Utilization of Artificial Intelligence in Predicting Crime

Joan Stacia Carissa, Mardi Turnip*
Universitas Prima Indonesia, Indonesia
jscarissa@gmail.com, marditurnip@unprimdn.ac.id*

ABSTRACT
The problem of crime in Indonesia is an urgent issue, with crime rates continuing to increase. High crime rates have serious impacts on societal security, social stability, and economic development. Amidst the complexity of types of crime, motives and methods of handling them, Artificial Intelligence (AI) and Machine Learning (ML) technology has emerged as a promising solution. Through analysis of a literature review with the keywords "AI and crime," this research aims to understand the differences between the use of AI in crime prediction and traditional methods. The literature review method will identify and analyze the latest knowledge regarding the use of AI technology in overcoming crime problems. The use of AI in analyzing crime data, identifying complex patterns, and providing accurate predictions will be emphasized. The research will also explain how AI is able to overcome problems that are difficult to solve with conventional methods. It is hoped that the results of this literature review will provide deeper insight into the potential of AI in reducing crime rates and creating a safer environment for people in Indonesia.

Keywords: Crime; artificial intelligent; machine learning; method; technology

INTRODUCTION
The escalating crime rates in Indonesia, recording 276,507 cases in 2022 with a 7.3% increase from the previous year, have turned into an urgent concern. With a crime occurring every two minutes, the repercussions extend beyond individual safety, affecting societal stability, economic progress, and overall living standards. Several interconnected social issues like unemployment, inequality, and mental well-being contribute to criminal behavior, compounded by geographic and environmental factors such as inadequate lighting and surveillance. Limited resources, educational gaps, and soaring youth unemployment rates further exacerbate crime rates in various regions.

Understanding and predicting these complex crime patterns pose a challenge in crime prevention efforts. Leveraging Artificial Intelligence (AI) and Machine Learning (ML) technologies emerge as promising solutions to this challenge. Previous studies, notably in Vancouver, have utilized AI techniques like "K-nearest neighbors" to predict high-risk crime areas successfully. Globally, AI is increasingly utilized to analyze crime data, identify patterns, and optimize law enforcement resource allocation. Promising results, such as reduced crime rates in cities like Chicago and improved crime prevention in London, reflect the potential for enhancing crime prediction accuracy through more sophisticated AI approaches.

AI's effectiveness in analyzing crime-related data, including police records and demographics, enables precise predictions of crime-prone areas, facilitating efficient resource allocation and targeted preventative actions. Its application in combatting organized crime by analyzing communication and financial data has significantly curbed crime rates, creating a safer societal environment. This research aims to conduct a literature review focusing on AI's role in crime prediction. By examining literature using keywords like AI and crime, we seek to comprehend AI's functioning in analyzing crime data, identifying intricate patterns, and delivering accurate predictions. Through the compilation of relevant literature and research, this study endeavors to explore AI's potential as an innovative solution to reduce crime rates and foster a safer environment for Indonesia's populace.

LITERATURE REVIEW
The literature review aims to explore the current landscape of AI utilization in crime prediction, focusing on its advancements, limitations, and potential implications for reducing crime rates. This review synthesizes various studies, theories, and methodologies to identify gaps in the existing research, serving as a foundation for further investigation in this domain.

* Corresponding author

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0).
METHOD

The chosen research method is a literature review, aimed at consolidating current knowledge in the field. It involves gathering information from various sources such as scientific journals and conferences, focusing on Artificial Intelligence (AI) in crime prediction.

A. Inclusion and Exclusion Criteria

In literature review research, determining inclusion and exclusion criteria is essential to ensure that relevant and appropriate research will be included in the literature review.

Inclusion Criteria:
• Research published in Indonesian or English, aligning with Indonesia's official and internationally used languages.
• Studies focusing on AI's use in crime prediction, including Machine Learning's role in analyzing and predicting criminal events.
• Research emphasizing AI's role in improving crime prediction and prevention processes.

Exclusion Criteria:
• Studies not centered on AI in crime prediction won't be included.
• Research unrelated to crime prediction or prevention won't be part of the review.
• Books, editorials, or non-empirical reviews unrelated to AI's role in crime prediction won't be considered.

Applying these criteria ensures the inclusion of relevant literature aligned with the research's objectives, offering comprehensive insights into AI's application in crime prediction.

B. Search Strategy

The search strategy is a crucial step in literature review research, aiming to efficiently find relevant and in-depth research on using Artificial Intelligence for crime prediction. It ensures the validity, reliability, and sustainability of the research. Keywords like "Artificial Intelligence," "Machine Learning," "Crime Prediction," "Crime Analysis," and "Predictive Policing" are used in combinations with logical operators (AND, OR) to enhance search relevance. For instance, ("Artificial Intelligence" OR "Machine Learning") AND ("Crime Prediction" OR "Predictive Policing"). Journal databases such as IEEE Xplore, Scopus, Google Scholar, and PubMed are utilized to gather information published between 2019 and 2023, ensuring access to the most recent data.

C. Filtering, Selection and Data Extraction

In the literature review process, Data Filtering, Selection, and Extraction are crucial steps. Filtering involves using keywords and filters in academic databases to find relevant sources. Selection focuses on picking high-quality journals based on criteria like publication year, relevance, and methodology. Finally, Extraction entails extracting key information from chosen journals, including findings, methodology, results, and conclusions.

To facilitate the examination and understanding of the gathered studies, chosen reviews were systematically arranged in a table following an extensive literature search.

D. Quality Assesment
Quality assessment in a literature review is an important step to ensure that the data used in a literature review is of good quality and does not have defects that could affect the results. This assessment process involves transparency and vigilance to ensure the integrity and validity of the data used.

In gauging the reliability of the findings and conclusions of a specific review, queries related to quality control and assurance are posed. These questions are responded to and assigned a "yes" or "no" score. A criterion for the inclusion of reviews in this study mandated addressing a minimum of three of these questions, specifically QAC1, QAC2, QAC3, and QAC4.

**TABLE 1**

<table>
<thead>
<tr>
<th>QAC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QAC1</td>
<td>Are the review inclusion and exclusion criteria explained and appropriate?</td>
</tr>
<tr>
<td>QAC2</td>
<td>Does the literature review search tend to include all relevant studies?</td>
</tr>
<tr>
<td>QAC3</td>
<td>Does the review assess the quality/validity of the included studies?</td>
</tr>
<tr>
<td>QAC4</td>
<td>Is the study described adequately?</td>
</tr>
</tbody>
</table>

By utilizing these questions, evaluations can be categorized as "strong," "moderate," or "weak."

**RESULT**

**Utilization of Artificial Intelligence in Cyber Defense**

AI has become crucial in cyber defense, monitoring and analyzing network activity to detect potential threats. It shows promise in enhancing defense effectiveness by predicting and preventing attacks based on abnormal behavior patterns. Yet, AI has its limitations, including accuracy issues and pattern recognition errors. Therefore, its implementation should be part of a comprehensive defense strategy, considering data privacy and security regulations. While AI holds potential for better defense, its implementation requires wisdom and compliance with regulations for data protection and security.

**Protection of Customer Data Regarding the Use of Artificial Intelligence in Banking Activities in Indonesia**

The evolution of technology through four industrial revolutions, from the 18th-century Industrial Revolution 1.0 to today's Industrial Revolution 4.0, introduced Artificial Intelligence (AI), transforming various sectors, including banking. AI implementation in banking streamlines operations for customers and banks, offering enhanced efficiency and convenience. However, despite technological advancements, vulnerabilities persist, especially concerning customer data security. The increasing threat of cybercrime and data breaches highlights the necessity for robust regulations governing AI use in banking. Safeguarding customer information is paramount, urging the evaluation of AI's benefits, mitigation of potential risks, and the creation of tailored regulations for AI in Indonesia's banking landscape.

**Use of Artificial Intelligence in Armed Conflicts According to International Law**

AI's integration into human life has extended its use as a defense tool in armed conflicts like Remotely Piloted Aircraft and Lethal Autonomous Weapon Systems (LAWS). AI aims to minimize combatant casualties but faces challenges regarding security and the inability to distinguish combatants from non-combatants, posing risks of harm to civilians. Legal ambiguity surrounds AI's regulation in defense, raising concerns about liability when AI malfunctions or is misused. This study delves into AI regulation in armed conflict within international law, examining adherence to legal frameworks, AI's role, liability for breaches, consequences, obligations, and accountability standards. It aims to clarify AI's accountability within the context of international law in armed conflicts.

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
The Urgency of Special Regulations and the Use of Artificial Intelligence in Realizing Personal Data Protection in Indonesia

Indonesia has several personal data protection legal instruments that are scattered and only adapt to the main content of each law, so that the legal protection provided is still not optimal. The use of artificial intelligence (AI) as a tool to protect personal data and reviewing the urgency of a special regulation in Indonesia in creating protection for personal data. Legislative approach and comparative legal approach. The Indonesian government needs to immediately form and ratify a special legal instrument to regulate personal data protection. Apart from that, efforts that can be maximized in protecting personal data are by utilizing the potential of AI. The use of AI in protecting personal data will minimize the occurrence of human error so that the protection of personal data can be more guaranteed.

Analysis of Criminal Law Responsibility for the Use of Artificial Intelligence in Indonesia

The rapid development of technology underlies the presence of Artificial Intelligence (AI) in human activities and life, where AI can provide many benefits in helping human work in terms of speed and accuracy. Of course, it can be seen that AI can carry out actions and actions like humans, and this will give rise to legal problems if AI commits a criminal act that harms other parties, considering that there are no legal regulations that specifically regulate AI in Indonesia. Therefore, to see how the development of AI regulations in Indonesia and how responsible for the use of AI is from a criminal law perspective. In Indonesia, AI is an electronic system and an electronic agent. AI is not a legal subject and does not have awareness in determining its will in carrying out its actions, therefore responsibility for AI's actions and actions is borne by the creators and users of AI as an absolute legal subject in criminal law.

Application of Explainable Artificial Intelligence in Cybersecurity

Explainable Artificial Intelligence (XAI) plays a crucial role in cybersecurity amid the rapid growth of internet-connected tech and AI. While AI, like Machine Learning (ML) and Deep Learning (DL), enhances cybersecurity activities like intrusion detection and malware identification, the 'black box' nature of these methods limits their transparency and users' understanding. Despite extensive research in XAI in various fields, a notable gap exists in survey articles addressing XAI's application in cybersecurity. This survey aims to fill this void by providing an up-to-date overview of XAI methodologies tailored to cybersecurity challenges, offering a roadmap for navigating XAI literature in cybersecurity applications.

Crime Prediction Using Machine Learning and Deep Learning

Recent research has heavily focused on using machine learning and deep learning for crime prediction, aiming to identify patterns and trends in criminal activities. This journal delves into the datasets and methodologies utilized, offering insights into varied criminal behavior patterns. It not only highlights current limitations but also suggests future enhancements for more accurate crime predictions. Serving as a valuable resource, this journal aids researchers specializing in crime prediction, empowering law enforcement agencies to develop more effective crime prevention and response strategies.

Spatio-Temporal Crime Prediction by Utilizing Artificial Intelligence (AI) for Citizen Security in Smart Cities

This study introduces an innovative safety enhancement method for smart cities amidst rising urban populations. By employing Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN), it efficiently detects high-crime areas. Additionally, the study utilizes the Seasonal Auto-Regressive Integrated Moving Average (SARIMA) model to forecast future criminal activity in these regions. Evaluated using ten years of New York City (NYC) crime data, this approach displays remarkable accuracy with an average Mean Absolute Error (MAE) of 11.47, outperforming the DBSCAN-based method's highest MAE of 27.03. This method holds significant promise in improving crime prediction within urban landscapes.

Crime Prediction Using Machine Learning and Deep Learning

This paper uses AI for preventing juvenile delinquency and guiding therapy. It introduces two crime prediction algorithms: one based on temporal crime type calculation and a dense neural network, the other merging neural networks to enhance predictions. The focus is on understanding teen behavior and using text data effectively. It covers practical applications, exploring juvenile delinquency in Internet culture, and suggests measures like strengthening

* Corresponding author
cyber culture, responsible internet guidance, establishing prevention systems, and improving cyber-era crime prevention education.

Cyber-attack methods and perpetrator predictions use machine learning algorithms

The rise in global cyberattacks leads to substantial financial losses and increased cybercrimes. Recent strides in artificial intelligence offer solutions to detect and prevent these crimes. Existing crime prediction methods often miss anticipating cybercrimes, necessitating the analysis of actual data, including crime type, attacker details, and methods. This study uses machine learning to analyze cybercrimes, predicting attack methods and attacker traits. Support Vector Machine Linear performs best in predicting attack types (95.02%), while Logistic Regression leads in identifying attackers (65.42%). This model suggests higher education and income reduce the likelihood of a cyberattack, aiding cybercrime units in bolstering attack detection and response efficacy.

DISCUSSIONS

Artificial Intelligence (AI) has become a pivotal force reshaping various sectors, from cybersecurity and banking to international law and predictive analytics. This comprehensive literature review aims to provide an in-depth exploration of key studies in each domain, drawing insightful comparisons and identifying overarching trends.

1. "Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber" - Ishak Farid, Agus HS Reksoprodjo, Suhirwan
   This seminal work navigates the complex landscape of AI in cybersecurity. Ishak Farid et al. delve into the intricacies of threat detection, pattern recognition, and the responsive measures required for effective cybersecurity. By scrutinizing the interplay of AI technologies in fortifying digital defenses, the study establishes a foundational understanding of AI's role in safeguarding digital assets.
   Advantages:
   • In-depth analysis of the use of AI in cyber defense.
   • Application of deep learning models for complex cyber threat detection.
   • Has the potential to increase the effectiveness and efficiency of cyber defense.
   Weakness:
   • Not considering the interpretability aspect of the AI model.
   • It is necessary to take into account the problems of accuracy and error in pattern recognition.

2. "Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktivitas Perbankan di Indonesia" - Rahmi Ayunda, Rusdianto
   Examining the integration of AI within the Indonesian banking sector, Rahmi Ayunda and Rusdianto shed light on its role in ensuring the security of customer data and transactions. The study delves into the intricate mechanisms of data protection and cybersecurity strategies deployed within the banking sector, offering crucial insights into the evolving landscape of AI in finance.
   Advantages:
   • Applying Natural Language Processing (NLP) for financial transaction text analysis.
   • Reinforcement learning based AI model to detect anomalies in transaction behavior.
   • Highlighting technological advancements and their positive impact on banking efficiency.
   Weakness:
   • The need for strict regulations to prevent data leaks.
   • An emphasis is needed on establishing new regulations to protect data.

   This scholarly work explores the ethical and legal dimensions of employing AI in armed conflicts within the framework of international law. NAEK Siregar and Ahmad Syofyan meticulously examine the implications of AI applications in conflict scenarios, drawing comparisons between various perspectives and contributing to the ongoing discourse on regulating AI in the context of international law.
   Advantages:
   • Analyzing the use of AI in armed conflict with concrete examples.

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
Highlights a vision to reduce combatant casualties through replacing soldiers with AI.

Emphasizes higher effectiveness of work completion thanks to AI characteristics.

Weakness:
- Still in the adjustment and security stages of implementing AI in the military.
- There is no comprehensive regulation to regulate AI in armed conflict.


This research critically addresses the pressing need for specific regulations governing AI and personal data protection in Indonesia. Hari Sutra Disemadi's study not only underscores the urgency of tailored regulations but also engages in a comparative analysis of the existing regulatory landscape. It provides valuable insights into the challenges and opportunities associated with crafting effective data privacy laws in the era of increasing AI integration.

Advantages:
- Highlights the need for special regulations in protecting personal data in Indonesia.
- Proposing the use of AI to minimize human error in data protection.

Weakness:
- It is necessary to address the issue of ambiguity in the legal arrangements regarding AI.
- AI implementation requires careful steps to maintain data privacy.


Delving into the realm of criminal liability, this study by Muhammad Tan Abdul Rahman Haris and Tantimin scrutinizes the legal dimensions of AI utilization in Indonesia. By comparing legal frameworks and dissecting the intricacies of criminal responsibility tied to AI applications, the research provides a nuanced understanding of the evolving legal landscape.

Advantages:
- Analyze the development of legal regulations related to AI in Indonesia.
- Highlights the responsibilities AI imposes on creators and users.

Weakness:
- AI as an electronic system is not considered a legal subject.
- There is still a lack of specific legal provisions to address AI criminal acts.


Zhibo Zhang and Hussam Al Hamadi offer a comprehensive overview of explainable AI applications in cybersecurity. This state-of-the-art review explores the methodologies and recent advancements in making AI decisions more interpretable. Comparisons between different explainability techniques contribute to a deeper understanding of the transparency and trustworthiness of AI systems in the cybersecurity domain.

Advantages:
- Highlights the importance of Explainable AI (XAI) in cybersecurity.
- Proposing a roadmap for applying XAI in cybersecurity literature.

Weakness:
- There is a lack of survey literature that focuses on the application of XAI in the field of cybersecurity.
- A lack of transparency and interpretability in AI techniques can reduce user trust.


In the realm of predictive analytics, this systematic review by Varun Mandalapu et al. explores crime prediction using both Machine Learning (ML) and Deep Learning (DL) techniques. The research provides a meticulous comparison of methodologies, weaknesses, and future directions, contributing to a comprehensive understanding of the evolving landscape of crime prediction through AI.

Advantages:
- Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
- In-depth analysis of the use of machine learning and deep learning in crime prediction.
- Highlights potential gaps and future directions to improve the accuracy of crime predictions.
- Provides insight into various trends and factors related to criminal activity.

Weakness:
- There is no specific mention of the machine learning method or algorithm used.
- Conclusions on specific levels of performance or success may need to be added.


This study by Ummair Munner Butt et al. focuses on the predictive analytics of crime in smart cities, leveraging AI for enhanced citizen security. The research engages in a comparative analysis of spatial and temporal crime predictions, shedding light on the effectiveness of AI applications in creating safer urban environments.

Advantages:
- Using a new approach with HDBSCAN to detect crime hot spots.
- Application of SARIMA for spatio-temporal crime prediction in smart cities.
- Evaluate the model with ten years of crime data for New York City (NYC).

Weakness:
- Lack of information about key factors taken into account in predictions.
- There may be a need for further experimentation in different smart city environments.

9. "Echoing Mechanism of Juvenile Delinquency Prevention and Occupational Therapy Education Guidance Based on Artificial Intelligence" - Fang Hou

Fang Hou's research takes a unique angle by exploring AI applications in preventing juvenile delinquency and providing educational guidance. The study delves into the echoing mechanisms employed for juvenile delinquency prevention, drawing comparisons between different AI-driven strategies to guide education and mitigate delinquency among the youth.

Advantages:
- Predict crime by leveraging machine learning and deep approaches.
- Details the type of machine learning algorithm used.
- Highlights the potential for deeper understanding of crime prediction techniques.

Weakness:
- May need more information about success rates or model validation.
- Does not discuss in detail the future direction and challenges faced.

10. "Cyber-attack method and perpetrator prediction using machine learning algorithms" - Abdulkadir Bilen, Ahmet Bedri Özer

In the domain of cybersecurity, Abdulkadir Bilen and Ahmet Bedri Özer contribute a study on cyber-attack methods and the prediction of perpetrators using machine learning algorithms. The research involves a meticulous comparison of various machine learning algorithms, providing insights into improving the understanding of cyber threats and the identification of potential perpetrators.

Advantages:
- Focus on cybercrime prediction and attack methods using artificial intelligence.
- Using actual data from people's apps affected by cyberattacks.
- Provides a comparison between eight machine learning methods.

Weakness:
- It does not provide a detailed comparison or evaluation between the eight methods.
- It may be necessary to further evaluate other factors that influence cyber attacks.

Comparative Analysis:

Across these diverse domains, a common thread emerges—the critical role of AI in shaping the landscape of each field. While the applications vary, from enhancing cybersecurity to predicting crime and navigating legal complexities, the studies collectively underscore the transformative potential of AI. Comparative analyses within and between these domains offer a nuanced understanding of both the challenges and opportunities associated with the integration of AI.

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
technologies. Moreover, they highlight the need for interdisciplinary collaboration to harness the full potential of AI while addressing ethical, legal, and societal implications.

Linkages to the Use of AI in Crime Prediction:

- Cybersecurity Review (Journals 1, 6, 10): Provides a foundational understanding of the use of AI in addressing cyber threats, relevant to research approaches to improving societal security.
- Application of AI in Banking (Journal 2): Related to data protection, relevant to efforts to create a safer environment.
- Criminal Law Implications (Journals 3, 5): Offers an important legal perspective regarding criminal liability regarding the use of AI in criminal contexts.
- Applications of AI in Smart Cities (Journal 8): Contributes to the understanding of how AI can be used to improve public safety in urban environments.
- Juvenile Delinquency Prevention (Journal 9): Provides insight into the application of AI in the context of juvenile delinquency prevention, which can embrace holistic solutions.

<table>
<thead>
<tr>
<th>No</th>
<th>Author</th>
<th>Year</th>
<th>Volume</th>
<th>Judul</th>
<th>Method</th>
<th>Result</th>
<th>Data Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ishak Farid, Agus HS Reksoprodjo, Suhirwan</td>
<td>2023</td>
<td>Volume 10 No 2</td>
<td>Pemanfaatan Artificial Intelligence Dalam Pertahanan Siber</td>
<td>Qualitative Descriptive Analytical</td>
<td>This study highlights AI's substantial role in boosting cyber defense by monitoring and analyzing network activities for potential threats. While AI aids in predicting and preventing attacks by identifying abnormal behavior, it's essential to note its limitations, like accuracy problems and errors in pattern recognition, when implementing AI in cyber defense.</td>
<td>Google Scholar</td>
</tr>
<tr>
<td>2</td>
<td>Rahmi Ayunda, Rusdianto</td>
<td>2021</td>
<td>Volume 7 Nomor 2</td>
<td>Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktifitas Perbankan di Indonesia</td>
<td>Normative Research Methods</td>
<td>AI's use in banking lacks specific regulations, relying on interpretations of existing laws like the Banking Law and ITE Law. This leads to lenient sanctions, failing to deter cyber acts effectively. To address this, it's crucial to establish dedicated regulations alongside AI implementation in banking to prevent negative impacts and actions stemming from its application.</td>
<td>Google Scholar</td>
</tr>
<tr>
<td>3</td>
<td>Naek Siregar, Ahmad Sofyan</td>
<td>2022</td>
<td></td>
<td>Penggunaan Artificial Intelligence Dalam Konflik Bersenjata Menurut Hukum Internasional</td>
<td>Normative Research Methods</td>
<td>There's a gap in international law regarding AI in international humanitarian law. A specialized regulation is necessary to set limits on excessive weapons development. The absence of human intervention in autonomous weapons challenges fundamental principles like indiscrimination, military necessity, and proportionality, requiring specific guidelines rather than outright prohibitions.</td>
<td>Google Scholar</td>
</tr>
<tr>
<td>4</td>
<td>Hari Sutra Disemadi</td>
<td>2021</td>
<td>Volume 7 Nomor 2</td>
<td>Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia</td>
<td>Normative Juridical</td>
<td>Indonesia urgently needs dedicated laws for safeguarding personal data. Leveraging AI could fortify data protection by minimizing human errors and ensuring more robust safeguards for personal information.</td>
<td>Google Scholar</td>
</tr>
</tbody>
</table>

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
5 Muhammad Tan Abdul Rahman Haris, Tantimin 2022 Volume 8 Nomor 1 Analisis Pertanggung Jawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia

Normative Law As AI advances in Indonesia, aligning legal frameworks with technological progress is crucial. Currently, there's a gap in specific AI regulations, prompting expansions in laws like the ITE Law to accommodate AI characteristics within electronic system regulations.

6 Zhibo Zhang, Hussam Al Hamadi 2023 Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research Intelligencce (XAI) XAI, or Explainable AI, greatly enhances the transparency of AI models, including those in cybersecurity. This survey paper delves into cutting-edge research on XAI's applications in cybersecurity. It covers basic concepts, taxonomy, and advanced models. It explores how XAI defends against various cyber threats like malware, fraud, phishing, and network intrusion, offering insights into defensive strategies.

7 Varun Mandalapu, Lavanya Elluri, Piyasuh Vyas, Nirmalya Roy 2023 Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions Literature review Technological advancements have complicated criminal activities, prompting interest in using machine learning and deep learning for crime prediction. These methods reveal potential in detecting criminal behavior, offering more accurate models using extensive datasets and advanced algorithms. However, there's a gap in applying this technology to address crime prediction challenges. Our findings aim to guide future research in understanding diverse techniques, datasets, and directions in this field.

8 Ummair Munner Butt, Sukumar Letchmunan, Fadratul Hafaniz Hassan, Mubashir Ali, Anes Baqir, Tieng Wei Koh, Hafiz Husain Raza Sherazis 2021 Spatio-Temporal Crime Predictions by Leveraging Artificial Intelligence for Citizens Security in Smart Cities Microwave assisted extraction (MAE) This paper outlines an efficient approach for creating a secure environment in smart cities using data analysis from a decade of police reports. Our method outperforms existing systems with a lower Mean Absolute Error. Future plans involve improving the model through transfer learning, leveraging past crime prediction models for better performance. We also aim to explore ensemble clustering to enhance the accuracy and resilience of crime detection and prediction.

9 Fang Hou 2022 Echoing Mechanism of Juvenile Delinquency Prevention and Occupational Therapy Education Guidance Based on Artificial Intelligence Intelligent Systems Analysis This study introduces a novel method using feature vectorization to calculate crime types over time, enhancing the neural network's ability to predict crime types accurately. It emphasizes the importance of addressing juvenile delinquency and presents a refined early warning model. The study explores various evaluation methods and management strategies for juvenile crime, concluding with insights into early warning mechanisms and effective management strategies.

10 Abdulkadir Bilen, Ahmet Bedri Ozer 2021 Cyber-attack method and perpetrator Linier SVM The model achieved a 60% success rate in identifying cyber attack perpetrators, with potential for improvement using...

* Corresponding author

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.
prediction using machine learning algorithms | other AI methods. It highlights the importance of focusing on malware attacks and social engineering. Interestingly, higher education and income correlate with lower susceptibility to cyber attacks. The research aims to aid law enforcement by offering faster crime detection and criminal identification solutions. It suggests developing new training and alert systems based on victim profiles identified in the analysis. Future plans involve using deep learning algorithms to predict crimes, victim profiles, and cyber attacks for further evaluation.

CONCLUSION

The research undertakes a comprehensive literature review, exploring AI's pivotal role in crime prediction by analyzing its function in deciphering crime data, intricate pattern recognition, and precise predictions. This exploration aligns with the objective of seeking innovative solutions to diminish crime rates and foster a safer environment in Indonesia. The correlation observed between the reviewed literature and the study's objectives solidifies the significance of AI across diverse realms such as cyber defense, data protection, and legal accountability. By synthesizing this knowledge, the research aims to propose pragmatic steps bolstered by AI's potential, emphasizing the necessity for informed regulations and innovative solutions to effectively reduce crime rates, thereby contributing to Indonesia's enhanced security and societal safety.

ACKNOWLEDGMENT

This research is fully supported by the program study of Information System in Universitas Prima Indonesia. Huge appreciation to the Dean of Faculty of Technology and Computer Science, Mr. Mardi Turnip, my adviser, who oversaw and advised us in this project, and also to all friends (senior and junior) who participate in my project.

REFERENCES


* Corresponding author


