for updated evidence rules is emphasized by the technical challenges related to data integrity and the possibility for manipulation.

In order to successfully investigate, prosecute, and defend cases in the ever-changing environment of electronic crimes and artificial intelligence (AI), it is imperative for legal professionals and law enforcement organizations to possess a comprehensive understanding of these complex domains. This necessitates the development of capacity building initiatives and the acquisition of legal expertise in the nuances of electronic crimes and AI. It is crucial to address the knowledge disparity.

The regulation of artificial intelligence (AI) in the context of criminal activities is a pressing concern due to its potential exploitation for illicit purposes, including the creation of malicious software and the execution of sophisticated fraudulent schemes. It is of utmost importance to establish policies that effectively tackle these developing concerns, all the while promoting the responsible development of artificial intelligence.

The determination of suitable penalties for electronic crimes, taking into account the intangible character of harm, necessitates the use of creative methodologies. Furthermore, it is imperative that the rehabilitation of criminals is in accordance with the dynamic and evolving technology environment.

The objective of this issue statement is to promote collaborative study across several disciplines, including legal academics, technologists, ethicists, policymakers, and law enforcement organizations. The objective is to formulate inclusive and flexible approaches within the context of criminal law frameworks in order to effectively tackle the difficulties presented by electronic crimes and the emergence of artificial intelligence. In an era characterized by the proliferation of digital technologies and the rise of artificial intelligence, it is imperative to devise efficacious strategies that prioritize the preservation of justice, the protection of civil rights, and the preservation of the rule of law..

Research Questions

Examining the Dynamic Terrain of Criminal Law: Navigating the Realm of Electronic Offenses and Artificial Intelligence. The present study aims to examine the profound effects of electronic crimes and artificial intelligence on the domain of criminal law. This study seeks to predict the necessary legal adjustments to successfully manage new dangers posed by cybercrimes, including hacking and identity theft, as well as the increasing involvement of artificial intelligence in criminal activities. Through an analysis of these difficulties, the study attempts to provide insights into the appropriate legal measures needed to tackle these evolving issues. This analysis explores many aspects related to jurisdiction, privacy, evidential standards, and responsibility within the dynamic framework under consideration. This research makes a valuable contribution to the field by examining the complex relationship between technology improvements and legal frameworks. By analyzing this interaction, the study aims to enhance the creation of legal tactics that are both adaptable and successful. The ultimate goal is to safeguard justice and security in the midst of evolving criminal landscapes.

Relevance and Significance

In contemporary society, a wide range of activities, spanning from individuals' personal lives to their financial transactions, are being handled through online platforms. All elements inside our environment are interconnected, accompanied by various forms of adaptable processing of electronic data. The numerous advancements that have been made have resulted in an increased susceptibility and vulnerability of human life to potential damage. This phenomenon possesses the capacity to engender

financial calamities, individuals engaging in dishonest practices, and other unfavorable outcomes. Therefore, it is imperative to prioritize the safeguarding of networks in the contemporary era of extensive automation. It offers individuals with a sense of security, safeguarding them against fraudulent activities and many types of violations. Nevertheless, the efficacy of digital protection will be subject to scrutiny. Both individual individuals and major organizations alike are increasingly susceptible to various cyber threats, including phishing scams, ransomware attacks, personal assaults, data breaches, and financial damages. According to a NetScout investigation, it has been observed that malevolent actors possess the capability to infiltrate any internet-connected gadget, including but not limited to smartphones, wristwatches, computers, and televisions, within a very short span of five minutes.

Currently, the predominant function of artificial intelligence (AI) is to deploy sophisticated, knowledge-based systems capable of efficiently and precisely managing a wide range of cybercrimes, both of little and big significance. The advancement of artificial intelligence necessitates the capability of AI applications to effectively respond and adjust to emerging obstacles and dangers. The utilization of artificial intelligence is imperative in network security due to the substantial magnitude of sensitive data being communicated across the internet. In order to effectively handle the vast quantities of data and mitigate the risk of unauthorized access, the implementation of a network security framework reliant on artificial intelligence is needed. The utilization of this tool has the potential to enhance the efficiency of problem identification. It is quite probable that cybercriminals have already gained unauthorized access to these systems and are already biding their time for an opportune moment to execute their malicious activities. Artificial intelligence possesses the capacity to effectively perform rapid situational analysis, recognize potential threats, and implement appropriate measures for mitigation. Nevertheless, it has become a conventional instrument for achieving the highest level of network security and efficiently handling substantial volumes of data to enhance threat detection and optimize response strategies.

LITERATURE REVIEW

The methodologies employed and the objectives pursued in the many crime prediction research and applications documented in our collected publications exhibited considerable variation. Numerous crime prediction methodologies have been devised for general crimes and scenarios, employing diverse models that have been evaluated in order to identify the most efficacious approach based on the given dataset. In a study done by Kim et al. (2019a), machine learning techniques were employed to forecast general criminal activities. Nevertheless, several approaches have been devised to address certain types or classifications of crimes. For instance, Srivastava et al. (2008) employed a hidden Markov model (HMM) to analyze the sequence of activities in credit card transactions. Previous studies have concentrated on conducting a comparative examination of various learning model types. For instance, Babakura et al. (2015) conducted a study in which they compared two classification algorithms, namely naïve Bayes and backpropagation, to predict crime categories using a specific dataset. The experiment was conducted using a 10-fold cross-validation technique. The results indicate that the naïve Bayes algorithm outperformed the backpropagation algorithm when applied to the crime dataset using the Weka software. Furthermore, a subset of the publications exhibited notable distinctions with respect to their stated goals. For instance, Nasridinov et al. (2013) conducted a study whereby they utilized several learning models and algorithms to examine their efficacy across diverse datasets. The researchers reached the conclusion that the selection of a model type should be done with careful consideration of the dataset at hand, since different model types exhibit varying degrees of compatibility with certain datasets.

Data Mining Techniques for Crime Prediction

Conversely, several recent surveys have investigated techniques for crime prediction. Saravanan et al. (2021) conducted a survey that examines several data mining techniques for crime prediction, focusing on elements such as socioeconomic indicators, spatial-temporal patterns, demographic characteristics, and geographic qualities. Moreover, Butt et al. (2020) conducted a comprehensive assessment of the literature, focusing on the identification and forecasting of spatiotemporal crime hotspots. The authors presented their findings and insights in this regard. The authors presented the methodologies of machine learning (ML) and data mining in the context of hotspot identification. They also discussed the efficacy of these techniques and highlighted the difficulties associated with constructing a spatiotemporal crime prediction model. In a separate study, Kawthalkar et al. (2020) conducted a comprehensive analysis of several technology mapping approaches used in the context of crime prediction inside smart cities. The researchers considered many variations of criminal portrayals and conducted a comparison analysis. The authors posit that a multitude of concepts and methodologies have been established for the purpose of crime prediction; nonetheless, they contend that the practicality and effectiveness of these techniques can only be ascertained via rigorous field testing. Furthermore, the authors in the study conducted by Albo (n.d.) place their emphasis on artificial neural networks and convolutional network approaches in the context of crime prediction.

Urban Safety and Security in Crime Analysis

Safety and security are crucial elements that enhance the overall quality of life in urban environments. In their work, Zhao and Tang (2018) provided a comprehensive review that encapsulated the field of crime analysis in urban data. They examined several criminal task algorithms and delved into the theoretical underpinnings of criminology. Furthermore, Shamsuddin et al. (2017) conducted a concise and accessible survey about the utilization of crime prediction tools and the potential for their enhancement in further research. The researchers employed Support Vector Machines (SVM), fuzzy theory, artificial neural networks, and multivariate time series as machine learning techniques. In contrast, a comprehensive analysis and prediction of criminal activities were conducted by Fredrick David KR et al. (2017), who examined both supervised and unsupervised methodologies for crime detection

APPROACH AND METHODOLOGY

The fundamental principles of information security theory as they pertain to the management of extensive repositories of data. The use of this resides in the application of artificial intelligence and its diverse range of methodologies. These tactics can be subject to various alterations, and there is an ongoing development of new resources to accommodate their evolving usage and scope. These measures can be included into pre-existing or newly developed software to mitigate or eradicate cyber security risks and attacks. The use of this technology extends to several practical domains, such as email security, detection of phishing attacks, identification of malware, detection of anomalies in network behavior, prevention of network attacks, safeguarding sensitive data, prevention of fraudulent activities, and mitigation of identity theft risks. The future talks will focus on the idea of applying various algorithms for the identification of strategies.

Using Artificial Intelligence to Recognize Potential Dangers in Email

Due to technological developments, the quantity of email traffic is increasing. Currently, email is the most secure mode of internal business communication for confidential information. This has led to an increase in attempts to prevent spam emails from being sent from corporations and other institutions. Email is the most common vector for cyberattacks because of the sheer volume of information it transports. The creation of algorithmic methods of machine learning is urgently required. The perceptron, in its purest form, is analogous to a neuron in the brain. By constructing layered structures at varying input levels, the perceptron model can achieve a functioning that is functionally comparable.

The input data is turned into the output based on the importance of the synthesized input values. These weighted input values are then used to trigger an activation function at a predetermined threshold. The key distinction between classical models and AI models is the latter's usage of iterations to attain optimal value. To make the most of AI for spam detection, it is necessary to create tasks at which spam filters can excel. The filters' algorithms are in charge of sorting emails based on whether or not they include a set of potentially malicious phrases. The frequency with which certain suspicious words or symbols appear can be used to assign a weight to them. Once the cutoff point is established, the incoming emails may be sorted accordingly. By definition, ham messages have values below the threshold limit, whereas spam messages have values over the limit. The AI is supposed to use the data about spam and ham to fine-tune the threshold value.

Initial spam detections are created using static rules and regular expressions. A threshold study must be performed, and new approaches must be developed, to bring the spam filters up to date. This is because spammers are constantly adapting their strategies. The filters need to be constantly updated, thus it's best to choose a dynamic approach, since static rules may become outdated very soon. The user's participation is also required for success in this endeavor. Numerous methods exist for verifying text, including computer vision and natural language processing, which may be used to spot any discrepancies or questionable passages.

Malware Analysis and DetectionMalware, short for "malicious software," is created by hackers and other bad actors with the goal of infecting a single computer or a network of computers. The objective is to get unauthorized access to the organization's data by means of an assault on the system or networks or by exploiting vulnerabilities in such systems or networks. If the assault is successful, it might lead to the loss of private data and possible harm to the network infrastructure. Threats of this nature pose the greatest risk to the system. Spam emails are sent with the intent of spreading malware across a computer network. It is crucial to detect any malicious software since it is simple to conduct additional assaults after a machine or network has been breached. As a result, identifying the binary files that make up the malware is the first step in the analysis process. These binary files must be partitioned from any files that might contain malicious code before being saved to the system. Sometimes even non-executable file types like documents might harbor malware. An infected internet connection, generally a local area network or wireless network, compromises the machine files on an infected computer.Human intervention is no longer practical for reliably recognizing potentially harmful threats in light of the ever-increasing influx of information. To counteract this, experts have created algorithms to analyze malware automatically. In this method, a professional in malware conducts an initial investigation. After that, AI technologies are used in these assessments to classify the numerous dangers that have been identified. Analysts often adjust analyses in order to enhance algorithm updates and hence the defenses against cyberattacks. The procedure of fine tuning can be done either automatically or by hand. Malware poses a wide range of potential threats. A handful of them will be discussed in the following paragraphs:

Trojans are a type of harmful software that have the ability to disguise themselves as legitimate applications. The major purpose of this particular form of malicious software is to gain unauthorized access to the user's computer system and assume control over it.

Downloaders are a type of software that, when launched, can result in the installation of malware on a computer. Once an internet connection is established, this malware allows infected distant servers to gain unauthorized access to the compromised system.

Rootkits are a type of files that are specifically crafted to evade detection inside the operating system of a user, all the while acquiring unfettered privileges to access the user's data.

Botnets are a form of malicious software that is orchestrated by individuals with malicious intent or criminal motives, with the objective of acquiring personal or financial information.

A zero-day exploit refers to a type of malicious software that lacks antivirus signatures. The lack of these fingerprints hinders the system's ability to discern the pathogen.

Ransomware is a type of malicious software that involves the infiltration of a computer system with the intention of preventing the user from accessing specific critical documents or data. Access to the premises is contingent upon the completion of a monetary transaction; thus, it is imperative that you promptly proceed with the payment.

These many circumstances can be merged into a unified file, with the subsequent course of action being determined by the system's security settings administration. Given the extensive range of malware in existence, it is imperative to devise distinct approaches for the identification of each specific threat. Calculating file hashes, monitoring system and network activities, and doing system monitoring are all crucial undertakings. The identification of potential hazards inside the system can be facilitated by the utilization of hash file computations. System monitoring becomes important when either the hardware or the software exhibits abnormal behavior. The necessity of network monitoring arises when there is evidence of atypical associations, whether observed on the internet or inside the internal network of an organization.

Attacks from the Internet and Strange Behavior from Networks

In recent years, there has been a significant increase in the prevalence of interconnected devices. The obsolescence of traditional approaches to perimeter security has been brought about by the increasing prevalence of network-based breaches. Therefore, it is imperative to utilize automated methods for detecting possible security breaches within the network. One such strategy that may be employed is the utilization of the signature-based detection method. This approach may be utilized to establish a comprehensive repository of attack signatures that have been previously detected. The integration of this database with others results in the activation of an alarm system if the presence of questionable signatures is detected. The artificial intelligence has the capability to automate the task of ensuring the database remains up-to-date, a crucial aspect in this particular context. The subsequent stage is identifying any inconsistencies. This technique involves the monitoring and analysis of network activity in order to create a baseline for typical behavior. Data is collected and assessed about the typical patterns exhibited by traffic, encompassing the quantity of connections coming from a certain host, any atypical connections, any instances of heightened traffic, and any fluctuations in network capacity. An anomaly may be characterized as any departure from the established norm or a potentially questionable trend observed within the dataset.

FINDINGS AND RESULTS

Methods for Crime Prediction

Supervised learning and unsupervised learning are the primary methodologies employed in the fields of artificial intelligence (AI) and machine learning (ML), respectively. The primary differentiation between supervised and unsupervised learning is in the utilization of labeled data for direct prediction. There are other variations, exclusions, and significant domains in which one technique demonstrates superiority over the other.

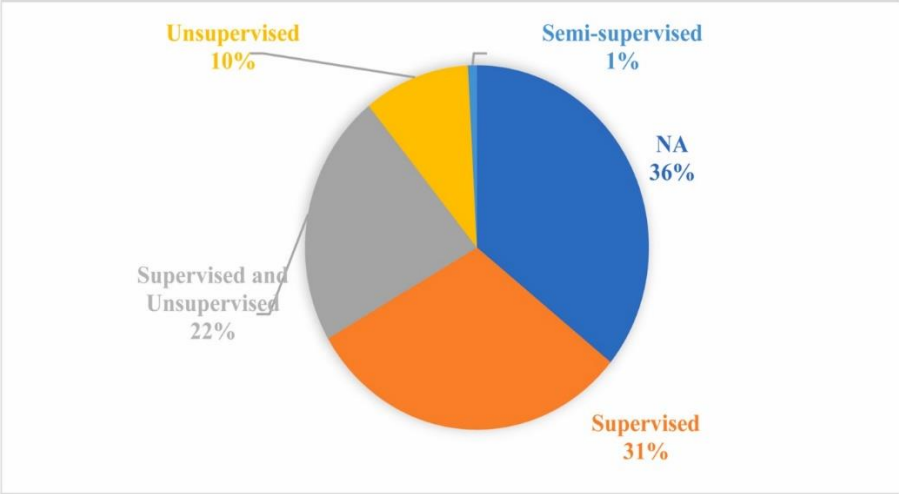
The utilization of labeled datasets is of paramount importance in the implementation of the supervised learning approach. The purpose of these data sets is to be utilized in the training and monitoring of algorithms for accurate data identification and prediction. By utilizing the annotated inputs and corresponding outputs, the model will autonomously assess its own correctness and progressively enhance its performance over a period of time. Moreover, within the realm of supervised learning, there are two distinct categories of problems, namely classification and regression.

In order to effectively differentiate between dogs and cats, the field of Machine Learning employs a classification algorithm to classify and categorize test data. Another practical example is the act of

filtering one's email inbox to identify and subsequently delete unsolicited and unwanted communications, commonly referred to as spam.

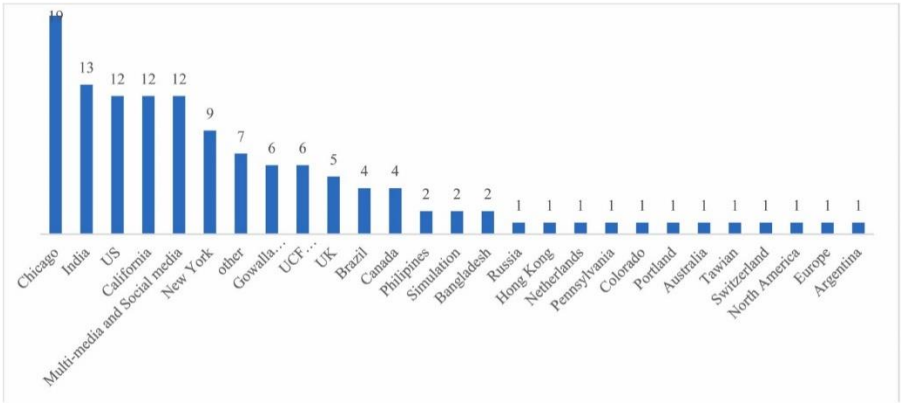
The differentiation between supervised learning and unsupervised learning lies in the presence of labeled input and output data in the former, whereas the latter lacks such labeling. In the context of supervised learning, the algorithm is provided with feedback in the form of corrected predictions and weights, which are derived from the training data. The objective of unsupervised learning is to train a model to comprehend the inherent structure of unlabeled data. In contrast, semisupervised learning is a hybrid approach that can be employed when the training dataset comprises both labeled and unlabeled instances. The performance of the semisupervised technique is enhanced when the number of labeled samples in the dataset is smaller than the number of unlabeled samples. Despite its reputation for complexity, researchers continue to utilize this strategy. In the study conducted by Tundis et al. (2019), the authors employed a semi-supervised approach utilizing bags of words to assess textual data, namely tweets pertaining to criminal activities, in the context of A108.

According to the depicted figure, around 31% of the existing research on crime prediction pertains to the domain of supervised learning. Furthermore, it is worth noting that 22% of the overall research articles used a combination of supervised and unsupervised methods. This is attributed to the fact that several studies utilized more than one machine learning methodology. However, just a mere 10% of individuals employed unsupervised learning techniques. Remarkably, a mere 1% of the investigations implemented a semisupervised approach, suggesting that the utilization of this technique in the realm of crime prediction is infrequent. Ultimately, a notable proportion of the research, specifically 36%, exhibited a lack of clarity on the specific approach employed.



Benefits and limitations associated with contemporary prediction technologies.

The random forest model has gained significant popularity in the field of crime prediction due to its ability to effectively handle colinear information, high dimensionality, and heterogeneous space (Rumi et al., 2018; Umair et al., 2020; Wheeler & Steenbeek, 2020). Additionally, A93 has discovered that the model demonstrates a high level of accuracy in predicting crime rates over an extended period of time. Nevertheless, the random forest model does include significant limitations. Due to the repetitive nature of learning the model and creating the tree, the effectiveness of these processes is constrained by time limitations. Furthermore, the model's performance is limited due to insufficient data and a scarcity of accessible resources. The use of deep learning techniques to the issue of crime prediction has exhibited promising preliminary outcomes.



There are several advantages and merits associated with the utilization of advanced neural network approaches, such as deep neural networks, partially generative neural networks, hierarchical recurrent networks, and enhanced associative neural networks. As mentioned in prior studies (Huang et al., 2018; Lin et al., 2018; Seo et al., 2018), the models under consideration exhibit higher AUROCs, effectively capturing the temporal significance of crime incidents. Additionally, these models demonstrate the ability to predict crime occurrences across various categories within different sectors of urban areas. Furthermore, they facilitate the replication, transmission, and ongoing enhancement of the knowledge model, while also offering a more objective foundation for comparative analysis.

CONCLUSION AND RECOMMENDATIONS

The convergence of electronic crimes and artificial intelligence heralds a new era in criminal law. This paper has explored the dynamic landscape of criminal behavior in the digital age, examining the evolution of electronic crimes, the integration of AI in criminal justice, legal responses to emerging challenges, the delicate balance between individual rights and security, and relevant case studies. As society grapples with these transformative forces, the role of criminal law must adapt to ensure justice, security, and respect for human rights in an increasingly interconnected world.

As AI has a variety of tools that contribute to cyber security, there are still some areas that need additional research that is more focused. There are certain inaccuracies associated with the models that are currently available. As was just mentioned, there is a possibility of producing false alarms when testing such models. In areas where research is still being done, there is also the possibility of malware attacks that are carried out by themselves. Due to the design of increasingly complex models, there is an ongoing requirement to provide training and support in order to enhance these models. However, the same technologies that are used to prevent and detect cyber threats can also be used to activate similarly dangerous attacks. Attacks on the security of computer systems or computer networks can be made more flexible and critical when AI techniques are used. As a result, more robust models are required to detect attacks of this critical nature.

The most applied algorithm utilized in crime prediction is random forest and naïve Bayes. Twenty-five papers applied random forest and 20 papers applied naïve Bayes, whereas 17 papers utilized the decision tree algorithm. In addition, most of the scientific papers used hybrid models that applied more than one ML algorithm. Furthermore, the most utilized approach in the field of crime prediction is the supervised learning approach, with a percentage of 31%. Moreover, 22% of the research papers collected used a supervised and unsupervised approach. 10% applied unsupervised learning. The most applied algorithm utilized in crime prediction is random forest and naïve Bayes. Twenty-five papers applied random forest and 20 papers applied naïve Bayes, whereas 17 papers utilized the decision tree algorithm. In addition, most of the scientific papers used hybrid models that applied more than one ML algorithm. Furthermore, the most utilized approach in the field of crime prediction is the supervised learning approach, with a percentage of 31%. Moreover, 22% of the research papers collected used a supervised and unsupervised approach. 10% applied unsupervised learning. The most applied

algorithm utilized in crime prediction is random forest and naïve Bayes. Twenty-five papers applied random forest and 20 papers applied naïve Bayes, whereas 17 papers utilized the decision tree algorithm. In addition, most of the scientific papers used hybrid models that applied more than one ML algorithm. Furthermore, the most utilized approach in the field of crime prediction is the supervised learning approach, with a percentage of 31%. Moreover, 22% of the research papers collected used a supervised and unsupervised approach. 10% applied unsupervised learning.

The current increase in technology has led to an increase in the number of cyber attacks and security threats. It is essential to have models that are not only flexible but also more robust and can be scaled according to the data that is at hand. Throughout the course of this report, a variety of AI strategies for detecting and preventing potential breaches of cyber security have been discussed. In addition to the applications of artificial intelligence, there are also applications of deep learning that protect the network's security. Combinations of techniques drawn from biology and those based on machine learning can provide enhanced defense against these kindsof dangers. There are still new areas that need to be developed so that knowledge of artificial intelligence can be used to improve the capabilities of systems and create cyber security. One of these areas is the field of artificial intelligence.

REFERENCES

Al-Yaseen W. L., et el (2017) Multi Level Hybrid support vector machine and extreme learningmachine based on modified K-means for intrusion detection. Future Generation Computational Systems Vol 79.

Garg S., Batra S. (2018) Fuzzified Cuckoo based clustering technique for network anomalydetection, Computational Electronic Engineering, Vol 71.

Hashemi H., Azmoodeh A., Hamzeh A. (2017) Graph embedding as a new approach for unknown malware detection. Journal of Computational Viral Hacking Techniques Vol 13p.153-166.

Parisi A. (2019) Hands on Artificial intelligence for Cyber Security, Packt Publishing Ltd.

Sahingoz O. K., et el (2019) Machine Learning based phishing detection from URLs, ExpertSystem Application, p.345-357.

Kim, S., Joshi, P., Kalsi, P. S., & Taheri, P. (2019a). Crime Analysis Through Machine Learning. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018, 415–420. https://doi.org/10.1109/IEMCON.2018.8614828

Kim, S., Joshi, P., Kalsi, P. S., & Taheri, P. (2019b). Crime Analysis Through Machine Learning. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018, 415–420. https://doi.org/10.1109/IEMCON.2018.8614828

Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. K. (2008). Credit card fraud detection using Hidden Markov Model. IEEE Transactions on Dependable and Secure Computing, 5(1), 37–48. https://doi.org/10.1109/TDSC.2007.70228

Babakura, A., Sulaiman, M. N., & Yusuf, M. A. (2015). Improved method of classification algorithms for crime prediction. Proceedings - 2014 International Symposium on Biometrics and SecurityTechnologies, ISBAST 2014, 250–255. https://doi.org/10.1109/ISBAST.2014.7013130

Nasridinov, A., Byun, J. Y., Um, N., & Shin, H. S. (2016). Application of data mining for crime analysis. Lecture Notes in Electrical Engineering, 354, 503–508. https://doi.org/10.1007/978-3-662-47895- 0_61

Nasridinov, A., Ihm, S. Y., & Park, Y. H. (2013). A decision tree-based classification model for crime prediction. Lecture Notes in Electrical Engineering, 253 LNEE, 531–538. https://doi.org/10.1007/978-94-007-6996-0_56

Saravanan, P., Selvaprabu, J., Arun Raj, L., Abdul Azeez Khan, A., & Javubar Sathick, K. (2021). Survey on Crime Analysis and Prediction Using Data Mining and Machine Learning Techniques. Lecture Notes in Electrical Engineering, 688, 435–448. https://doi.org/10.1007/978-981-15-7241-8_31

Butt, U. M., Letchmunan, S., Hassan, F. H., Ali, M., Baqir, A., & Sherazi, H. H. R. (2020). SpatioTemporal Crime HotSpot Detection and Prediction: A Systematic Literature Review. In IEEE Access (Vol. 8, pp. 166553–166574). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3022808

Kawthalkar, I., Jadhav, S., Jain, D., & Nimkar, A. V. (2020, February 1). A Survey of Predictive Crime Mapping Techniques for Smart Cities. 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020. https://doi.org/10.1109/NCETSTEA48365.2020.9119948

Albo, F. (n.d.). A Survey of Research into Artificial Neural Networks for Crime Prediction. Retrieved May 21, 2021, from https://www.researchgate.net/publication/336116157

Zhao, X., & Tang, J. (2017). Modeling temporal-spatial correlations for crime prediction. International Conference on Information and Knowledge Management, Proceedings, Part F1318, 497–506. https://doi.org/10.1145/3132847.3133024

Zhao, X., & Tang, J. (2018). Crime in urban areas: A data mining perspective. In arXiv. arXiv. https://doi.org/10.1145/3229329.3229331

Zhu, Q., Zhang, F., Liu, S., & Li, Y. (2019). An anticrime information support system design: Application of K-means-VMD-BiGRU in the city of Chicago. Information and Management, 103247. https://doi.org/10.1016/j.im.2019.103247

Shamsuddin, N. H. M., Ali, N. A., & Alwee, R. (2017). An overview on crime prediction methods. 6th ICT International Student Project Conference: Elevating Community Through ICT, ICT-ISPC 2017, 2017-Janua, 1–5. https://doi.org/10.1109/ICT-ISPC.2017.8075335

Fredrick David, H. B., & Suruliandi, A. (2017). Survey on Crime Analysis and Prediction Using Data Mining Techniques. ICTACT Journal on Soft Computing, 7(3), 1459–1466. https://doi.org/10.21917/ijsc.2017.0202

Fredrick David KR, B. H., Benjamin Fredrick David, H., & Suruliandi, A. (2017). SURVEY ON CRIME ANALYSIS AND PREDICTION USING DATA MINING TECHNIQUES Crime analysis and prediction View project Content Based Image Retrieval View project SURVEY ON CRIME ANALYSIS AND PREDICTION USING DATA MINING TECHNIQUES. Article in ICTACT Journal on Soft Computing, 3. https://doi.org/10.21917/ijsc.2017.0202

Dilek S., Huseyin C., Aydm M. (Jan 2015) Applications of Artificial Intelligence techniques to combating cybercrimes. International Journal of Artificial intelligence and applications,Vol 6 No 1.

McLaughlin N., et el (Mar 2017) Deep android malware detection, Conference on Data andApplication Security and Privacy, p 301-308

Xu Z., Ray S., Subramanyan P., Malik S. (Mar 2017) Malware Detection using machine learningbased analysis of virtual memory access patterns, Conference on Design, Automation & Test.

Patil P. (May 2019) Artificial Intelligence in Cyber Security, International Journal of research in computer applications and robotics, Vol 4 Issue 5 p. 1-5.

Truong T. C., Diep B. Q., Zelinka I. (Mar 2020) Artificial Intelligence in Cyber Domain: Offenseand Defense, Symmetry 2020, Vol 12, Issue 410.

Table 1: Strength and Weakness of ML Models

ID	Strength, weakness	Model
A54	* Positive prediction is guaranteed by count-based regression models.	Negative binomial regression
A55	*Able to detect high potential hotspots at which crime will have the highest chances of being committed in the future by setting a larger α	ensemble spatiotemporal pattern (ESTP)
A56	*More robust to different time granularities	temporal-spatial correlations
A59	*Does not overfit the training data, resulting in near-optimal predicting on previously encountered events.	Genetic programming – LSGP
A60	*More robust and has higher AUROCs	Partially Generative Neural Networks (PGNN)
A62	*The feature space is heterogeneous and high-dimensional.	Random Forest
	*It can handle with colinear features and will not make any assumptions about data on firsthand.	
A63	*Captures the significance of crime occurrences across time periods.	Category Dependency Encoder + hierarchical Recurrent neural network + Multilayer Perceptron (MLP)
	* Predicts crime occurrences in many categories in each sector of a city.	
A66	* Allows for the replication, transmission, and continual enhancement of the knowledge model, as well as a more objective basis for comparison.	Deep Neural Networks
A67	* Accurate geographical and functional affinity, activity preferences, and daily schedules descriptions for places and users	feed-forward neural networks + Spatio-Temporal Embedding Similarity
	*Applications in a variety of situations are possible.	
A73	* Can be used to designate priority regions targeted by other nonpolice agencies	Risk Terrain Modeling
A74	* Neural network-based methods might capture multidimensional spatial-temporal data's complex underlying structures in a nonlinear manner.	"Multi-View and Multi-Modal Spatial-Temporal learning (a multimodal pattern fusion module + a hierarchical recurrent framework)"
A75	* Effectively predict crime activity-related features.	"Fireflies-based fuzzy cognitive map neural networks (FFCM), Enhanced associative neural networks (EANN)"

A82	* Not only will this improve the accuracy of mobility-based crime predictors, but it also ensures that performance is balanced across protected groups.	* Bayesian hierarchical model
A83	* This algorithm works well with datasets that are nonlinear and have a high order of complexity.	* K-NN
		* Random forest
A84	(−) Learning the model is a time-consuming iterative process, rendering it unsuitable for use as an online tool.	* k-NN predictions
	(−) This method is ineffective for streets with little or no data.	* demographic features
		*Weighted Multimodal Latent Dirichlet Allocation (WMLDA)
A86	* Relatively resistant to overfitting, which is useful in this case because there are only a few thousand grid cells to learn from and almost a hundred POI properties (SVM, Random Forest)	“logistic regression, support vector machines, decision trees, and random forests”
	* Capable of using the fullest of available attributes without overfitting - (SVM, Random Forest)	
A87	(−)Because of the nonlinear nature of social data, LASSO prediction accuracy is relatively low.	* Extremely randomized Trees (Extra-Trees)
		”Least Absolute Shrinkage and Selection Operator (LASSO)”
A88	* No iteration steps are required for maximizing or decreasing likelihood or cost functions, as in the EM method and other machine learning techniques.	”self-exciting point process models (SEPP)”
	* The DDGF technique allows us to discover the buried causal effects of criminal events.	* data-driven Green's function
		* prospective hotspot maps
		* Expectation Maximization
A93	* Accurate long-term crime forecasting in micro places with respect to other common techniques	Random Forests
A106	* Simple to comprehend and implement in cybercrime investigations	J48 Decision Tree

A110	* Less sensitive to spatiotemporal resolution, which allows it to perform effectively in sparse areas.	Random Forest Regression (RFR)
		Support Vector Regression (SVR)
		Multi-Layer Perceptron Regression (MLPR)
A113	* Effectively avoid the problem of overfitting	Random forest
A118	* Secure, user-friendly and accurate with predicting criminal activity	K-Means Clustering

Utilized Datasets per Category

Country/State	**City**	**Details**	**Open**	**From**	**To**	**%**	**Freq.**
Chicago Illinois	* Na	*Police Data Portal	yes	* 2001	* 2019	15%	19
		*Violent crimes		* 2007	* 2012		
		* Police Data Portal		* Jan 1st, 2017	* Dec 31st, 2017		
		* Citizen Law Enforcement Analysis and Reporting (CLEAR)		*2013	*2017		
India	* Gujarat	* Police department	Yes	Na	Na	10%	13
	* Bureau	* National Crime records					
	* Bengaluru	* GVK Emergency Management and Research Institute					
US	* Cambridge - England	* Crime Analysis Unit Police Department	Na	*Na *Na *Jan 1st, 2006 * Feb 10, 2010	*Na *Na *Dec 31st, 2009 * Aug 4, 2016	9%	12
	* Cheltenham - England	* Crime data					
	* Northeast	* police department - residential burglary report					

Country/State	**City**	**Details**	**Open**	**From**	**To**	**%**	**Freq.**
	* Southern	*Department of public safety at USC					
	*Baltimore	*Baltimore Police Department's Victim Based Crime Data					
California	* San Francisco * Mississippi * Los Angeles	*Homicide dataset	Na	*1981	*2014	9%	12
		*Na		*Na	*Na		
		*Police department		*2014	*2016		
Multi-media and Social media	Na	* News sites, blogs, RSS feeds * Images of Knives, guns, and blood * Surveillance videos * Titter * Open street map	Na	Na	Na	9%	12
New York		* Police department * Crime data * Crime data	Yes	*2015 *July 1, 2012 *Jan 1, 2014 * 2014	*2017 *June 30, 2013 *Dec 31, 2014 *2015	7%	9
Other	Na	* Point of Interest	Na	*Na	*Na	6%	7
		* Public Service Complaint Data		*Na	*Na		
		* Taxi flow data		*Na	*Na		
		* News data		*2011	*2019		
		* Global Terrorism Database (GTD)		*2015	*2016		

Country/State	**City**	**Details**	**Open**	**From**	**To**	**%**	**Freq.**
Gowalla Foursquare	Na	Na	Na	*Feb 2009	* Oct 2010	5%	6
UCF UCI	Na	*Crime dataset * The Communities and Crime Unnormalized Data Set	yes	Na	Na	5%	6
UK	* London Borough	*Profiles (68 metrics) * police crime data	Na	Na	Na	4%	5
Brazil	*Na *Fortaleza *Cearra	* healthcare system	Yes	*Na * July 2016 * July 2016	Na * Nov 2017 * Nov 2017	3%	4
Canada	* Edmonton * Vancouver	* Last 15 years	Yes	Na	Na	3%	4
Philippines	*Misamis Occidental *Manila	*Na *Manila Police District (MPD)	Na	*Na *2012	*Na *2016	2%	2
Bangladesh	Na	*Dhaka Metropolitan Police (DMP)	Na	*June 2013	* May 2014	2%	2
Russia	*Saint-Petersburg	* Crime records	Private	1/1/2014	2/28/2017	1%	1
Hong Kong	* Guangzhou	* traffic violation	Na	2012	2016	1%	1
Netherlands	* Amsterdam	* Police Department	Na	Na	Na	1%	1
Pennsylvania	* Philadelphia	Na	Na	Na	Na	1%	1
Colorado	* Denver	Na	Yes	Na	Na	1%	1
Portland	* Oregon	* Crime occurrences	yes	* March 2012	* December 2016	1%	1

Country/State	**City**	**Details**	**Open**	**From**	**To**	**%**	**Freq.**
Australia	* Queensland	Na	Na	Na	Na	1%	1
Taiwan	* Taoyuan	* Vehicle theft	Na	* Jan 2015	* April 2018	1%	1
Switzerland	* Aargau	*burglary incidents	Na	* Jan 14, 2014	* Jan 13, 2017	1%	1
Mexico	Na	* Secretary-General of National Public Security * The National Council for the Evaluation of Social Development Policy	Na	* 2011	* na	1%	1
Belgium	Na	* local police department	Na	* 2007	* 2017	1%	1
Argentina	* Buenos Aires	Na	Na	*2016	*2019	1%	1