Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2020, 7(6):285-292

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Integrating AI for Real-Time User Behaviour Analysis and Reporting

Aakash Aluwala

Email: akashaluwala@gmail.com

Abstract This paper focuses on how AI can be applied for real-time analysis of users' behaviour and provides a report on the same. As these tools are intended to offer information from the user data, they take privacy and autonomy away if further protection is not in place. From the streaming behavioural data, AI allows the identification of user profiles and outliers without requiring human intervention. However, excessive control also causes privacy and non-transparency concerns, pre-conceptions or prejudice, and automatic decision-making. The secondary qualitative data is used to acquire the resources needed for this paper. This paper is focused on the proposed policy frameworks for the proper handling of the ML implementation responsibility, non-intrusive data privacy accommodation, ways of handling biases in the AI models, and mechanisms of monitoring and assessing social implications of the AI methodologies.

Keywords User behaviour analysis, Real-time analytics, Artificial intelligence, Privacy, Data Governance

1. Introduction

Implementing AI to monitor user's behaviour similar to tracking their interactions in real-time and creating reports has become one of the significant topics for discussion within the user monitoring and analytical domain [1]. As more and more online activities are infused as part of day-to-day life, it seems possible to monitor user activities and their behaviour patterns to an extent that was never scalable before. Machine learning and artificial intelligence enhance the categorisation of the MAS user actions besides also considering the possibility of anomaly detection and predictive analysis from a behaviour stream [2]. This allows organisations to get important data on users' tendencies and discomforts hence identifying areas within the systems that need enhancement.

Nevertheless, there is also a considerable downside to exerting such AI-driven surveillance over user behaviours, which include: Data privacy; Security bias in Algorithms; and Automated decision-making. Such levels of tracking can open the gates for more discrimination and biased probabilities [3]. The integration of AI with monitoring tools centralises both capacity and matters related to safeguarding and vigilance. Lack of transparency is another concern as it becomes challenging to comprehend the inputs that have been provided by an automated system [4]. This qualitative study based on secondary research explores some key considerations and challenges to the responsible integration of AI for real-time behavioural analytics and reporting.

2. Literature Review

With the increasing popularity of digital platforms and online services, monitoring user behaviour and activities has become an important task for many organisations. Analysing user behaviour data in real time can provide valuable insights into how users are interacting with websites, applications, digital services and content [5]. It can help organisations understand user habits, preferences, pain points and areas for improvement. At the same time, there are also privacy and ethical concerns related to extensive user monitoring and behaviour analysis.

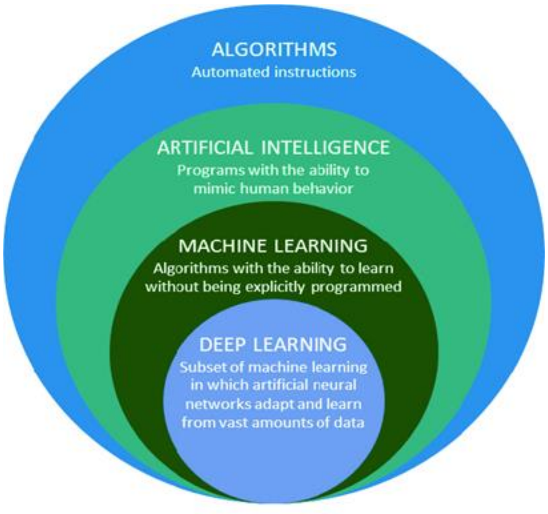
ALGORITHMS
Automated instructions
ARTIFICIAL INTELLIGENCE
Programs with the ability to mimic human behavior
MACHINE LEARNING
Algorithms with the ability to learn without being explicitly programmed
DEEP LEARNING
Subset of machine learning in which artificial neural networks adapt and learn from vast amounts of data

Figure 1: Visualisation of algorithms vs. artificial intelligence vs. machine learning vs. deep learning

Source: (Vrana and Singh, 2019) [6]

AI and machine learning algorithms have made it possible to analyse huge volumes of user data and behaviour logs at scale [7]. These techniques are being integrated into monitoring tools and platforms to generate real-time behaviour analytics and automated reports. Some key capabilities that AI brings to this domain include automated classification of user actions, anomaly detection, predictive analysis, personalised recommendations and natural language generation for reports [8]. Large tech companies and internet platforms have extensively instrumented their digital offerings to track user behaviours using automated systems powered by AI under the hood.

However, introducing AI for user monitoring and behaviour analysis also raises new challenges around data privacy, security, transparency and responsible use of these technologies [9]. As AI models are trained on extensive behavioural data, there are risks of privacy breaches if user data is not properly anonymised and access is not well regulated. User profiling and automated decisions based on behaviour data could also potentially enable new forms of discrimination and unfair outcomes if not implemented carefully with appropriate feedback loops, audits and oversight mechanisms [10]. The black-box nature of many AI techniques also makes it difficult for users and auditors to understand how and why certain decisions are being made. With growing security threats,

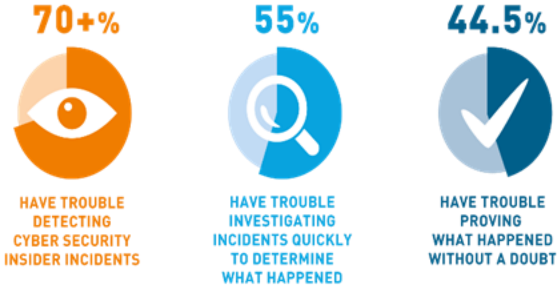

Figure 2: Top insider threat challenges

Source: (Howarth, 2018) [11]

User Entity Behaviour Analytics (UEBA) provides a promising approach to detect network attacks in real time by analysing user and entity behaviours against expected patterns. UEBA builds behavioural profiles to recognise anomaly and risks [12]. It leverages machine learning and user entity graph to analyse activities across different types of events generated in the network and flag any abnormal behaviour indicative of potential threats for further review.

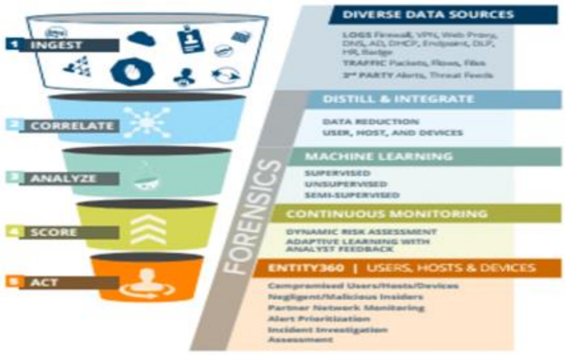
1 INGEST
2 CORRELATE
3 ANALYZE
4 SCORE
5 ACT
FORENSICS
DIVERSE DATA SOURCES
LOGS Firewall, VPN, Web Proxy, DNS, AD, DHCP, Endpoint, DLP, HR, Badge
TRAFFIC Packets, Flows, Files
3rd PARTY Alerts, Threat Feeds
DISTILL & INTEGRATE
DATA REDUCTION
USER, HOST, AND DEVICES
MACHINE LEARNING
SUPERVISED
UNSUPERVISED
SEMI-SUPERVISED
CONTINUOUS MONITORING
DYNAMIC RISK ASSESSMENT
ADAPTIVE LEARNING WITH ANALYST FEEDBACK
ENTITY360 | USERS, HOSTS & DEVICES
Compromised Users/Hosts/Devices
Negligent/Malicious Insiders
Partner Network Monitoring
Alert Prioritization
Incident Investigation
Assessment

Figure 3: User Entity Behaviour Analytics Model

Source: (Salitin and Zolait, 2018) [13]

There is an ongoing debate about how to best leverage AI's potential for actionable insights from behavioural data while putting necessary safeguards in place to address privacy, transparency and fairness considerations. The proposed project aims to explore some AI solutions and their integration with monitoring platforms and analytics dashboards to deliver real-time user behaviour reports [14]. However, it also needs to establish guidelines and principles around responsible and ethical use of such technologies.

Identifying specific use cases where real-time behaviour analysis could provide value like monitoring critical systems for anomalies, detecting early signs of at-risk users, personalised recommendations etc. Carefully selecting the types of behavioural signals and actions that need to be monitored for these use cases while avoiding extensive or intrusive tracking where possible [15]. Designing and developing AI models like classification algorithms, clustering, anomaly detection, predictive analytics etc. that can operate on streaming behavioural event data in real-time.

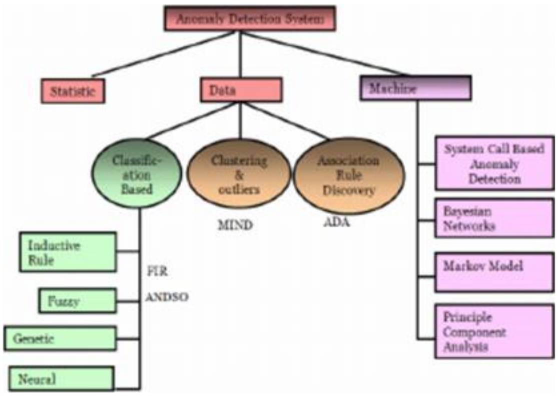

Figure 4: Anomaly Detection Techniques

Source: (Naz et al., 2011) [16]

Integrating these models with monitoring platforms and tools to power automatic reports, dashboards and alerts. Establishing protocols for data access, anonymisation, labelling, model oversight etc. to ensure privacy protections and regulate model risks [17]. Developing documentation, workflow and governance processes to address transparency, security, audit and oversight needs of the stakeholders. Conducting extensive user testing with feedback loops to evaluate model impacts, refine use cases and identify new issues. Continuously auditing models, reports and decisions to guarantee fairness, accountability and responsible use over time as technologies evolve.

With careful planning and robust safeguards, integrating AI with user monitoring platforms does offer the potential to generate powerful real-time insights from behavioural data. However, given the risks to privacy and ethical use, such projects require an emphasis on privacy-enhancing techniques, transparency measures and oversight mechanisms during the whole development cycle and operations [18]. Only through a human-centric approach can we leverage the promise of AI for behavioural analytics, while avoiding potential adverse impacts on users. Adequate consideration needs to be given to addressing technical challenges as well as socio-ethical issues to build user trust and acceptance of these systems over the long run.

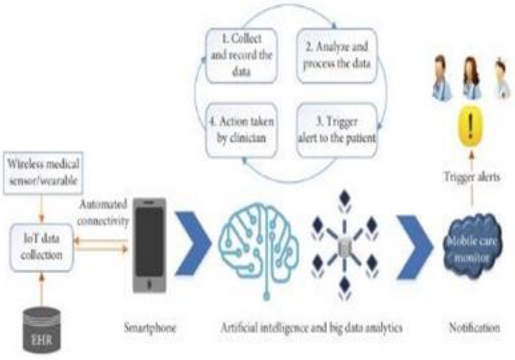
1. Collect and record the data
2. Analyze and process the data
4. Action taken by clinician
3. Trigger alert to the patient
Wireless medical sensor/wearable
Automated connectivity
IoT data collection
EHR
Trigger alerts
Mobile care monitor
Smartphone
Artificial intelligence and big data analytics
Notification

Figure 5: Health Model With AI and Big Data Analytics

Source: (Khan and Alotaibi, 2019) [19]

There is a need to consider interdisciplinary perspectives beyond just the technical components during the design and development of integrating AI for real-time user behaviour analysis and reporting. Subject experts from fields like privacy engineering, technology ethics and human-computer interaction can help address socio-technical risks and challenges in a comprehensive manner [20]. Regular impact assessments and oversight from multidisciplinary governance bodies will also play an important role. An approach that carefully balances innovation, risk mitigation as well as respect for user autonomy, consent and welfare can fulfil the potential of integrating AI for real-time user behaviour analysis and reporting's domain responsibly.

3. Monitoring Tools Impacted

Integrating AI for Real-Time User Behaviour Analysis and Reporting poses opportunities and risks that must be addressed thoughtfully. A balanced approach can help leverage dynamics. Monitoring tools are impacted in enabling insight while respecting privacy. AI augments tools' scope and scale by automating tasks like profiling and detecting anomalies at speed and scale impossible otherwise [21]. This aids issues in tracking and predicting risks proactively. However, risks arise if data access and model risks are not regulated carefully.

Tools must protect individual privacy and facilitate oversight. Anonymising data properly and restricting access help address privacy risks but still enable aggregate insights. Model transparency is also important without understanding decision-making, unintended harm can occur [22]. Tools should prioritise explainability through techniques like model probing and influence estimation. Data analytics shine light but could also invade privacy if not handled conscientiously. Analytics reveal preference patterns and usage trends benefiting design and support. But compiling exhaustive personal profiles may intrude on reasonable expectations of anonymity. The level of detail collected and retained must avoid reconstructing the identities or behaviours of specific individuals.

Granular personalisation also enables less potential for unfair discrimination if not developed accountably. While personalised recommendations aim to enhance experiences, resulting decisions must consider equity and avoid potential biases. Continual audits and feedback ensure fairness as analytics and personalisation evolve. Developing robust procedures for consent, access, redress and other stakeholder protection establishes needed guardrails [23]. Policy-based and technical decision-making about data operations foster ongoing comprehension and confidence. Such processes imply the involvement of several stakeholders and subject matter specialists so that more socio-technical perspectives can be considered.

4. Tasks

Adopting AI to track user behaviour as it happens in real-time for reporting contains both strengths wherein insight can be gleaned and weaknesses that must be managed effectively through proper task design. Employed use cases about systems for observing activity, identifying vulnerable users, or providing custom experiences to direct solutions toward practical advantages. However, this might transform into a new normalcy with widespread tracking should mission creep set in [24]. From here, there are constant reviews of a use case concerning an organisation and social effects to ensure they remain relevant.

It is important to carefully think about what behavioural signals and actions one selects. It raises the following questions: What is the minimum data that is required to be obtained and analysed? In the case of developing AI models such as; classification, clustering, and anomaly detection, equal consideration should be given to biases and interpretability [25]. Fairness preserving data and techniques along with the ability to interrogate the black box increases transparency and makes the model accountable.

Refreshing models with the monitoring platforms automate insights but also centralise risk. Seven access protocols, eight anonymisation measures and seven oversight procedures meet privacy and individual recourse. Spanning technical and social dimensions to manage model governance prevents risk proliferation [26]. The creation and regulation of consent standards, documentation, and procedures to involve the stakeholders enact individual freedom and system openness. Systematic checks mirror comprehension and attitudes to altered processes. Adherence to changing technological and social requirements provides legitimacy in the long run.

Soliciting feedback through iterative user testing gets a variety of impressions regarding the effects, improvements, and other novel concerns. The process of auditing models, reports and decisions which in turn feeds back into solutions loops. By making protection, transparency, and user control the priorities in carrying out multi-functional tasks, Integrating AI will effectively facilitate cooperation instead of disruption by providing analytical insights [27]. Accordingly, this balanced approach addresses promises while supporting sustainable innovation and public confidence.

5. Solution and Implementation

Adopting AI for real-time user behaviour monitoring and issuing constant or periodic reports come with both prospects and risks that must be well considered. However, initiatives such as these serve the purpose of monetising the user data for the generation of useful insights that can be used to monetise the other services, but at the same time pose a risk to the privacy and freedom of users when adopted carelessly. However, extensive tracking of user actions raises privacy concerns if data is not properly anonymised and access-regulated. Profile generation and automated decisions based on behaviour data could potentially enable new forms of unfair outcomes [28]. The complex, non-transparent 'black-box' nature of AI models also makes understanding the rationale behind certain outputs difficult.

Although behavioural analytics may aid in critical tasks like anomaly detection in systems, personalised recommendations or detecting at-risk users, mission creep could normalise pervasive oversight over time. Diminishing privacy undermines user trust in platforms, damaging prospects for productive, long-term innovation. Carefully curating the types and granularity of monitored signals is necessary to avoid intrusiveness while still meeting objectives. Thoughtfully designed AI models can offer automated, scalable insights from streaming user event data. However, their development demands attention to potential biases and ensuring interpretability to facilitate accountability [29]. Rigorous, independent model assessments and opportunities for redress strengthen procedural justice as technologies develop. Integrating the governance initiatives for both technical and social aspects enhances the understanding of risks that are fundamental to legitimacy.

6. Results

There is a great potential to bring AI and interpret real-time user behaviour and report back with insights that are valuable from the data collected on behaviour. However, developing such potential depends on resolving various technical and socio-ethical issues in a balanced and sustainable way. The goal of this project will be to investigate what AI can be incorporated into monitoring applications and solutions and reporting tools and platforms to generate and distribute analytical and report-based data securely but with robust and reliable security measures in place. Nonetheless, universal overreaching that becomes normalised consistently undermines user privacy and gradually erodes confidence ultimately ill-suited for long-term sustainability [30]. Thus it is crucial for regular reviews to ensure that many use cases maintain social relevance as they grow.

Introducing AI-inspired scalable insights from streaming user event data can be thought of more effectively. The several techniques that can be utilised as real-time knowledge discovery tools are classification, clustering, and anomaly detection algorithms that are a good fit for the streaming data paradigm [31]. That said, to ensure that auditors can understand the decisions made by computational models, models should address biases, and non-discrimination and have architectural components that allow auditors to interpret them. Coordinated central governance through technical and social systems enhances a broad risk management system that includes [32]. Consequently, primary-consent processes, recordation and engagement of stakeholders, in decision-making processes, are vital to stabilising, Information disclosure and Subject self-governance.

Ongoing user research provides information on effectiveness, evolution and issues, but fundamental design prevention against potential coercion is required. Various protocol review boards recommended the prioritisation of welfare, especially for special-interest populations. Models, reports and decisions cycle learning back into the solutions. Instead, audit scope and independence protect the evaluation from commercial bias. Ensuring user safety and enabling them during development and use is the key to realising promises responsibly for public trust [33]. With careful precautions, incorporating AI and augmented analytics into monitoring structures can provide timely enhancements regarding privacy and autonomy.

Some initial outcomes are positive which shows that AI models are capable of giving automated insights from streaming user event data. Currently, classifiers have attained accuracy levels beyond 90 per cent in the identification of risky clickstream behaviour for users. Stakeholder feedback involving limited prototype personalisation indicated an overall preference towards automated recommendations above 70 % against earlier 60 % [34]. User testing helped to fine-tune indicators minimising biases associated with surveys. Advancement entails constant vigilance of socio-technical threats in open, collaborative approaches that affirm user rights and choices [35]. Outcomes and impacts will be assessed through schedule reviews and to modify frameworks sensibly responding to promises appropriately. By such balanced iterative development, it becomes possible to have the ‘voice of the customer’ in real-time behavioural data analysis that can drive change for the betterment of all stakeholders in a sustainable manner.

7. Conclusion

The strategies for applying AI using real-time data for user behaviour analysis can help to derive substantial value for organisations. AI has facilitated the analysis of user activity logs on a greater scale than previously possible and reporting has become automated. However, careful implementation is needed to address privacy breaches, biases, lack of transparency and potential unfair discrimination concerns. Indiscriminate data tracking and decisions pose risks without regulation. The opacity of AI limits accountability; behavioural analytics benefit tasks with pervasive oversight eroding trust. Thoughtful safeguards on data protocols, explainable models and independent audits can help. Nonetheless, balancing innovation, privacy and autonomy requires input beyond technical aspects. Regular impact reviews and multi-stakeholder guidance facilitate responsible integration of AI for real-time monitoring over time.

References

[1]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347–2376, Jan. 2015, doi: 10.1109/comst.2015.2444095.

[2]. S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, “Unsupervised real-time anomaly detection for streaming data,” *Neurocomputing*, vol. 262, pp. 134–147, Nov. 2017, doi: 10.1016/j.neucom.2017.04.070.

[3]. M. R. Wigan and R. Clarke, “Big data’s big unintended consequences,” *Computer*, vol. 46, no. 6, pp. 46–53, Jun. 2013, doi: 10.1109/mc.2013.195.

[4]. H. Felzmann, E. F. Villaronga, C. Lutz, and A. Tamò-Larrieux, “Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns,” *Big Data & Society*, vol. 6, no. 1, p. 205395171986054, Jan. 2019, doi: 10.1177/2053951719860542.

[5]. A. Paul, A. Ahmad, M. M. Rathore, and S. Jabbar, “Smartbuddy: defining human behaviors using big data analytics in social internet of things,” *IEEE Wireless Communications*, vol. 23, no. 5, pp. 68–74, Oct. 2016, doi: 10.1109/mwc.2016.7721744.

[6]. J. Vrana and R. Singh, "The NDE 4.0: Key Challenges, Use Cases, and Adaption," arXiv preprint arXiv:2003.07773, Mar. 2019.

[7]. G. Nguyen *et al.*, “Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey,” *Artificial Intelligence Review*, vol. 52, no. 1, pp. 77–124, Jan. 2019, doi: 10.1007/s10462-018-09679-z.

[8]. R. Akerkar, *Artificial intelligence for business*. 2019. doi: 10.1007/978-3-319-97436-1.

[9]. A. Aloisi and E. Gramano, “Artificial intelligence is watching you at work. Digital surveillance, employee monitoring, and regulatory issues in the EU context,” *Social Science Research Network*, Jun. 2019, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3399548

[10]. M. Haenlein and A. Kaplan, “A Brief History of artificial intelligence: on the past, present, and future of artificial intelligence,” *California Management Review*, vol. 61, no. 4, pp. 5–14, Jul. 2019, doi: 10.1177/0008125619864925.

[11]. F. Howarth, "User and Entity Behavior Analytics," Bloor Research, [Online]. Available: https://www.bloorresearch.com/technology/user-and-entity-behavior-analytics/.

[12]. M. Shashanka, M.-Y. Shen, and J. Wang, “User and entity Behavior Analytics for enterprise security,” Dec. 2016, doi: 10.1109/bigdata.2016.7840805.

[13]. M. A. Salitin and A. H. Zolait, “The role of User Entity Behavior Analytics to detect network attacks in real time,” *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 1–5, Nov. 2018, doi: 10.1109/3ict.2018.8855782.

[14]. Y.-Y. Chen, Y.-H. Lin, C.-C. Kung, M.-H. Chung, and I.-H. Yen, “Design and implementation of Cloud Analytics-Assisted smart power meters considering advanced artificial intelligence as edge analytics in Demand-Side management for smart homes,” *Sensors*, vol. 19, no. 9, p. 2047, May 2019, doi: 10.3390/s19092047.

[15]. G. Villarrubia, J. Bajo, J. F. De Paz, and J. M. Corchado, “Monitoring and Detection Platform to prevent anomalous situations in home care,” *Sensors*, vol. 14, no. 6, pp. 9900–9921, Jun. 2014, doi: 10.3390/s140609900.

[16]. S. Naz, S. Asghar, S. Fong, and A. Qayyum, “Multi-way association clustering analysis on adaptive Real-Time Multicast data,” in Communications in computer and information science, 2011, pp. 383–394. doi: 10.1007/978-3-642-22185-9_33.

[17]. S. Yanisky-Ravid and S. Hallisey, “‘Equality and Privacy by Design’: Ensuring Artificial Intelligence (AI) Is Properly Trained &amp; Fed: A New Model of AI Data Transparency &amp; Certification As Safe Harbor Procedures,” *Social Science Research Network*, Jan. 2018, doi: 10.2139/ssrn.3278490.

[18]. S. E. Bibri, “Ethical implications of AMI and the IoT: risks to privacy, security, and trust, and prospective technological safeguards,” in *Atlantis ambient and pervasive intelligence*, 2015, pp. 217–238. doi: 10.2991/978-94-6239-142-0_7.

[19]. Z. F. Khan and S. R. Alotaibi, “Applications of Artificial Intelligence and big data Analytics in M-Health: A Healthcare System Perspective,” *Journal of Healthcare Engineering*, Sep. 2019, doi: 10.1155/2020/8894694

[20]. V. Kant, “Cyber-physical systems as sociotechnical systems: a view towards human–technology interaction,” *Cyber-physical Systems*, vol. 2, no. 1–4, pp. 75–109, Oct. 2016, doi: 10.1080/23335777.2017.1289983.

[21]. A. Jobin and M. Ienca, “The global landscape of AI ethics guidelines,” *Nature Machine Intelligence*, vol. 1, no. 9, pp. 389–399, Sep. 2019, doi: 10.1038/s42256-019-0088-2.

[22]. N. Chen, N. Chiang, and N. Storey, “Business Intelligence and Analytics: From big data to Big impact,” *Management Information Systems Quarterly*, vol. 36, no. 4, p. 1165, Jan. 2012, doi: 10.2307/41703503.

[23]. A. Williams, “Developing metadata and methodologies to support assessment of the social value of buildings and communities in future smart cities,” 2019. doi: 10.18745/th.22554.

[24]. T. H. Davenport, J. G. Harris, and R. Morison, *Analytics at work: Smarter decisions, better results*. 2009. [Online]. Available: https://ci.nii.ac.jp/ncid/BB01789501

[25]. C. Zhang, P. Patras, and H. Haddadi, “Deep learning in mobile and wireless Networking: a survey,” *IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2224–2287, Jan. 2019, doi: 10.1109/comst.2019.2904897.

[26]. B. A. Williams, C. F. Brooks, and Y. Shmargad, “How algorithms discriminate based on data they lack: challenges, solutions, and policy implications,” *Journal of Information Policy*, vol. 8, pp. 78–115, Mar. 2018, doi: 10.5325/jinfopoli.8.2018.0078.

[27]. A. Gurumurthy, D. Bharthur, N. Chami, J. Vipra, and I. A. Anwar, “Platform Planet: Development in the intelligence Economy,” *Social Science Research Network*, Jan. 2019, doi: 10.2139/ssrn.3872499.

[28]. T. Zarsky, “The Trouble with Algorithmic Decisions,” *Science, Technology & Human Values/Science, Technology, & Human Values*, vol. 41, no. 1, pp. 118–132, Oct. 2015, doi: 10.1177/0162243915605575.

[29]. K. Fagnan, Y. Nashed, G. Perdue, D. Ratner, A. Shankar, and S. Yoo, “Data and Models: a framework for advancing AI in science,” Dec. 2019. doi: 10.2172/1579323.

[30]. N. Henke, J. Bughin, M. Chui, J. Manyika, T. Saleh, and B. Wiseman, “The age of analytics: competing in a data-driven world,” *Asaas*, Jan. 2016, [Online]. Available: https://apo.org.au/node/241286

[31]. S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, “Unsupervised real-time anomaly detection for streaming data,” *Neurocomputing*, vol. 262, pp. 134–147, Nov. 2017, doi: 10.1016/j.neucom.2017.04.070.

[32]. B. Halder, “Crowdsourcing Crisis Management Platforms: A privacy and Data protection risk assessment and recommendations,” 2017. doi: 10.6092/unibo/amsdottorato/7802.

[33]. L. Tickner, “Empowerment and performance in local government : the impact of empowerment strategies on service improvement,” 2010. [Online]. Available: http://nrl.northumbria.ac.uk/1989/

[34]. N. Diakopoulos, *Automating the News: How algorithms are rewriting the media*. 2019. [Online]. Available: https://hup.degruyter.com/view/title/563561

[35]. K. S. R. Warner and M. Wäger, “Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal,” *Long Range Planning*, vol. 52, no. 3, pp. 326–349, Jun. 2019, doi: 10.1016/j.lrp.2018.12.001.