Al-Zaytoonah Journal of Business, Vol. 01 No. 03, November 2025

Challenges and Opportunities for Artificial Intelligence in Auditing

Bob Castaneda[1], John Palmer[2]
[1,2] Walden University, University of Missouri, St. Louis Castaneda@waldenu.edu, JohnPalmr@umsl.edu

Abstract Artificial Intelligence (AI) is rapidly transforming industries, and auditing is no exception. As AI technologies evolve, they offer unprecedented opportunities to enhance audit quality, efficiency, and effectiveness. AI can automate complex and repetitive audit tasks, analyze large volumes of financial data in real-time, and detect anomalies or fraud patterns that may elude traditional methods. However, this integration also presents significant challenges, including concerns about data privacy, algorithmic bias, lack of transparency, and ethical accountability. The complexity and opacity of AI systems may reduce auditors' ability to interpret outcomes or explain decision-making processes, potentially undermining trust. Moreover, regulatory uncertainties and the fast-paced development of AI tools necessitate a rethinking of audit standards and professional responsibilities. This paper explores the dual landscape of AI in auditing—its transformative potential and the pressing concerns that must be addressed to ensure its responsible and effective implementation.

Keywords: Artificial Intelligence, Auditing, Audit Automation, AI Challenges, AI Opportunities, Explainability, Algorithmic Bias, Audit Efficiency, Ethical AI, Trust in AI Systems

1 Introduction

Artificial Intelligence (AI) is undoubtedly one of the biggest driving forces behind the next technological revolution. AI is already interacting with its users in many applications, from daily tasks like using Google Maps and language translations to serious applications in healthcare, finance, and law as well as threatening applications like hacking, producing fake news, and generating hate speeches. All such tasks can be performed more or less automatically (Belle, 2019). Advancements in AI are widely anticipated to deeply and irreversibly affect business and economic models, economic productivity, wealth distribution, and even humanity itself. This leads to grand overhyped predictions and anxieties. At the same time, an explosion of research into what constitutes responsible or interpretable AI (from understandability to explain ability) is observed. An ethical debate, partly driven by the potential social consequences of AI technology, is ongoing. Governments, NGOs, and big tech companies are working to devise regulations to avoid catastrophes.

The field of AI goes hand in hand with the research on its understanding, interpretation, explainability, trustworthiness, acceptability, and accountability. An explanation refers to what information should be given to the human user for him or her to trust the AI system. An explanation could exhibit all kinds of reasons as to why something happened, why something was predicted, and why something was concluded. This could be a single number, a chart, a picture, a structured report, a natural language explanation, and so on, either directly or indirectly related to the data. The recent advancement of big data, internet of things, and cheap storage has allowed the accumulation of massive data, together with the rapid advancement of computing power and algorithms, has led to AI systems that could discover patterns and structures in these massive data in an automated manner. Highly sophisticated AI systems are now adopted across a wide spectrum of applications. One such application domain is auditing.

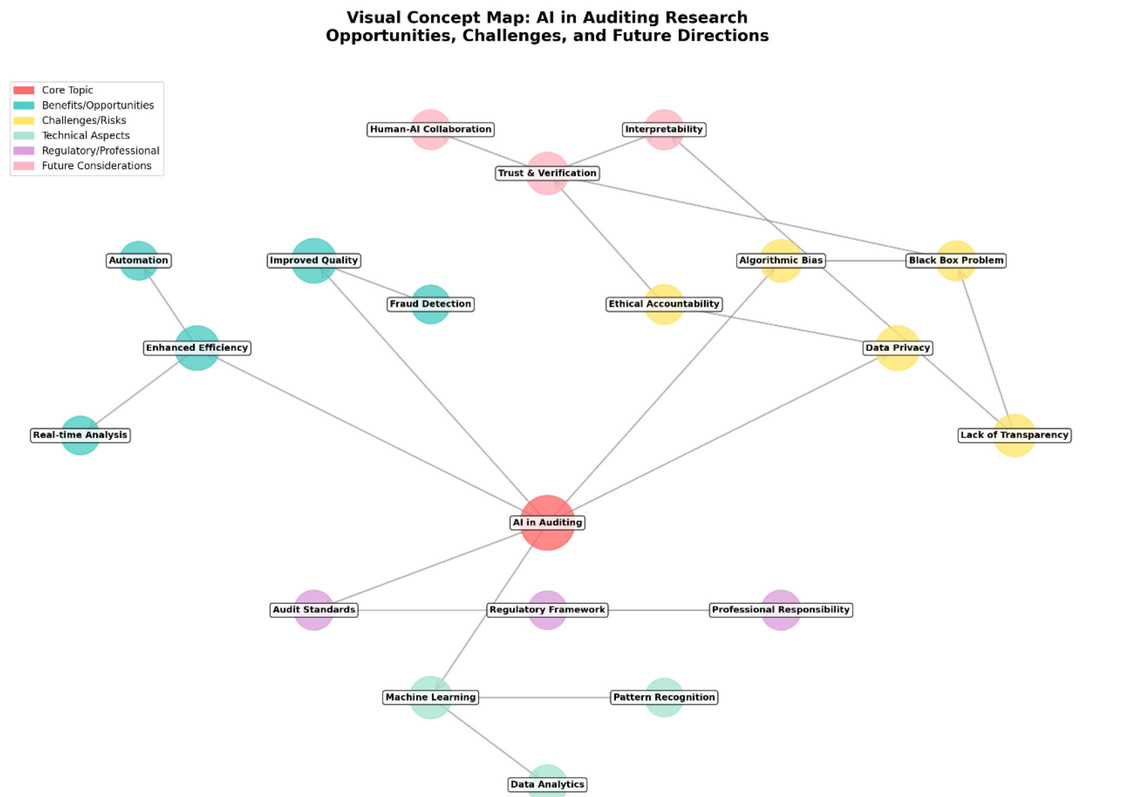
Business organizations are very much interested in the interaction with AI systems in the audit domain. AI systems could improve audit efficiency by multitasking many audit subtasks and processing huge volume of data simultaneously, and improve audit effectiveness by better and more comprehensive detection of errors and fraud. On the other hand, large-scale AI systems may introduce new challenges for audit as the sheer scale and complexity may render the systems unmanageable. Lack of understanding and interpretability, coupled with biased training data and rogue algorithms and systems, may lead to biased and unfair outcomes, raising concerns for fairness, accountability, and compliance with regulations (Lal Joshi & Marthandan, 2019).

2 Overview of Artificial Intelligence in Auditing

Technology is evolving rapidly and playing a crucial role in almost every area of business and life. One of the most popular technologies is Artificial Intelligence (AI), which refers to any device that is powered by a computer that is being controlled by software, simulating human thoughts or behaviors. Mobile phones, intelligent cameras, robots, and drones are just a few examples of AI-based devices. It's hardly conceivable that private and public life can exist without AI (Belle, 2019). AI has already transformed personal lives: just think about automatic spelling corrections, navigation apps, stock prediction programs, or predefined computer-generated recommendations. The application of AI to discover patterns or structures in large troves of data in an automated manner is a core component of the now-omnipresent and widely used data science tools.

An overwhelming share of familiar applications derives from data science techniques and mass data availability: these techniques, examining and predicting intimate feelings and behavior of millions of permanent and temporary users can be found in financial predictions, marriage-matching systems, search engines, social networks, tv-series suggestions, blog applications, police surveillance, and even voting forecasts (Lal Joshi & Marthandan, 2019). However, the unique potential of machines working potentially better than humans is coupled with risks and challenges. The unprecedented intelligence and speed of the machines surrounding humanity can make undesired decisions, being it visible as one-sided honey traps or just unnoticed threats stemming from privacy violations. Exploiting personal but sensitive data for discrimination is another issue.

The waxing influence of AI experts can be abused, who can produce the necessary datasets or exploit the software coded functioning in complicated wise. Finally, successful machines can make any decisions but most of the time, humans are unable or at least not straightforward to understand and verify machine decisions. Hence, to avoid dropping faith in technology, the responsibility and meaningful verifiability of machine decisions should become a civic right just as the right for privacy. Unfortunately, there is currently a lack of efficient, transparent, or at least interpretable white box candidate systems. To ensure transparent and responsible robustness of AI-based systems, understanding black boxes is essential.



3 Historical Context of Auditing Practices

Auditing is the practice of examining the corporate records of a company and serving as a reminder of the limits of management. Auditing focuses on economically important information and is practiced in the private sector for regulatory as well as quality assurance concerns (Manheim et al., 2024). Financial auditing is the best-established form of auditing. It began in Italy in the 15th century with emphasis on inventory security; once companies grew larger, the need for independent auditors grew, leading to the establishment of the profession in Great Britain in the 19th century. Efforts to standardize practices began in the early 20th century. Auditing practices, technology, and regulation were adapted to grapple with problems raised by the growing digitization of data, and issues of systemic risk and public trust remain unresolved. Software auditing has taken place under the rubric of virus scanning, vulnerability assessments, and source code reviews. New processes for documenting requirements and generating software artifacts that are not seen prior to deployment are problematic. The lack of structure makes it difficult to notice problems and remember what decisions were made. Similarly, automated processes can use data in unexpected ways that are difficult and time-consuming to track. With massive amounts of data scrapped, it is essential to better manage safeguards and expectations for accounting and data retention. Data is often considered disposable, and concerns about collection purposes and lengths of retention are often not explicitly considered. Those charged with governance often lack sophistication in how models, data, and dependencies interact in practice, leading to chaos and inconsistent consideration. Furthermore, reliance on one vendor creates rigidity in processes and awareness of systems. There is also a massive disparity between AI developers invested in using the technology and governments, regulators, and the public tasked with understanding it.

4 Current Trends in Artificial Intelligence

Developments in AI come from research programs that seek to reproduce particular cognitive processes deemed intelligent, with the most successful working with the neural networks that are loosely inspired by the brain. From a complex thrash of connections, hierarchies form, which can recognize higher order composites. These trains of processing can be parallel, and they undertake computing in a radically different way to human minds. The trained networks are capable of making predictions, ranking images that contain desired attributes, and undertaking complex tasks SKU search, detecting fraud, or even writing music. AI systems are far beyond the ability of the developers to explain the processes that led to a given result. They are more approaches than systems, but as such can be combined. For example, some type of NLP models take a second, more extensible, form that generates explanation candidates. These candidates can then be filtered further, using other ML techniques (Belle, 2019).

Machine Learning and AI currently work best in contexts that are well defined and limited. These ranges afford supervision, allowing for the development of good models using large troves of labelled data. Successful systems also require the task to be well established, clearly articulated, and agreed upon. None of these systems are intelligent in the ways in which human intelligence would normally be defined and understood. CNNs have no notion of concepts such as ‘car’ or ‘spaceship’ they simply process pixel data and produce a value that is later interpreted. Once the DSL and the model are in place, there is little that a human operator can do other than indicative testing and evaluation of new input data (Tredinnick, 2016).

5 Key Technologies in AI for Auditing

Machine learning interpretable models such as Generalized Additive Models, Generalized Additive Mixed Models, LIME, SHAP, Bayesian Rule Lists, and Anchors will rise in popularity as users demand an explanation of predictions to building trust in the AI model and its building blocks. This explanation sufficiency leads to further investigation into ulterior motives by users. Knowing that AI systems reveal patterns and structures from the data, an on-going battle attempts to interpret the resulting analysis. Current efforts focus on providing credence or explainability in retrospect to the AI inputs. This leads to the desire for interpretability by transparency, where one seeks the comprehension of the decision process of DL models via the AI outputs (Belle, 2019). Current discover and predict ML-covered patterns in the data are oblivious to the users unless the model or its predictions are adapted to provide explanations. Helping users comprehend why an explanation is deemed appropriate, tradeoffs between action and destruction of a lack of explanation poison further action framed by an explanation.

Important, the key regulators emphasize the deep-rooted desire for explainable designs. Consequently, the ongoing EU AI Act implies a need for compliance with discovery by design. Tradeoffs with trust, a large portion of implementations become unregulated black boxes. Independent research could encompass the broader situation faced when expected to rationally consider AI-based expert guidance. Incorporation of introduction uncertainty under equivocality in controlled socio-technology experimentation could study whether algorithmically induced radical pro-predictions sufficed as a sufficient change to defeat somewhat informed majority blocks. Additional research could gainsay this question by studying how to combat it (C. Oldhouser, 2016).

5.1. Machine Learning

Machine learning is regarded as one of the important aspects of AI. It is implemented as systems that automatically learn from experience X and improve on their own. In general, machine learning systems realize the problem involving X in one of the three following frameworks: Supervised, Unsupervised, and Reinforcement learning (Belle, 2019). It is a setup that has both a learning algorithm and a teacher. The teacher provides an example with a correct answer and the machine learns the relationship between the input and the output. The learning process continues with a new example that it has never seen before. Every time the machine makes a mistake, the teacher corrects it. Through experience X, the tasks with the training set T are done better by these methods (Shook et al., 2018).

The task to be learned T is normally specified in an indirect way. This is a kind of game played with an environment E, which provides a piece of information about the state S and an act A directly affecting S. The detailing action generates a reinforcement value R, which is a reward if positive and a punishment if negative. A reinforcement learning algorithm aims at acquiring a good policy (A|S) mapping the state S into the act A. Since it sets the reinforcement value R as a consequence of a chosen act A, the learning algorithm does not require a teacher. It can make use of its own experience to improve its performance. RL problems have usually been formalized as a temporal discounting stochastic dynamic programming problem. In general it contains a set of possible states and actions resulting in both a new state and a reinforcement value.

On the other hand, the approach does not uniquely solve all the issues. Because of this circumstance, the model selection is part of the learning. Two types of machines are pointed out. The market selection machines will control a large variety of either very general machines or very specialized machines. By executing a random selection scheme or trial-and-error exercise the user tends to find a machine best suited to the problem at hand, also for dynamic problems. The auction selection machines will provide a number of alternative solution schemes that are mathematically closely related to the mathematical model adopted.

.5.2. Robotic Process Automation

Robotic Process Automation (RPA) refers to a set of tools for automating the execution of routine activities that are carried out manually by users in systems, on which they act as "software robots" (Gajjar et al., 2022). RPA lies between screen-scraping, which is the pure low-level automation of Graphical User Interfaces (GUIs) at the pixel level, and tools that use computerization, which is the re-implementation of human-made business logic. So, there is not a single RPA tool; generally, there are two types of tools used for RPA, which are process automation tools and software robots. The basic understanding of RPA is either through software robots or through automation tools using robots. Organizations worldwide can implement RPA to partially or entirely automate the execution of routine follow-up processes controlled by business logic and structured inputs. These processes can range from high-volume data entry and transaction processing across multiple systems to complex back-office support for financial services with minimal human intervention.

This type of software robots can be called bots. A bot is defined as a piece of software that can act automatically on a computer network, executing repetitive tasks at a lower cost and possibly at a higher speed than human labor. RPA can be implemented in virtually any industry. RPA software robots can automate a simple task or full-fledged business processes across organizations running different systems, located in different countries, and using different languages. Popular usages of RPA include processing credit card applications, matching invoices to purchase orders, sending e-mails over certain trigger events, and putting downloaded statements or data into a database. However, the classification of RPA depends on the capabilities of the bots. RPA tools available nowadays range from fairly simple and low-cost on-line chat bots answering customer inquiries to multi-million-dollar deployments that automate large back-office processes for banks, insurance companies, or credit card firms.

6 Potential Benefits of AI in Auditing

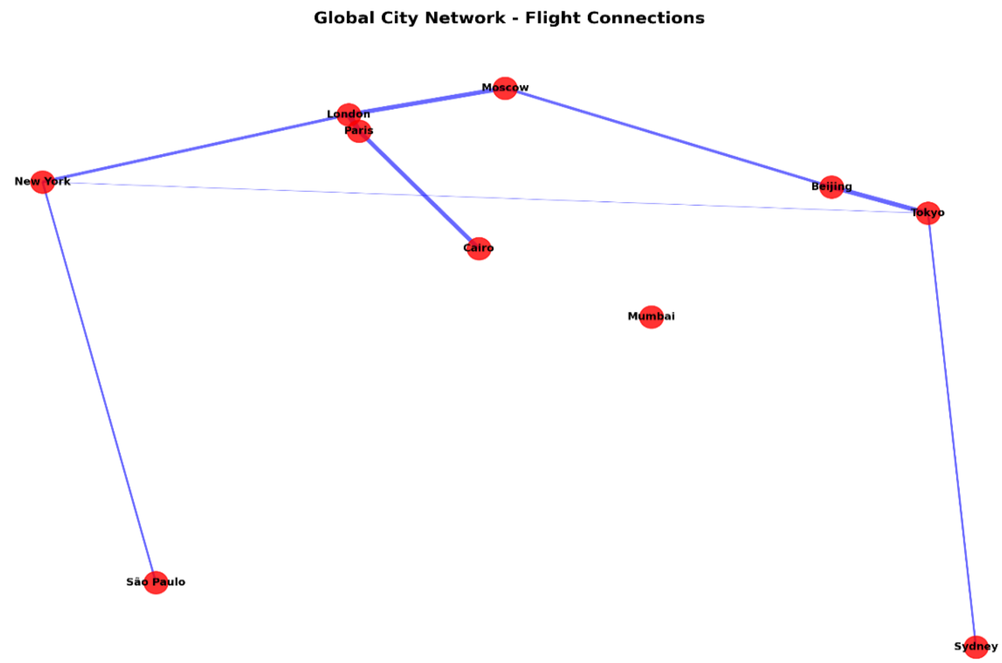
Artificial Intelligence (AI) is not only able to succinct and comprehensively summarize documents, but it is also assumed to have the potential, through the use of sentiment analysis, to analyze news and financial reports for parameters that are relevant for stock market changes. Through the aforementioned techniques, AI could come up with efficient introduction algorithms which aggregate the data describing an IPO and assess its pricing and after-market stability. AI techniques can be used to implement execution algorithms that will price and time the orders considering the trade-off between liquidity and market impact. In secondary markets, AI could facilitate proprietary order flow generation by learning clients' data. It could be used to price derivatives and assess the risk for trading desks as well as to exploit price discrepancies in and across exchanges by trading agents which learn from transactions using reinforcement learning. In the second-best market, AI could automate surveillance and control based on statistically analyzing/learning trade behavior and market micro-structure tailoring.

A bespoke personalization of the digitized regulatory framework means adapting the ones fitting the institution's needs in terms of risk profile, internal workings, client and product characteristics, and which will be delivered to each employee. Each financial institution could proactively identify gaps in compliance and supervision through benchmarking institutions with the market and client universe in terms of breaches. Supervision could be performed in a much more focused way through examining behavioral, network, transaction data of fewer grand clients/users, focusing on the ones showing signs towards undesirable behaviors such as complaints, possible fraud, AML risks, etc. AI could inform the regulators supervisions on the level of automation and compliance enhancing regulators as a whole prerequisite to compliance. Regulators could foresee firm departures/leavings offside policy through examining behavioral data, and anticipation of float-ons to another system through connections with equally positioned known financial institutions (Brozović, 2019).

6.1. Enhanced Data Analysis

Artificial Intelligence techniques can be leveraged to improve data analytics by auditors, increasing their quality and efficiency. One of the advantages of data analytics is the ability to analyze all audited transactions rather than a sample, thus allowing for greater quality. In addition, the results of the analysis can also be compared with previous periods of data, thus supporting analytical review procedures. There is a clear opportunity for auditors to improve data analytics based on Artificial Intelligence and added machine learning techniques. Where a human audit assistant is required to understand an audit case, the written text of the auditor's understanding and risk assessment will be analysed by an intelligent machine audit assistant through natural language processing to determine analytical queries of machine learning models that create historical audit trial patterns. Based on this query, a query language is produced that creates a larger data set on analytics. Based on both the query language and the "risk" parameters of the case, data analytics that quantifies "risk" is generated. Lastly, data analytics will aid the auditor in maintaining and documenting the audit record and their professional considerations.

One opportunity involves enhancing auditing in client systems with Artificial Intelligence analytics. Artificial Intelligence and machine learning-based analytics can be deployed in client ERP systems to enhance data coverages and normalizations. Where a human audit assistant attends the client's queries and requests missing documents and data, a machine learning and Artificial Intelligence agent will interrogate the client's machine through intelligent bots and robotic processing. Through text mining, the intelligent bot will interrogate the query "what is the desired document," thus gathering information on document formats, sending queries to the original ERP system. Furthermore, similar bots will classify document contents and catalogue documents into acquired management systems database. In turn, the analytic probes will crawl the client system. First, with case-related keywords and queries, normalizations are performed to improve short sampling data and create analytic-friendly data spaces. Then, continuous-monitoring rules of data extraction are generated as analytic probes for quick re-assessment (Lal Joshi & Marthandan, 2019).



7 Challenges in Implementing AI in Auditing

Auditing AI refers to the ongoing analysis of, methods for examining, and standards for resource allocation and decision-making in AI systems in order to achieve specific social goals regarding risks and ethical behavior. Auditing AI has attracted significant interest as a way to help understand and manage the ethical problems and social risks that are some of the most visible concerns regarding modern AI systems. This idea is often connected to a proposal for very specific forms of auditing, often described as algorithmic audit or fairness audit. These audits would review only the final models and data of a trialed ML system to evaluate a score along a single axis, for example, that it "is not biased" or "is interpretable," and often issuing only a narrow assurance of equivalence to other models rather than any strong conclusions about the underlying machinery or control over it.

An enormous numbers of bodies seeking to develop audit standards for AI systems have sprung up, with different approaches and much duplication of effort. There are many well-meaning groups trying to create a large number of standards for many specific aspects of AI and indeed, there are standards that address various aspects of algorithms that are already before it. But the clear concerns raised by current AI systems have only increased the scale of this problem, as they have already outstripped existing standards intended to manage their risks (Manheim et al., 2024).

There are many reasons to question the utility of auditing AI as it is commonly conceived, but three clearly stand out: it is very likely to be incomplete; that very incompleteness will, in turn, be leveraged to advance undemocratic, harmful goals; and no existing body has the necessary breadth, skillset, or mandate to consider the underlying issues. In the absence of thoughtful auditing standards for AI, there would be not only a poor quality audit but a competing industry of grifts and snake oil salesmen, each of them trying to audit with a different and contradictory set of strategies and being able to claim that they complied with the standards.

7.1. Data Quality Issues

Digitisation and the consequent emergence of Big Data has invited auditing firms to either rethink their way of performing audits or risk being rendered redundant by technological audits. Clients are more aware of audit quality and audit outcomes today, and, as a result, this mounting scrutiny has resulted in auditors feeling pressure to manage a portfolio of clients with reduced fees and greater risk (Lal Joshi & Marthandan, 2019).

The emergence of new data, more data sources, new types of data, and faster data results in higher demands on reporting, new risks, new risk assessments, and stakeholder expectations. These developments have drawn attention from regulators as well as organizations as the importance of data has dramatically increased concerning the reporting of a broader set of factors. The emergence of Big Data, Internet of Things (IoT), and rapidly developing data generation tools has made the conduct of audits or assurance increasingly pervasive. Increasing volumes of data generated by not only enterprise systems, but also operation technology, IoT devices, sensors and streaming data introduces complexity for auditors. This is further accentuated by the rapidly changing technology landscape. Auditors increasingly have to integrate client provided data extracted through multiple tools into formats and systems used for audit evidence evaluation, while ensuring that the data provided is sufficiently accurate, complete and relevant to the audit. The diversity, volume and velocity of Big Data create quicker schedules and deadlines for audits. In times of growing complexity, budgetary concerns can negatively impact audit quality, as can diverse and rapidly changing technology on audit performance. However, auditors need to realize that biggest gains are to be had by auditing in the era of Big Data. Mainly, paradigm shifts in audit approaches need to be reflected in the audit profession. More widespread use of data analytics offers opportunities for auditors to exploit the full potential of comprehensively covering the entire data set in rapid timescales. Predictive based monitoring using streaming methods offers the potential to forecast the data future and subsequently report irregularities to management early in the data life cycle. Therefore, Big Data can potentially enhance audit quality if adequately monitored. Such potential will require shifting paradigms on audit expectations and upfront planning choices.

7.2. Integration with Existing Systems

As previously mentioned, the deployment of AI or ML systems requires the creation of a pipeline to update the model with new data and re-train it as needed. Businesses frequently lack experience utilizing AI systems. Some specific contexts may call for a closed research system that is infeasible to adapt or implement universally (Barta, 2018). As a consequence, a general AI that can examine a wide range of datasets without further training is not easy to develop. Nevertheless, some techniques employed in existing models for comparable use cases could be broadly adapted. Moreover, the dataset is seldom presentable in a final form immediately. Most data privacy laws and compliance frameworks mandate data minimization. Organizations should train AI exclusively on anonymized data applicable to the domain of interest, such as logs and declarations. As a result, the implementation of AI systems tends to be a multi-stage and lengthy process.

Utilizing AI for auditing requires exceeding current practices with a more complex pipeline. Data manipulations require greater expertise. Workforce capabilities may need upskilling or hiring to implement and retain the new system. Furthermore, strict laws are also prevalent for AI. They require justification for using a model and transparency for it. As a result, most complex models are black-box ones, which cannot provide justifications for certain results. Nonetheless, consulting third-party organizations or using simpler adaptable alternatives could be transparent enough. Furthermore, audits for algorithms may be implementing in practice as well. All things considered, the use of AI is relatively challenging but could lead to competent insights and findings requiring further testing.

7.3. Regulatory Compliance

Artificial Intelligence (AI) models are increasingly utilized in diverse sectors, such as finance, healthcare, and manufacturing, to support broader and more significantly critical decisions. The resulting compliance concerns are heightened due to an implicit responsibility gap. As regulatory scrutiny escalates, cohesive compliance across diverse stages of the model lifecycle becomes indispensable. Furthermore, the complexity of AI systems is ever-increasing, leading to concerns about the scalability and effectiveness of current compliance practices. This paper outlines the challenges faced by financial institutions concerning the compliance of complex AI systems and discusses opportunities to structure integrated and sustainable AI model governance frameworks.

A self-regulating, system-level structure is proposed to address compliance concerns across the AI model lifecycle in a more coherent manner for increased automation. The increased sophistication of AI systems raises concerns about structural robustness in compliance processes, highlighting the importance of a more systematic approach. The assessment of legislation abidance would benefit from a wider view of AI systems, enabling examination of how downstream processes digitally ingest upstream modeling artifacts (Kurshan et al., 2020). The model governance practices for AI systems find their precedence in audit, validation, and model governance frameworks for traditional modeling enhancements. However, the unprecedentedness of AI technologies in industries such as finance, credit risk, and anti-money laundering raises uncertainties concerning the effectiveness of current practices. The integration of inspection outlooks of design and operations through AI system models would flatten the structures of the model compliance process as much as possible.

Compliance with Trustworthy Artificial Intelligence (TAI) governance best practices and regulatory frameworks is a fragmented process across various organizational units. This fragmentation generates compliance gaps that may expose organizations to compliance risks. Organizations struggle to comply with TAI best practices, such as data governance, conformance testing, and transparency requirements (Pery et al., 2021). Moreover, compliance with new TAI regulations adds layers of complexity and uncertainty to the governance environment. Some requirements can be ambiguous, incomplete, and inconsistent, providing leeway for interpretation that may lead to non-compliance. The set of compliance requirements is also expected to evolve over time. Process mining offers several opportunities to counter these challenges regarding TAI regulatory compliance. Automated mining of standard operating procedures significantly enhances overall process transparency and accountability across the organization.

8 Case Studies of AI in Auditing

Artificial Intelligence (AI) holds significant promise to radically improve the performance of current auditing practices. Discovering novel patterns and structures underlying large data is a core component of the emerging field of data science, and this aspect of data science–driven auditing is beginning to have a noteworthy impact on the practice of auditing (Belle, 2019). Data auditing on large data sets can yield counterintuitive insights that could not be obtained from the limited perspectives of human auditors. Nonetheless, this impact raises important challenges: In the data science group, these new opportunities are accompanied by innovative data science and probabilistic/statistical, computational, and visualization methods that come with technical, theoretical, and statistical difficulties. Such new mathematical methods are typically considered black boxes, and auditing the inner workings of these methods is challenging. Patterns discovered in data remain abstract without an ontological interpretation, exemplifying the necessity of an effective connection between data science and domain knowledge (Khaliq et al., 2022). The underlying decisions suggested by many of these trained models to clients, on which someone's wealth could depend, must be interpretable to ensure that the decisions may be trusted. Although auditing practices and the field of AI can be said to be using methods and technologies aligned with their classification, a gap exists in the literature on the intertwining of the two. An unanswered question of practical significance to the auditing community is how AI can improve auditing decisions and performance; in turn, the auditing literature should provide insights into the information requirements of client firms in order to expand AI applicability in other settings. Additional research questions that arise from the auditing literature include defining the general scope of expected decision performance; distinguishing areas of easier application of AI, where economic and public benefits may be cognized sooner, from outlier domains of inherently limited applicability; and covering methods adopted by humans, which their organizations view as core and central to success, with other methods that are potentially more transparent.

8.1. Success Stories

Numerous companies are incorporating the automation of analysis into their audit processes. (C. Oldhouser, 2016)

The analytical tools market includes many new entrants, especially in the field of data mining. The three main areas are process mining, security mining, and data mining. Process mining involves mapping data into process models and setting it as a baseline for continuous monitoring or auditing. This field currently experiences a higher influx of tools. Security analytics encompass log and event correlation approaches to prevent unauthorized access to systems. Industrial data mining encompasses statistical have-a-go tools for early detection of risks in the processing, such as clustering for operational effectiveness purposes.

The use of prediction markets to assess the effectiveness of analysts or others in forecasting audit risk is in its infancy but could gather momentum. In theory, data scientists could determine the outcome of a significant one-off transaction and construct a prediction market for it. If this market leveled on a particular analyst being incorrect, sufficient interest could develop (Belle, 2019). Another development is the increasing dependence on external cloud providers for large-scale data processing. This either relocates the auditing requirement to the cloud or imposes new data access restrictions on the auditors established by the cloud provider. Academic literature's self-sustainability, especially revolutions outside the US, is of concern. The decline of auditing research in Europe could be a harbinger of unsustainability elsewhere.

8.2. Failures and Lessons Learned

In late 2022, OpenAI's Chat GPT garnered extreme attention and user growth. As the API was opened up for third-party applications, and usage exploded, serious failures began occurring. One cherry-picked example, which illustrates a variety of pre-existing issues with LLMs, including the rate of such issues, is a series of legal documents forfeit that were adjusted to be inaccurate but still repeated back plausible-sounding specifics after one prompt. Other examples relevant to financial audits include an online aggregator of multiple large LLM services returning correct, but harmful answers, and an example explained directly to entirely exploit a fault that allowed special access to single API keys to be leaked. Financial engagements related to these were similarly work-generalizable and undid the level of effort put into them, possibly dating back to the private training phase of these products. In all these documented cases, if there had been a reasonable third-party audit performed before public availability, these outcomes could be avoided.

Common questions, requests, and pats on the back flew around on online discussion forums for marketing teams, PR, and legal departments. Watching the industry grapple with the results of the extreme decisions was painful, especially with regards to the security shoulder systems that had evidently been overlooked (Manheim et al., 2024). Regardless of how external scrutiny might prioritize and encourage a logical response, LLMs had long been trained in largely private ways, and obvious issues along with their dependencies had been ignored. Communications and alignment remained optional, and development plans were self-imposed. The general feeling was that there were now few clear paths to control the damages; notable examples were now beforehand and were seemingly indiscriminate in their demands. As the public expected greater scrutiny, the frantic efforts were sub-scoped to out of sight areas.

Amazing progress had been made via the use of remote service and zero-zero deployments, but it came at an extreme risk and reliance. An initially inspired surge of new capabilities had generated threats to existing businesses, but insisting on rapid changes to business model and strategy quickly leveled off. Audits of availability and of systems security could highlight gaps and as time would show them to be severe, but a successful upgrade-downgrade system to be different and equally successful was never devised. Exploitation attempts had undoubtedly begun on the devices that were now removed from general data feeds. The side-channels at vastly greater-than-human prompt frequency were clearly useless. But there was no effort towards understanding nor any due or limit calculations of medial costs. Near extremes made for great demos and prompt systems which continued to produce eye-opening results, but defence by dumb luck was no defence.

9 Future Trends in AI and Auditing

AI auditing technologies automate and streamline the audit process, enabling remote audit processes to improve efficiency without incurring additional costs as they grow. With the development of these technologies, there is a growing fear that machines will replace human auditors. This fear is warranted, especially for basic, repetitive, and low-level audit tasks that add no value to the audit. However, machines are not fully autonomous and require auditing by human auditors. Therefore, it is imperative to discuss how some opportunities are available for auditors to exploit the advanced AI audit technologies and cope with the coming disruption.

Auditors must study AI technologies, especially ML, to understand the underlying mechanisms. Basic requirements of AI, including data issues, need to be understood. AI and human collaboration can be built by interpreting the decision-making process of AI models. Contemporary research in interpretable ML is creating models that are not only accurate but can also be explained in terms of human-understandable attributes (Belle, 2019). Discussions should move to practical aspects of how to audit AI models. AI becomes a black box when the number of inputs and the size of the model increase. Future research should focus on investigating how AI model training can be re-formulated in an auditable way.

Auditors should explore advanced AI technologies like ML. These technologies have been effectively used in generic domains. Researchers have recently explored the application of ML in auditing, including anomaly detection, classification, natural language processing, clustering, and extraction and analysis (Lal Joshi & Marthandan, 2019). Currently, AI audit technologies deal with common and sector-specific deviations in data distributions. However, such opportunities are often neglected by auditors to exploit these advanced technologies – i.e. advanced AI technologies in generic domains should be explored in audit contexts and compared with emerging AI audit technologies.

9.1. Predictive Analytics

According to (Belle, 2019), while uncovering patterns and structures in large troves of data in an automated manner is a core component of data science and a great opportunity to organizations, this highly positive impact is accompanied by significant negative effects and challenges. An automatic system may turn out to be biased and unfair. Treating a person unfairly may be the result of a biased dataset. Automated predictive policing may disproportionately target a certain area and lead to a vicious cycle of crime. Nevertheless, this only addresses the problem of data bias and cannot guarantee that if the data is considered fair, the predictions and recommendations will still be. Following the same logic of pattern discovery, when humans build machine learning classifiers, they are provided with a specific dataset of normal and abnormal instances. Instead of directly providing the complete criteria for separation, humans simply provide training examples.

(Lal Joshi & Marthandan, 2019) discuss the issues arising from the availability of Big Data to firms as well as the various consequences of using Big Data in audits. Big Data may be highly informative and rapidly democratized and as a result a democratized society of economic agents that is far more efficient and deserving. Big Data may act as a threat to various aspects of democracy. This scenario ultimately focuses on the easier and less expensive surveillance of Big Data by companies and governments; a growing income and wealth inequality; fraud detection, avoidance and prevention; threats to consumer privacy and human rights; and advance fraud and manipulation.

It enables auditors to work smarter with the analysis of patterns in numerous sources of unstructured data. By providing a wealth of information to the auditors, Big Data helps auditors discover complex relationships within the model and relevant constraints. It enables auditors to test complete sets of accounts on a given range of transactions, instead of sample testing, and hence providing greater assurance of detection of material misstatements. Big Data can be used in planning field works, fraud detection through continuous transactions monitoring, and improving forensic accounting. Extensive usage of Big Data in accounting systems increases the need for a fully automated audit process. Major auditing firms are developing software for the complete automation of audits and the development of tools and frameworks that greatly facilitate auditing systems have been proposed. There has been no mention of how predictive approaches may improve forecasting.

9.2. Continuous Auditing

Today, firms are constantly gathering large volumes of events and transactions, but this data is underused and unevenly corrected. Compiling and analyzing this information at the end of the accounting period in a traditional audit is equivalent to performing an analysis ex-ante after an event. As a preventive approach to ensure information integrity, it is essential to enable discussions, verifications, and analysis ex-post just after the events have occurred. Continuous auditing is an audit approach that operates at the transactions or events level, incorporating new event-driven technologies to automatically collect and analyze the data relevant to the audit. Continuous auditing refocuses the audit on the audit assurance points, incorporating intelligent streaming engines to detect fraudulent events, anomalies, and other significant events. New event-driven architectures come into play to support the event-driven continuous audit and compliance functions. Continuous auditing could eliminate the spreadsheet time lag and poor controls over financial error checks. With continuous auditing, checks would be completed instantaneously as entries were seconded between systems (Pierre Junior D Aboa, 2014).

Over the past decade, the structure of corporate auditing has undergone tremendous changes. The development of increasingly cost-efficient computing technology, the introduction of the Internet, the rapid advancement of database technology, the inception of enterprise resource planning (ERP) systems, and the strong competition with consulting firms have forced auditors to rethink their roles and to develop new audit strategies. Auditors are eagerly exploring new strategies to enhance the efficiency and effectiveness of audit processes. Nevertheless, the crisis of confidence in accounting assurance quality raised profound questions on auditor independence and the provision of non-audit services. History suggests that the emergence of any new major technology takes time before organizations understand it and assimilate it into their practices. The slow internalization of continuous auditing and its correspondent acceptance might be considered as a systematic resistance to change.

10 Stakeholder Perspectives on AI in Auditing

The introduction and continued development of artificial intelligence (AI) creating great uncertainty throughout the world. In several professional fields, however, AI is seen as beneficial, or even transformative. Notably, AI has the potential to significantly alter and enhance auditing. Such a transformation would not be unprecedented; similarly transformative technologies have infiltrated auditing in the past to mixed reception and effect. Auditing, and audit firms, must understand what AI is, how it works, and how it will interface with auditing in order to best incorporate the technology and prepare for its proliferation. AI consists of a collection of technologies that together afford machines the capacity to take in data, analyze it, use it to create predictions, and use those predictions to generate output (Manheim et al., 2024). These technologies include machine learning methods, natural language processing methods, and machine vision methods. In order to understand the capabilities of these methods, audit firms must understand how these inputs are used to generate predictions, how those predictions are used to generate output, and the potential difficulties and complications that ensue from their design and use.

Auditing is broadly defined as an independent examination of financial statements to express an opinion on their fairness, out of respect for a marketplace's need to protect investments. Aspects of the profession that will not be altered by AI deployment include inquiry and analytic review. However, other aspects of the audit process, such as planning, control testing, substantive testing, and documentation will be altered. The gradual insertion of AI into auditing is therefore an appropriate time for audit firms to consider how to embrace this new technology. Enhanced documentation of the audit process can be an incremental response to AI risk. As AI becomes incorporated into audit, control risks will evolve, their presentation will change, and audit tests will need to adapt. These changes must be made clear in order to maintain audit quality. Audit firms must anticipate these changes in risk before AI is widely adopted. AI integration will have a mixed impact on audit quality. However, if AI is incorporated properly, the benefits should outweigh the drawbacks. A comprehensive inquiry into the capabilities and ramifications of AI on auditing is necessary to understand how its design and use will impact data processing and information generation.

10.1. Auditors

By definition, auditing is an evidence-driven scientific rational and judgment process designed to evaluate the integrity of an organization's products and services. Creditability is a critical component of an audit quality that is threatened amid globalization, increasing complexity of financial instruments, accelerating change of technologies, heightened regulatory scrutiny, and severe scandals that shook market confidence. Honesty can only be credible by rely-on audit trails, and therein come the demand on securing data integrity and traceability through log files verification (Lal Joshi & Marthandan, 2019). Yet, log security was hardly effective due to either a hacker can easily dump the log file logs, or a privileged user is able to delete security logs with no traces. The computer forensic based analyzers including commercial and academic ones are ground-up direct verifiers on the database logs. Nonetheless, they are either proprietary-based closed products with unsound motivation or costly investment for small organizations or college systems.

While many researchers study algorithms and designs for log files verification, computer forensics is still a new discipline and still missing standards thereof. The dissertation is the first to study top-down metrics to mathematically ensure accuracy in mission-critical data management. The findings suggest that the log integrity can be verified through a hybrid of both hardware and software means. The trust-query verification in SQL is proposed to check on-the-fly in contrast to log analysis with reviews.

What is worth noting, told (C. Oldhouser, 2016) that the audit profession is facing a myriad of challenges nowadays, but the auditing is not to be dead. The social reformation in transparency, objectivity and independence is a must to retain confidence in financial audits, to comply audit requirements in data privacy, and to foster a community to share and review audit knowledge and materials, and for data auditors a need to innovate a verifiable transparency scheme, for organization auditors something is wrong as to why two opinion?

Many believe that those challenging situations in auditing are risks that prohibit auditors from doing their work. Otherwise, they may view such highlighted issues as opportunities to help audit firms in facilitating clients, and regulators in monitoring activities, and silly companies in-ranking. Nevertheless, there need to be more rigorous and transparent in providing relevant backgrounds.

10.2. Clients

The auditing profession has been continually evolving with the development of the business environment and the advent of information technology. The latest topics such as the digital economy and Artificial Intelligence (AI) catch the attention of auditors, researchers, and regulators. AI is gradually becoming an essential part of modern businesses and lifestyles and considered the second wave of the IT revolution after the Internet. AI has attracted mass attention due to its impacts on various aspects of individual lives. For instance, social media platforms recommend products through its intelligent algorithms.

The growing importance of AI encourages audits and researches in the auditing profession. Aspects of AI such as Machine Learning (ML), a part of AI affecting multiple fields, can do huge data analysis and similar tasks. Auditors and audit support documents such as working papers traditionally use systems of risk assessment and tests that rely on human analysis. However, such traditional systems will cause low efficiency and low effectiveness as a person's limited experience to handle the growing complexity of audit environments. Meanwhile, illegal tusks may bring lost data mass, and it is challenging to search and check all.

Most external auditors, especially in a small scale, do routine tasks and fields that prevent them from doing impossible ones. Generally, auditors are short of ICT researchers or less advanced XP techniques for carrying out AI research projects (Lal Joshi & Marthandan, 2019). Currently, most machine models and heuristic algorithms remain less transparent and easily able to leave joint log evidence on the audited system, raising questions on assessing participants' professional care and competence.

Although the AI applications in auditing are at the nascent stage, it provides auditees with several indisputable opportunities. For example, process automation and applied ML techniques could help scape and analyse financial statements to generate evidence-based questions, which will require auditor responses and further investigation. Also, acoustics modelling tools such as trajectory analysis could be used to improve or design documentation templates.

Specifically, auditing, risk assessment, and collecting audit evidence tasks can benefit from applications of AI in financial statement analysis, anomaly detection, or attribute extraction. However, it will also require audit and regulator intervention to avoid applications from overlooking common threats of deeply analysing, producing, and deciding upon mathematical based automated systems. It will need auditor tech-savvy to upskill and watch out for system blind side effects.

10.3. Regulators

With an eye toward practicality, a number of more specific recommendations can be made about what the regulators should do. Where possible, these recommendations fall into a hierarchy, with those that are the most straightforward and least controversial presented first, and those that are more ambitious presented later. The list will be pared down to the most important and actionable items, but there are many other possibilities that could be explored to good effect.

Formulate a regulatory framework that values and builds upon existing auditing frameworks and techniques rather than dismissing them out of hand. Moving too quickly in imposing new frameworks or techniques risks outrage from critics who are wary of these technologies but who might otherwise have been allies.

Establish a whitelist for allowable systems along the lines of a framework for defining allowable cryptographic algorithms. This would include more specific recommendations about acceptable methods for auditing. For instance, it would outlaw the use of LLMs in high-stakes scenarios like determining bail.

Create incentives for institutions to establish their own auditing frameworks. These would warrant public attention, particularly if there is a mechanism for cross auditing. One could also avoid creating new regulatory rules by emphasizing existing rules that apply to new technologies as much as to old technologies.

Establish a regulatory agency to implement the list. In practice, much of this work will require vigorous involvement in scientific and technical discussions. While excessive and overly granular regulation by rule is what happens when agencies don't do this. A specialist agency is necessary. With sufficiently robust authority and mechanisms for public transparency and input, even if it fails, it could provide fertile ground for the development of norms propagated by other sources.

11 Conclusion

Artificial Intelligence (AI) takes the world by storm, affecting all facets of our lives. It seems the whole world has suddenly leapt into a futuristic world where all processes are more intuitive, productive, and organized. However, integrating AI technologies and systems is a complex process that requires the careful handling of various aspects of the processes. Many scholars have highlighted some key challenges of AI-based systems as well as their respective, longer-term implications. The importance of auditing and documenting AI decisions, models, training processes, and important interactions between classic AI and new models has been explained, as well as the ethical implications. Criticism is accompanied by early attempts of organizations and political entities worldwide to create an attractive and comprehensive regulatory framework, explicitly stating desired outcomes and ethical considerations.

While self-regulation mechanisms, guidelines, and white papers exist, they were deemed insufficient for all the reasons mentioned above. Auditing of AI systems should be a people-driven, human-oriented business with people in charge of the auditing process. The widening gap between business and science is pointed out, which is expected to perpetuate by new challenges introduced by AI technology. Scientists develop appropriate algorithms, many times disregarding other dimensions of the technology, while businesses are forced to accept and implement black boxes to stay competitive. There is consensus within some systemic, holistic framing regarding how to assess the viability of an AI regime, its control mechanisms, and ways of keeping such mechanisms aligned with ever-evolving and self-learning systems.

A shortage of scholars is turning to the huge gray area of comprehensive auditing frameworks and processes dedicated to understanding and assessing AI systems given their structure and functioning. Government and major companies have established proxies to study, discuss, and eventually chief the design and regulations of AI systems. A host of questions remains unanswered as to how to audit and access AI systems and how to handle their enormous complexity and always-evolving nature. Extensive literature exists as to what should be considered when auditing AI systems, but the discourse lacks how to practically act on such visions. There are calls for the emergence of a new field, namely, AI auditing with a programmatic overview of topics and methodological avenues to explore those questions. Such field will draw also on the well-established and burgeoning schools of audit and management science.

12 References:

1. Barta, G. (2018). The increasing role of it auditors in financial audit: risks and intelligent answers. [PDF]
2. Belle, V. (2019). The Quest for Interpretable and Responsible Artificial Intelligence. [PDF]
3. Brozović, V. (2019). PRIMJENA UMJETNE INTELIGENCIJE U SEKTORU INVESTICIJSKIH FONDOVA. [PDF]
4. Bubinger, H. & David Dinneen, J. (2021). Actionable Approaches to Promote Ethical AI in Libraries. [PDF]
5. Burger, B., Kanbach, D. K., Kraus, S., Breier, M., & Corvello, V. (2023). On the use of AI-based tools like ChatGPT to support management research. European Journal of Innovation Management, 26(7), 233-241. emerald.com
6. C. Oldhouser, M. (2016). The Effects of Emerging Technologies on Data in Auditing. [PDF]
7. Cui, Z., Jing, X., Zhao, P., Zhang, W., & Chen, J. (2021). A new subspace clustering strategy for AI-based data analysis in IoT system. IEEE Internet of Things Journal, 8(16), 12540-12549. [HTML]
8. Gajjar, N., Rathod, K., & Jani, K. (2022). A systematic literature review on Robotic Process Automation security. [PDF]

9. Ganapathy, V. (2023). AI in auditing: A comprehensive review of applications, benefits and challenges. Shodh Sari-An International Multidisciplinary Journal, 2(4), 328-343. icertpublication.com
10. H. Sarker, I., Janicke, H., Mohammad, N., Watters, P., & Nepal, S. (2023). AI Potentiality and Awareness: A Position Paper from the Perspective of Human-AI Teaming in Cybersecurity. [PDF]
11. Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. Government Information Quarterly, 40(1), 101784. sciencedirect.com
12. Khaliq, Z., Umar Farooq, S., & Ashraf Khan, D. (2022). Artificial Intelligence in Software Testing : Impact, Problems, Challenges and Prospect. [PDF]
13. Khanmohammadi, R., M. Ghassemi, M., Verdecchia, K., I. Ghanem, A., Bing, L., J. Chetty, I., Bagher-Ebadian, H., Siddiqui, F., Elshaikh, M., Movsas, B., & Thind, K. (2023). An Introduction to Natural Language Processing Techniques and Framework for Clinical Implementation in Radiation Oncology. [PDF]
14. Kurshan, E., Shen, H., & Chen, J. (2020). Towards Self-Regulating AI: Challenges and Opportunities of AI Model Governance in Financial Services. [PDF]
15. Lal Joshi, P. & Marthandan, G. (2019). The Hype of Big Data Analytics and Auditors. [PDF]
16. Liang, W., Tadesse, G. A., Ho, D., Fei-Fei, L., Zaharia, M., Zhang, C., & Zou, J. (2022). Advances, challenges and opportunities in creating data for trustworthy AI. Nature Machine Intelligence, 4(8), 669-677. google.com
17. Manheim, D., Martin, S., Bailey, M., Samin, M., & Greutzmacher, R. (2024). The Necessity of AI Audit Standards Boards. [PDF]
18. Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2021). Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations. Science and Engineering Ethics, 27(4), 44. springer.com
19. Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. Big Data and Cognitive Computing, 7(2), 93. mdpi.com
20. Onososen, A. O. & Musonda, I. (2022). Perceived benefits of automation and artificial intelligence in the AEC sector: An interpretive structural modeling approach. Frontiers in built environment. frontiersin.org
21. Pery, A., Rafiei, M., Simon, M., & M. P. van der Aalst, W. (2021). Trustworthy Artificial Intelligence and Process Mining: Challenges and Opportunities. [PDF]
22. Pierre Junior D Aboa, Y. (2014). Continuous Auditing: Technology Involved. [PDF]
23. Shook, J., Smith, R., & Antonio, A. (2018). Transparency and Fairness in Machine Learning Applications. [PDF]
24. Tredinnick, L. (2016). Artificial intelligence and professional roles. [PDF]
25. Whang, S. E., Roh, Y., Song, H., & Lee, J. G. (2023). Data collection and quality challenges in deep learning: A data-centric ai perspective. The VLDB Journal. [PDF]
26. Zhang, L., & Zhang, L. (2022). Artificial intelligence for remote sensing data analysis: A review of challenges and opportunities. IEEE Geoscience and Remote Sensing Magazine, 10(2), 270-294. [HTML]
27. Zhou, C., Liu, X., Yu, C., Tao, Y., & Shao, Y. (2023). Trust in AI-augmented design: Applying structural equation modeling to AI-augmented design acceptance. ncbi.nlm.nih.gov