Spring 6-29-2023

Artificial Intelligence Adoption in Criminal Incestigations: Challenges and Opportunities for Research

Oluwatunmike Olowe
Loughborough University, o.i.olowe@lboro.ac.uk

Peter Kawalek
Loughborough University, p.kawalek@lboro.ac.uk

Kayode Odusanya
Loughborough University, k.odusanya@lboro.ac.uk

Artificial Intelligence Adoption in Criminal Investigations: Challenges and Opportunities for Research

Oluwatunmike Olowe, Peter Kawalek, Kayode Odusanya
Centre for Information Management, Loughborough Business School, Loughborough University
Loughborough, Leicestershire, LE11 3TU, United Kingdom
o.i.olowe@lboro.ac.uk; p.kawalek@lboro.ac.uk; k.odusanya@lboro.ac.uk

Abstract

Artificial Intelligence (AI) offers the potential to transform organisational decision-making and knowledge-sharing processes that support criminal investigations. Yet, there is still limited evidence-based knowledge concerning the successful use of AI for criminal investigations in literature. This paper identifies the main areas and current dynamics of the adoption of AI in criminal investigations using bibliometric analysis. We synthesise existing research by identifying key themes researchers have delved into on AI in criminal investigations. The themes include crime prediction and human-centred issues relating to AI use in criminal investigations. Finally, the paper elaborates on the challenges that may influence AI adoption in criminal investigations by police professionals. These challenges include possible laggard effects with AI adoption, implementation challenges, lack of government oversight, and a skills gap.

Keywords: Artificial intelligence, AI adoption, Criminal investigations, Policing

1.0 Introduction

Crime is a threat to the safety of society. For example, within the United Kingdom (UK), the number of recorded kidnapping offences in England and Wales increased by 51.32% from 4,563 to 6,905 in the last five years[1]. Furthermore, data from the Office of National Statistics (ONS, 2021) shows that 81% of females and 39% of males feel very or relatively unsafe when walking home after dark[2]. Meanwhile, over the last decade, the landscape of conducting criminal investigations – investigating crime, collecting evidence, and arresting or apprehending suspected offenders (The Crown Prosecution Service, 2020) – has experienced a developing deployment of Artificial Intelligence (AI) technologies. AI enables criminal investigations by supporting police professionals through increasing information and knowledge sharing (Babuta and Oswald, 2020; Bromberg et al., 2020). Yet, despite the profound capabilities AI tools afford, there are ethical concerns about its deployment in criminal investigations. For instance, the police force's use of Facial Recognition Technology (FRT) in the UK has

[1] https://www.statista.com/statistics/303548/kidnapping-in-england-and-wales-uk/

[2] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/perceptionsofpersonalsafetyandexperiencesofharassmentgreatbritain/2to27june2021

been under constant scrutiny by the public due to privacy concerns under Article 8 of human rights to privacy (Fussey and Murray, 2019; Batabyal et al., 2020; Duan, 2020; Almeida et al., 2021). Also, the FRT procedure in criminal investigations involves scanning images and matching them against a watchlist database. This process has reportedly raised bias and discriminatory concerns (Fussey and Murray, 2019). Additionally, the risk of using AI tools in criminal investigations can lead to false identification/wrongful predictions (Almeida et al., 2022). Evidently, extant research indicates that the high cost of adopting AI tools has not always resulted in effectively achieving expected goals but has instead given rise to several problems and criticisms. These concerns raise important questions about the need to understand the deeper complexities of deploying AI tools in criminal investigations (Duan, 2020).

Consequently, there is a need to review the current state of research concerning the use of AI tools in criminal investigations and understand the challenges associated with its deployment. This paper addresses this need through the following research questions:

- ***RQ1:*** *What are the current publication dynamics on the use of AI in criminal investigations?*
- ***RQ2:*** *What are the challenges faced by police professionals in adopting AI in criminal investigations?*

Exploring these questions is crucial for several reasons. Criminal investigations are essential for the promotion of public safety, and police professionals are the primary actors in carrying out criminal investigations. Meanwhile, extant studies have called for more purposeful policies and standards to guide how AI tools are deployed for criminal investigations (Babuta and Oswald, 2020; Fussey and Murray, 2019). Policies, guidelines, and frameworks are essential for an organisation’s effective and successful operation as they help reduce liability risk, build a healthy reputation, and enable consistent processes (Gillespie & Dietz, 2009).

This paper is structured as follows: section two explains the research approach and methodology using a bibliometric review and semi-structured qualitative interviews with police professionals in England and Wales who are key stakeholders with varying levels of experience with AI technologies use and implementation. Section three reports the findings from the bibliometric study and interviews carried out thus far in the research. Section four concludes with the paper’s contributions, limitations, and next steps.

2.0 Research Approach and Methods

To answer the research questions in this paper, we used multiple data collection approaches that consist of primary and secondary data collection techniques. The approach to data collection includes a bibliometric analysis and semi-structured interviews. The use of semi-structured interviews stems from an interpretive stance. The interpretive approach has been used in the Information Systems (IS) field to explore the experiences people attach to information systems design, management, intervention, and social implications (Walsham, 1995; Noir and Walsham, 2007; Stacey and Tether, 2015). Using semi-structured interviews for this stance allows us to capture the experiences and meanings police professionals have as regards using AI in their criminal investigations. The following sub-section details the bibliometric analysis and semi-structured interview approach adopted for this paper.

2.1 Bibliometric analysis

The bibliometric analysis provides metrics for the quantitative investigation of scholarly work in a discipline (Beydoun et al., 2019; Wamba and Queiroz, 2021). It is a powerful technique that helps identify published work patterns, trends, and characteristics (Ferreira et al., 2014; Kim et al., 2021). Beydoun et al. (2019) best practice approach is adopted for the bibliometric analysis. Descriptive, citation and co-word analyses are used to understand the current publication dynamics on AI in criminal investigations. Citation analysis is a bibliometric method that measures the impact of research publication using citations as a unit of analysis (Baker et al., 2020). The co-word analysis helped to observe the conceptualisation of the research topic in the literature and explore the literature's themes (Baker et al., 2020; Donthu et al., 2021).

The research protocol adopted for the bibliometric analysis is depicted in Table 1. Data was collected from the Scopus database from 2012 – 2022 using keywords related to the title to perform the search. The keywords are “crime” OR “criminal investigations” OR “police” OR “policing” AND “AI” OR “artificial intelligence” OR “facial recognition” OR “deep learning” OR “machine learning” OR “neural network” OR “natural language processing” OR “computer vision”. The subject areas in the inclusion criteria were computer science, arts & humanities, psychology, business, management and accounting, decision sciences, social sciences, and multidisciplinary fields. We also restricted our sample to include journal articles and IS conference papers at the final publication stage. Information Systems (IS) conference papers were selected from the top IS conferences according to Association for Information Systems (AIS). The conferences include the International Conference on Information Systems (ICIS), the American Conference on Information Systems (AMCIS), Pacific Asia Conference on Information Systems (PACIS) and European Conference on Information Systems (ECIS).

Criteria	Metrics
Keywords	"crime" OR "criminal investigations" OR "police" OR "policing" AND "AI" OR "artificial intelligence" OR "facial recognition" OR "deep learning" OR "machine learning" OR "neural network" OR "natural language processing" OR "computer vision"
Year range	2012-2022
Subject area	Computer Science, Arts & Humanities, Psychology, Business, Management and Accounting, Decision Sciences, Social Sciences and Multidisciplinary
Document type	Journal Articles and IS Conference Papers
Source type	Journal and Conference Proceedings
Publication stage	Final
Language	English

Table 1. Research protocol for bibliometric review.

The next step involved manually cleaning the data extracted from Scopus by removing erroneous entries and limiting the data to those required for citation and co-word analysis. The data for citation analysis were author names, citation numbers, titles, journal titles, DOI and references, while for Co-word analysis, we used titles and author keywords (Donthu et al., 2021). We used VOS viewer software to conduct the bibliometric analysis (Van Eck and Waltman, 2023). The bibliometric analysis includes the number of articles published annually (descriptive analysis), the most cited published research on AI for criminal investigations in IS journals and conferences, analysis of author keywords and top 20 most cited articles. The research protocol yielded 105 papers for bibliometric analysis.

2.2 Semi-structured Interviews

The qualitative data collection technique is semi-structured interviews with police professionals who have varying experience of AI technologies. Semi-structured interviews in IS literature capture the lived experiences of respondents undergoing a phenomenon and focus on the participants (Noir and Walsham, 2007). Respondents can express their lived experiences using their own words, allowing the researcher to concentrate on their world (Myers, 2013). Semi-structured interviews are popular in qualitative research and stem from the interpretive stance adopted in this paper (Creswell, 2007; Denzin and Lincoln, 2005; Saunders et al., 2019). The semi-structured approach fits well for this research, allowing a reflective thought process. The reflective thought process allows for the extraction of rich and in-depth information regarding the *challenges faced by police professionals in adopting AI in criminal investigations.*

3.0 Results and Discussion

The results of the bibliometric analysis and semi-structured interviews are presented below. The first three sections show the results of the bibliometric study, followed by findings from the semi-structured interviews.

3.1 Descriptive Analysis

The annual publication of articles shows the number of articles released each year on the related topics of this paper in the IS field. Figure 1 illustrates the number of articles published annually on AI in criminal investigations from early 2012 to late 2022. The number of articles published during the period, as shown in Figure 1, is 105. There has been a general fluctuation in the number of articles published annually. However, most articles on AI in criminal investigations were published in the last five years, with 2022 having the highest number of articles.

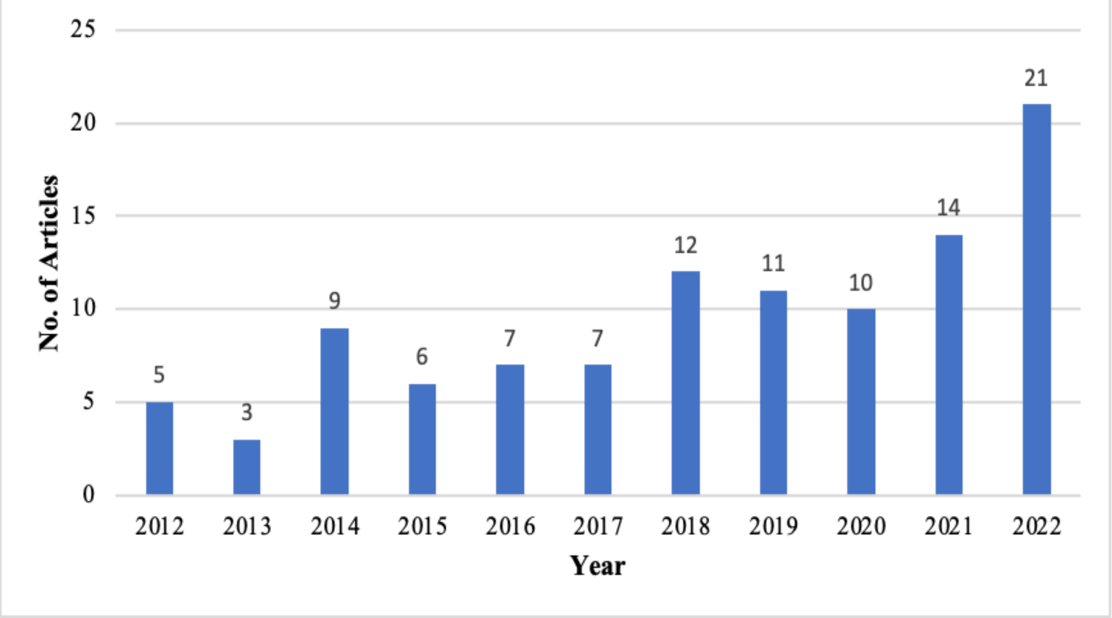

Figure 1. The number of articles published annually from 2012 - 2022.

Next, Table 2 shows the citations spread across IS journals and conferences. These journals represent the sources for the most cited published articles on AI for criminal investigations. The top cited journals include Expert Systems with Applications (3,172 citations), followed by Decision Support Systems (993 citations), Computers in Human Behaviour (374 citations) and Journal of Management Information Systems (75 citations). In addition, for IS conference journals, European Conference on Information Systems (ECIS) has the highest number of citations (34), followed by the Americas Conference on Information Systems (AMCIS) (19) citations. We surmise that in the top journals for IS field from the Scopus database search, journal articles have an 87% (91) share, while top IS conference journals have a 13% (14) share of the published articles. These figures show the need for more IS journals to encourage research at the intersection of AI and criminal investigations.

Source Type and Journal	**Citations**	**No. of Articles**
Journals		
Expert Systems with Applications	3172	61
Decision Support Systems	993	14
Computers in Human Behavior	374	8
Journal of Management Information Systems	75	1
Government Information Quarterly	72	2
Information Systems Journal	57	1
Journal of Information Technology	32	2
Information and Management	6	1
European Journal of Information Systems	1	1
Conferences		
European Conference on Information Systems (ECIS)	34	1
The Americas Conference on Information Systems (AMCIS)	19	9
Pacific Asia Conference on Information Systems (PACIS)	13	2
The International Conference on Information Systems (ICIS)	12	2

Table 2. Most cited published research on AI for Criminal Investigations in IS journals and conferences.

3.2 Keyword Analysis

Keyword analysis provides an understanding of how authors have conceptualised research on a domain over the period analysed. A visual representation of keyword dynamics used by authors is also presented in Figure 2. The most prominent keyword in Figure 2 is “machine learning”. The “Red” cluster includes “big data”, “classification”, “decision support”, “finance”, “fraud”, “natural language processing”, “social media”, and “taxonomy”. The “Green” cluster depicts machine learning techniques used by extant research, such as “adaptive boosting”, adversarial learning”, “cost-sensitive learning” and information technology security such as “cyber security”. The Blue” cluster includes “detection”, “fraud detection”, “machine learning”, “malware”, “random forest”, “supervised learning”. The “Yellow” and “Purple” cluster includes keywords such as “class imbalance”, “deep learning”, “intrusion detection”, “malware detection”, “blockchain”, and “intrusion detection system”. The “Pink” cluster includes “artificial intelligence” and “Bayesian networks”. The “Orange” and “Grey” clusters include “anomaly detection”, “cyberbullying”, “social contagion”, “crime prediction”, “Twitter”, and “topic modelling”.

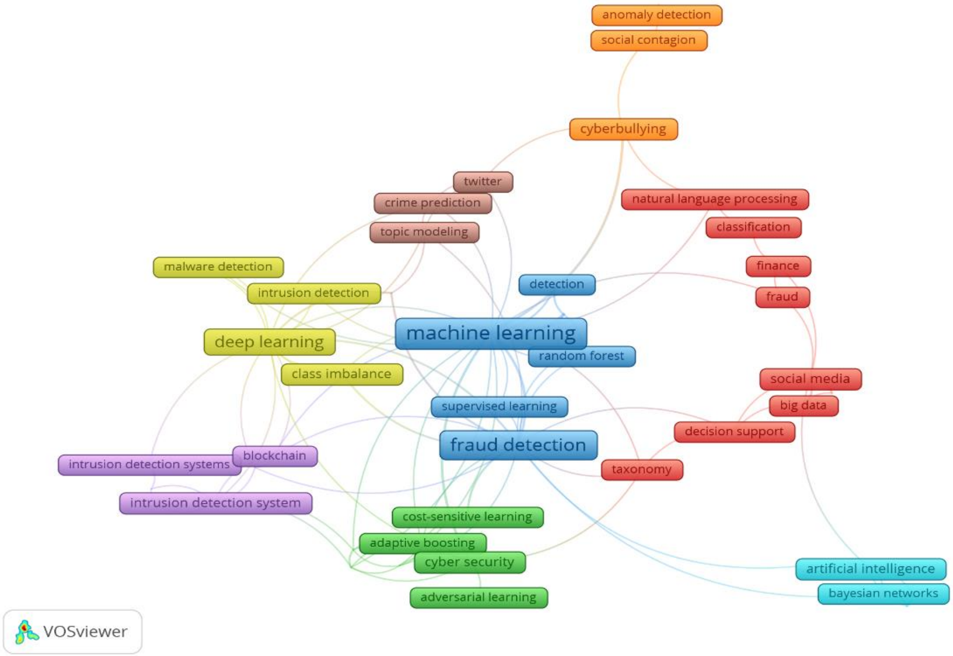

Figure 2. Author keyword visualisation

Furthermore, the top 15 most occurring keywords by authors are depicted in Table 3, and artificial intelligence methods such as machine learning and deep learning are at the top of the list. Machine learning is the most occurring word in the list at 27 occurrences (25.71%), making it the most occurring term used by extant research when investigating AI in criminal investigations. Meanwhile, keyword terms like fraud detection and deep learning followed with 18.10% and 11.43% occurrences, respectively. Network security methods, computer security, crime detection, crime prediction, online crime, and social media platforms (Twitter) also feature in the top 15 keywords.

Rank	Keyword	Occurrences
1	Machine Learning	27
2	Fraud Detection	19
3	Deep Learning	12
4	Malware	6
5	Cyber Security	5
6	Social Media	5
7	Intrusion Detection System	4
8	Cyberbullying	4
9	Artificial Intelligence	4
10	Class Imbalance	4
11	Crime Prediction	3
12	Twitter	3
13	Malware Detection	3
14	Anomaly Detection	3
15	Text Mining	3

Table 3. Top 15 most occurring author keywords

Next, we generated a word cloud using the manuscript titles to provide further insights about the main themes featuring prominently in extant research. The word cloud (see Figure 3) signifies where research interest lies in the literature. Figure 3 shows that "Detection" is a prominent topic among the top 20 most cited articles. Artificial intelligence approach such as deep learning, machine learning, supervised learning, reinforcement learning are methods used to investigate AI adoption in criminal investigations. Online forms of crime such as cyberbullying, cybercrime, phishing, malware, credit card fraud is depicted in top cited articles. Social media platforms such as Twitter are areas for criminal investigations.

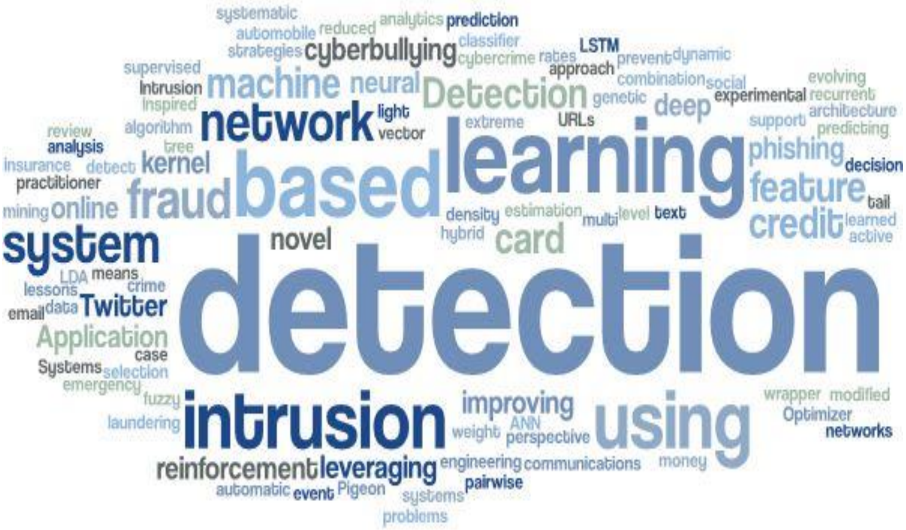

Figure 3 Word cloud based on the titles of the top 20 most cited articles.

The 20 most cited documents, their authors, title, year of publication and number of citations are depicted in Table 4. Gerber’s (2014) paper on predicting crime using Twitter and kernel density estimation is the most highly cited IS publication. Also, prediction and detection through AI methods such as deep learning, neural networks, and algorithms in the top 20 most cited articles are reinforced. Prediction and detection were made in areas such as malware detection, financial fraud, cyberbullying, and phishing. Other methods include network intrusion detection and data mining. Expert System with Applications and Decision Support Systems journals published the most cited papers. Notably, the earliest paper was published in 2012 by Sindhu et al. (2012), while the latest was published in 2019. Our data suggest that more recent articles, such as those published between 2020-2022, have not had enough time to gain attention in the literature like older publications. According to Zupic and Cater (2015), this is a limitation of using citation analysis.

Authors	Title	Year	No of Citations
Gerber MS.	Predicting crime using Twitter and kernel density estimation	2014	406
Al-Yaseen W.L., Othman Z.A., Nazri M.Z.A.	Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system	2017	272
Sahingoz O.K., Buber E., Demir O., Diri B.	Machine learning based phishing detection from URLs	2019	257
Dal Pozzolo A., Caelen O., Le Borgne Y.-A., Waterschoot S., Bontempi G.	Learned lessons in credit card fraud detection from a practitioner perspective	2014	243
Sivatha Sindhu S.S., Geetha S., Kannan A.	Decision tree based light weight intrusion detection using a wrapper approach	2012	237
Al-Garadi M.A., Varathan K.D., Ravana SD.	Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network	2016	199
Correa Bahnsen A., Aouada D., Stojanovic A., Ottersten B.	Feature engineering strategies for credit card fraud detection	2016	183
Akashdeep, Manzoor I., Kumar N.	A feature reduced intrusion detection system using ANN classifier	2017	166
Alazzam H., Sharieh A., Sabri K.E.	A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer	2020	152
Carneiro N., Figueira G., Costa M.	A data mining-based system for credit-card fraud detection in e-tail	2017	151
Wang Y., Xu W.	Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud	2018	150
Elhag S., Fernández A., Bawakid A., Alshomrani S., Herrera F.	On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems	2015	149
Fronzetti Colladon A., Remondi E.	Using social network analysis to prevent money laundering	2017	105
Cortez B., Carrera B., Kim Y.-J., Jung J.-Y.	An architecture for emergency event prediction using LSTM recurrent neural networks	2018	105
Lopez-Martin M., Carro B., Sanchez-Esguevillas A.	Application of deep reinforcement learning to intrusion detection for supervised problems	2020	104
Rosa H., Pereira N., Ribeiro R., Ferreira P.C., Carvalho J.P., Oliveira S., Coheur L., Paulino P., Veiga Simão A.M., Trancoso I.	Automatic cyberbullying detection: A systematic review	2019	101

Smadi S., Aslam N., Zhang L.	Detection of online phishing email using dynamic evolving neural network based on reinforcement learning	2018	91
Nissim N., Moskovitch R., Rokach L., Elovici Y.	Novel active learning methods for enhanced PC malware detection in windows OS	2014	79
Fossaceca J.M., Mazzuchi T.A., Sarkani S.	MARK-ELM: Application of a novel multiple kernel learning framework for improving the robustness of network intrusion detection	2015	76
Dong W., Liao S., Zhang Z.	Leveraging Financial Social Media Data for Corporate Fraud Detection	2018	75

Table 4. Top 20 most cited articles with their authors

3.3 Themes Observed from Bibliometric Data

Based on the citation, keyword analysis and filtering bibliometric data in Excel with ABS ranking journals, we observe two main themes in the literature, which we discuss below:

First, a widely discussed theme in the literature is predicting crime using artificial intelligence techniques such as machine learning, deep learning, and neural networks. These techniques were observed in different contexts, such as within *financial institutions, on social media and network security* (Dal Pozzolo et al., 2014; Gerber, 2014; Zhong and Gu, 2019; Al-Garadi et al., 2016;). "Detection" is a prevalent word used by studies to address this theme. It describes attempts to observe crime patterns in different situations, such as practices that defer from the norm. In extant literature, the observation of crime patterns' aim is to propose crime prevention strategies by developing predictive tools with AI techniques (Colladon and Remondi, 2017). Research papers on this theme developed models and frameworks using algorithms and natural language processing to help detect and prevent felonies, money laundering, cybercrime, credit card fraud and address cyberbullying on Twitter platforms (Wong et al., 2012; Gerber, 2014; Balci and Salah, 2014). The coverage of crime prediction has been studied in various contexts.

For instance, in the context of financial crimes, extant research has explored how AI can predict money laundering and financial fraud behaviours, such as financial statement fraud, credit card fraud etc. (Wang et al., 2020; Wu et al., 2019; Sun et al., 2020). Wang et al.'s (2020) use of an arson case in China proposed a growth algorithm of the Bayesian network to aid crime reconstruction and prevention by providing practical investigation suggestions. Colladon and Remondi (2017) addressed the prevention of money laundering using social network analysis on the financial operations of an Italian factoring company. Sun et al., (2020) study depicts how an ensemble long short-term memory model can be utilised to detect financial statement fraud. They used a data set consisting of fraudulent and non-fraudulent reports.

Another notable crime prediction context explored by previous research is digital platforms such as social media and email engines. Social media allows people to air their opinions and express themselves, while email engines act as avenues for communication between individuals who may not be able to communicate with one another physically (Middleton and Cukier, 2006; Stieglitz and Dang-Xuan, 2013). These online platforms have enabled criminals and served as a crime prediction medium. Crimes such as cyberbullying, sexual assault, battery, and homicide, amongst others, are crimes observed in the literature as regards the prediction of crime on social networks (Gerber, 2014; Al-Garadi, 2016).

Gerber (2014) portrayed how incorporating Twitter data in the kernel density model could help predict 25 types of crime, such as theft, sexual assault, battery, narcotics, homicide etc. The data was from the Data Portal provided by the Chicago Police department and included 60,876 crimes. It was deduced from the developed crime prediction model that 76% of the crime types studied, i.e., 19 out of 25, can be predicted through topic modelling using Twitter-specific tokenizer and part-of-speech tagger with kernel density estimation. Similarly, Al-Garadi et al. (2016) study on cybercrime detection using a feature-based model, included network information, activity information, user information and tweet content to uncover cyberbullying behaviour on Twitter. Their model incorporated a machine learning classifier categorising tweet into cyberbullying and non-cyberbullying behaviours.

A further context that features in the literature on crime prediction using AI is Cyberspace. Cyberspace is a term used to describe the interlinked infrastructure network (Hui et al., 2017). Extant research highlights the need for network security in a world increasingly connected through data. This data originates from devices and objects such as large-scale infrastructure used by organisations to individual household devices such as smartphones, intelligent home systems, smartwatches, etc. - thereby creating an avenue for malicious behaviours from hackers and criminals through phishing and malware creation (Zhong and Gu, 2019; Biswas and Mukhopadhyay, 2022). Biswas and Mukhopadhyay (2022) proposed a framework for organisations cybersecurity controls. They employed hacker messages in dark forums to propose recommendation in their framework which consists of cyber-risk assessment and cyber-risk mitigation. Finally, phishing is a different type of cybercrime involving identification, typically done through emails and text messages (Wright, 2014). In this case, the criminal takes on the identity of a reputable company or person to draw information from a third party. The data extracted could be credit card details, login credentials, an individual's name, address, or any other information the criminal can use to exploit the third party. Sahingoz et al., (2019) used seven classification algorithms and natural language processing-based features to develop a real-time anti-phishing system for URLs. The best result from their study was the random forest algorithm with only NLP based features which yielded a 97.98% accuracy rate for detecting phishing URLs.

Several studies focused on predicting and detecting crime using AI tools and techniques in the literature. For instance, Smadi et al. (2018) proposed an adaptable model for detecting phishing emails using dynamic evolving neural network based on reinforcement learning. Furthermore, Craja et al. (2020) proposed a deep learning model consisting of financial ratios and textual data from corporate annual reports to detect financial statement fraud.

The second strand of research from the literature review focused on studies that highlight socio-technical problems with using AI technologies like body cams (Bromberg et al., 2020; Yokotani and Takano, 2021). Bromberg et al. (2020) utilized the Technology Acceptance Model (TAM) to investigate the extent of public support for police use of facial recognition via body-worn cameras in the state of New Hampshire, USA. They employed the use of phone and web surveys, to investigate this phenomenon. The findings of their study indicate that social norms, particularly the influence of public pressure, play a crucial role in shaping individuals' willingness to support the use of facial recognition technology through body-worn cameras. Yokotani and Takano (2021) conducted a study to examine the association between social contagion of social norms that facilitate cyberbullying and an elevated risk of victimisation or perpetration. Their study revealed that non-victims who interacted with cyberbullying victims had a higher probability of becoming perpetrators themselves, thus contributing to the prevalence of online cyberbullying. Moreover, their results indicate that gender minorities may be vulnerable to cyberbullying victimisation due to potential discrimination associated with their avatar's appearance.

This study complements prior research by including human perspectives and opinions on administering AI in criminal investigations. Thus, by employing semi-structured interviews with police specialists, the following section examines the key difficulties they encounter when integrating AI into criminal investigations.

3.4 Semi-structured Interviews: Preliminary Findings

In this section, we report preliminary findings based on interviews conducted. The respondents include two retired police professionals who have had consultancy roles at national level and one police professional. The semi-structured interview transcripts are analysed using Braun and Clarke's (2012) six-step thematic analysis methodology. The first step involved familiarisation with the data by transcribing the interview and re-reading the transcripts to gain richer insights. The second step comprises coding the data. We used an inductive approach to code the data, which involved making notes on printed transcripts and using the MS Word comment function to highlight material. The early themes are shown in Table 5, and they illustrate law enforcement officials' difficulties in implementing AI in criminal investigations.

The analysis in Table 5 reveals a possible laggard effect associated with AI adoption in criminal investigations by police professionals. The laggard effect is drawn from the diffusion of innovation theory (Rogers, 1962). The possible laggard effect is observed as a hold-back stance by police professionals as they wait to see who among their social system would pioneer the adoption of AI in criminal investigations. This stance allows them to learn from the experiences of the pioneer before adopting the AI tool or technology in their jurisdiction. CO's comments below reflect a possible laggard effect when it comes to the adoption of AI in criminal investigations by police professionals:

"I think it's almost like a, it's not a race, but it's almost like who wants to, who wants to use the big data first, and then everybody else will follow. Because if you're a pathfinder

in that particular area, it's always an uncomfortable position to be in if you're leading it because you then get hit with [..] from a lot of external agencies" - CO

When AI adoption eventually happens, it is often fraught with implementation challenges.

"We were using data in a more proactive way [...], but we've stopped using that methodology at the moment because of the way that we have identified some ethical issues with it" - CO

"There is a real challenge around balancing the operational decisions with the, what's the term, evidential efficacy of the application of AI tools" – CON1

The intricacies that stall AI implementation by police professionals includes an ethical dilemma which needs to be addressed for AI adoption by police professionals to be effective. The ethical dilemma includes fairness in AI models and eliminating bias.

"I suppose the challenge for policing around the use of AI is the fairness aspect of it and actually the variables that you use in the model." – CO

"Concerns around the bias in the training data sets that have been used for basically training the discriminatory approach and algorithms you used in that particular application" – CON1

Another challenge with AI adoption by police professionals is a skills gap in developing and using AI technologies for criminal investigations. CON1 and CON2 have similar comments regarding the skills gap needed to be filled for effective AI adoption by police professionals.

"I think there's a huge gap around skills and knowledge and I think that will probably extend to a professional standard around AI" – CON1

"We don't have enough highly skilled human resources, and the human brain cannot, cannot process the IT in the same way as a machine can" – CON2

Also, when a skills gap is filled, there is still the challenge of a lack of regulatory oversight to guide the variety of data processed for criminal investigations.

"We have analysts in policing and the great people but there is no tested standard of competence around how they would manage either an AI analytic solution or data generated in the wild, AI used commercially for example" – CON1

Emerging Challenges	Representative Quote
Implementation Challenges	"We were using data in a more proactive way […] but we've stopped using that methodology at the moment because of the way that we have identified some ethical issues with it" - CO "I suppose policing want to use AI but how would you do it in a fair and transparent way that promotes what you want to achieve from the outcome?" - CO
Ethical Dilemma	"I suppose the challenge for policing around the use of AI is the fairness aspect of it and actually the variables that you use in the model." – CO "Concerns around the bias in the training data sets that have been used for basically training the discriminatory approach and algorithms you used in that particular application" – CON1
Possible Laggard Effect	"I think it's almost like a, it's not a race, but it's almost like who wants to, who wants to use the big data first, and then everybody else will follow. Because if you're a pathfinder in that particular area, it's always an uncomfortable position to be in if you're leading it because you then get hit with [..] from a lot of external agencies" - CO
Shortage in Regulatory Oversight	"We have analysts in policing and the great people but there is no tested standard of competence around how they would manage either an AI analytic solution or data generated in the wild, AI used commercially for example" – CON1
Skills Gap	"I think there's a huge gap around skills and knowledge and I think that will probably extend to a professional standard around AI" – CON1 "We don't have enough highly skilled human resources, and the human brain cannot, cannot process the IT in the same way as a machine can" – CON2 "There has to be a professionalisation focus on analytics, data professionals. It's no surprise it's been highlighted as the biggest risk to policing for the last seven years that I'm aware of people, skills and knowledge and yet we seem to be stuck with, you know not much progress" – CON1

Table 5. Emerging challenges facing police professionals' adoption of AI in criminal investigations

4.0 Conclusion

Technology advancements have provided a platform for adopting Artificial Intelligence (AI) technologies across various sectors of the economy. Yet, there is a paucity of research investigating how AI is used in criminal investigations in the Information

System field (Al-Garadi et al., 2016; Bromberg et al., 2020; Colladon & Romondi, 2017). This study contributes to the IS field by exploring the adoption of AI in criminal investigations. By focusing on criminal investigations, this research broadens the discussion of AI in the literature to a significant phenomenon that has received little attention despite being of societal significance. The extant literature analysed shows that studies around AI adoption in criminal investigations are focused mainly on proactive measures to deter and prevent crimes through prediction (Shabtai et al., 2012; Gerber, 2014; Wang et al., 2020). Furthermore, human-centred issues such as behaviours and perceptions regarding AI technologies are captured in the literature reviewed (Clarke and Parsell, 2019; Pyo, 2021; Wright & Headley, 2021).

The emerging themes suggest a possible laggard effect regarding AI adoption in criminal investigations by police professionals in England and Wales. Furthermore, the analysis of the semi-structured interviews brings to the foreground the challenges practitioners have with embedding AI within criminal investigations. Moreover, when police forces adopt AI in criminal investigations, an implementation challenge stems from an ethical dilemma, a skills gap, and a lack of government oversight. These findings highlight key challenges as a viable pathway to guide the development of policies promoting the responsible use of AI for criminal investigations.

As the research progresses, deeper insights and understanding of the challenges police professionals face in AI adoption will be gained. The number of interviews conducted at the time of writing this paper is three, and the findings are limited to these interviews. The next phase of this study is to collect additional data through more semi-structured interviews, and further in-depth analysis of current semi-structured interviews conducted at this time. The additional semi-structured interviews will contribute to how the challenges identified can be overcome and incorporated into policy decisions. We expect our work will ultimately contribute to the rapidly growing literature on using AI to support the enactment of inter-organisational processes.

References

Al-Garadi, M. A., Varathan, K. D., & Ravana, S. D. (2016). Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior,* 63, 433-443. https://doi.org/10.1016/j.chb.2016.05.051

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI, and Ethics*, 2(3), 377-387.

Batabyal, A. A., Kourtit, K., & Nijkamp, P. (2020). A political-economy analysis of the provision of urban anti-crime technologies in a model with three cities. *Technological Forecasting and Social Change*, 160, 120211. https://doi.org/10.1016/j.techfore.2020.120211

Babuta, A., & Oswald, M. (2020). *Data analytics and algorithms in policing in England and Wales: Towards a new policy framework*.

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research, 108,* 232-246. https://doi.org/10.1016/j.jbusres.2019.11.025

Balci, K., & Salah, A. A. (2015). Automatic analysis and identification of verbal aggression and abusive behaviors for online social games. *Computers in Human Behavior, 53*, 517–526. https://doi.org/10.1016/j.chb.2014.10.025

Beydoun, G., Abedin, B., Merigó, J. M., & Vera, M. (2019). Twenty Years of Information Systems Frontiers. *Information Systems Frontiers*, *21*(2), 485–494. https://doi.org/10.1007/s10796-019-09925-x

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2021). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. *Decision Support Systems*, 113651. https://doi.org/10.1016/j.dss.2021.113651

Braun, V., & Clarke, V. (2012). *Thematic analysis*, American Psychological Association, Handbook of Research Methods in Psychology: Vol. 2, Research Designs.

Bromberg, D. E., Charbonneau, É., & Smith, A. (2019). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly*, *37*(1), 101415. https://doi.org/10.1016/j.giq.2019.101415

Clarke, A., & Parsell, C. (2018). The potential for urban surveillance to help support people who are homeless: Evidence from Cairns, Australia. *Urban Studies, 56*(10), 1951–1967. https://doi.org/10.1177/0042098018789057

Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications*, *67*, 49–58. https://doi.org/10.1016/j.eswa.2016.09.029

Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems*, 113421. https://doi.org/10.1016/j.dss.2020.113421

Creswell, J. W. (2007). *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, Sage.

Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, *41*(10), 4915–4928. https://doi.org/10.1016/j.eswa.2014.02.026

Denzin, N. K., & Lincoln, Y. S. (2011). *The SAGE handbook of qualitative research* (4th ed.). Sage.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Duan, F. I. (2020). Governing Live Automated Facial Recognition Systems for Policing in England and Wales.

Ferreira, M. P., Santos, J. C., de Almeida, M. I. R., & Reis, N. R. (2014). Mergers & acquisitions research: A bibliometric study of top strategy and international business journals, 1980–2010. *Journal of Business Research*, *67*(12), 2550–2558. https://doi.org/10.1016/j.jbusres.2014.03.015

Fosso Wamba, S., & Queiroz, M. M. (2021). Responsible Artificial Intelligence as a Secret Ingredient for Digital Health: Bibliometric Analysis, Insights, and Research Directions. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10142-8

Fronzetti Colladon, A., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications*, *67*, 49–58. https://doi.org/10.1016/j.eswa.2016.09.029

Fussey, P., & Murray, D. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

Gerber, M. S. (2014). Predicting crime using Twitter and kernel density estimation. *Decision Support Systems*, *61*, 115–125. https://doi.org/10.1016/j.dss.2014.02.003

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, *41*(2), 497–523. https://doi.org/10.25300/misq/2017/41.2.08

Kim, J., Kang, S., & Lee, K. H. (2021). Evolution of digital marketing communication: Bibliometric analysis and network visualisation from key articles. *Journal of Business Research*, *130*, 552-563. https://doi.org/10.1016/j.jbusres.2019.09.043

Middleton, C. A., & Cukier, W. (2006). Is mobile email functional or dysfunctional? Two perspectives on mobile email usage. *European Journal of Information Systems*, *15*(3), 252–260. https://doi.org/10.1057/palgrave.ejis.3000614

Myers, M.D., & Avison, D.E. (2002*) Qualitative Research in Information Systems: A Reader (Introducing Qualitative Methods).* Sage Publications.

Noir, C., & Walsham, G. (2007). The great legitimiser: ICT as myth and ceremony in the Indian healthcare sector. *Information Technology & People, 20*(4), 313-333.

Rogers, E. M. (1962). *Diffusion of innovations*, New York: Free Press.

Saunders, M., Lewis, P. & Thornhill, A. (2019). *Research Methods for Business Students*, Harlow: Prentice Hall.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (7th ed.). Pearson Education Limited.

Sivatha Sindhu, S. S., Geetha, S., & Kannan, A. (2012). Decision tree based light weight intrusion detection using a wrapper approach. *Expert Systems with Applications*, *39*(1), 129–141. https://doi.org/10.1016/j.eswa.2011.06.013

Smadi, S., Aslam, N., & Zhang, L. (2018). Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. *Decision Support Systems*, *107*, 88–102. https://doi.org/10.1016/j.dss.2018.01.001

Stacey, P. K., & Tether, B. S. (2015). Designing emotion-centred Product Service Systems: The case of a cancer care facility. *Design Studies*, *40*, 85–118. https://doi.org/10.1016/j.destud.2015.06.001

Stieglitz, S., & Dang-Xuan, L. (2013). Emotions and Information Diffusion in Social Media—Sentiment of Microblogs and Sharing Behavior. *Journal of Management Information Systems*, *29*(4), 217–248. https://doi.org/10.2753/mis0742-1222290408

Sun, Y., Wu, Y., & Xu, Y. C. (2020). Using an ensemble LSTM model for financial statement fraud detection. *Pacific Asia Conference on Information Systems (PACIS).*

Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, *4*(2), 74–81. https://doi.org/10.1057/ejis.1995.9

Wang, L., Jia, M., Shi, Y., Chen, F., Ni, S., & Shen, S. (2020). A knowledge-based reasoning model for crime reconstruction and investigation. *Expert Systems with Applications*, *159, 113611.* https://doi.org/10.1016/j.eswa.2020.113611.

Wong, N., Ray, P., Stephens, G., & Lewis, L. (2012). Artificial immune systems for the detection of credit card fraud: an architecture, prototype, and preliminary results. *Information Systems Journal*, *22*(1), 53-76. https://doi.org/10.1111/j.1365-2575.2011.00369.x

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research*, *25*(2), 385–400. https://doi.org/10.1287/isre.2014.0522

Wu, Y., Xu, Y., & Li, J. (2019). Feature construction for fraudulent credit card cash-out detection. *Decision Support Systems*, *127*, 113155. https://doi.org/10.1016/j.dss.2019.113155

van Eck, N. J., & Waltman, L. (2023). VOSviewer Manual. https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.10.pdf

Yokotani, K., & Takano, M. (2021). Social Contagion of Cyberbullying via Online Perpetrator and Victim Networks. *Computers in Human Behavior*, 106719. https://doi.org/10.1016/j.chb.2021.106719

Zhong, W., & Gu, F. (2019). A multi-level deep learning system for malware detection. *Expert Systems with Applications*, *133*, 151–162. https://doi.org/10.1016/j.eswa.2019.04.064

Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organisation. *Organisational Research Methods*, *18*(3), 429-472.