Artificial intelligence and algorithmic decisions in fraud detection

Tan, Evrim; Petit Jean, Maxime; Simonofski, Anthony; Tombal, Thomas; Kleizen, Bjorn; Sabbe, Mathias; Bechoux, Lucas; Willem, Pauline

Published in:
Data & Policy

DOI:
10.1017/dap.2023.22

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Data & Policy (2023), 5: e25
doi:10.1017/dap.2023.22

RESEARCH ARTICLE

Artificial intelligence and algorithmic decisions in fraud detection: An interpretive structural model

Evrim Tan[1], Maxime Petit Jean[2], Anthony Simonofski[3], Thomas Tombal[4], Bjorn Kleizen[5], Mathias Sabbe[6], Lucas Bechoux[6] and Pauline Willem[7]

[1]Public Governance Institute, KU Leuven, Leuven, Belgium
[2]High Strategic Council, Walloon Government, Namur, Belgium
[3]Department of Management Sciences, UNamur, Namur, Belgium
[4]Tilburg Law and Economic Center (TILEC), Tilburg Institute for Law, Technology, and Society, Tilburg, The Netherlands
[5]Political Sciences Department, UAntwerpen, Antwerp, Belgium
[6]SPIRAL, ULiège, Liege, Belgium
[7]Research Centre in Information, Law and Society (CRIDS), UNamur-CRIDS, Namur, Belgium
Corresponding author: Evrim Tan; Email: evrim.tan@kuleuven.be

Received: 06 December 2022; **Revised:** 18 May 2023; **Accepted:** 20 June 2023

Keywords: advanced analytics; artificial intelligence; data governance; digital governance; fraud detection

Abstract

The use of artificial intelligence and algorithmic decision-making in public policy processes is influenced by a range of diverse drivers. This article provides a comprehensive view of 13 drivers and their interrelationships, identified through empirical findings from the taxation and social security domains in Belgium. These drivers are organized into five hierarchical layers that policy designers need to focus on when introducing advanced analytics in fraud detection: (a) trust layer, (b) interoperability layer, (c) perceived benefits layer, (d) data governance layer, and (e) digital governance layer. The layered approach enables a holistic view of assessing adoption challenges concerning new digital technologies. The research uses thematic analysis and interpretive structural modeling.

Policy Significance Statement

The model suggests two key takeaways for policy designers interested in using advanced analytics in fraud detection. First, understanding the trust conditions, interoperability factors, and perceived usefulness of advanced analytics for the application area needs to be assessed before developing policy strategies for data governance and digital governance. Second, the high interdependencies among all drivers confirm the complexity surrounding the introduction of advanced analytics in public policy processes. Therefore, digital transformation policies and their effectiveness in public policy areas should be subject to periodic and cyclical policy evaluations.

1. Introduction

The use of new digital technologies and algorithmic decision-making in government and managerial practices has become ubiquitous in recent years. Scholars and practitioners across information sciences, administrative and social sciences are studying the impact and implications of data-driven technologies

such as artificial intelligence (AI), big data analytics, machine learning, and blockchain on managerial and organizational systems and practices (Tan and Taeihagh, 2021; Dickinson et al., 2021; Leiman, 2021; Radu, 2021; Taeihagh, 2021; Ulnicane et al., 2021). These technologies are overhauling the existing administrative systems and practices into new types of interactions between humans and machines, which is sometimes called algorithmic bureaucracy (Vogl et al., 2020; Tan and Crompvoets, 2022). However, the adoption of new digital technologies is challenging for public sector organizations due to various value-laden reservations driven by perceived technical, systemic, administrative, and regulative barriers inside and outside of organizations (Tan et al., 2022; Bullock et al., 2020; Vogl et al., 2020; Tangi et al., 2021, Sun and Medaglia, 2019).

Public administration research has begun to investigate challenges associated with the use of AI and algorithmic decision-making on system applications (Exmeyer and Hall, 2022; Neumann et al., 2022), accountability mechanisms (Busuioc, 2021), citizen trust and explainability of decisions (Grimmelikhuijsen, 2022), organizational rearrangements (Meijer et al., 2021), administrative discretion and willingness to implement (Alshallaqi, 2022; Wang et al., 2022), ethical principles and citizen's privacy (Willems et al., 2022), capacity gaps and knowledge management (Wilson and Broomfield, 2022).

However, this nascent literature provides a fragmented picture of how to integrate AI and algorithmic decision-making in public policy processes. Two strands of theoretical models assess technology adoption in public policy processes: *behavioral models* that explain technology adoption processes through the analysis of user perceptions of the technology and the mediating influence of user-level characteristics, and *structural models* that explain technology adoption processes through the interaction of organizational and institutional factors with user behaviors. Both strands of models focus on the perception of users but do not provide a holistic view to explain the perceived relationships between different institutional, organizational, technological, and individual-level drivers and their influence on system applications (Dawes, 2009; Engvall and Flak, 2022). This complicates developing viable digital transformation strategies for AI and algorithmic decisions in public policy processes.

This article aims to address this gap in the literature by developing a holistic model[1] that can explain the interrelationships between perceived drivers that influence the integration of AI and algorithmic tools in public policy processes. Specifically, this research focuses on the case of fraud detection in the taxation and social security domains, which are primary policy areas that use machine learning and AI-driven advanced analytics techniques. Although these technologies have the potential to improve fraud detection processes, their wider adoption is hindered by procurement obstacles, insufficiently trained workers, data limitations, a lack of technical standards, cultural barriers to organizational change, and the need to adhere to responsible AI principles (West, 2021).

Our specific research questions are:

RQ1: What are the perceived drivers[2] of the use of advanced analytics for fraud detection in social security and taxation domains?

RQ2: How are these drivers interrelated to each other?

To answer these questions, a cross-sectional study was conducted based on interview data collected from different stakeholder organizations in Belgian taxation and social security ecosystems. Thematic analysis was used to identify the main drivers in the adoption of advanced analytics in fraud detection, and interpretive structure modeling (ISM) and MICMAC technique were used to identify their interrelationships and their dependence and driving powers.

The analysis has resulted in a hierarchical ordering of the drivers, indicating that there are five hierarchical layers that policy designers need to focus on when introducing advanced analytics in fraud

[1] We use the term "holistic model" to refer to a model that looks at the system/process as a whole and explains the relationship between all of the parts of a whole. Please note that we do not use the term for a generalizable model.

[2] The term "drivers" is used in this article to refer to factors that can positively or negatively influence the adoption of advanced analytics in fraud detection processes.

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

detection: (a) trust layer, (b) interoperability layer, (c) perceived benefits layer, (d) data governance layer, and (e) digital governance layer. The choices made in a previous layer influence the choices in the following layers, enabling policy designers to anticipate the implications of policy choices. The analysis section elaborates on the drivers and their interrelationships at each layer.

The structure of the article is as follows. Section 2 provides a theoretical framework for the behavioral and structural models of digital transformation in public administration. Section 3 provides background information on the institutional and legal framework in Belgian public administration for the taxation and social security domains. It also provides an overview of the literature on the use of advanced analytics in fraud detection. Section 4 introduces the research methods and presents the variables identified through thematic analysis of interview transcripts. Section 5 explains the steps followed in constructing the ISM model and MICMAC analysis. Section 6 lists the main findings on the interrelationships between identified variables. Section 7 discusses the implications of these findings for policy processes and the limitations of the research. Section 8 summarizes the key takeaways and provides future recommendations.

2. Theoretical Framework

2.1. Models of digital transformation in public administration

Models of digital transformation and technology adoption in public administration can be divided into two categories: (a) structural models, and (b) behavioral models. In this section, we provide an overview of these models and critically engage with their limitations in analyzing the drivers in policy-making processes.

2.1.1. Structural models

Structural models of technology adoption focus on how interactions between institutions/organizations and agents lead the technology adoption inside public administration. Orlikovski's (1992, 2000) "structurational model of technology" posits that as people interact with technology in their ongoing practices, they enact structures that shape their emergent and situated use of that technology. The use of technology is a process of enactment that enables a deeper understanding of the constitutive role of social practices in the ongoing use and change of technologies in the workplace. Orlikovski's structurational model identifies four types of influences that can affect digital transformation: (a) technology as a product of human action, (b) technology as a medium of human action, (c) institutional conditions with the interaction of technology, and (d) institutional consequences of interaction with technology. Each type of influence shape human action as design, appropriation, development, and modification, but also standards, norms, facilities, and infrastructures around technology adoption.

Another similar model, Fountain's "technology enactment framework" draws from bureaucracy, neo-institutionalism, networks, and governance literature (Fountain, 2001). One distinct element of Fountain's framework is the distinction between the objective IT (e.g., hardware, software, Internet) and the actors' perception and use of these technologies ("enacted technologies"). Enacted technology has four specific elements: perception, design, implementation, and use. In Fountain's view, the objective IT influences organizational forms such as bureaucratic structure and networks, and the interactions between institutional arrangements (i.e., cognitive, cultural, sociocultural, and legal format) and organizational forms influence and are influenced by enacted technology. Enacted technologies, in return, influence and are influenced by the policy outcomes, which eventually shape the objective IT systems and institutional arrangements. A strength of the "technology enactment framework" is its holistic view of perceptions, institutions, and organizational interactions to explain digital transformation policies. The model provides insight into how organizations often resist or prevent IT adoption or modify IT to fit their interests (Grafton, 2003). Yet, the model does not provide a temporal alignment among individual, organizational, and institutional drivers to position technology adoption strategies. Such insights mostly come from behavioral models.

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

2.1.2. Behavioral models

Behavioral models take their origins in the information sciences. Behavioral models theorize and identify key drivers influencing user intentions and their actual behavior in using new technologies. The literature provides a variety of user-driven theories including Technology Acceptance Model (TAM) and its extended version TAM2 (Davis, 1989; Venkatesh and Davis, 2000, Fathema et al., 2015), the Theory of Planned Behavior (TPB; Ajzen, 1991), the Theory of Reasoned Action (TRA; Fishbein and Ajzen, 1975), Motivational Model (MM; Davis et al., 1992), Model of PC Utilization (MPCU; Thompson et al., 1991), Innovation Diffusion Theory (IDT; Moore and Benbasat, 1996), Social Cognitive Theory (SCT; Compeau and Higgins, 1995), Unified Theory of Acceptance and Use of Technology (UTAUT) and its extended version (UTAUT 2) (Venkatesh et al., 2012, Venkatesh et al., 2003), and a more specific model designed to explain the user behavior on e-government adoption "Unified Model of E-government adoption" (UMEGA) (Dwivedi et al., 2017; Mensah et al., 2020). These models use variables such as perceived usefulness, perceived ease of use of the system, social influence, cognitive instrumental processes, performance expectancy, effort expectancy, social influence, facilitating conditions, perceived risk, computer self-efficacy, trust in the Internet, and trust in government to predict behavioral variances in technology adoption.

Shin et al. (2020) developed a behavioral model to explain the drivers of algorithm acceptance. The "Algorithm Acceptance Model" shows that the credibility of algorithms in terms of transparency, accountability, and fairness affects users' trust, which in turn influences their attitude toward adoption through the impact of the usefulness and convenience of the algorithm.

Behavioral models are insightful in understanding the underlying mechanisms that explain how individuals accept the use of a particular technology. However, they are user-focused, and policy designers consider different organizational, institutional, and political factors while developing policies for technology adoption. In that sense, behavioral models do not provide a full account of the factors influencing technology adoption for public policy purposes. Our aim is to develop a model that can take into account both individual perceptions of technology adoption and the perceptions of decision-makers about the interrelationships of the factors that influence the adoption of a particular technology in policy-making processes.

3. Contextual Framework

3.1. Institutional landscape

Belgium is a federal state where tax and social security policies are mostly controlled at the federal level. However, regional and local governments have some authority in specific tax areas. Nonetheless, the fight against tax and social security fraud is the responsibility of the federal government.

Several layers of actors in the Belgian institutional landscape are involved in tax fraud detection. The first layer comprises the Federal Public Service (FPS) Finance and its directorate generals who are the primary responsible public bodies in fraud detection concerning tax collection, customs, and excise. The second layer of public sector organizations includes the financial intelligence processing unit (CTIF/CFI), several services of the police forces in charge of corruption (OCRC/CDBC) and of major crimes (DJSOC), the national bank (that has a point of contact—PCC/CAP—to alert it about frauds), the financial services and markets authority (FSMA), the college of attorneys-general and the gaming commission that provide information about potential tax infractions to FPS Finance. The third layer of actors is composed of individuals, public, and private organizations such as lawyers, accountants, notaries, banks, major auditing firms, and judges, who are mandated to provide information about fraud they encounter to FPS Finance. Lastly, some transversal actors at the EU and national level that enforce specific tax policy provisions act as external stakeholders (technology providers, unions, business federations, and NGOs in charge of fair taxation and/or privacy rights).

Social security infringement detection is part of the federal social security policy. Unlike the taxation domain, the policy domain on social security provisions is rather fragmented. The FPS Social Security

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

oversees part of the policy design, but most of the policy implementation, including the fight against social security infringements, is led by a multitude of public bodies called social security public institutions (SSPI). There are five distinct SSPIs that are responsible for the detection of social security infringements: employment (ONEM/RVA), healthcare insurance (INAMI/RIZIV), social security for contractual workers (ONSS/RSZ), and social security for self-employed workers (INASTI/RSVZ), and control of social legislation (FPS Employment). These five organizations work together under the coordination of the SIRS/SIOD, which is responsible for developing an overall policy vision in the fight against social fraud. Some peripheral actors outside the federal government support the digital and data-sharing processes in this policy domain, such as SMALS, a nonprofit that acts as the federal IT support service, and the Crossroads Bank for Social Security (CBSS), which organizes data-sharing among SSPI. Nongovernmental actors such as social partners, social secretariats, and mutual health funds also contribute to the organization and management of social security policies. Eventually, the EU institutions can influence fraud detection processes in some social policy areas (e.g., social dumping) through the creation of specific regulations.

In addition to these domain-specific actors, there are also overarching political and administrative actors involved in both policy domains. These include the federal government, the federal parliament, the data protection authority (DPA/APD), and the Court of Audit (see the Supplementary Material for a detailed overview of the institutional landscape).

3.2. The use of advanced analytics in fraud detection

Advanced analytics is a data analysis methodology that uses predictive modeling, machine learning algorithms, natural language processing, deep learning, business process automation, and other statistical methods to analyze business information from a variety of data sources (Hanna et al., 2022). Unlike traditional descriptive analytics, advanced analytics applies automation and AI to produce far deeper behavioral insights and predictions from complex datasets.

Fraud detection is a primary policy domain that uses advanced analytics. Advanced analytics can be used to analyze financial transactions, gain operational efficiency in fraud detection, and become more effective at investigating unwarranted spending on a large scale (West, 2021). A 2020 report for the Administrative Conference of the United States found that 45% of the 142 agencies surveyed were using AI and/or machine learning (Freeman Engstrom et al., 2020). Similarly, the UK and the Netherlands are other countries that have developed AI-led solutions for processing social benefit claims (Booth, 2019; Kleizen et al., 2022).

The annual report of the OECD Tax series shows that the importance of advanced analytics is growing among tax authorities where data-driven insight is used against tax fraud such as in smart compliance with risk management and compliance by design (OECD, 2021). Advanced analytics are used in automating repetitive processes, extracting key data, scanning tax reports, identifying tax evasion, identifying tax deductions and credits, forecasting the burden of tax and improving transparency, and fighting against corruption (*Forbes*, January 9, 2020). Through supervised or unsupervised machine learning it is possible to find patterns of an anomaly in a large amount of data for predictive analysis and smart auditing that can outperform traditional data mining techniques (Van Vlasselaer et al., 2017; De Roux et al., 2018). For example, the British Connect System uses advanced analytics on big data to detect fraud (Maciejewski, 2017).

However, technological, organizational, behavioral, trust, and regulative challenges, along with traditional digital barriers, seemingly affect the adoption processes of advanced analytics among taxation and social security authorities. Black boxes, biases, and model drift are certain concerns against the use of advanced analytics (Busuioc, 2021). In a black box recidivism model, it may be unclear whether the high predicted risk of committing further crimes is based on admissible criteria (e.g., prior record) or potentially unlawful and/or discriminatory criteria (e.g., ethnicity) (Sandvig et al., 2016; Chander, 2017). Moreover, policy choices for the area of application can cause algorithmic biases. For instance, in the Dutch SyRi case, the policy choices of municipalities to

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

use advanced analytics in specific neighborhoods have led to false positives and discriminatory policies (Meuwese, 2020). Where such biases eventually become public, they may give rise to major trust breaches among groups that the model was biased against, or even wider society (Kleizen et al., 2022).

Moreover, where an algorithm is a true black box, it may be difficult even for developers to ascertain the predictors used by the algorithm. The inability to supply an explanation of advanced analytics not only strands the trust toward public sector organizations but also may undermine the principle of transparency (Ananny and Crawford, 2018; Ahonen and Erkkilä, 2020). Research shows that user cognitive routes concerning fairness, accountability, transparency, and explainability (Shin, 2020), privacy (Shin et al., 2022a), transparent fairness (Shin et al., 2022b), and perceived humanness (Shin, 2022) of algorithms may influence the perceived benefits and the willingness to use advanced analytics in policy-making processes.

Regulations also play a role in the way advanced analytics can be used in public policy domains. The use of advanced analytics in fraud detection by the Belgian public administration requires compliance with personal data protection rules and administrative law principles. The GDPR's purpose limitation and data minimization principles must be observed, and data subjects' rights, such as the right to information, access, and erasure, must be respected. Additionally, the algorithms used must not be biased and must not entail discrimination. The administration should also ensure that citizens have the right to understand the administrative decision, which is linked to the explainability of the decisions (Tombal et al., 2022).

4. Methodology

The objective of this study is to construct a model that considers both the individual perceptions of technology adoption and the perceptions of decision-makers regarding the interrelationships among the factors that influence the adoption of a specific technology in policy-making processes. To achieve this goal, thematic analysis and ISM-MICMAC methods were utilized.

Thematic analysis was used on interview data to identify the perceived drivers in the adoption of advanced analytics in fraud detection. This allowed for inductive identification of perceived drivers, overcoming limitations of technology acceptance models in including contextual factors and broader social, cultural, and institutional factors that can affect adoption decisions. ISM-MICMAC was used to understand the interrelationship between identified drivers. ISM-MICMAC allows for the adjudication of the direction and hierarchy of relationships among various variables, reducing complexity and turning relationships into tractable policies.

Data was collected through semi-structured interviews with public officials and technical, business, and policy experts from public sector and stakeholder organizations in the taxation and social security domains in Belgium (see the Supplementary Material). A total of 66 interviews were conducted from October 2020 to June 2021. The interview questions were clustered under the thematic areas of "tax fraud/social security infringement," "fraud analytics," "data collection and combination," and "data storage." Supplementary Table A gives an overview of the interviewees and their corresponding organization and administrative position.

4.1. Thematic analysis

To address the first research question, we conducted thematic analysis on the interview transcripts to identify the variables perceived to be influential in the use of advanced analytics in fraud detection (Braun and Clarke, 2006; Fereday and Muir-Cochrane, 2006). The codification processes followed different cyclical processes, where an initial set of codes generated from interview transcripts were used to identify patterns and interrelations among initial themes, which were later categorized under overarching constructs and associated with the drivers identified by the theoretical models. For each transcript, we produced a theme record that synthesized all the themes, corresponding quotations, and theme categories.

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

Themes and categories conveying similar meanings and substance were regrouped. The thematization process was conducted using a combination of inductive and deductive coding. Inductive processes are used in open and axial coding to uncover factors and their interrelationships that influence technology adoption processes. The categorized interrelationships were used later to interpret the direction of relationships during the development of the structural self-interaction matrix (see Section 5.1). Deductive coding was used to categorize themes from the behavioral and structural theories, while inductive (open) coding was used to identify new unforeseen themes and categories. To improve the reliability of the analysis, a researcher who was not involved in the initial data collection level performed a separate thematic analysis on the interview transcripts, and the results were compared before the final selection of categories. Through thematic analysis, we identified 13 variables perceived to be influential in the adoption of advanced analytics in the fight against tax and social security fraud in Belgium. Table 1 gives the categorization of constructs (i.e., variables), their definition, and the elements identified through thematic analysis. The subthemes used for the categorization of elements can be found in the Supplementary Material.

4.2. ISM-MICMAC

Interpretative structural modeling (ISM) is a methodical and collaborative approach that mathematically derives and analyzes contextual relationships among factors identified through expert opinion, enabling scholars to establish hierarchical levels of challenges (Warfield, 1974). ISM analysis entails developing a directed graph that configures the relationships hierarchically as interpreted by the scholars. MICMAC (Matrices d'Impacts Croises Multiplication Appliqué a un Classement) analysis complements ISM by classifying factors based on driving power and dependence power (Ahmad et al., 2019). ISM has been employed in e-government literature to explore critical success factors in e-service delivery (Lal and Haleem, 2009), citizen's perceptions of e-government's trustworthiness (Janssen et al., 2018), challenges for implementing the Internet of Things (IoT) in smart cities (Janssen et al., 2019). In this study, we used ISM and MICMAC to explore and describe the dependency and driving powers between the variables identified by the thematic analysis. Typically, ISM begins with a literature review to identify key variables before interpreting the direction of relationships. However, in this study, we have adopted a novel approach and used thematic analysis as a preceding step, allowing us to integrate the perception of Belgian stakeholders in identifying the variables that influence the technology adoption processes. Moreover, we have used extracts from interviews to interpret the direction of relationships between drivers, ensuring that the interpretation was not solely based on the research team's interpretation but also supported by the substance of the interviews. The adaptation of ISM in this research is illustrated in Figure 1.

5. Data Analysis

5.1. Structural self-interaction matrix

In developing the SSIM, there are four possible ways to relate variables, represented by "*V*," "*A*," "*X*," and "*O*" symbols (Hughes et al., 2020). The SSIM presented in Table 2 outlines the relationships between variables, with rows and columns indicated by "*i*" and "*j*," respectively. The symbols are interpreted as follows: *V*, Variable *i* influences variable *j*; *A*, Variable *j* influences variable *i*; *X*, Both variables *i* and *j* are influenced by each other; *O*, Variables *i* and *j* are not related to each other or do not influence each other.

The research team, consisting of eight researchers, individually and separately assessed the relationships between variables before making a final decision. The relationships among the variables are interpreted through the links disclosed by the thematic analysis. Specifically, if an underlying subtheme for a variable is related to another variable, this relationship is used to interpret the nature of the relationship. Table 2 presents the final decision taken by the research team on the nature of the relationship between each pair of variables.

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

Table 1. *Categorization of variables*

Drivers	Codes	Constructs	Elements	Definitions
Performance expectancy	1	Technological maturity	Bias and noise Technology convergence Blockchain/DLT AI/ machine learning Fraud detection technologies	This variable captures the maturity of new digital technologies that are used in the fight against fraud
	2	Perceived usefulness	Automation Improved social security and taxation Better data collection and analysis Past experiences Indirect added value of new digital technologies	This variable captures the perception of stakeholders about the usefulness of new digital technologies in improving the fight against fraud
Self-efficacy	3	Capacities, skills, and competencies	Resources Digital skills Training	This variable captures the resources, digital skills, and training of the administrations concerning the use of new digital technologies in the fight against fraud
	4	Management/ operational systems	Guidelines Rules and standards Principles Processes Strategies	This variable captures management systems and means in the administrations concerning the use of new digital technologies in the fight against fraud
Perceived risk	5	Perceived risk	Legal challenge Control of data Democratic challenge Administrative challenges Societal challenges	This variable captures the perception of stakeholders about the risk of using new digital technologies in the fight against fraud
Effort expectancy	6	Governance system	Data governance Open governance Multi-level governance Network governance	This variable captures the modes of governance in relation to new digital technologies that influence the fight against fraud

Table 1. *Continued*

Drivers	Codes	Constructs	Elements	Definitions
	7	Technical infrastructure	Security Quality of database Data collection and analysis Softwares Computer maturity Reliance/dependence on external actors	This variable captures the technical capacity of the system infrastructure that influence the use of new digital technologies in the fight against fraud
Social influence	8	Public values	Appropriateness of technology Respecting privacy Tax fairness	This variable captures the public values in relation to the use of new digital technologies in the fight against fraud
	9	Trust	Trust in administration Trust in society Trust in technology Trust in system Trust in tech providers/private sector	This variable captures the trust dimensions in relation to the use of new digital technologies in the fight against fraud
	10	Socio-cultural elements	Digital culture Digital divide Willingness to share data	This variable captures the socio-cultural conditions in relation to the use of new digital technologies in the fight against fraud
Facilitating conditions	11	Interoperability	Technical interoperability Semantic interoperability Organizational interoperability Regulative interoperability	This variable captures the interoperability conditions in relation to the use of new digital technologies in the fight against fraud
	12	Policy priorities	EU-level policy priorities Fight against fraud Political support Geopolitical aspects	This variable captures the national and international policy priorities in relation to the use of new digital technologies in the fight against fraud
	13	Regulations	Data	This variable captures the national and supranational regulations in relation to the use of new digital technologies in the fight against fraud

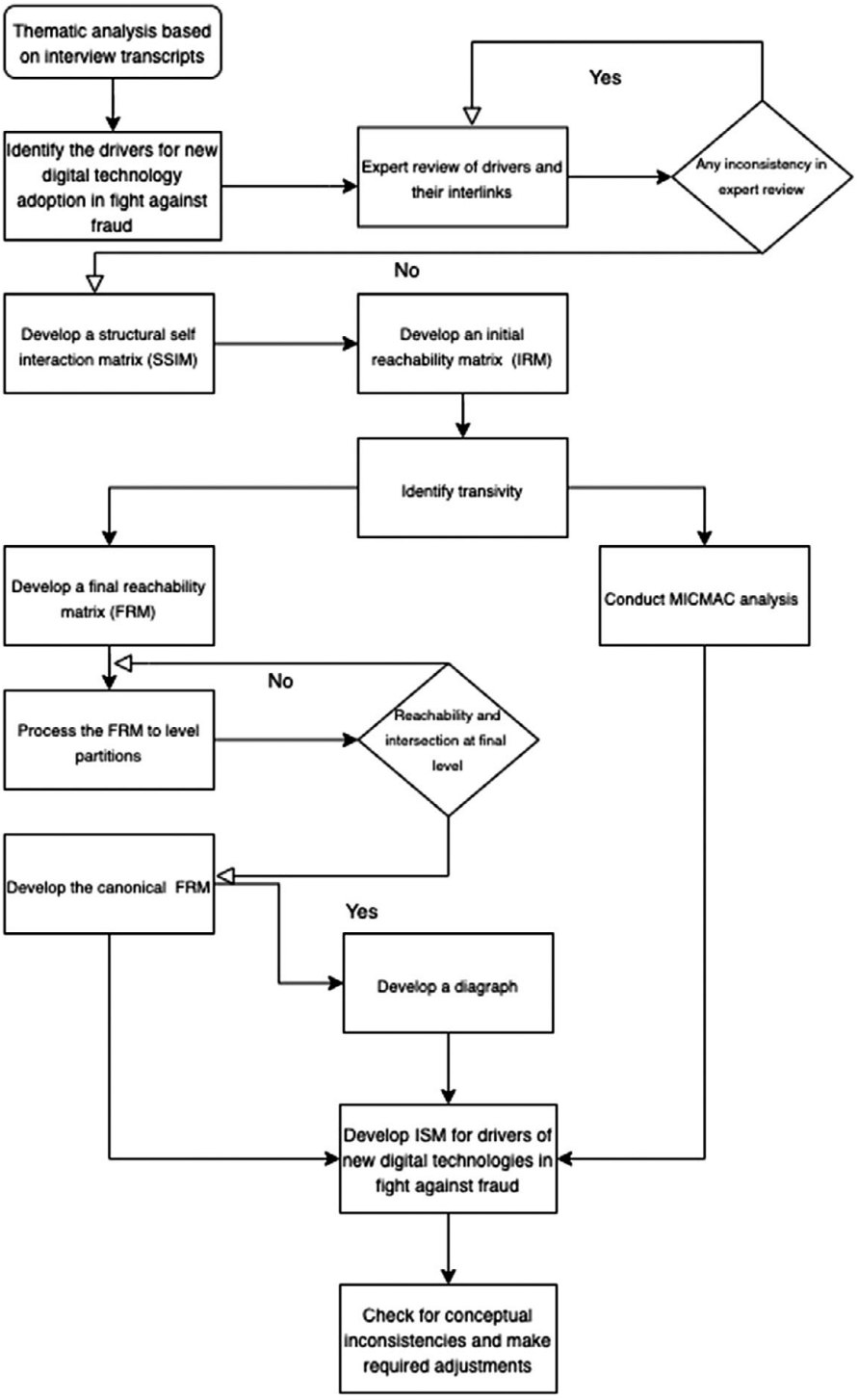

Figure 1. *ISM flowchart.*

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

Table 2. *Structural self-interactional matrix*

VR [*i*, *j*]	13	12	11	10	9	8	7	6	5	4	3	2	1
1	*X*	0	0	0	*X*	0	*V*	0	*X*	*V*	*X*	*X*	
2	0	*X*	0	0	*A*	0	*V*	0	*V*	*X*	0		
3	0	*A*	0	*X*	*x*	*V*	0	*V*	*A*	*V*			
4	*A*	*A*	1	0	*V*	*A*	*X*	*X*	*A*				
5	*A*	*X*	0	0	*V*	0	0	*X*					
6	*A*	*A*	*X*	*X*	*V*	0	*X*						
7	0	*A*	*A*	0	0	0							
8	0	*X*	0	*A*	*X*								
9	0	0	0	*X*									
10	0	0	0										
11	0	*A*											
12	*X*												
13													

Note. 1, Technological maturity; 2, Perceived usefulness; 3, Capacities, skills, and competencies; 4, Management/operational systems; 5, Perceived risk; 6, Governance system; 7, Technical infrastructure; 8, Public values; 9, Trust; 10, Sociocultural elements; 11, Interoperability; 12, Policy priorities; 13, Regulations; VR[*i*/*j*], variable *i*/variable *j*; *i,* row; *j,* column; *V*, Variable *i* influences variable *j*; *A*, Variable *j* influences variable *i*; *X*, Both variables *i* and *j* are influenced by each other; *O*, Variables *i* and *j* are not related to each other or are not influenced each other.

5.2. Reachability matrix

The SSIM was first converted to an Initial Reachability Matrix (IRM), which was then converted to a Final Reachability Matrix (FRM). The IRM illustrates the relationships described by SSIM in a binary way, with the following substitution rules: [1] if the (i, j) entry in the SSIM is *V*, the (i, j) entry in the reachability matrix becomes 1 and the (j, i) entry becomes 0; [2] if the (i, j) entry in the SSIM is A, the (i, j) entry in the reachability matrix becomes 0 and the (j, i) entry becomes 1; [3] if the (i, j) entry in the SSIM is *X*, both the (i, j) entry and (j, i) entry in the reachability matrix become 1; [4] if the (i, j) entry in the SSIM is 0, both the (i, j) entry and (j, i) entry in the reachability matrix become 0.

Next, the IRM was converted into an FRM, which includes transitive relations. Transitive relations occur when a variable *X* influences variable *Y*, and variable *Y* influences *Z*, so variable *X* should also influence variable *Z*, even if no mutual relationship is interpreted between variables *X* and *Z*. In such cases, an initial "no relationship" (i.e., "0") was recoded as "1." The IRM and FRM can be found in the Supplementary Material.

The FRM also shows the driving and dependence power of each variable. The driving power of a variable is the total number of variables, including itself, that it may help achieve. On the other hand, dependence power is the total number of variables, including itself, which may help in achieving it. These driving powers and dependence powers are later used in the classification of variables as part of the MICMAC analysis.

5.3. Level partitions

The FRM is used to create reachability and antecedent sets for each of the variables in the matrix. The reachability set, $R(P_i)$, for a particular variable, includes the variable itself and other variables that may help achieve it (i.e., the corresponding value is 1). Similarly, the antecedent set, $A(P_i)$ consists of the variable itself and other elements that may help in achieving it. The variables for which the interaction of these sets, $R(Pi) \cap A(Pi) = R(Pi)$, matches the reachability set, are considered the top-level variables of the ISM hierarchy. Each iteration of the level partition matrix identifies the hierarchy of variables in achieving other variables. The top-level variables do not assist in achieving other variables above their hierarchy level. Once the top levels are identified, they are separated, and the same process is repeated. The iteration

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

Table 3. *Canonical matrix*

VR	1	3	5	8	12	13	4	6	7	10	2	11	9	DRP	Level
3	1	1	1	1	1	1	1	1	1	1	1	1	1	*13*	I
5	1	1	1	1	1	1	1	1	1	1	1	1	1	*13*	I
8	1	1	1	1	1	1	1	1	1	1	1	1	1	*13*	I
12	1	1	1	1	1	1	1	1	1	1	1	1	1	*13*	I
13	1	1	1	1	1	1	1	1	1	1	1	1	1	*13*	I
1	1	1	1	1	1	1	1	1	1	1	1	0	1	*12*	I
4	1	1	1	1	1	0	1	1	1	1	1	1	1	*12*	II
6	1	1	1	1	1	0	1	1	1	1	1	1	1	*12*	II
10	1	1	1	1	1	0	1	1	1	1	1	1	1	*12*	II
7	0	0	1	0	0	0	1	1	1	1	1	1	1	*8*	II
2	1	1	1	1	1	1	1	1	1	0	1	1	1	*12*	III
11	0	0	1	0	0	0	1	1	1	1	0	1	1	*7*	IV
9	1	1	1	1	1	1	1	1	1	1	1	0	1	*12*	V
DEP	*11*	*11*	*13*	*11*	*11*	*8*	*13*	*13*	*13*	*12*	*12*	*11*	*13*		
Level	I	I	I	I	I	I	II	II	II	II	III	IV	V		

Note. 1, Technological maturity; 2, Perceived usefulness; 3, Capacities, skills, and competencies; 4, Management/operational systems; 5, Perceived risk; 6, Governance system; 7, Technical infrastructure; 8, Public values; 9, Trust; 10, Sociocultural elements; 11, Interoperability; 12, Policy priorities; 13, Regulations; VR, variable; DEP, Dependence power; DRP, Driving power.

process continues until all levels of partitions are established. The level partition matrix of each iteration is provided in the Supplementary Material. Table 3 displays the canonical matrix, which shows the level of each variable, along with their driving and dependence powers.

5.4. MICMAC diagram and ISM modeling

The MICMAC diagram visually categorizes variables based on their driving and dependency powers along the *x*- and *y*-axis. It contains four categories: autonomous, driving, dependent, and linkage. Autonomous variables have weak dependency and driving powers, and they are mostly disconnected from the system. Driving variables have higher driving power and weak dependency power, and they determine the changes in other variables without necessarily being dependent on changes in other variables. Dependent variables have higher dependency power and weak driving power, and they vary with changes in other variables without necessarily affecting the changes in other variables. Linkage variables are the most influential in the system with higher dependency and driving power. The cut-off point for each quadrant is arbitrarily designated by the number of variables. Since there are 13 variables, the cut-off point is designated at 6,5 on both axes. Figure 2 shows the positions of variables in the four quadrants.

The MICMAC diagram reveals that all variables are categorized as linkage, indicating that all identified variables hold significant influence in the adoption of advanced analytics in fraud detection. This finding implies that any changes in these variables could potentially result in systemic changes and impact the adoption strategies of AI and advanced analytics in fraud detection.

In the last stage, we developed the ISM based on the canonical matrix, and the direction of relationships identified in SSIM. The ISM in Figure 3 shows the direct and indirect relationships among variables. The direction of relationships is shown with an arrow. The interpretation of the model goes from bottom to up, where the variables at lower levels shape the perceptions regarding the variables in the following levels. Accordingly, the trust variable (variable 9) is based at the bottom of the ISM hierarchy, implying that the introduction of advanced analytics in fraud detection should start with evaluating the perceptions of trust determinants. The second level of hierarchy includes the interoperability variable (variable 11). The third level includes the perceived usefulness (variable 2) of advanced analytics in fraud detection. The fourth

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

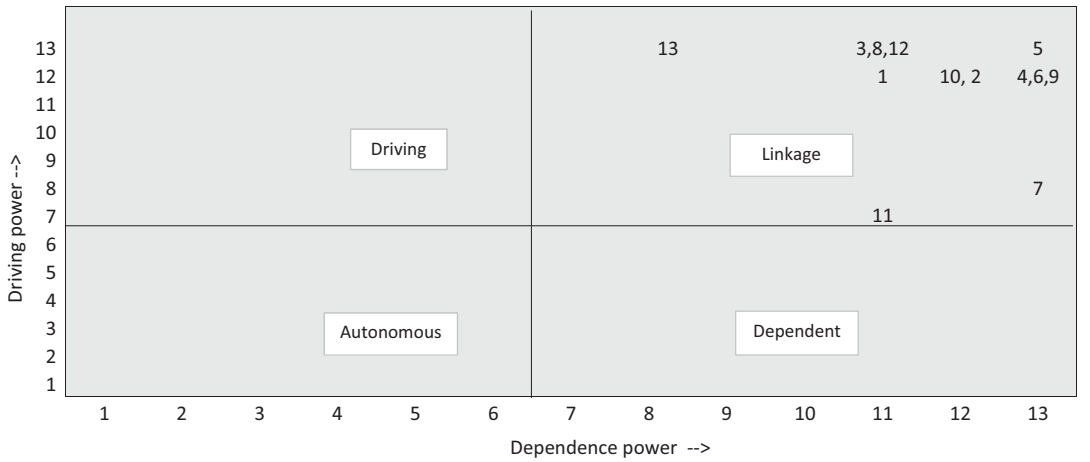

Figure 2. *MICMAC diagram.*

level is composed of the interrelationships between socio-cultural elements (variable 10), governance conditions (variable 6), technical infrastructure (variable 7), and management/operational systems (variable 4) in place. At the highest level, we observe a series of interrelationships between policy priorities (variable 12), regulation (variable 13), perceived risk (variable 5), public values (variable 8), the maturity of technologies (variable 1), and the capacity conditions (variable 3). In the following section, we interpret the directions of these relationships in terms of policy formulation processes concerning the use of advanced analytics in public policy processes.

6. Results

The thematic analysis of interview data has resulted in the identification of 13 variables that are perceived as influential in the adoption of advanced analytics in fraud detection. These variables capture various dimensions such as social, behavioral, organizational, institutional, regulative, and technological aspects. The analysis of the relationships between these drivers through ISM has revealed a hierarchical ordering that can aid in policy design. Furthermore, the MICMAC analysis showed that all these variables have strong dependence and driving powers, indicating their interdependencies and the complex nature of introducing data-driven predictive analytics in policy processes. Thus, any policy intervention should consider the interdependence and volatility of these variables.

However, the ISM analysis provides a pathway to simplify the adoption of advanced analytics in public policy processes. The model positions the "trust" factors as the starting point of policy formulation processes. The trust variable includes elements such as trust in the administration, technology, technology providers, system, and society itself. A study by Janssen et al. (2018) shows that the trustworthiness of e-government services is determined by cognitive factors, personal qualities (e.g., responsiveness, competence), prior experiences in the service area, and perceived prior knowledge of technology. However, the trust variable in our model goes beyond the trustworthiness of e-government services and includes the perceptions of stakeholders on citizen trust in the institutions responsible for collecting and managing personal data and citizens' trust in the role of technology in fraud detection processes. Therefore, it is crucial to integrate key stakeholders, including service producers and receivers, into the policy-design processes to address the key trust challenges associated with the use of advanced analytics.

After the trust variable, the ISM hierarchy positions interoperability as the second factor to consider in policy-design processes. The interoperability variable includes technical, organizational, regulatory, and semantic factors that determine the ease of data transfer between data providers and consumers. The

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

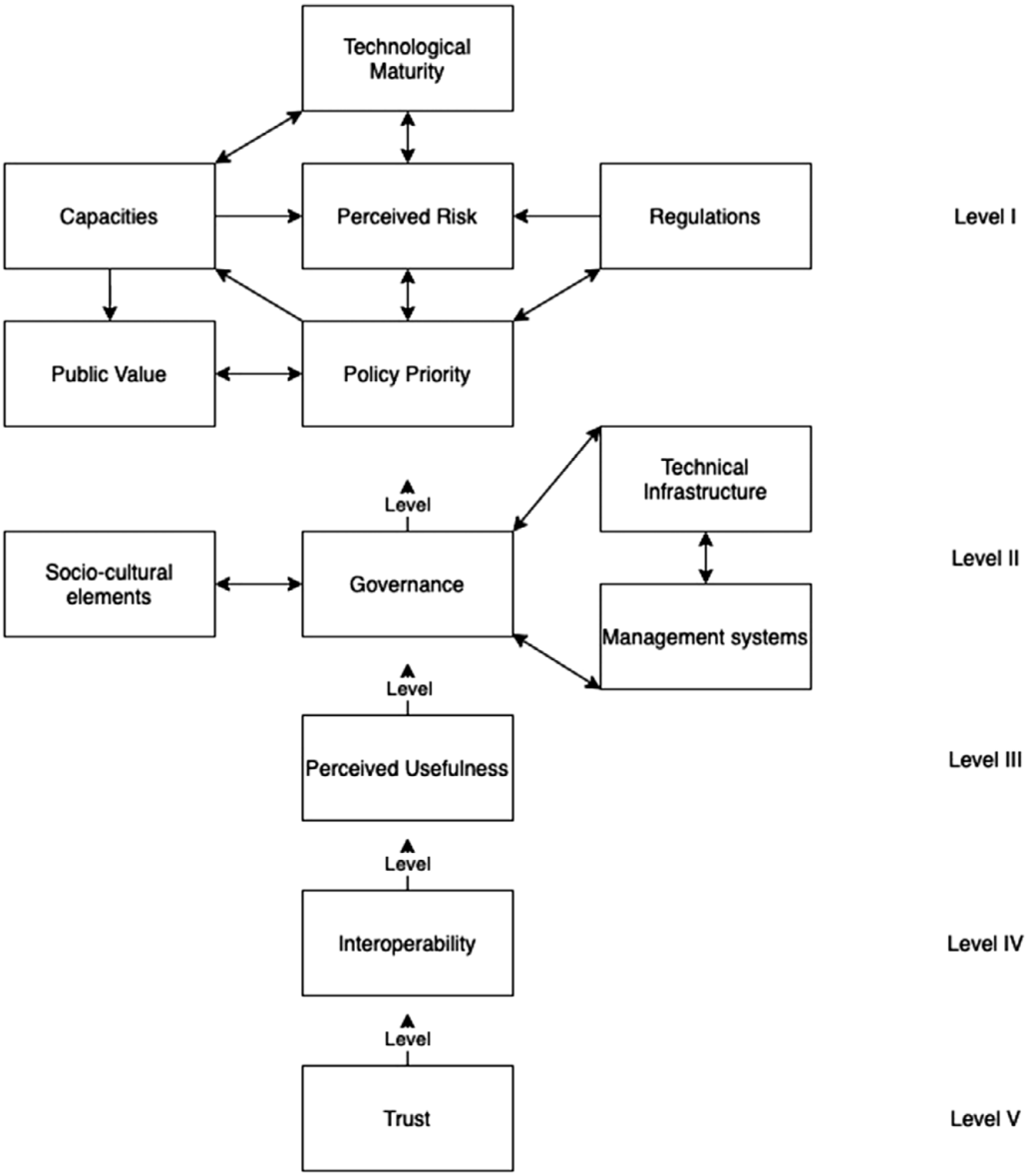

Figure 3. *ISM model.*

choices and factors affecting the trust dynamics in the use of advanced analytics are expected to shape the policy choices concerning interoperability considerations.

The third driver in the ISM hierarchy is the perceived usefulness of advanced analytics in fraud detection. This variable contains a wide range of perceptions about the perceived usefulness of digital transformation, including the automation of services, digitization of social security and taxation services, the use of advanced data collection and analysis methods in social security and taxation services, past experiences with the use of digital technologies/infrastructures in the fight against fraud, and the indirect added value of digitization in other related sectoral areas (e.g., development of better predictive medicines) on taxation and social security systems. Some of these factors are expected to be influenced by the choices and factors related to trust and interoperability conditions, while some cognitive factors (e.g., past experiences) may be influenced by the past or similar experiences in the use of advanced

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

analytics. The perceived usefulness of advanced analytics is expected to shape the scope and the extent of policy choices in the following rungs of the ISM hierarchy.

The next level of the ISM hierarchy (i.e., level II) is related to the notion of *data governance.* Variables related to governance systems, technical infrastructure, management/operational systems, and socio-cultural factors create a cluster of drivers that are closely interrelated to each other, and this stage in the policy design mostly captures the decisions concerning data governance mechanisms. The examination of the relationships suggests that policy choices concerning various modes of governance (e.g., multi-level governance, data governance, network governance, open governance) are directly influenced by the socio-cultural conditions concerning digitalization (e.g., digital divide, digital culture, willingness to share data), and the technical infrastructure conditions (e.g., security, quality of the database, data collection and analysis methods, software, computer maturity, and reliance on external actors) and management/operational systems (e.g., guidelines, rules and standards, principles, processes, and strategies) concerning the use of data.

The top level of the ISM hierarchy is composed of a cluster of six variables, namely technological maturity of advanced analytics in fraud detection; related capacities, skills, and competencies inside and outside of administration; relevant national and supranational regulations; public values concerning the use of advanced analytics in fraud detection; policy priorities in the use of advanced analytics in fraud detection; and the perceived risks associated with the use of advanced analytics in fraud detection. The ISM predicts that these variables are the most influential in the adoption of advanced analytics in fraud detection. Theoretically, this level can be best described by the concept of *digital governance.* According to the definition of Engvall and Flak (2022), digital governance is digital technology ingrained in structures or processes of governance and their reciprocal relationships with governance objectives and normative values. Digital governance includes the utilization of digital capabilities and involved a transformation of structures, processes, or normative values. Indeed, the sets of relationships identified by ISM show the interrelationships between normative values, capabilities, digital technology, governance objectives (or policy priorities in our model), and structure and processes of governance (or regulative framework in our model) in the use of advanced analytics. Thus, we assess that the model complies well with theoretical expectations.

Policy-design processes concerning the top tier of the hierarchy should consider the digital governance variables jointly and holistically. However, discernable subclusters of relationships can reduce the complexity of policy-design processes. For instance, one subcluster consists of regulation, policy priorities, and perceived risks. The direction of relationships indicates that the regulation variable (i.e., laws concerning data, social security, and taxation; laws concerning the justification of decisions in fraud detection; and transcending laws affecting the use of new digital technologies) directly affects the policy priorities and perceived risks in the use of advanced analytics in fraud detection. Meanwhile, perceived risks associated with control of data, and legal, societal, administrative, and democratic challenges, directly affect and are influenced by policy priorities. Policy priorities include elements related to the EU policies but also national policies on fraud detection, the level of political support in the use of advanced analytics in fraud detection, and other geopolitical aspects that can affect the policy decisions concerning the use of new digital technologies (e.g., impact of high-energy consuming technologies on the environment). Such policy priorities also influence the regulatory conditions that can affect the way advanced analytics are used in policy areas.

Another subcluster is observable among the variables of capacities, public value, and policy priorities. Administrative capacities, such as resources, digital skills, and training are expected to influence public values regarding the appropriateness of advanced analytics in fraud detection, including respecting the privacy of individuals and ensuring tax fairness. Meanwhile, these public value conditions influence policy priorities, and policy priorities, in turn, influence the capacity conditions.

A third subcluster exists between technological maturity, capacity conditions, and perceived risks. Technological maturity includes perceptions about the maturity of AI and machine learning systems, blockchain and distributed ledger technologies, and other fraud detection technologies leveraging advanced analytics, the convergence of these technologies, and how the maturity of these technologies

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

influences the bias and noise considerations. Technological maturity directly affects and is affected by capacity conditions and associated perceived risks.

A final observation concerns the position of perceived risks associated with the use of advanced analytics in fraud detection. The perceived risks variable is situated at the center of the interrelationships identified at the top level and is directly influenced by capacity conditions, technological maturity, regulations, and policy priorities. The close-knit relationships between perceived risks and technological, regulative, political, and capacity factors confirm the complexity of policy-design processes concerning the introduction of advanced analytics in public service processes.

7. Discussion

The interpretation of the model suggests two key takeaways for the policy designers interested in using advanced analytics in fraud detection. First, the model suggests that understanding the trust conditions, interoperability factors, and perceived usefulness of advanced analytics for the application area needs to be assessed before developing policy strategies for data governance and digital governance. Second, the high interdependencies among all drivers confirm the complexity surrounding the introduction of advanced analytics in public policy processes and suggest that digital transformation policies and their effectiveness in public policy areas should be subject to periodic and cyclical policy evaluations.

In developing the model, we have benefited from the behavioral and structural theories to categorize the elements identified through thematic analysis. Although these strands of theories are useful in explaining why users adopt or do not adopt certain technologies or how administrative processes influence the way certain technologies are adopted, they have limited explicability to support policy-design processes in digital transformation. Our model fills this gap by adding further levels of abstraction in explaining how various drivers affect technology adoption in the public sector context.

As a theoretical contribution, the model brings together behavioral variables (e.g., perceived benefits, perceived risks) with organizational forms and institutional arrangements in an analytical way and by creating hierarchies of importance. For instance, the model suggests that conditions concerning trust and interoperability drive the perception concerning the perceived benefit of the proposed solution. This is indeed compatible with the prior work of Shin (2020) which suggests that trust influences the perceived benefit of technology and the subsequent behavior of the user.

Moreover, through this model, it would be possible to test the causal relationships among variables and to develop propositions to test the impact of policy innovation processes on actual technology adoption. For instance, the model can serve as the basis of a structural equation model to measure the direct and indirect influences among drivers. Furthermore, the model can be used to measure the effectiveness of various policy innovations (e.g., trust-generating activities, improving data interoperability, capacity-building activities) in actual technology adoption.

At a policy-design level, our model facilitates a holistic approach by integrating system design considerations into policy-design processes and assessing the political and administrative feasibility of different technical solutions for introducing advanced analytics in fraud detection. In our model, we identified five hierarchical layers that policy designers need to focus on introducing advanced analytics in fraud detection: (a) trust layer, (b) interoperability layer, (c) perceived benefits layer, (d) data governance layer, and (e) digital governance layer. This layered approach provides a comprehensive view of adoption challenges related to new digital technologies. For example, according to our model, a proposed solution should address the following questions in sequence: (a) Can the proposed solution enhance trust in the use of algorithms in fraud detection? (b) Is the proposed solution interoperable with the existing technical, organizational, and institutional conditions in data sharing? (c) Is the proposed solution compatible with the existing systems and policies of data governance? and (d) Is the proposed solution compatible with related digital governance conditions, including the technological maturity of the proposed solution, the perceived risks, and the organizational capacities, political, and regulatory conditions? Through this inquiry, policy and technical designers can assess the concrete effects and impacts expected on fraud detection systems by the proposed AI-based solution.

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

However, there are some caveats to the interpretation of our model for other application areas. The drivers and their interrelationships are dependent on the perceptions of the public and private actors, which are influenced by contextual and sector-specific conditions. In our research, contextual factors were shaped by the institutional framework of the Belgian state in the taxation and social security domains. Similar cross-sectoral or cross-country research can provide deeper insight into the robustness of the model and check whether differences in socio-administrative contexts (e.g., trust, public values, regulations) affect the presumed relationships in the model.

Moreover, our model was developed specifically for advanced analytics based on AI and fraud detection. Different data-driven technologies, such as AI, IoT, and blockchain, may have varying impacts on user and stakeholder perceptions and associated public value provisions. For instance, blockchain may be associated more with creating trust in the information management system, while AI may be perceived as a tool to increase the policy efficiency and effectiveness. Furthermore, different technological configurations may invoke value trade-offs concerning transparency, efficiency, effectiveness, and accountability. The way technologies are used in organizational processes may lead to different interpretations of how drivers influence each other. Therefore, we recommend further research to explore the impact of separate technologies and the variances in their technological configurations to gain a better understanding of how different digital technologies affect technology adoption in public administration.

8. Conclusion

Our findings were based on the use of advanced analytics in fraud detection and relied on the perception of the Belgian stakeholders. However, the theoretical conformity of our findings with other studies on technology adoption in public sector organizations suggests that we can draw some lessons for digital transformation strategies concerning new digital technologies (Tan and Crompvoets, 2022). In summary, the following points are crucial for developing reliable and pertinent digital transformation strategies: (a) trust and interoperability conditions, (b) the perceived benefits of digital technologies in administrative systems and policy objectives, (c) the match of socio-cultural conditions with the characteristics of the digital technologies and their ease of adoption in the existing data governance processes, and (d) the interplay between policy priorities, technological maturity, associated resources and digital skills in the digital governance domain, comprehensiveness of the regulative framework, public values, and perceived risks associated with the implications of digital technologies for public administration and society.

Our model suggests that policy designers need to assess the challenges in each layer successively to have a holistic view of underlying challenges in technology adoption and the combined needs of policy design and system design. We recommend repeating this research in other sectoral and country settings to assess the generalizability of the model. The growing discrepancies between the EU, China, British, and North American data privacy laws, along with technology anti-trust laws, make the regulative and institutional context crucial in indicating the theoretical boundaries of the proposed model for the applicability of data-driven technologies and the scope of available data. Furthermore, lower tiers of government (e.g., district or local level) or other sectors (e.g., health) may face different sets of constraints toward access, development, and deployment of such data-driven technologies. Cross-sectoral, cross-level, and cross-country analyses can help to test the generalizability of the model and may lead to a theory of digital governance.

Supplementary material. The supplementary material for this article can be found at https://doi.org/10.1017/dap.2023.22.

Funding statement. This work was supported by the Belgian Federal Science Policy Office (BELSPO) under research grant B2/191/P3/DIGI4FED. The funder had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing interest. The authors declare no competing interests exist.

Author contribution. Conceptualization: E.T.; Data curation: E.T.; Formal analysis: E.T.; Funding acquisition: E.T.; Investigation: M.P.J., A.S., T.T., B.K., M.S., L.B., P.W.; Methodology: E.T., M.P.J., A.S., T.T., B.K.; Project administration: E.T.; Writing—original draft preparation: E.T.; Writing—review and editing: M.P.J., A.S., T.T., B.K., M.S., L.B., P.W.

Data availability statement. The data that support the findings of this study are available from KU Leuven. Restrictions apply to the availability of these data, which were used under license for this study. Data are available from the authors with the permission of BELSPO.

References

Ahmad M, **Tang X-W**, **Qiu J-N and Ahmad F** (2019) Interpretive structural modeling and MICMAC analysis for identifying and benchmarking significant factors of seismic soil liquefaction. *Applied Sciences 9*(2), 233. https://doi.org/10.3390/app9020233

Ahonen P and Erkkilä T (2020) Transparency in algorithmic decision-making: Ideational tensions and conceptual shifts in Finland. *Information Polity 25*(4), 419–432.

Ajzen I (1991) The theory of planned behavior. *Organizational Behaviour and Human Decision Processes 50*(2), 179–211.

Alshallaqi M (2022) The complexities of digitization and street-level discretion: A socio-materiality perspective. *Public Management Review*, 1–23. https://doi.org/10.1080/14719037.2022.2042726.

Ananny M and Crawford K (2018) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society 20*(3), 973–989.

Booth R (2019) Benefits system automation could plunge claimants deeper into poverty. *The Guardian*, October 14.

Braun V and Clarke V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology 3*(2), 77–101.

Bullock J, **Young M and Wang YF** (2020) Artificial intelligence, bureaucratic form, and discretion in public service. *Information Polity 25*(4), 491–506.

Busuioc M (2021) Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review 81*, 825–836. https://doi.org/10.1111/puar.13293

Chander A (2017) The racist algorithm? *Michigan Law Review 115*(6), 1023–1045.

Compeau DR and Higgins CA (1995) Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly 19*(2), 189–211.

Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly 13*(3), 319–340. http://doi.org/10.2307/249008

Davis FD, **Bagozzi RP and Warshaw PR** (1992) Extrinsic and intrinsic motivation to use computers in the workspace. *Journal of Applied Social Psychology 22*(14), 1111–1132.

Dawes SS (2009) Governance in the digital age: A research and action framework for an uncertain future. *Government Information Quarterly 26*(2), 257–264.

De Roux D, **Perez B**, **Moreno A**, **del Pilar Villamil M and Figueroa C** (2018) Tax fraud detection for under-reporting declarations using an unsupervised machine learning approach. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '18)*. New York: Association for Computing Machinery, pp. 215–222. https://doi.org/10.1145/3219819.3219878

Dickinson H, **Smith C**, **Carey N and Carey G** (2021) Exploring governance tensions of disruptive technologies: The case of care robots in Australia and New Zealand. *Policy and Society 40*(2), 232–249. https://doi.org/10.1080/14494035.2021.1927588

Dwivedi YK, **Rana NP**, **Janssen M**, **Lal B**, **Williams MD and Clement M** (2017) An empirical validation of a unified model of electronic government adoption (UMEGA). *Government Information Quarterly 34*(2), 211–230.

Engvall T and Flak LS (2022) Digital governance as a scientific concept. In Charalabidis Y, Flak LS and Viale Pereira G (eds), *Scientific Foundations of Digital Governance and Transformation. Public Administration and Information Technology*, Vol. *38*. Cham: Springer. https://doi.org/10.1007/978-3-030-92945-9_2

Exmeyer PC and Hall JL (2022) High time for a higher-level look at high technology: Plotting a course for managing government information in an age of governance. *Public Administration Review 83*(2), 429–434. https://doi.org/10.1111/puar.13513

Fathema N, **Shannon D and Ross M** (2015) Expanding the technology acceptance model (TAM) to examine faculty use of learning management systems (LMS). *Journal of Online Learning and Teaching 11*(2), 210–233.

Fereday J and Muir-Cochrane E (2006) Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods 5*(1), 80–92.

Fishbein M and Ajzen I (1975) *Belief, Attitude, Intention, and Behaviour: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Fountain JE (2001) *Building the Virtual State: Information Technology and Institutional Change*. Washington, DC: Brookings Institution Press.

Freeman Engstrom D, **Ho DE**, **Sharkey C and Cuellar M-F** (2020) *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies.* Administrative Conference of the United States, February 2020.

Grafton C (2003) "Shadow theories" in Fountain's theory of technology enactment. *Social Science Computer Review 21*(4), 411–416. https://doi.org/10.1177/0894439303256567

Grimmelikhuijsen S (2022) Explaining why the computer says no: Algorithmic transparency affects the perceived trustworthiness of automated decision-making. *Public Administration Review 83*, 241–262. https://doi.org/10.1111/puar.13483

Hanna KT, **Burns E and Presslar E** (2022) *Advanced Analytics. Techtarget.* Available at https://www.techtarget.com/searchbusinessanalytics/definition/advanced-analytics#:~:text=Advanced%20analytics%20is%20a%20data,a%20variety%20of%20data%20sources (accessed 15 October 2022).

Hughes DL, **Rana NP and Dwivedi YK** (2020) Elucidation of IS project success factors: An interpretive structural modeling approach. *Annals of Operations Research 285*, 35–66. https://doi.org/10.1007/s10479-019-03146-w

Janssen M, **Luthra S**, **Mangla S**, **Rana NP and Dwivedi YK** (2019) Challenges for adopting and implementing IoT in smart cities. *Internet Research 29*(6), 1589–1616.

Janssen M, **Rana NP**, **Slade EL and Dwivedi YK** (2018) Trustworthiness of digital government services: Deriving a comprehensive theory through interpretive structural modeling. *Public Management Review 20*(5), 647–671. http://doi.org/10.1080/14719037.2017.1305689

Kleizen B, **van Dooren W and Verhoest K** (2022) Trustworthiness in an era of data analytics: What are governments dealing with and how is civil society responding? In TanE and CrompvoetsJ (eds), *The New Digital Era Governance*. Wageningen: Wageningen Academic Publishers, pp. 179–199. https://doi.org/10.3920/978-90-8686-930-5_6

Lal R and Haleem A (2009) A structural modelling for E-governance service delivery in rural India. *International Journal of Electronic Governance 2*(1), 3–21. http://doi.org/10.1504/IJEG.2009.024962

Leiman T (2021) Law and tech collide: Foreseeability, reasonableness and advanced driver assistance systems. *Policy and Society 40*(2), 250–271. https://doi.org/10.1080/14494035.2020.1787696

Maciejewski M (2017) To do more, better, faster and more cheaply: Using big data in public administration. *International Review of Administrative Sciences 83*(1), 120–135. https://doi.org/10.1177/0020852316640058

Meijer A, **Lorenz L and Wessels M** (2021) Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems. *Public Administration Review 81*(5), 837–846. https://doi.org/10.1111/puar.13391

Mensah IK, **Zeng G and Luo C** (2020) E-government services adoption: An extension of the unified model of electronic government adoption. *SAGE Open 10*(2). https://doi.org/10.1177/2158244020933593

Meuwese A (2020) Regulating algorithmic decision-making one case at the time: A note on the Dutch 'SyRI' judgment. *European review of digital administration & law 1*(1), 209–212.

Moore GC and Benbasat I (1996) Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end-users. In KautzJ and Pries-HegeK (eds), *Diffusion and Adoption of Information Technology*. London: Chapman and Hall, pp. 132–146.

Neumann O, **Guirguis K and Steiner R** (2022) Exploring artificial intelligence adoption in public organizations: A comparative case study. *Public Management Review*, 1–27. https://doi.org/10.1080/14719037.2022.2048685

OECD (2021) *Tax Administration 2021: Comparative Information on OECD and Other Advanced and Emerging Economies*. Paris: OECD Publishing. https://doi.org/10.1787/cef472b9-en

Orlikowski WJ (1992) The duality of technology: Rethinking the concept of Technology in Organizations. *Organization Science 3*(3), 1–32. https://doi.org/10.1287/orsc.3.3.398

Orlikowski WJ (2000) Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science 11*(4), 404–428. https://doi.org/10.1287/orsc.11.4.404.14600

Radu R (2021) Steering the governance of artificial intelligence: National strategies in perspective. *Policy and Society 40*(2), 178–193. https://doi.org/10.1080/14494035.2021.1929728

Sandvig C, **Hamilton K**, **Karahalios K and Langbort C** (2016) Automation, algorithms, and politics| when the algorithm itself is a racist: Diagnosing ethical harm in the basic components of software. *International Journal of Communication 10*, 4972–4990.

Shin D (2020) User perceptions of algorithmic decisions in the personalized AI system: Perceptual evaluation of fairness, accountability, transparency, and Explainability. *Journal of Broadcasting & Electronic Media 64*(4), 541–565. http://doi.org/10.1080/08838151.2020.1843357

Shin D (2022) The perception of humanness in conversational journalism: An algorithmic information-processing perspective. *New Media & Society 24*(12), 2680–2704. https://doi.org/10.1177/1461444821993801

Shin D, **Lim JS**, **Ahmad N and Ibahrine M** (2022a) *Understanding User Sensemaking in Fairness and Transparency in Algorithms: Algorithmic Sensemaking in Over-the-Top Platform.* AI & Society. https://doi.org/10.1007/s00146-022-01525-9

Shin D, **Zhong B and Biocca F** (2020) Beyond user experience: What constitutes algorithmic experiences? *International Journal of Information Management 52*, 102061. https://doi.org/10.1016/j.ijinfomgt.2019.102061

Shin D, **Zhong B**, **Biocca F and Azmat R** (2022b) In platforms we trust? Unlocking the black-box of news algorithms through interpretable AI. *Journal of Broadcasting & Electronic Media 66*(2), 235–256. http://doi.org/10.1080/08838151.2022.2057984

Sun TQ and Medaglia R (2019) Mapping the challenges of artificial intelligence in the public sector: Evidence from public healthcare. *Government Information Quarterly 36*(2), 368–383. https://doi.org/10.1016/j.giq.2018.09.008

Taeihagh A (2021) Governance of artificial intelligence. *Policy and Society 40*(2), 137–157. https://doi.org/10.1080/14494035.2021.1928377

Tan E and Crompvoets J (2022) *The New Digital Era Governance: How New Digital Technologies Are Shaping Public Governance*. Wageningen: Wageningen Academic Publishers. https://doi.org/10.3920/978-90-8686-930-5

Tan E, **Mahula S and Crompvoets J** (2022) Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly 39*(1), 101625. https://doi.org/10.1016/j.giq.2021.101625

Tan SY and Taeihagh A (2021) Governing the adoption of robotics and autonomous systems in long-term care in Singapore. *Policy and Society 40*(2), 211–231. https://doi.org/10.1080/14494035.2020.1782627

Tangi L, **Janssen M**, **Benedetti M and Noci G** (2021) Digital government transformation: A structural equation modeling analysis of driving and impeding factors. *International Journal of Information Management 60*, 102356. https://doi.org/10.1016/j.ijinfomgt.2021.102356

https://doi.org/10.1017/dap.2023.22 Published online by Cambridge University Press

Thompson RL, **Higgins CA and Howell JM** (1991) Personal computing: Toward a conceptual model of utilization. *MIS Quarterly 15*(1), 124–143.

Tombal T, **Willem P and Terwangne CD** (2022) Legal framework for the use of artificial intelligence and automated decision-making in public governance? In TanE and CrompvoetsJ (eds), *The New Digital Era Governance*. Wageningen: Wageningen Academic Publishers, pp. 141–178.

Ulnicane I, **Knight W**, **Leach T**, **Stahl BC and Wanjiku W-G** (2021) Framing governance for a contested emerging technology: Insights from AI policy. *Policy and Society 40*(2), 158–177. https://doi.org/10.1080/14494035.2020.1855800

Van Vlasselaer V, **Eliassi-Rad T**, **Akoglu L**, **Snoeck M and Baesens B** (2017) GOTCHA! Network-based fraud detection for social security fraud. *Management Science 63*(9), 3090–3110.

Venkatesh V and Davis FD (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science 46*(2), 186–204. http://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh V, **Morris MG**, **Davis GB and Davis FD** (2003) User acceptance of information technology: Toward a unified view. *MIS Quarterly 27*(3), 425–478. http://doi.org/10.2307/30036540

Venkatesh V, **Thong J and Xu X** (2012) Consumer acceptance and user of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly 36*(1), 157–178.

Vogl TM, **Seidelin C**, **Ganesh B and Bright J** (2020) Smart technology and the emergence of algorithmic bureaucracy: Artificial intelligence in UK local authorities. *Public Administration Review 80*(6), 946–961. https://doi.org/10.1111/puar.13286

Wang G, **Xie S and Li X** (2022) Artificial intelligence, types of decisions, and street-level bureaucrats: Evidence from a survey experiment. *Public Management Review* 1–23. https://doi.org/10.1080/14719037.2022.2070243

Warfield JN (1974) Developing interconnection matrices in structural modeling. *IEEE Transactions on Systems, Man, & Cybernetics 1*, 81–87.

West DM (2021) *Using AI and Machine Learning to Reduce Government Fraud.* Brooking Institute Report, September 10.

Willems J, **Schmid MJ**, **Vanderelst D**, **Vogel D and Ebinger F** (2022) AI-driven public services and the privacy paradox: Do citizens really care about their privacy? *Public Management Review*, 1–19. https://doi.org/10.1080/14719037.2022.2063934

Wilson C and Broomfield H (2022) Learning how to do AI: Managing organizational boundaries in an intergovernmental learning forum. *Public Management Review* 1–20. https://doi.org/10.1080/14719037.2022.2055119

Cite this article: Tan E, Petit Jean M, Simonofski A, Tombal T, Kleizen B, Sabbe M, Bechoux L and Willem P (2023). Artificial intelligence and algorithmic decisions in fraud detection: An interpretive structural model. *Data & Policy*, 5: e25. doi:10.1017/dap.2023.22