Deep Science Publishing
https://doi.org/10.70593/978-93-49910-54-6_11

DeepScience
Open Access Books

Chapter 11: Safeguarding data integrity and trust in artificial intelligence-augmented government financial ecosystems

11.1 Introduction

This paper presents a cybersecurity protocol relevant to AI-enhanced government financial services, particularly governmental payment services such as disbursing social welfare payments, public sector payrolls, or stimulating the economy with rebate payments dispersed to taxpayers. This paper posits that an AI-enhanced government financial service environment must prioritize cybersecurity against external and internal adversarial threats. The need for a cybersecurity protocol supporting data integrity and user trust in modern public finance threatens the ability and authority of governments to ensure or regulate the use of such advanced systems. Data management risks leading to the deterioration of government fiscal capabilities and authorities highlight the need for a tailored data operations protocol. As governments delegate the task of delivering public service robustly during naturally occurring crisis events, natural disasters, market failures, pandemics, or war, to the broader market, a trusted data operations system using AI-enabled systems to create government services must be protected against data integrity and trust risks (Albrecht & Lang, 2023; Huang & Yu, 2022; Lee & Lee, 2020).

This research paper investigates possible supervisory measures and protections that existing frameworks establish for enabling a government to safeguard the integrity, security, and trust of data operation systems in peace or crisis times. To achieve this goal, the paper presents an overview of the relevant financial services – along with the encompassed threats to data integrity, systems security, and stakeholder trust – that AI technology could enhance. The objective is to show that no data integrity and security roadmap enhances the trust of all stakeholders in the AI-augmented ecosystem. Section

1.1 introduces the financial landscape likely enhanced by AI technology and discusses the emerging threats that AI poses to the integrity of existing financial transactional flows. Section 2 analyzes the governance framework enforcing the protection of current government services. Section 3 proposes a tailored mechanism made for an AI-augmented transaction service ecosystem, while Section 4 concludes (Kshetri & Voas, 2021; World Economic Forum, 2021).

11.1.1. Overview of the Financial Landscape Enhanced by AI

Artificial Intelligence (AI) is revolutionizing various sectors of the economy, including the global financial system. Machine Learning (ML) tools make financial systems more intelligent by enhancing the predictive management of risk and return, as well as improving the customer experience through chatbots. From dynamic pricing to algorithmic trading, liquidity management, and risk management, AI makes the financial ecosystem smarter and more resilient. Banks, lenders, and other financial institutions are adopting AI algorithms to assess the creditworthiness of customers efficiently while also avoiding bias. Investors are harnessing AI to improve their investment strategies, portfolio management, and performance evaluation, as it helps them to predict market fluctuations and economic crises. AI enjoys an edge over traditional econometric models, given its ability to identify patterns that cannot be detailed by humans on a large scale. Customers are also experiencing new financial products and services offered by FinTechs that are leveraging AI.

While AI has the potential to add great value to financial markets and institutions, the use of AI also introduces several risks and challenges, especially concerning consumer trust. High-stake decisions made by lenders and insurers hinge on the output of AI models, including those that are not explainable. Additionally, AI-driven trading strategies increase market volatility and lead to economic crises if the macro-economic fundamentals are ignored. With AI-enhanced customer experiences come risks regarding potential bias resulting from partial training data. Algorithmic bias may affect services, such as digital resumes, job interviews, and loan applications, leading to negative impacts on hiring, trading, lending, and credit. These challenges are aggravating the challenges associated with the prevention of money laundering, especially in cross-border transactions, which are already becoming more ubiquitous with the advent of cryptocurrency.

11.2. Understanding AI-Augmented Financial Ecosystems

AI machines or systems augment the human-in-the loop decision making process in an effort to achieve better outcomes. In the case of government financial systems, this

process becomes quite complex by integrating various macro and microeconomic data, various technologies and integration with public and private institutions.

1. Definition and Scope We define an AI-augmented financial ecosystem in a government setting as, “A system that holistically incorporates both human and AI agents to perform economic functions for the government”. Here we focus only on man and machine governance functions, and do not address the social function of public finance. Government financial systems deal with the intricacies of management of a country’s funds, its accounting and auditing policies, and its financial regulations. Role of AI in Financial Systems Governments with their central banks issue money, promote price stability, implement wealth, income, and trade policies, and invoke finance and currency regulations. These policies and their related mechanisms are hard to model and implement fully given the silent mechanics involved. AI/ML can help augment the human-in-the-loop systems, though they cannot fully replace the complex functions.

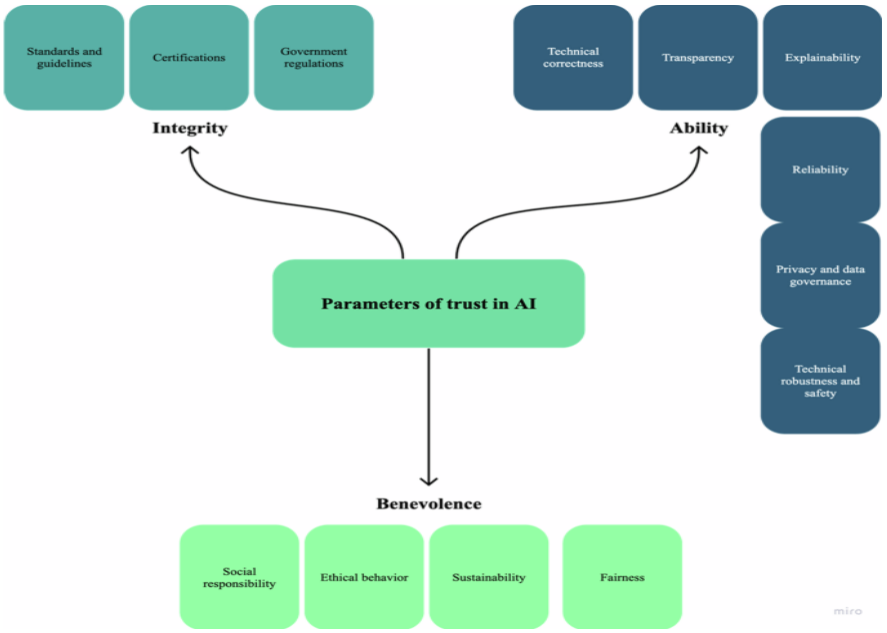

Fig 11.1: Trust in AI

2. Components of AI in Financial Systems Machine Learning and Artificial Intelligence Algorithms: These algorithms find ways to continuously learn from data and optimize functions that describe the behavior of complex systems in a black box fashion. AI involves pattern finding, solving problems, and minimizing probabilities of error through a technology called Neural Networks. Neural networks can be fed large amounts of data with its parameters tuned to predict with good accuracy a function(s) whose form is not known in advance. Such predictions are then used for decision-making.

11.2.1. Definition and Scope

Many aspects of people's daily lives now involve some form of interaction with AI, from the leisure and entertainment enjoyed while streaming videos, to the variety of tools offered to aid daily life, work, and travel decisions. And now, particularly in the wake of the pandemic, communication, including government communications, takes place online, using traditional email and up-and-coming tools that aim to mitigate challenges with response time and accuracy. However, as governments and constituents increasingly employ AI across the various functions of the financial ecosystem—such as tax and trade, spending, investing, and kiting—cybersecurity becomes a top priority in maintaining trust and the integrity of the data and outcomes being generated within this ecosystem. While there have been many advancements in AI, it is woefully inadequate in helping ensure data accuracy and quality within the augmented ecosystem. AI language model results can be falsely persuasive, resulting in an unquestioned dissemination of biased, incorrect, and even fabricated information, which trust is being placed into and relied upon to answer important, life-changing questions. Using AI for important government functions, which already struggle with accuracy and bias, could create grave national security risks and adversely impact citizen lives through the destruction of confidence in the financial ecosystem.

For example, if an individual or entity were to receive government tax and business information that is generated incorrectly due to prompt issues with an LLM, or is outdated and biased due to being used only as a predictive model, that individual or entity could see adverse effects to their social standing or investment choices through the dissemination and reliance upon faulty predictive results shared. Similarly, if a citizen has shown up at a government office with responses to questions fed into a chatbot for an appointment, they could be receiving incorrect information and waste valuable time in their day when a cumbersome LLM could be implemented to mitigate such issues.

11.2.2. Components of AI in Financial Systems

AI contributions, or ‘components’ of AI, offer a unique perspective, developing an understanding of both the actual capabilities of AI for task automation, and the complementary capabilities of its human counterpart — therefore suggesting where, in the future, this equilibrium of actions should lie. A brief overview of each of these unique AI capabilities for financial automation is provided in the following sub-sections. Automation of any task requires some degree of recognition to enable an interpretation of its context. This is AI’s most mature capability, from optical character recognition of a variety of documents to advanced applications of automated reading of credit, debit and prepaid cards, biometrics for validating identity, and availability of both high

resolution and low cost images and cloud solutions for image enrichment, all require some form of recognition. Image and object recognition are central to augmenting government capabilities for combating money laundering and fraud prevention, making it very difficult to deposit or transfer cash through ATMs; validating a suspect's identity during a digital video conference; for facial recognition at border control along with document authentication; and penalizing tax evasion through image recognition of luxury yachts or private jets. Over time, tasks that require some level of language interpretation, both spoken and written, have also been automated to varying effects. AI would take on the role of transcription, enabled by speech-to-text automated transcription ICs; the interpretation of intention, through rudimentary sentiment analysis of both incoming and outgoing communication flows; the enriching of existing documents with summarization, translation, and question answer features. The vision is developing ‘robots for process automation’ specific to government operations over time, though much of the actual development of these tailored bots is currently being done by corporate partners for government agencies.

11.2.3. Benefits of AI Integration

Loss and integrity management, AML, and risk control laws are becoming stricter for the finance and the government treasury. Meticulous case management at each level of anomaly detection and investigation is key to assuring quality of service and avoiding penalties. AI methods, integrated as auto-resolvers for administrative workloads, could scale up asset management as well as fraud risk detection. Increasingly complex rules or additionally implemented ‘what-if’ models could then be applied to higher risk areas, focusing increased scrutiny and attention of human experts where needed. Solutions are needed for the very large number of transactions, however few anomalies these may represent. More than half of all government transactions are performed or supported through digital media – bank transfers, credit and debit cards, online purchases, electronic transfers of funds, internet payments, and pay-at-the-pump options for gas services.

Fraud risk detection could be done in two ways. First, transaction risk could be estimated at real-time, online access – an immediate positive resolution would allow for an instant transaction. Otherwise would come an automatic unpaid or auto-rejected transaction. Second, batch offline detection, where subsequent checks would block reported transactions, send them to administrative units for case resolution, prior to completion and settlement. The methodologies used in detection rely on using different predictive modelling and risk algorithms for transaction scoring. These offer tuning parameters specific to each financial subsector, link detection to data attributes, set sensitivity measures, or use self-learning models for improved transaction risk detection. As a

general trend, AI allows detecting not just the large events, but also the very small, and to continuously learn to recognize changing behavioral patterns, rather than just detect anomalies based on past history.

11.3. Data Integrity in Financial Ecosystems

1. Concept of Data Integrity

The concept of data is the foundation of a commensal ecosystem, economy, and society. Data are everyday expressions of life around us in communities, ecosystems, economies, and the world. Data provides the basis for decisions, causative effects, mandates, regulations, economic values, and revenues. Without valid, trustworthy data the concepts of digital economies do not apply. In financial ecosystems, the legal frameworks, mandates for transparency, and accountability procedures require access to data as part of ethical and responsible practices in data sharing and re-use. The combined values of private and public data form the models of trust within which citizens engage with government agencies with respect to payments, regulation investments, revenues and spending. The realities of dependency on each other, the mutual objectives of improving financial state and prosperity require public agents to trust the integrity of the data providing input into the budget models if the financial ecosystem is to flourish.

2. Challenges to Data Integrity

As part of the movement toward digital transformation, governments have shifted emphasis to digital payments; the challenge is to create trust in both payments and the systems that generate, transmit and secure data. Organizations must understand the risks they face and take steps to mitigate them. Mitigation involves protecting the systems and devices responsible for data integrity — the endpoint devices used by local bureaus and taxpayers, the payment processor responsible for moving funds, the internal information systems involved in verifying and processing the payment, local bank systems issuing and clearing the check.

3. Impact of Data Breaches

The risk of incomplete, inaccurate, or misused data integrity exists at every step along this chain, and even a seemingly minor breach can introduce delays, stoppages, or errors that cost local governments substantial time and money. A data breach, ransomware attack, or social engineering incident may strain the integrity and trust that allow the financial ecosystem to function. But data is more than just assets, it must also be the rationale and motivation for the community to cooperate, to provide the revenue in taxes, fees and fines which allows the government to maintain and improve the quality of life in society.

11.3.1. Concept of Data Integrity

In this chapter, we review issues around data integrity in the operational context of financial ecosystems, discuss the role of such ecosystems, and discuss issues like trust, compliance, and cybersecurity, central to the discussion of data integrity in such ecosystems. We then discuss these themes in the context of a Business Intelligence and Analytics Unit, exploring the analytics and compliance role of a financial institution as well as challenges in developing a data integrity strategy in consultation with stakeholders, data users as well as data generators.

Data integrity is considered a constituent property of data quality. Data quality is the totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implicit needs. Note that while integrity is an essential property of data, it is not the sole property that determines that data can satisfy our needs; it is possible for integrity errors to exist without any consequence on the usability of the data because such integrity constraints may not be essential to the intended use of the data. But data integrity generally refers to the aspect of data quality that is concerned with ensuring that the data is not contravening some complex user-defined rules and constraints and ensuring that the data is true and accurate. Note that it is possible for data to be consistent, that is to satisfy all integrity constraints, but be meaningless in context; data may satisfy all structural constraints, but may still be incorrect. Data may satisfy all context-sensitive semantic constraints but can still be incorrect; for these reasons, data integrity is a more difficult concept to quantify.

11.3.2. Challenges to Data Integrity

Data integrity refers to the certainty that the data has not been changed, forged, or otherwise manipulated. It also often refers to the internal consistency and accuracy of data. Despite diverse interpretations of data integrity and differences in terminology used, the topic is of paramount importance, especially as the amount of stored data increases, and as more users and applications access and process that data. Once breached, data integrity can have dramatic consequences for organizations, businesses, and individuals. Cybercriminals can destroy, change, or manipulate data of any kind. Integrity of financial data is of particular importance at a time when the movement of money occurs at light speed, with humans seldom present to authorize transactions or double check accuracy. Data integrity is critical in any organization but particularly ones involved in payment processing. Financial organizations process immense amounts of transactions every single day. Each transaction requires the move of funds from one area to another and changes the overall financial standing of a customer, and many can take place simultaneously. Trust that this data will remain intact and accurate is essential. Loss of funds or a double-charging customer could result in financial ruin for many trust

investors or customers. Financial organizations conduct business on trust — trust of accuracy, trust of security, and trust of continued service. Maintaining data integrity means that the data remains authentic and is free from tampering. If this integrity is ever compromised, then the information is useless. Events may manipulate data intentionally or inadvertently. Attacks such as network intrusion, trojan horses, and subverting elevation of privilege prevention technologies, as well as system malfunctions such as software bugs or misconfigurations may disrupt data integrity. An attacker could therefore take action for the purpose of changing, corrupting, or permanently deleting data.

11.3.3. Impact of Data Breaches

The relevance of data integrity is at an all-time high considering how rapidly trust is eroding in AI-augmented critical systems. Data integrity underpins the trustworthiness of elections, criminal justice systems, and the organization's most valuable data assets: its customers. The importance of data integrity within an organization cannot be overstated. Poor data integrity not only can lead to wasted resources, but it also can lead to inaccurate reporting that in turn can influence executive and investor decision making. Consider also how difficult it can be to ensure data integrity among third-party providers when multiple information streams are being integrated into one system. Organizations with a high number of third-party providers see a significant increase in actual threats. Also, organizations that have been breached by ransomware and are slow to recover also begin seeing data integrity issues arise, or generally poor data, due to the stress on internal staff as the organization struggles to return to normal operations.

The full impact of poor data integrity can sometimes take months to surface as the organization begins to try to utilize the corrupted data for reporting. For organizations that are attempting to comply with regulations that require compliance, the penalties can be significant. In addition to financial losses, the organization can also face internal realignment as responsibilities are shuffled around in response to the incident along with a loss of trust from employees, customers, and investors. Rebuilding these relationships can be lengthy. Thus, for an organization that is facing a high degree of risk from cyberattacks and data breaches, it must adequately protect the integrity of its data while also being able to provide assurance to stakeholders of all levels that the organization is taking the necessary steps to protect their data and the reputation of the organization.

11.4. Trust in AI Systems

A diverse range of worldviews, considerations, applications, systems, and choices are at play in trust discussions in the world of AI. This is representative of the more granular

and technologically specific nature of AI trust, which is shaped by a combination of both AI-specific and generic trust factors. Research has imported the models and frameworks of human-human trust into human-AI collaboration, as these parallels help to inform the human-centered design and application of trust in AI. This is especially applicable to the application of trust in the area of AI-human collaboration in increasing stakeholder participation. However, these models do not adequately accommodate the subtle yet important differences between human trust and trust in AI systems. These parallels or gradients of trust between human-human and human AI are especially applicable in the construction, maintenance, and enhancement of interpersonal AI trustworthiness and the limited delegation of power to AI on behalf of a trustor interacting with a trustee in the context of AI-human collaboration and interactivity.

Trust in AI requires a radically different construction, focus, and lens than that on human trust. This construct is shaped by our very definition of what AI is, i.e. an agent or entity that analyzes the environment and autonomously chooses certain behaviors from among a set of possible actions, thereby affecting the state of the environment. This AI construct emphasizes certain absence, presence, and amalgams of factors and other demons of control because of the unique nature of AI. Some of these factors include predictability, transparency of underlying model, probabilistic and error-prone but accurate behavior, ability to explain its actions, verification of both algorithm and data used to train it, physical embodiment, fairness, and many others.

11.4.1. The Role of Trust in Financial Transactions

AI systems are becoming vital participants in the daily operations and decision-making of already heavily interconnected and interdependent global government and business financial ecosystems. Among these frequent financial interactions, a subset consists of one-sided financial transactions in which the payer makes a payment to the payee without any mutual exchange of goods or services. These one-sided financial transactions, which include taxes, fines, and fees, rely on a high level of trust that the payer will not be cheated by the receiving party. These trust relationships must be maintained through transactions conducted with integrity and without collusion, corruption, or favoritism. In the case of tax collection or monitoring for potential violations of tax law via audits, enforcement of fines or fees, and the micromanagement of potential noncompliance for government revenue generation purposes, interactions between the payer and the government can be far from satisfactory. If government agencies become focused on increasing one-sided financial transaction revenue at the expense of payer satisfaction, resentment surely will increase within the payer population of any nation.

Trust in a specific transaction is often defined as the willingness of one party to be vulnerable to the actions of another party that is believed to have the ability and the willingness to perform a particular action. In this sense, it is not trust that creates the reliable conditions for sound financial transactions, but the ability of financial transaction parties to create credible assurances about their performance. What is yet to be explained are the essential contextual factors that create such credible assurances. In particular, AI should not be perceived as a disembodied system that can create sound and reliable public relations and social comfort about the actions that take place.

11.4.2. Factors Influencing Trust in AI

Much academic research on trust has been conducted, from various disciplines' perspectives such as sociology, political science, or psychology. Trust has indeed been perceived as a central aspect of human interaction in these disciplines. In relation to our focus on artificial intelligence, other specific domains dealt also with trust. Research on Human-Robot Interaction explored the notion of trust in automation by studying the interplay between human trust and robot capabilities, transparency, user programming, and acceptance, as well as understanding social cues. Other applied-level insights can be drawn from studies in the domains of marketing, health, HRM, and cybersecurity. Research on trust in automation and trust in AI explored how people's trust in algorithms changed based on AI’s accuracy, consistency, transparency, and form. We summarize some of their findings and some recent studies on AI trust to identify the main factors that influence trust below.

We build on earlier models that outline the main levers of people's trust in AI systems. Such models helped us to sketch our trust in AI model in what follows based on trust in Human-Robot Interaction, company trust, risk management, and algorithmic trust studies. Our model comprises input trust factors that influence people's AI trust beliefs, as well as AI trust outcomes – our trust dynamic. These AI trust input factors can be subdivided into AI context factors and AI-specific factors. The context factors pertain to the person with a focus on their experience, the management, and their societal, company, and situational trust environment. The AI-specific factors are the people’s trust perceptions of the AI system itself, which comprises both its technical specifications as well as its perceived intelligent and social behavioral capabilities.

11.4.3. Trust-Building Strategies

In AI-augmented digital financial transactions involving government financial service agencies, the parties involved in a transaction require more knowledge about the potential risk involved in either side's or a third party's actions and the measures taken

to mitigate those risks. Transparency can encourage the parties to discuss potential transaction-related concerns such as information asymmetry, biased data, biased models, and biased transaction programming, enabling novel solutions to be created collaboratively. The design of trust-enhancing AI systems can also help. For example, by introducing intentionally biased measures for specific functions or affecting functions, a government financial ecosystem can achieve notable trust-building effects. The possible considerations include, but are not limited to, additional transaction time, pace of transactions, operators' flexibility, and effects on close monitoring of a specific potential party's actions. Openness can also be achieved through the emergence of new parties in the transaction; for example, introducing and spreading the knowledge about the rules, models, and systems the AI algorithms use in deciding the outcome of the digital transactions can help create trust.

In an ecosystem, parties engage in transactions infrequently but still want the trustee to provide the expected results every time. Any failure to deliver either the quality, validity, or outputs would result in an efficient possibility-shifting agreement of mutual control. In such a scenario, the trustee is expected to provide some basis on which it is deemed deserving of closure, resolution, forgiveness, and, if anywhere near possible, indemnification. In AI-driven soft law areas of digital economy transactions, the society must develop some basis for pursuing prudential rules and protocols and creating new styles of token contracts wherein the trustee can be self-enforced to return value to the afflicted party.

11.5. Regulatory Frameworks

AI will create pressures for regulatory frameworks at all levels of government, both at the national and local level. It will accelerate the tension between the need for greater democracy in government decision-making, and the apparent need for the government to operate in a more secretive and business-like manner. On the one hand, policy discussions around the regulatory frameworks governing the safety use of AI models may open the door to greater scrutiny of the data that is fed into available systems. Second, national governments also have a mission to keep their citizens safe, allowing them to put into place regulations that safeguard the use of AI by law enforcement and for national security ends. At the same time, issues of regulatory capture may appear in the design of governmental regulations, particularly in countries where stakeholders from the private sector have greater levels of influence over government. There is also an aspect of AI systems acting as regulatory agencies for the government making decisions over citizens' lives that is problematic, and which may not be effectively reviewed by other branches of government. The speed at which AI is capable of making decisions means that there is less opportunity for citizens to actually know they are being

governed by an AI system. In such contexts, the smart city and smart government become means of creating regulatory frameworks that amplify the exercise of lobbyist power by private sector financial interests. As financial authorities gradually adopt the use of AI systems for financial regulatory oversight, they will need to be aware of the existing level of regulation that is in place over other agencies. Indeed, some historical precedents warn that these regulatory agencies may actually operate in a fashion that goes against both democratic principles and the principles that inscribed their creation as public entities. In this way, we need to be careful about the way AI is proposed to envisage a different relationship between the public sector and the private sector, a relationship which is in reality already inflicted through ethical questions.

11.5.1. Existing Regulations on Data Integrity

Regulating the integrity of data has become imperative in light of high-profile cyber attacks, data breaches, and concerns about data integrity in respect of elections and the COVID-19 pandemic. Regulatory efforts have focused on designing frameworks to ensure that data are authentic, not subject to unauthorized changes, and accurate throughout their lifecycle. Data integrity is especially important in government financial reporting, auditing, and oversight of the government financial environment. Here, inaccurate or fraudulent data harms national security on a broader scale. For this reason, compliance standards formulated by various regulatory agencies are frequently used to help determine the accuracy and integrity of data used in audits, helping protect against the use of invalid or unreliable data in reporting.

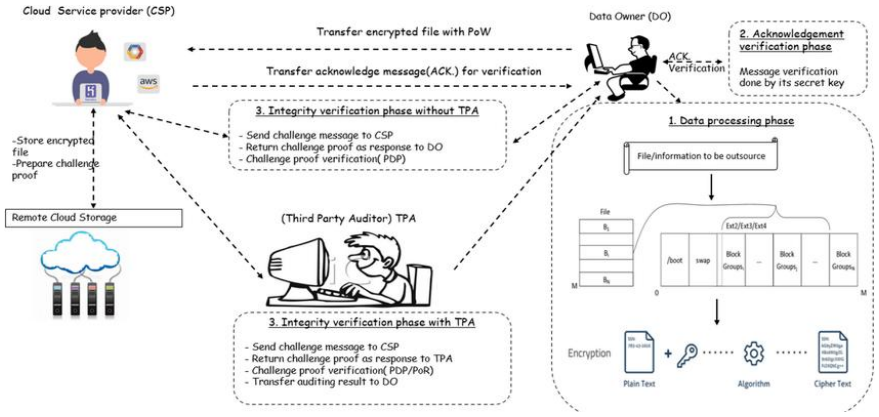

Fig 11 . 2 : Data Integrity Technique

Nonetheless, existing statutory and regulatory frameworks governing integrity remain perennially immature, and organizations often operate without consequence, employing technically brittle solutions for management of crucial customer data. Legislative and

regulatory formulas, listing requirements specified by federal or state agencies, and a range of informal compliance standards exist to oversee information management procedure adoption, but few provisions exist to combat the actual practice itself. In many jurisdictions, regulations merely push the entire question off to an employee's suitability or unblemished-good-character criterion, or to some imprecise notion of good practice codified for its currency or weight.

11.5.2. AI-Specific Regulations

One of the areas with significant activity is the establishment of AI-specific regulations. While these are primarily Data Protection or AI Act-related local mandate regulations, they are expected to evolve to become either based or driven by international standardization initiatives. In particular, we see a wave of countries developing AI Acts, such as the USA, the UK, Canada, Japan, Australia, and Omen. Many regional and local regulatory agencies have opened consultations to hear opinions from the business ecosystem, as they will be developing bills to further specify the requirements.

The European Parliament has started the debate on the AI Act that is currently under discussion. Despite the existence of the GDPR, the AI Act aims to regulate the "black box" nature of AI technologies by specifying how to provide and verify transparency, especially for "high-risk" AI systems. The European Commission has defined the high-risk use cases based on delegated regulations, which will subsequently be utilized to verify compliance. To facilitate this, several standardization initiatives have started in collaboration with many standardization organizations, trying to establish a set of common horizontal standards to facilitate the implementation, accreditations, assessment, and certifications based on the AI Act requirements on a voluntary basis. We expect other countries and regions like the USA to create similar mandates and report based on these standards to promote the responsible development, implementation, and deployment of AI technologies.

11.5.3. International Standards and Compliance

International standards are critical to ensuring that organizations agree on definitions, frameworks, processes, techniques, operations, controls, tools, methods, and utilities. The goal of these international standards is to ensure consistency, repeatability, and shared vocabulary to assist organizations and lawyers in working across national boundaries. It is also critical that these international standards evolve as the technology evolves. International standards develop conformance requests and monitoring via compliance and audit systems after defining the standards. International standards - how regulations become administrable, monitored, and dependent on consistent definitions -

and the inevitability of these compliance and conformance initiatives become the backbone of regulatory frameworks. As the technology ecosystem evolves, new international standards are being developed or existing international standards modified to align with new definitions and technical capabilities. Organizations need to be aware of, and prepared to adhere to, the scheduling of these new standards. Existing international standards supporting the digital identity ecosystem element are highlighted below. As the dialogues within cyber resilience, IT asset management, data classification, and trustworthiness areas expand, it is expected that new international standards will address these elements and enable their support of digital identity definitions. Conformity assessment is an important factor in trustworthiness as parties assess their confidence in risk management across the ecosystem.

11.6. Technological Solutions for Data Integrity

Different methods have been proposed to strengthen trust and facilitate the detection of corruption in publicly held datasets. In this section, we describe a variety of innovative technological solutions that are being developed or implemented to help preserve the integrity of data hosted in government databases. These tools can aid policy makers to introduce sound mechanisms for the protection of the state of the public informational asset, without relying solely on difficult to enforce regulations on data stewardship.

Blockchain technology has garnered considerable interest as a potential way to make government data-management infrastructure more resistant to corruption. Originally developed as a decentralised information structure for the digital currencies ecosystem, blockchains enforce integrity by storing the latest version of a dataset on a distributed ledger. In this way, to modify the data, malicious actors must hack all nodes that store a copy of the blockchain. The separate nodes continuously update their versions of the blockchain based on consensus rules, which define which new information can be appended to the ledger. Blockchains are open by default, which means access is unrestricted, enabling all users to verify the integrity of the stored information.

Despite its many advantages, blockchain technology has limitations for its use in government financial applications. By being open to everyone, public blockchains may expose sensitive information to malicious actors, who could take advantage of it for criminal purposes. Moreover, the need for a large computational effort from all nodes can lead to long delays in transactions – that is, the writing of data to the ledger. These delays make public blockchains unsuitable for the infrastructure of applications that require a very high number of transactions to be constantly executed – necessary in government functions with a daily volume of operations in the thousands, such as collecting taxes or issuing paychecks.

11.6.1. Blockchain Technology

The Financial Infrastructure ecosystem is based upon various participants and workflows, therefore, can be represented as a network model pertaining to data transfers and transactions between participants and process workflows controlled by business rules. The usage of encryption and hashing technologies allows data to be secured from alteration and provides necessary non-repudiation capabilities, however cannot prevent the risks related to business process integrity and data trust within hybrid shared data environments. This is where blockchain technology can provide the necessary remedies of security and trust while preserving business rules and workflows. Blockchain provides decentralized accountability and distributed trust at the transactional layer itself, therefore collectively ensuring the integrity of business rules of the cross-party data processing environment. The ultimate goal of any business process is serving end customers thus the whole process chain operating on a series of transactions is always linking them together. Supply chain business processes at each point-in-time are always represented by the last confirmed transaction summary. Blockchain provides the capability of an automated mechanism to record transactions in a way that it can never be altered and removed, therefore maintaining a complete transaction history. Blockchain helps secure the integrity of the addressed data layer of enterprise solutions, while workflow management can still be handled by appropriate business rule logics resident in enterprise workflow and document management applications which external create/update and execute and verify the transaction process on the blockchain network.

11.6.2. Encryption Techniques

The increasing dependence on web-based digital systems for the management of citizen data by governments and public financial institutions at all levels has dramatically increased vulnerabilities concerning the protection of such citizens' confidential and sensitive information. While the integration of Artificial Intelligence (AI) and related activities into routine government operations serves to improve accuracy, lessens the potential for human error, and can often increase speed, the potential ramifications created by system failures, inaccuracies, and other possible adverse outcomes drastically increase the need for regulations protecting the citizenry. The introduction of tools protecting data integrity such as Encryption Tools, Digital Signatures, Data Hiding, and Secure Multi-Party Computation (SMPC) which were developed specifically to address data integrity issues enhance not only trust in AI-Augmented Services provided by government financial units but also more broadly in Digital Economies. Additionally, the existence of Data Integrity Protection Tools serves as a bulwark against both internal nefarious actors and external malevolent hackers.

Encryption is a tool that prevents use and access. By protection against unauthorized access to data, Encryption by design on protected DB ensures that DB data is not used in an unexpected way. Digital signatures with time-stamp services enable digitally signed transaction files for the entire organization. Digital signatures help ensure the integrity and authenticity of a message, transaction, and data. Digital signatures with a timestamp are non repudiable; digital signatures cannot be altered and cannot be disavowed. Data hiding is due to an assertion that not all data has to be stored in a DB and not all relationships have to be established through an accessible link. Information not intended for disclosure can be made undetectable to unauthorized users. A pre-encryption data hiding tool was established to implement data integrity for relevant data integrity regulations.

11.6.3. Audit Trails and Monitoring

An audit trail is a record of what you did to a device or data set. Like many security features, audit trails are often enabled only after the device is installed; however, if data integrity is important, you should consider keeping an audit trail from day one. Audit trails may slow performance. Ideally, you wish to keep the cost of maintaining audit trails as low as possible, which may mean limiting the scope of an audit trail. Monitoring means you are currently watching, or at least capable of watching at any given second, what is going on within the AI model you are interested in. The main purposes of AI monitoring are keeping track of inputs and outputs of the AI systems and detecting alarmingly high input-output deviations. The challenge with monitoring a commercial AI application is that the developers of commercial systems provide little or no information about how their algorithms function.

The problem is that decisions made by development teams are rarely documented, and if they are, they are buried so deeply in a design document that no one can find them. In these cases, monitoring tools become critical, since it is the only way documentation might get created. AI monitoring tools achieve several objectives. First, monitoring tools capture execution traces of AI applications when they run. Such traces include information about the input and output to the AI algorithms involved in the final decision. Such traces are essential for data center operations, but they can also help debug an application if it goes awry.

11.7. Ethical Considerations

1. Ethics of AI in Government Finance

AI algorithms have the potential to transform government processes such as taxation, impact assessments, and social benefits. These processes must be created and managed, however, with utmost caution, vigilance, and ethical considerations. Ethical considerations prevent the overreach of AI, minimize harm, maximize benefits, promote good practices, and guide appropriate action concerning the deployment of AI in sensitive areas. Guidelines, audits, reviews, and instructions exist, but organizations vary in their ability and success in implementing the guidance and undergoing audits or reviews. Some sectors are under pressure to disclose their AI ethical safeguards and experiences, but the government finance ecosystem as a whole may be lagging in ethical self-policing with regard to the implementation and deployment of AI-based decision-making or recommendation systems. Ethical considerations are not only constraints but also active guides in what forms of AI-enabled systems and projects are worth undertaking and which are not worth deploying.

2. Bias and Fairness in AI Algorithms

Bias and fairness are complex problems. Bias in AI algorithms can stem from indirect discrimination in the form of selecting data and measures or variables that are affected by discrimination in society; failing to specify a variable that would address bias or very unequal impact for important groups; and model misspecification in which the usage of an algorithm that approximates the patterns present in historical data for prediction creates ethical problems. Regularization in models for estimation and prediction can alleviate these latter biases. Further, many developed economies have existing rules, protections, and policies against discriminatory behavior of firms and organizations. Examining whether or not firms and organizations that use AI-guided decision systems are violating existing rules, protections, and policies can provide a check on the deployment of AI in important decision-making areas. Such a bias check both provides needed scrutiny and creates a level playing field in decisions around fairness and bias.

11.7.1. Ethics of AI in Government Finance

Advocates for the wide deployment of AI across the public administration landscape laud its potential to deliver a range of benefits to governance and government finance. Scale and scope, speed and efficiency, impact assessment and outcomes, cut compliance costs, and improve the quality of engagement with citizens, individuals are all cited as advantages. Framed as part of the new wave, it is heralded as reducing the burdens of administration, improving public services, and adding to the efficiency and value of public services.

Skeptics about the timing, pace, and extent of deployment call for caution – particularly where incisive decision-making about individual cases is being pushed to the front stage of the public service agenda. In a field already plagued by poor data quality and bias, questions of reliability resound loudly. Reserved about the potential of full or near-full automation, academics warn about governance potentially sacrificing key tenets of good administration – privacy, fairness, due process, inclusiveness, accountability, and trust.

These ethical concerns grow out of the unique characteristics of algorithms. Rather than just reflecting contextual knowledge or human experience, AI is premised on the use of data for prediction, learning, and improvement. Learning happens at scale, as data is passed to the algorithm from multiple sources, merging and augmenting different inputs and reinforcing themselves in a process akin to self-learning. AI as a prediction machine is a radically different proposition than the templates previously used. AI machines are based on dark mathematical algorithms, whose inner workings, operating logic, rule-setting, and coding are largely opaque, even to their creators. As a result, they are significantly less transparent than traditional government finance management information systems.

11.7.2. Bias and Fairness in AI Algorithms

Governments utilize a variety of algorithms to optimize operations and deliver services, ranging from predictive policing algorithms to algorithms for hiring, firing, and prison sentencing. Such algorithms have the potential to perpetuate existing inequities if they are trained using biased data or are modeled heuristically without addressing the underlying features that give rise to unfairness in observed behavior, while also minimizing features that contribute to inequity. Such empirical, sociological, and legal concerns raise the important question of whether machine learning developers should take fairness considerations into account when developing algorithms for deployment.

Concerns about fairness can be framed in multiple ways: one key framework defines multiple notions of unbiased performance and proposes algorithmic solutions to optimizing for fairness as defined. The key avenue for bias in any AI system is through data collection, as the training data must be representative of the problem space and inputs to the system. For example, training a hiring algorithm using data collected from a company that predominantly hired men may propagate inequities. Three approaches can address bias inherent in data collection. Data auditing involves reviewing the training set and ensuring that it represents all relevant subpopulations. Fair-machine learning, a growing subfield, utilizes techniques from the machine learning literature to remove bias. Bias mitigation augments the training dataset in order to achieve a more equitable representation.

11.7.3. Transparency and Accountability

The voluntary or legislative enactment of regulations that dictate preferred design and implementation practices for algorithmic models can minimize cognitive cost of governance for end users. Therefore, policymakers must reinforce the development of moral codes and standards of practice that promote fairness, accountability, and transparency, allowing users to easily gauge the trustworthiness of the algorithms they are working with. External audits can contribute to the establishment of best practices and validation protocols for AI deployed by the public sector. Requiring that AI engines used in the public sector publish a comprehensible statistical summary of their training data sets, including any relevant input-output relationships, as well as the log-likelihood and uncertainty estimates when providing a solution to an inference problem can greatly assist the validation and populational fitness tests that must be regularly conducted by external reviewers.

Independently of any regulatory action, algorithm design teams should also come forth with assurances about the reliability of the information they provide. Research on bias detection could potentially create a path by which ethical concerns are incorporated into the decision-making processes of design teams building classifiers or selection systems that will be used in a public sector setting. If the AI model is incapable of guaranteeing reasonable reliability, the designers and future end users should have a clear-headed discussion about whether the model is appropriate for use in the first place.

11.8. Future Directions

Most government financial systems avoid experimentation. Resistance is often based on the belief that government financial processes and systems must be boring, and for good reason. The survivability and accountability of government are two core tenets of internal control and are both prime reasons to be cautious with changes to financial management. However, the demand for transformation comes from seeing the government continuously lag business in the development of IT systems that offer enhanced functionality and usability. Emerging Technologies. The reasons for adopting more emerging technologies into government financial ecosystems are compelling. Technologies that offer experimental change such as algorithms, robotics, and machine learning are being used to enhance risk-based financial analysis. Cloud provides a new backoffice eco-structure. Cybersecurity is a prerequisite to that new architecture, in both day-to-day management and in protection against crisis cyber-events. e-Procurement is transforming transactions. Mobile interfaces are being used for many state and local transactions. Predictive analytics enhance resource allocation and reject the concept that budgets consist of “just saying no” in negative variance dialogues long after budgets have been created, and add a multi-fiscal month capability to the surveillance function.

Predicted Trends in AI and Finance. The expanded use of AI to be worked alongside internal control staff and accountants is observing economists suggesting that the future workplace will require much more collaboration, and the finance functions will be adjusted towards more non-standard and advice-type decisions. Consolidation should lessen the average number of jobs in the finance functions. There will be a greater emphasis on expert systems that provide advice but don't hire people, and actors who address the unique aspects of the finance and advice linkage. Grouping of simple transaction functions with more complex ones will provide the opportunity for employee development.

11.8.1. Emerging Technologies

Achieving a fully autonomous state of AI-powered financial management and oversight requires us to efficiently tackle a number of key challenges in developing, deploying, and operating AI applications for government financial management. The current state of government financial management technology is one of a dependence on manual processes, dealing with historical data, and limited use of open source technologies. Such solutions are neither innovative nor diverse. They are variations on a theme — namely being hosted on a cloud and living and breathing via a web interface, and usually powered by structured data residing in a data warehouse. New and emerging technologies have the potential to catalyze a paradigm shift in how we think about government financial management technology.

Technologies such as AI, blockchain, federated learning, reinforcement learning, explainable AI, transfer learning, and open-source intelligence have the potential to play a disruptive role in refreshing the face of government financial management technology, given the right investments and resources. They can simplify and automate a range of government financial management activities, such as identifying and addressing improper payment review, and advance surveillance, detection, and investigation in complex corporate disclosure and public finance systems. The research challenge is bridging the knowledge gap between the finance experts who have a keen insight into the challenges and possible resolutions, and the engineering practitioners who can implement the viable solutions. A disciplined model is needed for using experimentation and pilot projects to find the most usable and useful combinations of technologies to change the game in government financial management. This would play a vital role in ensuring that other government functions such as fraud surveillance and prevention, and cyber defense get the digital transformation horses for the data integrity issue to tie onto.

11.8.2. Predicted Trends in AI and Finance

Both the private and public sectors are recognizing AI's transformative role, evidenced by ambitious large-scale initiatives. Many governments are also seeking data-led advances in their national competitiveness, and their goal-setting may involve AI for Finance projects spanning trillions of dollars. Furthermore, the digital economy has supported the private sector's adoption of advanced AI technology, and globally scaling firms are using it to ramp up economic efficiencies while dealing with recent traditional economic upsets, such as financial crises and inflationary price cycles. In Hong Kong, leading banks and other finance and business firms are moving aggressively, characterized by swift AI adoption and investment both internally and by the venture capital community.

There is enormous global capital market interest fueled by the belief that AI will greatly improve company bottom-lines and profits, currently being expressed for many tech industries market participants. Certain tech companies have positioned their patents to be in the leading cadre of AI innovators, and the rush to AI product development and version upgrades appears to have broken out, as they paint a bright picture of large revenues from digital products and services. Further, countries are targeting business sectors, especially those that are foundation building blocks for national fortunes in the digital economy. Many of these efforts are motivated by a belief that advanced Science and Technology, including AI, will drive national and global growth, ameliorating the current inflationary waves that are raising national cost priorities.

11.8.3. Preparing for Future Challenges

Research has pointed to public trust in government and its institutions being at a historic low point across multiple nations. Examples abound of governments that have addressed public trust and information integrity head-on: Canada's Digital Charter - Trust in a Digital World commits the Government to action in the domain of Trust. AI services deployed to the Government Financial Domain, and the wider Data World, by collaborating financial services companies, to restore public trust levels. Trust is eroded by the growth of nationless mega-platforms that offer both greatly reduced economic development activities locally, privatization of tax revenues, and privation of trust in the info eco-system by empowering AI to manipulate natural language generation. Nationless mega-platforms that assist with the technical capabilities that nation states urgently need, to have both the 21st century engagement eco-system tools, as well as the ethical tools, to restore trust levels in their nation states.

Potential future violations of Government Financial Domain data integrity and trust are widespread. Algorithmic Bias from lack of care and attention in the application of AI within government financial support decisions, highly consequential in high-stress times for the recipients, has the risk of causing serious Localized Upset. AI decisions within

government financial systems are in practice untrustable, and so should be used to augment Human Decision Making, not replace humans. The unpredictability and opacity of AI Bias violations across society, threatened rapidly changing behaviours of decision-making groups around AI Intentionality, mean changes in AI Model Focus and Intentionality are unpredictable. The continued invisibility of Financial Market Decision-Makers continues, for new Trust in Emerging Financial Market Impacts to be established. To restore trust in public institutions, Government leaders must put the welfare of their constituents ahead of political Milestones through transparent data exchanges and ethical data governance models.

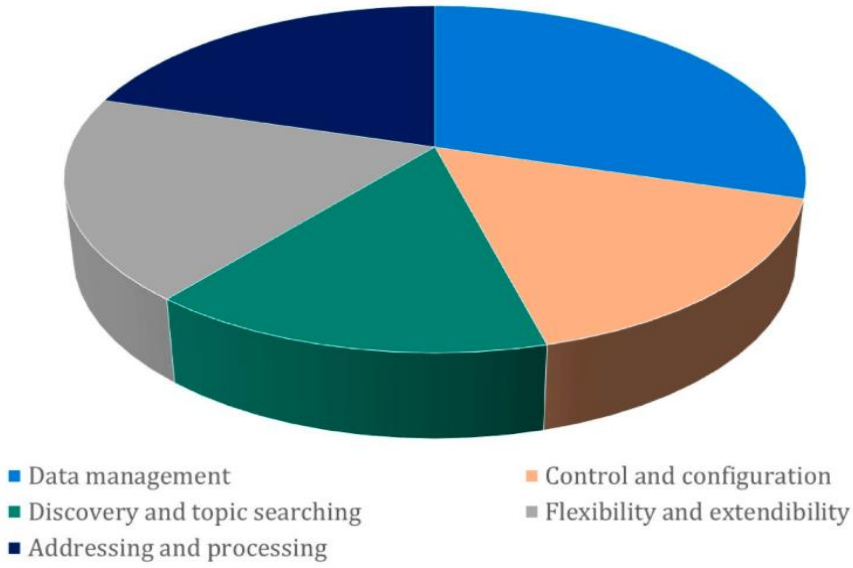

Fig 11 . 3 : Full Potentials of IoT for Better Financial Growth and Stability

11.9. Conclusion

In conclusion, the value proposition of AI-generated productivity increases in a government financial ecosystem depends on public trust – mediated by data integrity – in AI-affected functions, as well as on active participation of citizens in scenarios of co-design of AI-integrated services. Evidence shows that trust in government is conditional on data privacy, security, and accuracy. Addressing concerns in these areas requires the context-specific consideration of the privacy, ethical, and legal implications of algorithm development and technical parameters underpinning AI-integrated services. BPA must be proactive in establishing a disposable safeguards regime that limits the intrusion of AI services into a citizen's private space.

Trustworthiness in unconventional AI applications that propose to warn the state about a citizen's intention of performing atypical but legal and accepted activities hinges on higher authenticity standards used to construct novel datasets to train these AI systems than the ones that were adopted for the unreliable individuals' sets frequently used in supervised models. This could be further assured by obliging AI service vendors and developers to publicly inform stakeholders about their risk containment motivations, experience, and AI system bias mitigation practices and results. Implementation and operational design using technology-neutral data management and data governance standards will assist in translating value propositions into trusted services that can absorb the increase in complexity and costs.

And finally, the application of novel field-fitted methodologies for auditing somebody's decision-making based on AI-augmented supervised automata, disclosures about socio-ethical and political science provisions, along with reciprocity clauses in service provision contracts should be made mandatory when organizing the outsourcing of AI system design, training, support, or maintenance. These efforts should ensure that human decision-makers remain ultimately responsible for the decision-making provided to titulars of public services.

11.9.1. Final Thoughts and Implications for Stakeholders

Amidst the uncertainties of the twenty-first century, there is hope. It is that artificial intelligence, when implemented properly and used optimally, can support and lead to citizenry objectives long pursued but hardly attained. It can help citizens and their governments to achieve an economy where the wealth, opportunities, and prosperity of the few do not breed indignity and disrespect for life, liberty, and the pursuit of happiness by the many, nor confuse their hopes and wishes for justice with undeserved ignorance and unearned poverty. It may even be possible to achieve an economy with the characteristics defined by a meritocratic economy where success is based on fair and well-functioning competition that rewards relatively few winners and allows the vast majority of participants to receive reasonable compensation for their most important asset—their labor—rather than focused on consuming social security handouts for many years.

The future of artifice will hinge on building a balanced model of a new economy where human judgment may be used to guide collectively AI's recommendations to prevent disastrous outcomes of badly informed—or governed—decisionmakers. No algorithm is capable, on its own, of ensuring data integrity, nor prohibiting various methods of fraud and coercion. Protecting such integrity—and the privacy of voting and financial data—should be society's top objective in an age when data and AI are the new oil and global warming—it should be written in the PAD for an economy to become a model of human

destiny. The trust placed by citizens in their respective governments, and the role of trust in the relationships between citizens and their governments, is a much broader topic than that of privacy and security of data when citizens as well as government institutions use the new, augmented models and services offered by corporations based on trustless technology and AI.

References

Kshetri, N., & Voas, J. (2021). Trust in AI-Powered Financial Systems: Ensuring Data Integrity in Public Sector Applications. Government Information Quarterly, 38(4), 101574. https://doi.org/10.1016/j.giq.2021.101574

Lee, K., & Lee, S. (2020). Securing Financial Data Integrity in AI-Driven Government Systems: Challenges and Solutions. Journal of Information Privacy and Security, 16(3), 215–229. https://doi.org/10.1080/15536548.2020.1826671

World Economic Forum. (2021). AI and Financial Transparency: Safeguarding Data Integrity in Government Financial Operations. WEF White Paper. https://doi.org/10.3389/fdata.2021.00176

Huang, Y., & Yu, Z. (2022). Data Trustworthiness in AI-Enhanced Financial Governance: The Role of Blockchain and AI Verification Techniques. International Journal of Information Management, 62, 102436. https://doi.org/10.1016/j.ijinfomgt.2021.102436

Albrecht, M., & Lang, M. (2023). Building Trust in Government Financial Ecosystems: A Framework for AI, Data Security, and Ethical Governance. Public Administration Review, 83(1), 101–115. https://doi.org/10.1111/puar.13456