International Journal of Law and Public Policy
Vol. 2, Issue. 1, Mar 2026, pp. 56~67
ISSN: 3107-6017

Criminal Law in the Digital Era: Addressing Cybercrime and Emerging Security Threats

Geeny Mourya[1], Dr. Rekha[2]
[1]Research Scholar, Institute of Legal Studies and Research, Mangalayatan University, Aligarh, Uttar Pradesh, India.
[2]Professor, Institute of Legal Studies and Research, Mangalayatan University, Aligarh, Uttar Pradesh, India.

Article Info

Article History:
Received Jan 08, 2026
Revised Feb 10, 2026
Accepted Mar 09, 2026

Keywords:
Data breaches
identity theft
emerging threats
cybercrime
artificial intelligence
cyber security
cybercrimes

ABSTRACT

The nature and extent of criminal activity have been drastically altered by the quick development of digital technology, leading to the emergence of new security risks and sophisticated types of cybercrime. Data compromises, stolen identity, online scams, e-terrorism, and attacks on vital infrastructure are examples of borderless digital crimes that are posing a growing threat to traditional criminal laws frameworks that were created for bodily and spatial offenses. The field of criminal law is confronted with previously unheard-of opportunities and challenges as technology continues to transform our society. Artificial intelligence (AI) and the spread of electronic crimes have created complicated legal, moral, and practical issues for the justice system across the globe. This study explores the complex effects of AI and electronic crimes on criminal law, looking at how they change established legal paradigms, talking about new legal structures, and looking at the consequences for social norms and individual liberties. This essay aims to shed light on how criminal law is changing in the era of electronic crimes and AI by examining a number of case studies and examining the development of legislation. This study emphasizes the significance of protecting digital environments while maintaining safety, justice, and public confidence in the digital era by updating criminal legislation to reflect technological changes.

Corresponding Author:
Geeny Mourya,
Institute of Legal Studies and Research,
Mangalayatan University, Aligarh, UP.

1. INTRODUCTION

The development of the web and the spread of digital technologies have completely changed how people engage, interact, and do business. Although there are many advantages

to these developments, they have also led to the emergence of cybercrime, a new type of criminal behaviour [1]. Cybercrime is the term used to describe illicit activities that are enabled or carried out by the use of devices, networks, and the web. Cybercriminals carry out a variety of illegal actions by taking advantage of weaknesses in networks, computers, and internet-based venues. Hacking, stolen identities, phish, ransomware attacks, data compromises, online fraud, theft of proprietary information, and the dissemination of malicious software are some of these activities. Cybercrime can have serious financial, social, and psychological repercussions that impact individuals, businesses, governments, and even national security. The cross-border nature of crime and the quick advancement of technology provide special legal issues [2]. The complicated legal implications of cybercrime include jurisdictional concerns, challenges in obtaining and maintaining digital evidence, and the requirement for updated legislation. Policymakers and legal professionals can create strong legal frameworks to successfully tackle cybercrime by analyzing these issues.

Furthermore, cybercriminals can operate across national borders with impunity thanks to the internet's worldwide reach and privacy, which presents difficulties for authorities and regulatory agencies [3]. Attackers constantly modify their strategies to take advantage of new weaknesses and avoid detection, making efforts to prevent cybercrime more difficult due to the quick advancement of technologies. The wide-ranging effects of digital crime highlight how urgent it is to confront it. Cyber-attacks cause significant financial damage for companies of any kind and sectors. As demonstrated by assaults on vital infrastructure, governmental organizations, and election procedures, cybercrime poses a threat to national security in addition to its economic effects.

Proactive steps to improve cybersecurity resilience are necessary because the interruption caused by cyber disasters can have significant social and political repercussions. In light of this, the main goal of this study is to investigate new developments and difficulties in digital criminal activity, with a particular emphasis on cybercriminals. This study aims to contribute to a thorough understanding of the changing threat landscape by assessing current cybercriminals' techniques and looking at successful countermeasures and strategies. Developing strong cybersecurity regulations, improving incident response abilities, and encouraging cooperation among stakeholders in the battle against digital crime all depend on a grasp of these processes.

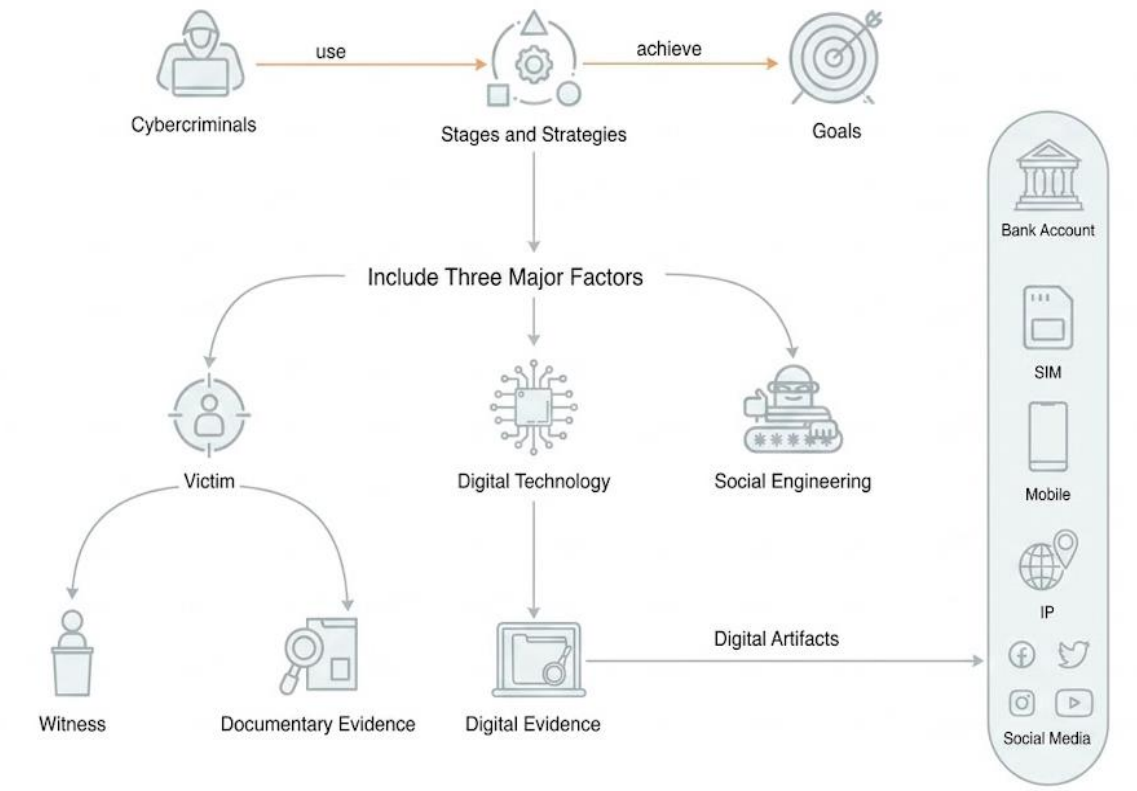

Figure 1. Evidence types related to the tactics and phases of a criminal

In summary, digital evidence plays a crucial part in the development of criminal tactics, which are entwined with the domain of digital artifacts. The foundation of evidence in nearly all of cybercrime investigations is found in the virtual or digital realm, with physical proof frequently playing a supporting role. However, both digital and written proof is essential cornerstones in the complex procedures of locating, examining, and punishing those responsible for cybercrimes. Figure 1 [4] provides a broad overview of the complex environment of evidence that officials painstakingly gather, serving as a graphic representation of these principles.

2. LITERATURE REVIEW

The term "cybercrime" refers to illegal activity that involves the direct or indirect use of ways to interact and electronic devices, including laptops, desktops, cell phones, and automobiles. According to the publication "Global Risks for 2012," one of the top five dangers facing governments and companies globally is cybercrime [5]. Cybersecurity can have long-lasting detrimental effects on individuals and presents substantial detection and avoidance issues. Cybercrime is becoming a common topic in the news as e-commerce and online banking become more common and include the usage of sensitive financial and personal information. It is crucial to comprehend the nature of these crimes and the tactics used by hackers in order to defend ourselves against them. An overview of hackers, the development of criminal activity, the many forms of criminal activity, case studies,

preventative measures, and the agencies fighting this sort of crime are all included in this article.

The goals include examining significant legal and technological turning points in cybercrimes during the past few decades [6]. Confirming growing cyber threats that require immediate action is the study's goal. Doctrinal technique makes use of industry information, case law, and academic journals. Important discoveries highlight the necessity for international cooperation by exposing advanced social engineering methods, weaknesses in legal deterrence regimes, and infrastructural vulnerabilities. To counter new dangers, proactive changes to cyber security laws, public education, and international cooperation are the main approaches.

The study uses grounded theory in conjunction with qualitative methods to examine how these innovations affect cybercrime and the efficacy of current legislation. Results show a considerable gap between legislative actions and technology breakthroughs, underscoring the necessity for flexible legislation that can anticipate and anticipate future technological advances [7]. Fostering global collaboration and revising legal definitions and sanctions to incorporate tech-driven crimes are among the suggestions. This study emphasizes how important it is to have flexible legislative procedures in order to address the always changing cybercrime scene.

The purpose of this study is to analyze the issues and difficulties that come up when applying traditional criminal law in cyberspace and to look into possible remedies. The nature of this research is qualitative [8]. Proper observation and thorough note-taking were the methods employed to collect information, which were then followed by analytical processes such data analysis, visualization, and conclusion. The study's findings demonstrate the complexity and diversity of the opportunities and difficulties associated with applying criminal law in the digital age. Technology for communication and information developments have altered the criminal scene and presented new difficulties for criminal prosecutors.

The results show a worldwide trend toward the formalization of cyber courts [9], modernisation of procedures, and development of legal capacity with the goal of giving judicial actors the technical know-how needed to deal with intricate digital proof. Concurrently, the analysis emphasizes how evidence standards are changing, including the formalization of digital forensic integrity techniques and the formalization of digital authentication methods. Significantly, a number of jurisdictions have adopted digital legal aid platforms, online courts, and accessible legal services models in an effort to close the digital gap, making availability of law in the digital age both a challenge and an opportunity for creativity.

Cybercrime includes unauthorized access, destruction, and tampering with computers, as well as typical crimes like fraud, identity theft, and adult pornography that are carried out quickly and to a large number of possible victims. The most harmful are harmful and malicious codes that disrupt computer operations globally and endanger e-commerce in addition to other cybercrimes. Even in developed countries [10], the "digital divide" gives cybercriminals "safe refuges," and the cross-national character of the majority of computer-related crimes has rendered many traditional techniques of police internationally and in cross-

border scenarios useless. It is imperative to build transnational policing capabilities and change MLA methodologies in reply to the risk of cyber.

Today [11], the majority of people in Asia play video games; the gaming business makes billions of dollars; everything got online overnight, including work from home, online learning, and e-commerce, which led to an increase in cybercrime incidents in India. Data in India is susceptible, and there is no cyber law that addresses privacy. Over 50% of people lost vital data online and there have been instances of debit and card fraud as well as online job fraud. India's cyber laws need to be changed to provide legal protection for cyberwarfare and phishing, as well as legal attention for data protection, privacy, and spam. Due to a weak cyber safety mechanism and lax cyber laws, banks are vulnerable to cybercriminals, which has impacted the economy and caused many people to lose a lot of money in recent years.

Through the use of AI, pattern recognition—a conventional research method—has become more popular in criminal investigations [12]. It extends its functionality to email content classification, including junk, photos, and audio, by using techniques like image recognition to reveal hidden features. Inference, research, and data usage are necessary for successful pattern identification. The effectiveness of the software relies on the ability to handle vast amounts of data via statistical evaluation and probabilistic methods, which presents difficulties for researchers, particularly when working with big datasets. Deep learning methods like facial identification for recognizing people and syntax evaluation for handwriting text comprehension are used by criminal detectives.

3. METHODS AND APPROACH

The basic ideas of safeguarding data theory in relation to the administration of large data repositories [13]. The use of AI and its wide range of approaches is where this is used. These strategies can be modified in a number of ways, and new resources are constantly being created to support their changing application and reach. To reduce or eliminate cyber security threats and assaults, these precautions can be incorporated into newly created or current software. This technology is used in a number of useful areas, including email security, phishing attempt detection, malware identification, network behavior anomaly detection, network attack detection, private information protection, preventing fraud, and identification theft risk mitigation. Future discussions will center on the concept of using different algorithms to identify tactics.

3.1 Digital indication

Digital evidence is anything stored on, received by, or sent by a mobile device that could be relevant to an investigation. This evidence may be found when gadgets are seized and made ready for examination. Data collected online and/or from digital devices may provide a wealth of information about individuals and events. Consider gaming consoles. These gadgets work similar to desktop computers and save a range of data, such as financial information, photos, movies, online browsing history, and personal data. Many organizations are lagging behind in handling digital evidence. Financial limitations, a lack of appropriate

training opportunities, and the quick development and wide accessibility of digital devices are all contributing reasons to this.

Digital forensics examinations are not always economical because of the high cost of personnel, equipment, and license. Demonstrating a cost-effective return on investment is necessary to gain command staff buy-in. Smaller organizations may find it particularly challenging to manage the intricate combination of the federal, state, and local funding sources that could be utilized to support these initiatives. Regional model and other forms of cooperation may be helpful, assuming law enforcement personnel are aware of available resources. Although advanced digital proof training is not currently required in police academies' educational programs, officers of any background may encounter enough digital evidence to influence the outcome of a case.

3.2 Technology attainment

Organizations are said to function logically when they set formal goals, create plans to reach those goals, and then employ technology to help and support those plans. However, it is well known that rationality has its limitations; organizations have limitations because of personnel and financial resources, goals are not always clear, and knowledge on the best ways to achieve them is occasionally inadequate. The contingency approach states that every firm has a different environment and that factors outside of its control may have an impact on the choices it makes. The institution's point of holds that organizations have their own objectives, such as preserving their existence, improving their reputation, maximizing the assets at their disposal, and fending off threats. Another perspective depicts companies as disorganized rather than effective machines and notes that they frequently develop strategies and technology to address issues before they are even aware that they exist. As a result, organizational options are sometimes just on the sidelines, waiting to be utilized at the appropriate moment.

3.3 Using AI to Identify Possible Risks in Email

The amount of email traffic is rising as a result of technology advancements. At the moment, email is the safest way for businesses to communicate internally about sensitive information. As a result, efforts to stop businesses and other organizations from sending spam emails have increased. Due to the enormous amount of data it transmits, email is the most popular vector for attacks. There is an urgent need to develop algorithmic machine learning techniques. 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.

Depending on the significance of the synthesis input values, the input data is transformed into the output. An activation function is then triggered at a predefined threshold using these weighted input values. The use of iterations to get optimal value is the primary difference between artificial intelligence models and traditional models. Creating jobs that spam filters can excel at is essential to maximizing AI for spam detection. Emails are sorted

by the filters' algorithms according to whether or not they contain a list of potentially harmful terms. It is possible to give questionable words or signs a weight based on how frequently they occur. Incoming emails can be sorted in accordance with the cutoff point once it has been determined.

Spam messages are defined as having values over the specified threshold limit, while ham signals have values below it. The AI is meant to adjust the threshold value using the spam and ham data. Regular expressions and static rules are used to build the initial spam identifications. To update the spam filtration systems, a threshold research must be carried out and new strategies must be created. This is due to the fact that spammers are always changing their tactics. Static rules can quickly turn out of date, thus it's ideal to use a dynamic method as the filters must be updated continuously. Success in this venture also depends on the user's involvement. There are many techniques for text verification, such as machine vision and processing of natural language, which can be used to identify any inconsistencies or dubious passages.

3.4 Internet Attacks and Odd Network Behavior

The prevalence of linked gadgets has significantly increased in recent years. The growing frequency of network-based intrusions has rendered conventional methods of perimeter protection obsolete. As a result, using automated techniques to identify potential incidents involving network security is essential. Using the signature-based detection approach is one such tactic that could be used. This method could be used to create an extensive database of previously identified attack signatures. When this database is integrated with others, a security system is triggered in the event that dubious signatures are found.

The task of keeping the database current, which is essential in this specific situation, can be automated using artificial intelligence [14]. Finding any discrepancies is the next step. Using this method, network activity is tracked and analyzed to provide the starting point for normal behavior. Information is gathered and evaluated regarding the typical traffic patterns, including the number of connections originating from a particular host, any unusual relationships, any cases of increased traffic, and any variations in network capacity. Any deviation from the accepted norm or a possibly dubious trend seen in the dataset might be classified as an abnormality.

4. FINDINGS AND RESULTS

4.1 Methods for Crime Prediction

The main approaches used in the domains of AI and ML are supervised learning and unsupervised learning, respectively [15]. The use of labeled data for direct prediction is the main distinction between supervised and unsupervised learning. There are other differences, exclusions, and important areas where one method is better than the other. When using the supervised learning approach, the use of labeled datasets is crucial. These data sets are intended to be used in the evaluation and training of systems for precise data identification and predictions.

The model will evaluate its own accuracy on its own and gradually improve its efficiency over time by using the annotated inputs and matching outputs. Additionally, there are two different types of issues in the field of supervised learning, namely regression and classification.

Machine learning uses a system for classification to classify and organize test data in order to distinguish between cats and dogs. Filtering one's email inbox to find and remove unsolicited and undesired communications—also known as spam—is another real-world example. Supervised learning differs from unsupervised learning in that the former has described input and output data, while the latter does not. In supervised supervised learning, the method receives input from the trained data in the form of scores and correct forecasts. Training a model to understand the intrinsic structure of labeled data is the aim of supervised learning. On the other hand, when the training dataset includes both labelled and unlabeled examples, a hybrid method known as semisupervised learning can be used. When there are fewer identified samples than unlabeled samples in the information set, the semisupervised approach performs better. This approach is still used by researchers notwithstanding its reputation for complexity. In order to evaluate textual data, such as tweets related to criminal activity, in the setting of A108, the writers of the study used a semi-supervised approach using bags of words.

About 31% of the present study on crime forecasting is related to the field of supervised learning, as seen in the figure. It's also important to note that 22% of all studies combined supervised and unsupervised techniques. This is explained by the fact that multiple machine learning approaches were used in various researches. But just 10% of people used unsupervised learning strategies. Surprisingly, just 1% of the studies used a semi-supervised methodology, indicating that this method is rarely used in the field of crime prediction. In the end, a significant percentage of the studies—36%—showed ambiguity regarding the precise methodology used.

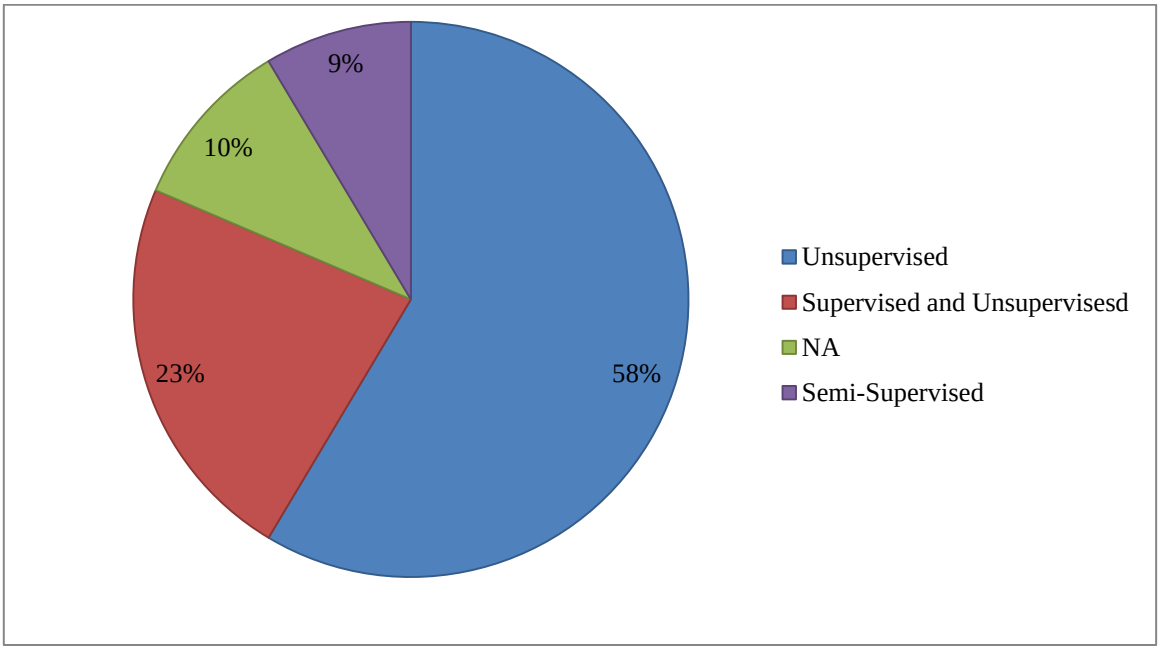

Figure 2. Advantages and drawbacks of modern prediction technology

The random forest model's capacity to handle colinear input, high dimension, and diverse space has made it extremely popular in the field of criminal predictions. Furthermore, A93 has found that the model exhibits a high degree of accuracy in forecasting criminal activity over a prolonged duration in Figure 2. However, there are some serious drawbacks to the random forest approach. Time constraints limit the efficacy of these procedures because learning the model and building the tree are recurring tasks. Additionally, a lack of available resources and inadequate data restrict the model's performance. The use of deep learning methods to the problem of crime prediction has shown encouraging initial results.

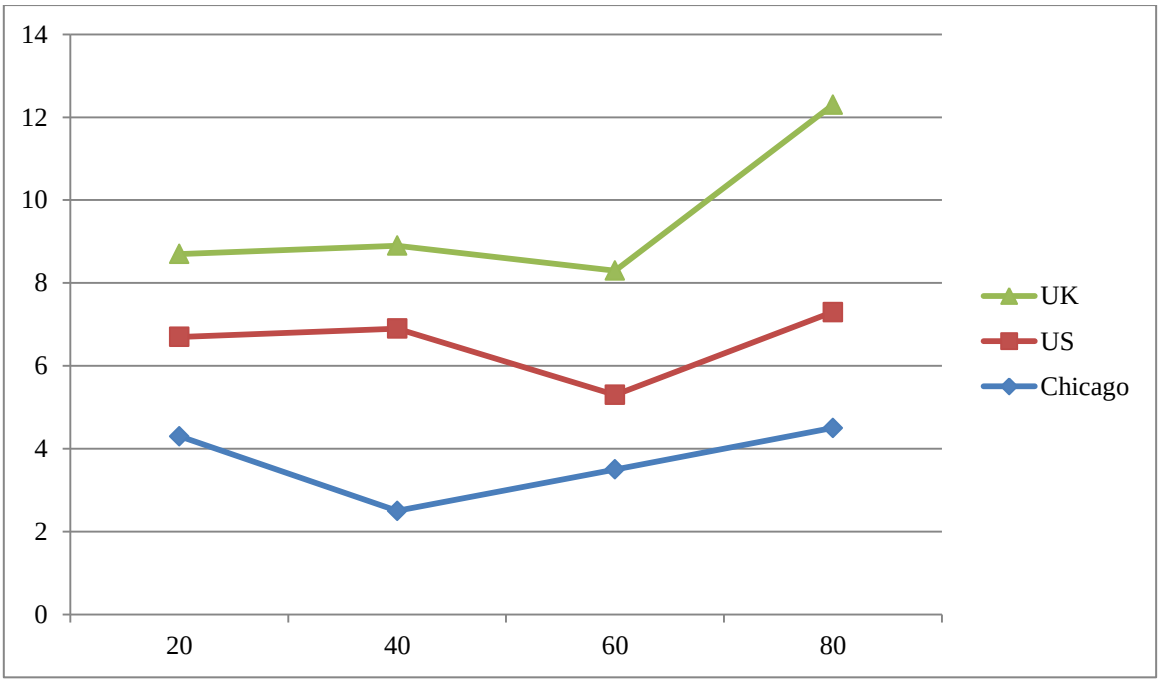

Figure 3. Advanced neural network approaches

The application of sophisticated neural network techniques, such as neural networks with deep layers, partially generated neural networks, hierarchical recurrent systems, and enhanced association neural networks, has a number of benefits in Figure 3. The models under evaluation show greater AUROCs, which effectively capture the temporal relevance of criminal episodes, as previously noted. Furthermore, these frameworks show the capacity to forecast crime incidents in a variety of subcategories within distinct metropolitan sectors. Additionally, they provide a more objective basis for comparison analysis and enable the knowledge model's reproduction, standard transmission, and continuous improvement.

5. CONCLUSION AND RECOMMENDATIONS

A new age in criminal law is ushered in by the combination of artificial intelligence and electronic crimes. The evolution of computerized crimes, the use of AI in criminal justice, legal reactions to new issues, the fine line between security and individual liberties, and pertinent case studies have all been examined in this paper's exploration of the dynamic landscape of criminal record in the digital age. The function of criminal law must change as society struggles with these revolutionary forces in order to provide safety, justice, and

acceptance of human rights in a world growing more connected by the day. Even though AI has many tools that help with cyber security, some areas still require more concentrated investigation.

The hypotheses that are currently in use include several errors. As was previously explained, testing these types of models may result in false alarms. Additionally, autonomous malware attacks are a potential in regions where research is currently ongoing. In order to improve these models, support and training are always needed due to the layout of more complex models. But the same tools that are used to identify and stop cyberthreats can also be used to launch assaults that are just as destructive. AI approaches can increase the flexibility and criticality of attacks on computer system or network safety. Therefore, stronger models are needed to identify attacks of this serious kind.

Naïve Bayes and random forest are the most often used algorithms in crime prediction. Twenty publications used naïve Bayes, twenty-five used random forest, and seventeen used the choice tree algorithm. Furthermore, hybrid models that employed multiple machine learning algorithms were used in the majority of scholarly publications. Additionally, with a proportion of 31%, the supervised learning approach is the most widely used method in the field of crime prediction. Additionally, a controlled and unstructured strategy was applied in 22% of the research publications that were gathered. 10% used unsupervised learning. Naïve Bayes and random forest are the most often used algorithms in crime prediction. Twenty publications used naïve Bayes, twenty-five used random forests, and seventeen used the decision tree algorithm. Furthermore, hybrid models that employed multiple machine learning algorithms were used in the majority of scholarly publications. Additionally, with a proportion of 31%, supervised learning methods is the most widely used method in the field of murder prediction.

Additionally, a controlled and unstructured strategy was applied in 22% of the research publications that were gathered. 10% used unsupervised learning. Naïve Bayes and random forest are the most often used algorithms in crime prediction. Twenty publications used naïve Bayes, twenty-five used random forests, and seventeen used a decision tree algorithm. Furthermore, hybrid models that employed multiple machine learning algorithms were used in the majority of scholarly publications. Additionally, with a proportion of 31%, the supervised learning approach is the most widely used method in the field of crime prediction. Additionally, a controlled and unstructured strategy was applied in 22% of the research publications that were gathered. 10% used unsupervised education.

The amount of cyber-attacks and security risks has increased due to the current advancements in technology. It is crucial to have systems that are more robust, adaptable, and scalable based on the available data. Numerous AI techniques for identifying and averting possible cyber security breaches have been covered in this paper. There are deep learning applications that safeguard network security in addition to AI technologies. Combinations of methods based on computer learning and biology can offer improved protection against these kinds of threats. In order to employ artificial intelligence knowledge to enhance system capabilities and build cyber safety, there are still new areas the requirement to be created. AI is one of these fields.

REFERENCES

[1] Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205-217.

[2] Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews*, *10*(3).

[3] Cassidy, A. A. T. J., Fuad, A., & Shofy, M. U. A. A. (2024). Emerging trends and challenges in digital crime: A study of cybercriminal tactics and countermeasures. *TechComp Innovations: Journal of Computer Science and Technology*, *1*(1), 38-45.

[4] AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28-36.

[5] Silalahi, J. A. S. (2023). The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities. *Innovative: Journal Of Social Science Research*, *3*(2), 3658-3668.

[6] Khan, M. N. I., & Ahmed, I. (2025). A systematic review of judicial reforms and legal access strategies in the age of cybercrime and digital evidence. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 01-29.

[7] Erikha, A., & Saptomo, A. (2024). Dilemma of Legal Policy to Address Cybercrime in the Digital Era. *Asian Journal of Social and Humanities*, *3*(3), 499-507.

[8] Pandey, A. K. (2023). The role of technology in modernizing criminal law: Addressing cybercrime and digital evidence.

[9] Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican law review*, *16*(2), 23-54.

[10] Mushtaq, S., & Shah, M. (2025). Threats to the digital ecosystem: Can information security management frameworks, guided by criminological literature, effectively prevent cybercrime and protect public data?. *Computers*, *14*(6), 219.

[11] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

[12] Kundu, A. (2021). Impact of Cyber Law in Modern Era with Advancement in Technology and Protection from Rising Threats of Cyber Crimes in Our Socio Economic Sector. *International Journal of Advanced Research*.

[13] Ambawta, M., & Chaudhary, A. (2025). DIGITAL PLATFORMS AND THE CHANGING LANDSCAPE OF CRIME: CHALLENGES AND OPPORTUNITIES FOR LAW ENFORCEMENT. *Lex Localis: Journal of Local Self-Government*, *23*(10).

[14] Godase, V. (2025). Navigating the digital battlefield: An in-depth analysis of cyber-attacks and cybercrime. *International Journal of Data Science, Bioinformatics and Cyber Security*, *1*(1), 16-27.

[15] Tawil, S., & Tarawneh, A. (2025). Technology and the law: countering cybercrime and fraud in the digital age. In *Artificial Intelligence in the Digital Era: Economic, Legislative and Media Perspectives* (pp. 1095-1105). Cham: Springer Nature Switzerland.

[16] Mustafa, A. H. (2024). The Future of Criminal Law in the Age of Electronic Crimes and Artificial Intelligence. *Pakistan Journal of Life & Social Sciences*, *22*(2).