Kurdish Studies
December 2022
Volume: 10, No: 2, pp 869-879
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

DOI: 10.53555/ks.v10i2.3834

Secure and Ethical Deployment of AI in Digital Payments: A Framework for the Future of Fintech

Abhishek Dodda*

*Engineering Manager, abhishek.dodda9@gmail.com, ORCID: 0009-0000-6728-945X

Abstract
Advances in Artificial Intelligence (AI) and Machine Learning (ML) are expected to create a new wave of inefficiencies in economic activities, leading to massive productivity gains and reduction of costs. In central banking, AI and ML can help with central bank objectives, such as maintaining price and financial stability, monitoring the business cycles, and serving as a basis for issuing Digital Currencies, for further adoption by users and businesses. At the same time, the massive adoption and deployment of AI technologies and products come with ethical and security risks, such as algorithmic biases and exploitation of VUCA situations with cyberattacks and prompt attacks for leading AI/ML Models, thus undermining Security and Safety, and reinforcing trust, key requirements for the modern Digital Payments platform Central Banks, Retail Banks, and other Payment Institutions are expected to build and scale.
How may Central Banks help secure and ethically deploy, by both the private sector and themselves, AI technologies applied to payments, particularly Digital Currencies? We identify priorities and the right regulatory guidelines and sandboxes, to ethically and securely develop financial services using these technologies. Our conclusions are based on a literature review and survey results with practitioners, in Central Banks and the Private Sector, working on or in charge of implementing these regulations to support the Central Bank Digital Currency in payment systems. We specifically address the following main questions. How are Central Banks currently supporting the Security and Trust of Digital Payments? What role may Central Banks play in creating the incentives for the Private Sector to ethically and securely leverage AI/ML technologies to build intelligent financial services in Digital Payments, while not crowding them out? At the Multi-Lateral Level, how to combine these efforts for interoperability and to better address Cybersecurity risks?

Keywords: Artificial Intelligence, Machine Learning, Central Banking, Price Stability, Financial Stability, Digital Currencies, AI Ethics, Algorithmic Bias, VUCA, Cybersecurity, Trust in Payments, Regulatory Guidelines, Central Bank Digital Currency, Private Sector, Financial Services, Payment Systems, Security and Trust, Interoperability, Multi-Lateral Cooperation.

1. Introduction

The exponentially increasing use of computing power in addition to the invention of large-scale AI and Machine Learning has given a major push toward digital transformation. Financial technology innovations in payments are also inextricably linked to the rise of computerization and the electrification of world economies. Payment technologies started with the invention of bills of exchange in 1200 CE and progressed with credit cards in 1950, ATMs in 1967, Internet banking in 1994, and peer-to-peer payments in 1998. However, the most significant transformation of payments came with the invention of mobile wallets, because it created an ecosystem for payment service providers to quickly launch non-traditional banking services. When AI-enabled recommendation engines are used to nudge users to adopt new service offerings, the benefits of AI in payments can be sustainable. Frictionless, invisible, inclusive, and sophisticated next-gen experiences powered by real-time and interpretive technologies will reign as the primary engines of payment change for banks, merchants, and consumers. We are now witnessing the changes with T+0 reconciliations, real-time fraud detection, and contactless payment card usage.

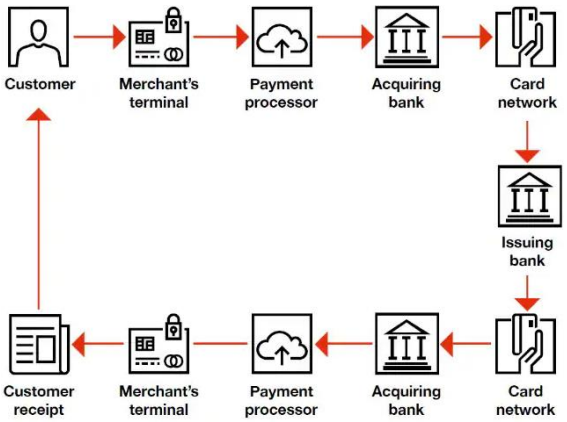

Fig 1: Combating fraud in the era of digital payments

AI's potential in digital payment functions such as underwriting, customer service, risk detection, and management are, however, limited by legacy systems and an initial tech stack that wasn't designed with adaptability in mind. Risk categorization, virtual customer assistants, identity verification, and anti-money laundering are the prime focus areas where we find AI and ML innovations. Digital payment service providers, along with the academic community and consortiums can leverage the technologies and approaches outlined in the next sections, to find conveniences for merchants, consumers, government regulators, and themselves.

1.1. Significance of AI in Transforming Financial Transactions

Digital payments are a critical component of everyday life, whether the transaction is in person or online; with time and convenience driving this need, continuous refining and innovation drive implementation. With market growth forecasts well over by 2026, advances in capabilities surrounding payments and discoverability services continue to drive this high demand. Artificial Intelligence tools such as real-time recommendations, risk and fraud prevention, and online security are all integral to the delivery of financial transaction capabilities with AI innovations continuing to deliver the enabling solutions and services. Financial institutions worldwide are employing AI to reduce operational costs, increase the efficiency of operational processes, and detect and eliminate fraud. AI could potentially add to the world economy through productivity gains and reduce the total incurred by fraud in the financial services sector, estimated at over 10%. AI in banking has grown worldwide, with the union market seeing an average investment of over annually across all types of AI verticals from 2021 to 2030, while the total worldwide spending estimate is well over for the same period. AI investments across the fintech space are expected to exceed annually as early as. Investment on this scale is enabling, and delivering enabling solutions into the market, both in partnership with and independent of traditional FIs at an ever-increasing pace.

Equation 1: Ethical AI Compliance Score

$$E_c = \alpha \cdot R_f + \beta \cdot T_a + \gamma \cdot F_e$$

Where

E_c: Ethical Compliance Score

R_f: Fairness and Bias Reduction (e.g., fairness metrics like disparate impact)

T_a: Transparency of AI Decisions (e.g., explainability measures)

F_e: Ethical Framework Adherence (e.g., adherence to regulatory standards)

α, β, γ: Weighting Factors for Each Component

2. Overview of AI in Digital Payments

AI has emerged as a significant trend in the global financial services industry. While installing digital payment systems provides customers with easy and fast payment, it incurs some transaction risks. A reduction in transaction security can have a devastating effect on a merchant's reputation. This has led to intensive competition among merchants to enhance transaction security. Digital payment service providers and acquirers respond to consumer demand by investing in AI technology to develop useful applications. They prefer to outsource the development of the AI process to software developers. The applications employ the deep learning methodology to analyze transaction data to provide fraud detection and prevention services on a 24/7 basis.

The development of AI applications stimulates the demand for deep learning to scale transaction data to develop optimal predictive models. In digital payments, AI applications improve transaction efficiency and security. AI can carry out data mapping, feature engineering, and model training at a large scale and in an automatic manner. This, in turn, delivers accuracy, shortens the time for deploying predictive models during payment transactions, and reflects cost-effectiveness. This means that many small players can take part in the digital payment business. In addition, AI technology is becoming more easily available as cloud-based payment services can be made through trusted third parties without installing complex onsite enterprise resource planning systems. This enables industry players in different countries to collaborate on joint projects to develop services with a wider geographical reach.

2.1. Key Roles of AI in Enhancing Payment Efficiency

Payment systems using digital means are important for the economy because they allow a simple and secure exchange of assets, such as money or goods. The inception of a payment processor company furthers economic activity by efficiently connecting buyers and sellers on both sides of a transaction. Security is paramount and involves not only securing the transaction against being listened to, altered, or replayed but also securing accounts from hijacking. Because of the high number of digital payments happening every day across the globe, payment processors not only create and store the software and hardware required to manage the payment system but also make use of a technology environment, which, because of its scale, is capable of managing multiple and simultaneous transactions within a millisecond globally. As transactions are validated and allowed to diffuse through the network, the state of the payment systems cannot be uniquely attributable to a single location and refers to the maintaining of lists with the state of many accounts across the payment system for a simultaneous vast number of participants. The presence of many participants and the multiple and concurrent transaction requests strains the system as it has to validate very quickly and allow for minimal response times, or below the time it takes for a human to validate and compare transactions visually, while at the same time assuring that potential fraud is eliminated. The ability of AI systems to train models on past behavior and exploit transfer learning, i.e. the ability to generalize, allows for being trained on other and similar models in other systems. AI makes use of heuristics and algorithms that are capable of performing these validation tasks for years at a scale feasible. AI has the potential to change digital payments by allowing for more flexibility in transactions, involving custodial systems such as banks or payment validation systems, by eliminating traditional structures that concentrate or bottleneck this financial intermediation.

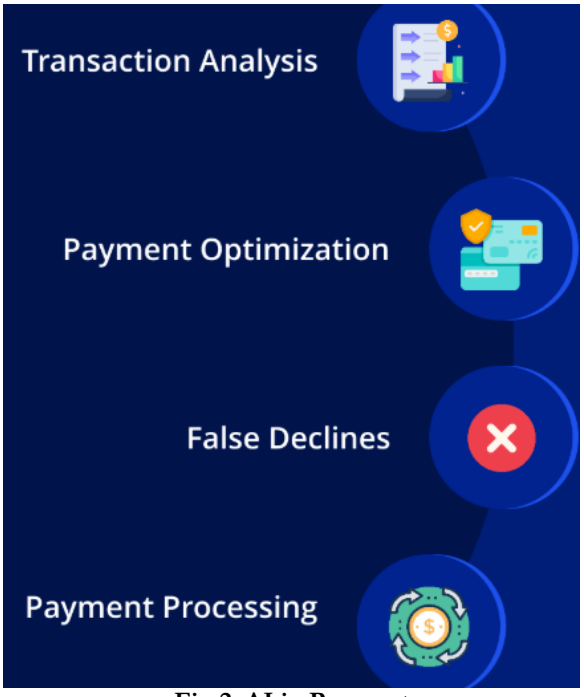

Fig 2: AI in Payment

3. Current Trends in Fintech

The fintech market is shifting away from traditional finance and toward a new financial infrastructure for digital payments. These emerging players may offer APIs or white-label solutions to help brands across media and eCommerce industries build and maintain their payment solutions in-house. These companies remove the need for payment processors to keep more of their revenue. The rise of open banking regulations opens opportunities for additional solutions that leverage consumer financial data to drive sales, offering both the potential for new kinds of products and services, as well as disrupting the value propositions of traditional players.

With social media commerce and live shopping expected to take off soon, payment companies should think about how their solutions can be integrated with these experiences. New figures found that nearly one in five users in the U.S. actively engage in live shopping or 21% of all Gen Z consumers. These events can drive revenue for brands and increase product demand by establishing a sense of urgency in consumers — there is only a limited time to buy the products that are presented. Successful events can help companies drive brand awareness and loyalty and ultimately build complete ecosystems that keep consumers returning. Some payment companies are already moving to enable such experiences. A live-stream shopping feature was rolled out on a site in 2016. Social media companies have also launched live shopping features, enabling merchants to sell their products while allowing viewers to ask questions about items in real-time.

3.1. Emerging Innovations in Financial Technology

Financial Technology, coined FinTech, is a catch-all term that refers to using technology to deliver financial services in a new and innovative manner. The financial services sector has undergone tremendous changes, wherein organizations are leveraging FinTech to improve or automate everything from banking and payments to wealth management. Banks are closely collaborating with several technology companies to develop cutting-edge financial technology products. Big players in Silicon Valley have invested heavily in this sector, wherein finance, technology, and retail companies are introducing emerging innovations in technology for financial services. Some of the key FinTech Tools that have emerged are Cloud Computing, Artificial Intelligence, Blockchain, Robotic Process Automation, Application Programming Interface, and Predictive and Descriptive analytics.

The global FinTech sector has also witnessed a boom in the mobile payments ecosystem, wherein companies are creating easy ways for sending, collecting, and processing payments, with mobile payments, e-wallets, and contactless cards that are paving the way and are all set to emerge as the next dominant force in payment processing. There is an increasing trend in money transfers to and from emerging markets in the Asia Pacific and the rest of the world, catering to the financial needs of underserved communities. In line with this, we can witness a rapidly growing cashless economy globally, with Cryptocurrency and Initial Coin Offerings dominating. Mobile payment wallets have an increasing share in driving cashless transactions, with adopting new payment methods, which also include biometrics, providing customers added security, thereby receiving their market acceptance. The blockchain and distributed ledger are ready to answer the banking services this segment has been lacking for a long.

4. Ethical Considerations in AI Deployment

Artificial Intelligence (AI) has emerged as a key component in reshaping digital payment systems through risk assessment frameworks that authenticate transactions and detect fraudulent activities; payment-related AI systems are proven to enhance

the management of chargebacks, streamline the Know Your Customer (KYC) process, increase the effectiveness of customer service inquiries, and reduce overall operational costs. However, the deployment of AI in payment processes, especially involving sensitive customer information and thus complex regulatory requirements, raises several ethical issues about fairness, accountability, and transparency; a deployment that is deemed as insecure, unethical, or illegal can undermine the technology and raise endless debates around its limitation. Broadly categorized, some major ethical considerations are bias and fairness, transparency and accountability, privacy and data governance, use of AI technology as weaponry, and dual use of the technology.

Bias and Fairness

Among others, bias and fairness-related issues are among the first applications and model training stages that encountered criticism. The risk assessment frameworks utilized in AI models are usually fed with data derived from historical cases that capture the humans and the events of intelligence exposure and the generated label is either successful or unsuccessful for the respective case. The models learn from this historical patterned data whenever a certain characteristic or characteristics are associated with a specific outcome which can then be classified as exposure to intelligence or not. For example, the propensity to commit terrorist acts or intention to corrupt public resources for private gains. The AI-generated risk label which essentially decides who is risky or not risky hinges on the model training and the data used for that purpose. Indeed the quality of the training data utilized is reflective of the socio-economic and demographic contexts of the society at that time. As a result, training data often encapsulates a wider population risk that over-represents specific characteristics related to the prior period or event, creating unequal risk distributions throughout the population.

4.1. Bias and Fairness

Finding the right balance between building accurate models in deployment and remaining fair is difficult. Model predictions that correlate with sensitive user attributes, even if those predictions are accurate, can cause harm. For example, a model that predicts the likelihood that someone will default on a loan may correlate with race or gender. Given the historical context of racism and sexism in lending institutions, if these correlations are present, the model may be biased against people from these groups—and subsequently cause harm. Eliminating correlation with sensitive user attributes, however, would also eliminate informative predictive signals and could lead the model to make less accurate predictions, making it less beneficial for all users. This presents the unhappy possibility that, for the sake of accuracy, we would allow the model to be biased against certain groups. Similarly, for the sake of fairness across groups, we would allow the model to be less accurate for all users. These are the consequences of trade-offs in different contexts.

In any specific case, the answer may depend on various considerations beyond the accuracy and fairness of the model. Financial services companies already face heightened scrutiny from regulators and the public regarding bias in model predictions, especially concerning lending and credit score models. Negative outcomes for marginalized communities from biased predictions could also invite regulatory scrutiny and legal challenges. Therefore, for financial services companies, it may be prudent to weigh fairness as more important than accuracy, especially as awareness of algorithmic bias, fairness, and discrimination increases and issues are taken up by regulators and the media.

4.2. Transparency and Accountability

In addition to the risk of biased decisions in sensitive sub-domains, including loan approvals, credit scores, and risk checks, negatively impacting people in their lives, jobs, and livelihoods, there are also many other ethical concerns about AI deployment in practice. Such concerns and their impact depend on the consumer and business context of the specific AI application. Generally, AI processing involves the processing of personal data for specific purposes, and consumers expect data protection by default and data protection through design, but they expect that this is not done at the expense of the rest of security and trust. Special attention should be paid to how the deployment and provision affect the three principles of access, control, and transparency, to what extent the technology is explainable and interpretable, and to what extent consumer expectations are met about these. Additional concerns relate to cybersecurity, algorithm dissemination, and associated new risks. For example, what repercussions could result from an intelligent chatbot giving misinformation responses to consumers, or, when bad actors influence a decision or take control of the system? Consideration should also be given to whether the technology causes new risks, and strengths, and which mechanism - if any - would be reasonable for limiting the resulting risk.

A major issue in AI deployments, including in fintech, is the transparency and accountability of decisions taken by proprietary algorithms. What is the rationale of the algorithm? Why did it choose A not B? Who would be liable if the AI system has an error, or generates wrongful behavior? Liability attribution could arise from responsibility for design errors, and those who deploy the model depending on how well the implementation and deployment are made. AI models need to comply with existing regulations or guidelines for model-risk frameworks at the stage of model validation, irrespective of the progress in technology.

Equation 2: AI Security Breach Detection in Payment Systems

$$P(B \mid D) = \frac{P(D \mid B) \cdot P(B)}{P(D)}$$

Where

$P(B \mid D)$: Posterior Probability of a Security Breach Given Observed Data

$P(D \mid B)$: Likelihood of Observed Data Given a Breach

$P(B)$: Prior Probability of a Security Breach

$P(D)$: Marginal Probability of Observing Data D

5. Security Challenges in AI Systems

Artificial Intelligence (AI) is used in a range of systems to achieve a range of functions. Its use in some safety- or security-critical applications requires the AI system to be protected in some well-defined way or on some well-defined criteria. Embedded AI systems, such as intelligent weapons, traffic control systems, and patient monitoring AI, are sensitive to the impact of accidents and adversarial attacks. Safety and security of these systems require handling of accidents caused by unpredictable system errors or unintentional misuse. Intelligent attackers could directly manipulate sensors in such systems, leading to serious safety issues.

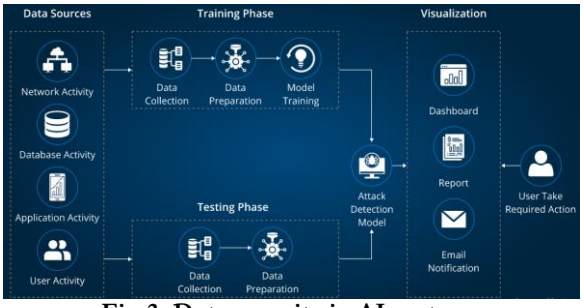

Fig 3: Data security in AI systems

Intelligent systems communicate and exchange data with other systems or humans — possibly sensitive data, such as financial transactions, driving routes, or personal conversations. Leakage of this sensitive data could result in severe privacy violations, as well as allow adversaries to predict and subsequently manipulate the system's behavior. They can also provide means for adversaries to manipulate or monitor the working of an AI system while not directly attacking it. Such a subtle kind of disturbance or monitoring may not be easy to identify. Interdependence of hybrid AI systems can create new escape routes from traditional security defenses. Hybrid AI systems are vulnerable to conventional cyberattacks as well as attacks based on the AI components of the system. In this interplay of dependencies and vulnerabilities, the traditional assumption of mutual trust among the components of a security system may not hold for hybrid AI systems. AI cybersecurity can be enhanced by making security systems "intelligent," such as the detection of zero-day attacks, or "secure," such as formal guarantees for intrusion detection systems.

5.1. Data Privacy Issues

Advancements in artificial intelligence (AI) have led to many innovations in digital payment solutions. However, the use of AI in payment systems raises several security and privacy challenges. For AI systems to work effectively, they should be trained on a considerable amount of high-quality data, which makes it necessary for payment providers to collect and store private information about individuals. Digital payments involve a large number of transactions from millions of customers, which provide sensitive information, including personal identification numbers, phone numbers, addresses, date of birth, and bank account details. This data can be exploited to commit identity fraud, gain unauthorized access to online banking services, create fake accounts, or facilitate terrorist funding.

AI systems requiring the processing of confidential data are also more likely to attract the attention of malicious attackers trying to steal sensitive information. Such systems can be used to train adversarial models that may attempt to collect sensitive data records, generate fake identities and signatures, or create accounts for committing money laundering or identity fraud. Generating imitated documents for gaining customer identity verification is another concern. Identity-based services can be manipulated by adversarial impersonation. As attackers use a wide range of methods to imitate customers, the scope of identity fraud attacks becomes extensive, preventing secure transactions. The storage and transport of sensitive data also raise data privacy issues. Data privacy violations can occur as user data is collected, shared, and transferred across different platforms and databases.

Knowing that AI systems can disclose sensitive user data and compromise data privacy can have dire consequences on individual privacy, even if the risks are small. Moreover, chatbots can display some inadvertent but sensitive data that can affect the individuals involved. There is no clear policy to ensure that model sharing and testing datasets do not violate agreements, so data privacy violations can result in significant penalties for payment service providers. AI vendors need to determine what is required for AI model sharing to avoid any privacy breaches and legal penalties.

5.2. Cybersecurity Threats

A report describes how existing cybersecurity problems become magnified when two or more AI technologies are integrated or when AI finds application in critical systems or in domains in which the adversary has a particular interest. Several AI-specific bugs, vulnerabilities, and exploitations are identified, including bugs and vulnerabilities in the design, development, and operation phases, as well as algorithm-level and implementation-level bugs. Over the past few years, we have witnessed an alarming increase in sophisticated cyberattacks that deploy AI to gain an advantage over targeted organizations. Currently, three types of adversarial attacks exist that either exclusively target AI models or exploit the properties of AI systems to achieve their criminal objectives. The first type of threat is the targeted poisoning of data available for AI training or inference. Sophisticated cyber-adversaries have devised a technique to confuse motion-detection AI by simply painting or placing stickers with specific colors on the model of people such that the AI system misclassifies the individuals' motion as static.

As another sample, in road traffic scenes, the AI-based traffic-light control system may infer that traffic flow is zero, such that lights stay green for longer periods, causing major traffic problems. Regarding this second target threat, AI-based monitoring

and intrusion detection systems designed to sense differences between externally observed system behavior and previously learned statistically normal behavioral patterns are frequently circumvented by smart, stealthy cyber-criminals who first engage in machine-learning-driven phase-in, and carefully construct an initial segment of the attack, such that the system falsely infers new, statistically normal behavior. To short-circuit the intrusion and detection process, cyber attackers may introduce subtle input perturbations or stealthy modifications of the currently running model, for the attack to remain invisible and asymptotically harmless.

6. Regulatory Frameworks for AI in Finance

Financial services are among the most extensively regulated parts of the economy. This is mainly due to an interest in promoting financial stability, consumer protection, and fairness. The regulation of financial services predates the emergence of AI technology but its particular objectives and requirements have implications for AI technology – especially in terms of the accountability of AI systems and how humans should be embedded in decision-making processes. Given the sensitivity of financial service provision, spaces for experimentation with new AI technologies are limited in financial services. Such experimentation is also prone to have detrimental effects if there are hiccups along the way. Consequently, the regulatory frameworks on AI in finance tend to be stricter in terms of both quality and quantity.

There is a patchwork of regulations in place that have been worded with an eye on the interactions of their domain with AI technology deployment and specific additional requirements related to AI systems. For example, even the necessity for human-in-the-loop requirements may be interpreted differently. AI-related legislation either currently under discussion or implementation is expected to create overlaying requirements regarding the AI technology component. In addition to the AI Act which creates requirements at the level of the technological deployment, there will be additional focus on the requirements for the AI-assisted outcome and specific additional sectoral legislation, some of which have been or are already in the process of being proposed or implemented.

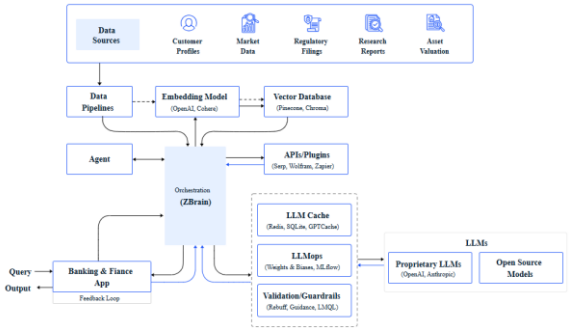

Fig 4: AI in banking and finance

6.1. Global Regulatory Landscape

The use of Artificial Intelligence (AI) technologies in Digital Payments (DPs) has the potential to radically improve their efficacy. However, these deployments also carry the risk of exacerbating existing inequities in DPs, such as exacerbating the gender gap in financial services access or increasing the potential for fraud through identity theft. Addressing these challenges would require thoughtful policymaking. There are many legal and regulatory instruments in place to ensure or guide secure and ethical AI deployments in Finance (AI4F). Specific Data Protection and Privacy Laws (DPPL) govern personal data use which is key to training an AI model. There are general legal instruments that cover both AI and DPs such as anti-discrimination laws and human rights laws that may influence AI4F for DPs. Finally, there are specific Financial Laws (FL) that specifically govern different types of DPs whose rules and mechanisms need to be considered in the context of any AI because many DPs are functionally focused.

Many governments are taking steps towards the establishment of formal legal frameworks for AI systems and so far, much of what exists are voluntary, non-binding principles or guidelines which vary from jurisdiction to jurisdiction. In this Global Regulatory Landscape (GRL), certain jurisdictions have fast-tracked developing formal frameworks for government deployment or use of AI systems aimed at high-risk categories. They have drafted formal proposals for AI regulatory frameworks that have specific stipulations that have consequences for secure and ethical AI4F deployments for using DPs. In this section, we explore the implications of the proposed formal AI frameworks for secure and ethical AI deployments in DPs and provide recommendations.

6.2. Compliance Requirements

Regulated entities in digital payments have existed well before the advent of AI. Some of these requirements restrict or curtail the use of certain technology or otherwise impose certain fiduciary responsibility upon entities, in particular where consumer welfare is at stake. Certain other regulations have been imposed due to data or tech being a core part of the particular transaction or the product or the dependent of the particular transaction or the product. In such cases, compliance of the deployer of AI solutions becomes a necessity to ensure the validity of the deployment of the technology and business efficacy. In payments, consumer and enterprise businesses rely on technology as a crucial component. Coupled with long-term data usage, the integration would be covered by the general tech regulation as an alignment. This is more pronounced for large-scale cases where the risk of failure breeds material risks for the stakeholders. However, there are certain characteristics of the deployers of AI fundamentals that require separate or specific considerations while determining the compliance requirements

as well as the responsibility for such deployments. Further, the compliance considerations also extend to the viability, impact, and importance of the deployment, particularly from a safety and soundness perspective.

7. Best Practices for Ethical AI Deployment

While many academic papers and workshops outline the need for "ethical" AI, it is much more complex to determine how this theoretical need translates into real-world practice. Practices and guidelines therefore fill the gap between theory and practice. This section outlines best practices to offer interim guidelines for ethical decision-making. These guidelines should be understood as a discussion framework for companies, developers, and data providers offering solutions and/or deploying AI. This does not propose concrete definitions of ethics, nor an extended ethical framework. Instead, it proposes interim guidelines for ethical AI decision-making.

Establishing Ethical Guidelines

To get practical, these principles cannot be comprehensive to every situation or context where AI deployment takes place. Mostly they need to be adapted and transformed on the fly in a collaborative and permanent manner. Furthermore, they should not be simply read as procedures and principles. They are outcomes of continuous discussions that help advance how our society can better control what technology becomes.

The creation and deployment of ethical AI systems should require the direct involvement of companies – and therefore themselves, their technologies, and their services for final users, and the oversight of national and international regulatory authorities and also the actors from society directly involved in the ethical AI regulation, given that the same companies develop the algorithms that contribute to determine these ethical AI regulations.

7.1. Establishing Ethical Guidelines

Enshrining ethical principles is an essential first step in the development of ethical AI systems. Various groups within society and global organizations have developed a series of different ethical frameworks in recent years. The AI4People initiative outlines a five-layer pyramid of ethical principles that can be applied to AI: beneficence, non-maleficence, autonomy, justice, and explicability. The Partnership on AI has published eight recommendations, focusing on issues such as safety and reliability, worker augmentation, and diversity and inclusion. The IEEE, through its P7000 series of standards, is developing a larger set of more specific ethics guidelines for those involved in the development of AI and autonomous systems. These guidelines outline ethical objectives such as transparency, accountability, and avoiding new sources of harm and bias. The European Commission High-Level Expert Group on Artificial Intelligence has published the Ethics Guidelines for Trustworthy AI, which more specifically address the issue of 'trustworthiness'. These guidelines state that AI is 'trustworthy' when it is lawful, ethical, and robust in both key ethical dimensions and key technical and socio-economic dimensions. These ethical principles are based on fundamental rights as laid out in the Charter of Fundamental Rights of the European Union.

It is essential to tailor these ethical guidelines to the area of application and context in which the AI system will be deployed, as well as to the organization involved. There is a growing realization that AI is the wider context of an organization, and indeed the wider sector or industry in which it operates can increase its ethical impact significantly. This discussion needs to take into account how ethical the actions of the organization have been up to the point at which it deploys an AI system, as well as its motivations for this deployment. These principles also need to be supported by corresponding internal structures and processes for them to be more than just a marketing exercise. In summary, creating and deploying a trusted AI system requires transparency and accountability during both the design and deployment phases, and also during the issues that arise from unanticipated consequences produced by the system during its active life.

7.2. Stakeholder Engagement

Considering the potential risks and impact of deploying Machine Learning in Digital Payments, we recommend making early and continuous efforts to engage with relevant stakeholder groups. These groups would include representatives from civil society, impacted communities, government, regulators, and industry to build dialogues and feedback loops iteratively. This offers many benefits, such as a better understanding of how the model training deals with sensitive variables to avoid bias and unethical proposals. These discussions can also raise awareness on the type of data being collected and the training labeling actions, if they are partly human-reinforced, helping to address Data Integrity issues and ensuring the data is relevant, of high quality, representative, and free of inaccuracies and biases. In the deployment phase, these channels can help in monitoring model bias, ethical considerations, and performance, especially for the populations and data segments that are not part of the model decision formulation, and continue raising ethical and legal concerns throughout the life cycle. These dialogues are also necessary for understanding and improving interpretability and for the continued effort to strike a fair balance between the utility of using highly predictive models and possible unintended harms. At a policy level, these dialogues can help make a case for legislation standards concerning how Data Protection is conducted by various stakeholders, helping the digital payments space build trust.

8. Technological Innovations in Digital Payments

An increased focus on user convenience and security and the demand for faster payment transactions drive the accelerated advancement of digital payment infrastructure. Growing battles amongst payment gateways have stimulated automatic application-driven integration to enable digital payments from any multichannel platform. Sophisticated and AI-enabled fraud detection systems bring down the risk factor. Blockchain-based digital payment is expected to touch USD 6.7 billion by 2026, reflecting a CAGR of 60.3% between 2021 and 2026. Blockchain is integrating with machine learning to accelerate blockchain transactions, to improve their quality, reliability, security, and transparency and machine learning is being increasingly adopted to achieve automation of blockchain-related tasks to verify and validate information.

Implementing machine learning in digital payments leads to the automation of interpreting behavioral data and filling in KYC forms. Machine learning algorithms are being developed to enhance anti-money laundering capabilities and to reduce transaction fraud at the operational level. Banks are leveraging AI chatbots to reduce their operational costs while boosting revenue. Even large account transactions are witnessing automation in information verification through machine learning algorithms that are designed for their specific purposes. Enabling faster settlements using blockchain technologies in cross-border payments is urgently required. With that, AI plays a vital role by capturing growth in advanced blockchain technology by allowing corporations to make primary payment flows on blockchain channels, while reconciliation can happen separately using separate trusted channels.

Fig 5: Technological Innovations in Digital Payments

8.1. Blockchain and AI Integration

Several technical innovations integrate Blockchains and AI. First, we discuss how Blockchains can store the trained models of AI that are generated using sensitive data Inputs by Individuals and Organizations. AI techniques that do not depend on sensitive data, like Reinforcement Learning for sparse reward problems, are outside the scope of this section. We then touch upon a few ideas on how AI can contribute to Blockchains.

AI Models Immutable Storage. Committing an AI model generated using sensitive data by the model creator onto an immutable Blockchain would provide individuals and organizations the assurance that the creator is not going to leak the model, thereby facilitating the use of sensitive data for training high-value models. Once the model is on the Blockchain, individuals and organizations can get compensated through smart contracts for using the model for further inference tasks because they are giving up additional privacy by using the AI model. Furthermore, a company or factory may get an incentive for deploying a model hosted on the Blockchain that would allow monitoring of the workflow for compliance against a regulatory code of conduct for smart contracts. Other tasks could also be included for incentive compensation. For example, a plant that produces carbon emissions may deploy a model for monitoring excess pollution or a company that provides customer service using chatbots may deploy an emotion detection model for detecting bad emotions in customer conversations. The performance of the model can be further enhanced by allowing other companies to develop additional models for specific demographics.

Equation 3: Privacy Risk Score for Transaction Data

$$P_r = \frac{1}{n} \sum_{i=1}^{n} w_i \cdot \text{PrivacyMetric}(x_i)$$

Where

P_r: Privacy Risk Score for Transaction Data

x_i: Data Feature (e.g., transaction amount, location, user ID)

$\text{PrivacyMetric}(x_i)$: Privacy Risk of Feature x_i

w_i: Weight Assigned to Each Feature i

n: Total Number of Features Analyzed

8.2. Machine Learning Applications

The advancements in computer technologies have laid the groundwork for the rapid growth of various artificial intelligence methods. Digital payment systems are not immune to the effects of this phenomenon. Machine learning in particular has been widely applied in the financial sector, from controlling financial risk to assessing consumer credit. Generating Public Key Infrastructure certificates, one of the essential technologies relied on to create secure communications, has become possible with the use of recurrent neural networks. Machine learning is also at the core of the Bitcoin and Ethereum-related blockchains that autonomously make the proof of work that validates transactions, but only serve the purpose of avoiding double spend attacks and keeping a distributed consensus of the current ledger state, without providing any form of data integrity against unauthorized modifications or allowing the transaction to be executed only by its rightful owner. In regards to data security, machine learning algorithms have enabled the entry into large-scale automatic prevention of income tax evasion and money laundering. Following a preventive law approach, they have reduced the required number of physical accountant audits and board of director investigations by predicting which companies were more likely to commit an infraction, and have put under scrutiny companies with cross-border transactions with countries with a high rate of money laundering. Money laundering, which has moved to digital payments with the advent of cryptocurrencies, has not escaped the predictive application of machine learning. Here, the goal is to identify flows in the blockchain that have their origin in illegally obtained virtual currency, so that they can be prevented from re-entering the financial system.

9. Conclusion

This paper presents a unified, multi-stakeholder perspective on the secure and ethical deployment of AI in the fledgling world of digital payments. AI holds significant promise for improving the speed, efficiency, and security of payment systems, but it also carries considerable risk as fraudsters increasingly seek to exploit potential weaknesses. Fortunately, many of the issues and dilemmas associated with deploying AI in payments are not unique. Indeed, many industries are currently grappling with similar questions and challenges as organizations leverage AI to improve the customer experience. This paper has sought to focus especially on the ethical considerations of employing AI in digital payments. The authors have incorporated diverse insights from a broad range of AI stakeholders to form a stakeholder-driven set of recommendations that balance ongoing innovation with the need to protect end-users and systems. To this end, we have organized guiding recommendations according to six themes that we believe capture the most critical lessons learned from both the stakeholder conversations and existing best practices. These themes include: 1) collaborating to improve digital payments; 2) establishing strong governance, transparency, and accountability regimes; 3) fostering diversity and inclusion; 4) pursuing responsible AI use; 5) designing for security, privacy, and safety; and 6) leveraging holistic risk management practices.

In the context of current public and governmental restiveness towards the promises of AI, we argue that responsible AI employment may be essential for the continued viability of both digital payments and the broader deployment of AI technologies. We look forward to improving upon these guiding recommendations over time and working with others to provide additional resources and cross-stakeholder forums to further explore the myriad of questions and possibilities in this space.

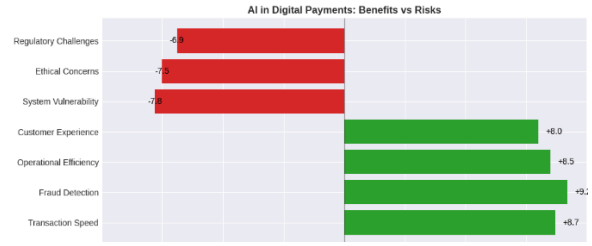

Fig 6: AI in Digital Payments: Benefits vs Risks

9.1. Final Thoughts and Future Directions

This chapter presents a detailed concern about the issues and challenges in the secure and ethical deployment of AI in digital payments, along with possible remedies. AI promises to disrupt several verticals in digital payment systems. It will couple the traditional features of digital payments with intelligent features such as adaptability, automation, improved user experience, and security. Substantial research continues on the design and architecture of responsible AI-based digital payment systems. However, deployment in production is not safe yet. Cyber-physical and application threats continue to affect current digital payment systems seriously. AI will enhance the capability of these threats, posing new challenges. Several areas need further research on risk-aware trustworthy development with secure and ethical deployment. The potential of AI to transform digital payments may remain unrealized if these issues are ignored.

Traditional security solutions in digital payments are troubled with heightened issues. Presently, AI-based digital payment systems are not particularly aware of cyber vulnerabilities or privacy exposure, damaging the broader digital economy. Responsible and accountable development of an AI payment system should consider these security issues. Research on AI pattern recognition and decision-making cannot continue to ignore the current security solutions in digital payments. Detect, Identify, Trust, and Regulation are the four pillars of security in AI-based digital payments. Methodologies for building these pillars as additional layers of AI-based digital payments will make the solution more acceptable for practical deployment. Frameworks such as adversarial training on threat exposure and model transparency will help provide dependable AI and responsible investment in the AI business model. The history of digital payment systems is marked by breaches and distrust. Continuing the same with AI will affect the long-term acceptance of AI systems in the payment space.

10. References

[1] Vankayalapati, R. K. (2020). AI-Driven Decision Support Systems: The Role Of High-Speed Storage And Cloud Integration In Business Insights. Available at SSRN 5103815.

[2] Sondinti, L. R. K., & Yasmeen, Z. (2022). Analyzing Behavioral Trends in Credit Card Fraud Patterns: Leveraging Federated Learning and Privacy-Preserving Artificial Intelligence Frameworks.

[3] Kannan, S. (2022). The Role Of AI And Machine Learning In Financial Services: A Neural Networkbased Framework For Predictive Analytics And Customercentric Innovations. Migration Letters, 19(6), 985-1000.

[4] Harish Kumar Sriram. (2022). AI-Driven Optimization of Intelligent Supply Chains and Payment Systems: Enhancing Security, Tax Compliance, and Audit Efficiency in Financial Operations. Mathematical Statistician and Engineering Applications, 71(4), 16729–16748. Retrieved from https://philstat.org/index.php/MSEA/article/view/2966

[5] Chava, K. (2022). Redefining Pharmaceutical Distribution With AI-Infused Neural Networks: Generative AI Applications In Predictive Compliance And Operational Efficiency. Migration Letters, 19(S8), 1905-1917.

[6] Komaragiri, V. B. (2022). AI-Driven Maintenance Algorithms For Intelligent Network Systems: Leveraging Neural Networks To Predict And Optimize Performance In Dynamic Environments. Migration Letters, 19, 1949-1964.

[7] Chakilam, C. (2022). Generative AI-Driven Frameworks for Streamlining Patient Education and Treatment Logistics in Complex Healthcare Ecosystems. Kurdish Studies. Green Publication. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3719.
[8] Nuka, S. T. (2022). The Role of AI Driven Clinical Research in Medical Device Development: A Data Driven Approach to Regulatory Compliance and Quality Assurance. Global Journal of Medical Case Reports, 2(1), 1275.
[9] Burugulla, J. K. R. (2022). The Role of Cloud Computing in Revolutionizing Business Banking Services: A Case Study on American Express's Digital Financial Ecosystem. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3720.
[10] Pamisetty, A. (2022). Enhancing Cloud native Applications WITH Ai AND Ml: A Multicloud Strategy FOR Secure AND Scalable Business Operations. Migration Letters, 19(6), 1268-1284.
[11] Anil Lokesh Gadi. (2022). Transforming Automotive Sales And Marketing: The Impact Of Data Engineering And Machine Learning On Consumer Behavior. Migration Letters, 19(S8), 2009–2024. Retrieved from https://migrationletters.com/index.php/ml/article/view/11852
[12] Someshwar Mashetty. (2022). Enhancing Financial Data Security And Business Resiliency In Housing Finance: Implementing AI-Powered Data Analytics, Deep Learning, And Cloud-Based Neural Networks For Cybersecurity And Risk Management. Migration Letters, 19(6), 1302–1818. Retrieved from https://migrationletters.com/index.php/ml/article/view/11741
[13] Pandiri, L., & Chitta, S. (2022). Leveraging AI and Big Data for Real-Time Risk Profiling and Claims Processing: A Case Study on Usage-Based Auto Insurance. In Kurdish Studies. Green Publication. https://doi.org/10.53555/ks.v10i2.3760
[14] Recharla, M., & Chitta, S. (2022). Cloud-Based Data Integration and Machine Learning Applications in Biopharmaceutical Supply Chain Optimization.
[15] Nandan, B. P., & Chitta, S. (2022). Advanced Optical Proximity Correction (OPC) Techniques in Computational Lithography: Addressing the Challenges of Pattern Fidelity and Edge Placement Error. Global Journal of Medical Case Reports, 2(1), 58–75. Retrieved from https://www.scipublications.com/journal/index.php/gjmcr/article/view/1292
[16] Srinivasarao Paleti. (2022). Adaptive AI In Banking Compliance: Leveraging Agentic AI For Real-Time KYC Verification, Anti-Money Laundering (AML) Detection, And Regulatory Intelligence. Migration Letters, 19(6), 1253–1267.
[17] Pallav Kumar Kaulwar. (2022). Data-Engineered Intelligence: An AI-Driven Framework for Scalable and Compliant Tax Consulting Ecosystems. Kurdish Studies, 10(2), 774–788. https://doi.org/10.53555/ks.v10i2.3796
[18] Koppolu, H. K. R. (2022). Advancing Customer Experience Personalization with AI-Driven Data Engineering: Leveraging Deep Learning for Real-Time Customer Interaction. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3736.
[19] Dodda, A. (2022). Strategic Financial Intelligence: Using Machine Learning to Inform Partnership Driven Growth in Global Payment Networks. International Journal of Scientific Research and Modern Technology, 1(12), 10–25. https://doi.org/10.38124/ijsrmt.v1i12.436
[20] Jeevani Singireddy,. (2022). Leveraging Artificial Intelligence and Machine Learning for Enhancing Automated Financial Advisory Systems: A Study on AIDriven Personalized Financial Planning and Credit Monitoring. Mathematical Statistician and Engineering Applications, 71(4), 16711–16728. Retrieved from https://philstat.org/index.php/MSEA/article/view/2964
[21] Challa, S. R. (2022). Optimizing Retirement Planning Strategies: A Comparative Analysis of Traditional, Roth, and Rollover IRAs in LongTerm Wealth Management. Universal Journal of Finance and Economics, 2(1), 1276.
[22] Lakkarasu, P., & Kalisetty, S. Hybrid Cloud and AI Integration for Scalable Data Engineering: Innovations in Enterprise AI Infrastructure
[23] Ganti, V. K. A. T., & Valiki, S. (2022). Leveraging Neural Networks for Real-Time Blood Analysis in Critical Care Units. KURDISH. Green Publication. https://doi. org/10.53555/ks. v10i2, 3642.
[24] Kothapalli Sondinti, L. R., & Syed, S. (2022). The Impact of Instant Credit Card Issuance and Personalized Financial Solutions on Enhancing Customer Experience in the Digital Banking Era. Universal Journal of Finance and Economics, 1(1), 1223. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1223
[25] Annapareddy, V. N. (2022). Innovative Aidriven Strategies For Seamless Integration Of Electric Vehicle Charging With Residential Solar Systems. Migration Letters, 19(6), 1221-1236.
[26] Sriram, H. K. (2022). AI Neural Networks In Credit Risk Assessment: Redefining Consumer Credit Monitoring And Fraud Protection Through Generative AI Techniques. Migration Letters, 19(6), 1017-1032.
[27] Komaragiri, V. B., & Edward, A. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. International Journal of Scientific Research and Management (IJSRM), 10(10), 981-998.
[28] Chakilam, C. (2022). Integrating Generative AI Models And Machine Learning Algorithms For Optimizing Clinical Trial Matching And Accessibility In Precision Medicine. Migration Letters, 19, 1918-1933.
[29] Malempati, M. (2022). Machine Learning and Generative Neural Networks in Adaptive Risk Management: Pioneering Secure Financial Frameworks. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3718.
[30] Challa, K. (2022). Generative AI-Powered Solutions for Sustainable Financial Ecosystems: A Neural Network Approach to Driving Social and Environmental Impact. Mathematical Statistician and Engineering.
[31] Anil Lokesh Gadi. (2022). Connected Financial Services in the Automotive Industry: AI-Powered Risk Assessment and Fraud Prevention. Journal of International Crisis and Risk Communication Research , 11–28. Retrieved from https://jicrcr.com/index.php/jicrcr/article/view/2965

[32] Srinivasarao Paleti. (2022). Fusion Bank: Integrating AI-Driven Financial Innovations with Risk-Aware Data Engineering in Modern Banking. Mathematical Statistician and Engineering Applications, 71(4), 16785–16800.
[33] Pallav Kumar Kaulwar. (2022). Securing The Neural Ledger: Deep Learning Approaches For Fraud Detection And Data Integrity In Tax Advisory Systems. Migration Letters, 19(S8), 1987–2008. Retrieved from https://migrationletters.com/index.php/ml/article/view/11851
[34] Dodda, A., Lakkarasu, P., Singireddy, J., Challa, K., & Pamisetty, V. (2022). Optimizing Digital Finance and Regulatory Systems Through Intelligent Automation, Secure Data Architectures, and Advanced Analytical Technologies.
[35] Operationalizing Intelligence: A Unified Approach to MLOps and Scalable AI Workflows in Hybrid Cloud Environments. (2022). International Journal of Engineering and Computer Science, 11(12), 25691-25710. https://doi.org/10.18535/ijecs.v11i12.4743
[36] Vankayalapati, R. K., & Pandugula, C. (2022). AI-Powered Self-Healing Cloud Infrastructures: A Paradigm For Autonomous Fault Recovery. Migration Letters, 19(6), 1173-1187.
[37] Kalisetty, S., Vankayalapati, R. K., Reddy, L., Sondinti, K., & Valiki, S. (2022). AI-Native Cloud Platforms: Redefining Scalability and Flexibility in Artificial Intelligence Workflows. Linguistic and Philosophical Investigations, 21(1), 1-15.
[38] Sriram, H. K. (2022). Integrating generative AI into financial reporting systems for automated insights and decision support. Universal Journal of Finance and Economics, 2(1), 115–131. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1299
[39] Malempati, M. (2022). AI Neural Network Architectures For Personalized Payment Systems: Exploring Machine Learning's Role In Real-Time Consumer Insights. Migration Letters, 19(S8), 1934-1948.
[40] Vamsee Pamisetty, Lahari Pandiri, Sneha Singireddy, Venkata Narasareddy Annapareddy, Harish Kumar Sriram. (2022). Leveraging AI, Machine Learning, And Big Data For Enhancing Tax Compliance, Fraud Detection, And Predictive Analytics In Government Financial Management. Migration Letters, 19(S5), 1770–1784. Retrieved from https://migrationletters.com/index.php/ml/article/view/11808
[41] Kishore Challa, Jai Kiran Reddy Burugulla, Lahari Pandiri, Vamsee Pamisetty, Srinivasarao Paleti. (2022). Optimizing Digital Payment Ecosystems: Ai-Enabled Risk Management, Regulatory Compliance, And Innovation In Financial Services. Migration Letters, 19(S5), 1748–1769. Retrieved from https://migrationletters.com/index.php/ml/article/view/11807
[42] Botlagunta Preethish Nadan. (2022). Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing. Mathematical Statistician and Engineering Applications, 71(4), 16749–16773. Retrieved from https://philstat.org/index.php/MSEA/article/view/2967
[43] Kaulwar, P. K. (2022). The Role of Digital Transformation in Financial Audit and Assurance: Leveraging AI and Blockchain for Enhanced Transparency and Accuracy. Mathematical Statistician and Engineering Applications, 71 (4), 16679–16695.
[44] Karaka, L. M. (2021). Optimising Product Enhancements Strategic Approaches to Managing Complexity. Available at SSRN 5147875.
[45] Katnapally, N., Murthy, L., & Sakuru, M. (2021). Automating Cyber Threat Response Using Agentic AI and Reinforcement Learning Techniques. J. Electrical Systems, 17(4), 138-148.
[46] Boppana, S. B., Moore, C. S., Bodepudi, V., Jha, K. M., Maka, S. R., & Sadaram, G. (2021). AI And ML Applications In Big Data Analytics: Transforming ERP Security Models For Modern Enterprises.
[47] Chinta, P. C. R., & Karaka, L. M.(2020). AGENTIC AI AND REINFORCEMENT LEARNING: TOWARDS MORE AUTONOMOUS AND ADAPTIVE AI SYSTEMS.
[48] Velaga, V. (2022). Enhancing Supply Chain Efficiency and Performance Through ERP Optimization Strategies.