ISSN: 2182-2069 / E-ISSN: 2182-2077

The Future of Trade: How Startups are Transforming Customs with AI and Internet Security Solutions

Marta Sarvas[1*], Solomiya Ohinok[2], Ihor Kulyniak[3], and Ivanna Havrylyuk[4]

[1*]Chicago-Kent College of Law, Chicago, IL, USA. martasarvas@gmail.com, https://orcid.org/0009-0002-8863-7622

[2]Lviv Polytechnic National University, Lviv, Ukraine. solomiia.v.ohinok@lpnu.ua, https://orcid.org/0000-0001-5462-5362

[3]Lviv Polytechnic National University, Lviv, Ukraine. ihor.y.kulyniak@lpnu.ua, https://orcid.org/0000-0002-8135-4614

[4]Lviv National Environmental University, Dubliany, Ukraine. ivanna110983@ukr.net, https://orcid.org/0000-0002-9517-3021

Received: April 30, 2025; Revised: June 16, 2025; Accepted: July 29, 2025; Published: August 30, 2025

Abstract

The operational difficulties faced by customs departments result from increasing international trade complexities that affect their security and efficiency procedures. Standard data infrastructures cannot quickly access needed information during new threat management which requires human assistance. Startups which implement strong cybersecurity measures create Artificial Intelligence systems that enhance efficiency in customs operations. The SAACE framework uses secure AI technology to provide advanced risk management solutions and automated compliance systems. Our data management system provides precise information management during every stage of customs processing. The SAACE framework uses Machine Learning for risk prediction and Natural Language Processing for document verification together with Computer Vision approaches for non-physical inspections. The blockchain technology ensures data integrity through defense mechanisms against unauthorized changes and it provides user information protection with end-to-end encryption based on Zero Trust Architecture principles. Technology updates to customs operations improve transparency and trade support services while strengthening border security systems. Global supply chain networks achieve quicker clearance processes and enhanced threat detection abilities when stakeholders share their data through the new system.

Keywords: Artificial Intelligence, Blockchain, Customs Modernization, Cybersecurity, International Trade, Machine Learning, Risk Management, Startups, Supply Chain Security, Zero Trust Architecture.

1 Introduction

1.1. Background

The connection of national markets through international trade leads to worldwide economic growth. Customs administrations enable international trade operations but struggle with growing

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 284-297.
DOI: *10.58346/JISIS.2025.I3.020*

*Corresponding author: Chicago-Kent College of Law, Chicago, IL, USA.

operational challenges. The growing number of shipments and intricate supply chain logistics outpace existing customs infrastructure because changing regulatory requirements create ongoing challenges (Shpak et al., 2024). Security breaches trigger enforcement actions in modern customs systems which integrate outdated manual document checks with separate information systems that delay threat detection.

1.2. Problem Statement

The practices of customs administration generate high operational costs for both public sector organizations and businesses and cause clearance delays in addition to inconsistent regulatory enforcement. More critically, they present security vulnerabilities (Saxena, 2024). Separation between data systems obstructs proper risk evaluation which hides dangerous materials and security weaknesses resulting in manual process mistakes and fraudulent activities by staff (Shpak et al., 2024; Saxena, 2024). As legacy systems fail to defend customs data integrity and maintain operational availability modern cyber threats require advanced security solutions. International customs systems require immediate modernization to deploy intelligent solutions aimed at enhancing security protocols as well as operational performance (Chopra & Patil, 2025).

1.3. Role of Startups

The transformation of technology through innovation requires strong backing from startup companies. Technology startups maintain their rapid pace of product development and innovation by avoiding outdated systems and administrative barriers (George & Baskar, 2024). AI and Cybersecurity startups create intelligent applications which will lead to major advancements in customs processes.

1.4. Emergence of AI & Security Solutions

Customs operations benefit from decision-making data insights produced by automated systems created through Machine Learning (ML), Natural Language Processing (NLP), and Computer Vision (CV) technologies (Chauhan & Desai, 2022; Chinnaiyan et al., 2025). Machine Learning helps identify risk patterns by analyzing datasets and Natural Language Processing accelerates trade document verification while Computer Vision develops non-contact inspection methods (Alsbatin et al., 2025; Chinnaiyan et al., 2025). Customs systems protect trade data infrastructure from emerging threats by implementing blockchain internet security together with advanced encryption standards and Zero Trust security models (Emiliaty, 2024; Chlaihawi, 2024).

1.5. Aim and Structure

The Secure AI-Augmented Customs Environment framework (SAACE) combines advanced internet security tools from startups with powerful artificial intelligence. Modernizing customs operations makes them more efficient, enhances security, and increases process transparency. This article is organized as follows: The conceptual framework development process receives a detailed explanation in Section 2. The SAACE framework proposal, with its architectural design and essential modules, is described in Section 3. Section four analyzes theoretical benefits while studying startup involvement in real-world applications and potential management challenges—section 5 functions as the paper's conclusion by reviewing the proposal and exploring its trade implications.

2 Methodology

2.1. Approach

The research team implemented conceptual methods to develop a new theoretical framework. The study linked customs administration data with international trade logistics expertise to artificial intelligence techniques such as ML, NLP, and CV and implemented cybersecurity methods, including blockchain technology and ZTA principles, during the examination of technology startup advancements. Academic studies and industry reports (Shpak et al., 2024; Saxena, 2024; Joshi, 2024) show that current customs practices create operational inefficiencies and substantial delays while exposing security vulnerabilities. Our potential solutions emerged from combining artificial intelligence systems with security technology capabilities (Ganesan et al., 2025). The SAACE framework evolved through iterative conceptual modeling which united various technological components to meet current customs operational requirements.

2.2. Framework Design Principles

The SAACE framework was created based on several important principles that allow for the development of advanced and efficient customs systems.

- **Security-by-Design** demands that developers incorporate security components into their systems from the beginning of the development process instead of implementing them after development is complete. Fundamental security components within the system framework consist of data encryption and strong access controls which function in conjunction with threat modelling (Khan, 2023; Masys, 2018).
- **Data-Driven Decision Making:** Leveraging AI to extract actionable intelligence from diverse data sources for improved risk assessment and resource allocation (Chinnaiyan et al., 2025).
- **Automation:** Automating repetitive, manual tasks (e.g., document checks, classification) to increase efficiency and reduce human error (George & Baskar, 2024).
- **Transparency & Auditability:** Utilizing technologies like blockchain to create secure, immutable records of key events, enhancing trust and accountability among stakeholders (Emiliaty, 2024; Adewale et al., 2022).
- **Interoperability:** Designing the framework with standardized APIs and data formats to facilitate seamless information exchange between customs authorities, trade partners, and other relevant agencies.
- **Scalability & Flexibility:** Ensuring the architecture can handle growing trade volumes and adapt to future technological advancements and regulatory changes.
- **User-Centricity:** Focusing on intuitive interfaces and streamlined processes for all users (customs officers, traders, brokers).

2.3. Technology Selection Rationale

The SAACE framework's architecture requires strategic integration of particular advanced technologies to function correctly. The choice of these technologies was deliberate because they demonstrated effective performance in resolving essential weaknesses and operational inefficiencies, which the first phase of problem analysis revealed. The evaluation of complex trade data required ML because its

superior pattern detection capabilities combined with its critical importance in risk management for high-volume trading environments made it indispensable (Saxena, 2024; Chinnaiyan et al., 2025). NLP was chosen for the solution of manual data entry and document verification because it independently analyzes trade documents to extract needed information while performing compliance verification and minimizing human intervention, and maximizing accuracy (George & Baskar, 2024; Joshi, 2024). Computer Vision technology enables non-intrusive inspection systems to automate the analysis of X-ray images, thereby increasing detection speed and accuracy for contraband and other anomalies (Emiliaty, 2024). A permissioned Blockchain system maintains transparent operations and trust among all customs operation stakeholders (Chang et al., 2020). The distributed ledger system protects essential supply chain data against tampering and produces a permanent transaction and event record that remains auditable (Emiliaty, 2024; Adewale et al., 2022; Mattsson, 2022). ZTA provides complete security for entire systems through a contemporary strategy that moves beyond traditional perimeter defenses. Zero Trust Architecture minimizes system vulnerabilities while strengthening defenses against advanced cyber threats through continuous identity checks and precise access control for all users and devices.

3 Proposed Solution

The SAACE system is an advanced AI security framework designed for smart customs operations. This system transforms traditional customs processes into one effective platform that uses modern technology. SAACE allows secure information sharing and gives decision-makers useful AI insights, helping to automate basic tasks. Technology startups create targeted solutions that improve the SAACE system (Khan, 2023; Masys, 2018).

3.1. Conceptual Architecture

The SAACE framework architecture uses a flexible modular system with different levels. This design allows components to work together effectively and adapt to future needs. The functional modules within this architecture are arranged into logical layers in Figure 1 to enable sequential data and command flow starting from ingestion and extending to decision support.

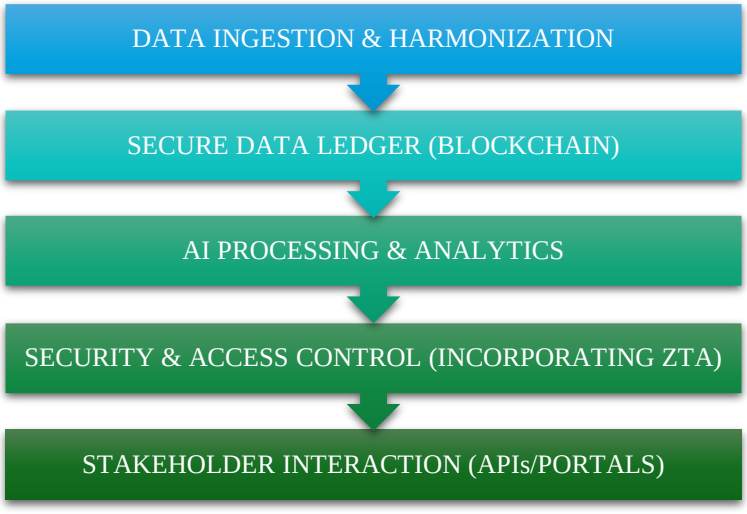

Figure 1: Conceptual Architecture – the SAACE Framework

The system architecture obtains declarations and sensor information from considerable sources through secure blockchain technology, which maintains data integrity. Artificial intelligence conducts

risk analysis, and specific security measures provide protection to stakeholders via customized interfaces.

3.2. AI Module for Risk Management & Compliance

The core SAACE framework module supports customs officials using automated advanced analysis to make informed risk management and regulatory compliance decisions. The system's intelligence capability relies on Advanced Machine Learning models as its fundamental building block. Moving beyond static rulesets or simple profiling, these supervised and unsupervised algorithms perform real-time risk scoring of shipments, associated declarations, and involved trade parties by integrating and analyzing highly diverse datasets (Shpak et al., 2024; Saxena, 2024).

Information sources ranging from structured historical clearance records and established trade partner profiles to dynamic data like shipping routes, vessel tracking (AIS), unstructured open-source intelligence (OSINT), and potentially real-time IoT sensor data are fused to identify subtle anomalies and complex patterns indicative of heightened risk. This sophisticated analysis allows for the prediction of high-risk transactions requiring customs intervention, enabling a crucial shift from resource-intensive random or static profile-based checks towards truly dynamic, intelligence-led targeting, thereby optimizing the allocation of inspection resources and expediting legitimate trade flow (Blahun et al., 2017; Karyy et al., 2021).

Complementing the risk analytics, Natural Language Processing techniques address the significant challenge of managing, understanding, and verifying the vast quantities of textual information inherent in international trade documentation (George & Baskar, 2024; Chinnaiyan et al., 2025). Manual processing of such documents is not only time-consuming but also prone to errors and inconsistencies, especially across different languages. NLP sub-modules within the SAACE framework automate the ingestion, semantic understanding, validation, and cross-referencing of critical documents such as commercial invoices, packing lists, certificates of origin, and bills of lading. These systems conduct automatic compliance evaluations against digitized regulations in knowledge bases and they detect document discrepancies or fraud signals while extracting key data entities for precise customs system entry with minimal human intervention and they provide significant help with the challenging task of automated Harmonized System (HS) code assignment using text-based product descriptions. The automated system cuts manual labor expenses and decreases data entry mistakes as machine translation speeds up compliance checks by removing language barriers.

Advanced Computer Vision solutions enhance Non-Intrusive Inspection technology efficiency and performance when operating with X-ray and gamma-ray systems and future cargo scanners that use CT technology (Emiliaty, 2024). Manual scan image review persists as essential but faces difficulties with slow processing speeds and operator fatigue, which limits the discovery of complex concealed discrepancies within packed cargo loads.

AI systems that learn from extensive image databases of secure items and threats can quickly and accurately analyze Non-Intrusive Inspection system results. They can automatically detect potential threats based on density, shape, texture, and location; identify misdeclared goods by comparing visual signatures against expected patterns for declared items; or flag subtle deviations that might warrant closer examination by an experienced officer. By automatically flagging only those specific containers or items deemed suspicious, CV components significantly increase overall threat detection probability while simultaneously offering the potential to drastically reduce the need for time-consuming and costly physical inspections of cargo assessed as low-risk by the integrated ML module. The key functions and interplay of these core AI components are summarized in Table 1 below.

Table 1: Summary of AI Component Functions Within the SAACE Framework

AI Technology	Primary Function(s) in Customs	Example Inputs	Example Outputs	Key Benefit(s)
Machine Learning (ML)	Predictive Risk Assessment (Fiscal, Security, Compliance); Anomaly Detection; Trade Volume Forecasting	Historical clearance & compliance data; manifests; shipping routes; party profiles/networks; OSINT; IoT sensor data; sanctions lists; commodity databases	Risk scores with confidence levels; anomaly alerts & descriptions; targeted inspection justifications; resource allocation recommendations; trend reports & forecasts	Proactive threat/non-compliance ID; optimized resource deployment; faster clearance for low-risk trade; improved compliance rates; enhanced strategic planning
Natural Language Processing (NLP)	Automated Document Verification; Data Extraction & Classification; Automated Translation; Chatbot Support	Trade documents (Invoices, B/L, CoO, Permits etc.); free-text descriptions; customs regulations DB; user queries via portals; communication logs	Compliance pass/fail flags; extracted & structured data; discrepancy/error alerts; suggested HS codes; translated text; chatbot responses & FAQs	Significantly reduced manual workload; improved data accuracy & consistency; faster compliance checks; reduced language barriers; enhanced stakeholder support
Computer Vision (CV)	Automated NII Scan Analysis (Anomaly/Threat Detection); Object Recognition; Manifest-Image Comparison	X-ray, Gamma-ray, CT scan images; drone/CCTV surveillance feeds; reference image libraries (threats, goods); declared manifest item lists	Highlighted regions of interest (ROIs) on images; anomaly/threat probability scores; identified objects list; scan vs. manifest discrepancy flags; alerts for physical inspection	Increased detection accuracy (incl. concealed items); reduced need for physical inspection of low-risk cargo; faster NII process throughput; support for remote image analysis centers

3.3. Secure Data Exchange & Integrity Module

Ensuring the robust security and verifiable integrity of the vast amounts of sensitive data involved in international trade is fundamental to the SAACE framework. With global losses from customs fraud, valuation discrepancies, and illicit trade estimated to run into hundreds of billions of euros annually, and cyberattacks increasingly targeting critical supply chain infrastructure (Khan, 2023), a multi-layered, modern security approach is imperative, moving beyond traditional defenses. The sheer volume of data handled, with major customs authorities processing potentially millions of declarations and associated data points daily, creates a vast attack surface that demands state-of-the-art protection.

A core component addressing data integrity and transparency within SAACE is the implementation of a permissioned blockchain ledger, potentially based on enterprise-grade technologies like Hyperledger Fabric or similar DLT solutions suitable for consortium environments (Joshi, 2024). Unlike

public blockchains accessible to anyone, a permissioned ledger restricts network participation and transaction validation rights to explicitly authorized stakeholders, such as customs authorities from participating countries, verified traders meeting specific compliance criteria, authorized logistics providers, and other relevant government agencies (e.g., phytosanitary authorities). This controlled environment maintains confidentiality while leveraging the core benefits of blockchain technology.

Key customs events and critical data points – such as the submission hash and timestamp of a declaration, container scan results or inspection outcomes, duty assessment details and payment confirmations, chain of custody updates from carriers, and the final goods release status – are recorded as timestamped, cryptographically linked transactions. This process creates an immutable, tamper-evident, and chronologically verifiable distributed audit trail for the entire customs lifecycle. Such a shared, secure ledger significantly enhances trust among participants by providing a reliable 'single source of truth', facilitates streamlined audits, simplifies dispute resolution, and increases overall transparency in the customs process. The interaction model, illustrating how various authorized parties securely contribute validated data to and access relevant information from this shared ledger based on their permissions, is depicted conceptually in Figure 2.

Figure 2: Blockchain Interaction in Customs Data Exchange

Complementing the ledger's integrity features, comprehensive data protection for all information flowing through or stored within the SAACE framework is ensured through the mandatory application of strong end-to-end encryption standards (Masys, 2018). Sensitive information, encompassing both Personally Identifiable Information (PII) of individuals involved in trade and valuable Commercially Sensitive Information (CSI) contained within trade documents, must be rigorously encrypted both while in transit across networks (e.g., utilizing robust protocols like TLS 1.3 or higher for APIs and communications) and while at rest within databases, file systems, or system components (e.g., employing AES-256 or stronger symmetric encryption algorithms with secure key management). Beyond data encryption, access control within the SAACE framework is governed by the principles of a Zero Trust Architecture (ZTA) (Khan, 2023; Adewale et al., 2022). This represents a critical paradigm

shift away from outdated perimeter-based security models ('trust but verify') that often grant excessive implicit trust to users and devices once they are inside the network boundary. ZTA, conversely, operates on the principle of "never trust, always verify." Every single access request, regardless of its origin (internal network, remote user, API call), must be strictly and continuously authenticated and authorized before granting access to any resource. Authorization decisions are made dynamically, based not just on user identity but also incorporating device health posture, location, time of access, the specific resource requested, and real-time risk assessment feeds. Utilizing a combination of core ZTA technologies – such as strong identity and access management (IAM) with multi-factor authentication (MFA), granular network micro-segmentation, continuous monitoring and behavioral analysis, and adaptive, policy-based access controls – ZTA significantly minimizes the potential attack surface and provides a much more resilient defense against common modern threats, including compromised user credentials, insider risks, sophisticated phishing attacks, and lateral movement by malicious actors within the network (Adewale et al., 2022). Adopting this modern security posture is essential for protecting the high-value data and critical functions of interconnected national and international customs systems.

3.4. Facilitating Stakeholder Interaction within SAACE

Effective interaction between the diverse range of stakeholders involved in international trade and the core SAACE system is paramount for realizing the framework's potential benefits in streamlining processes and enhancing collaboration. This crucial interaction is primarily facilitated through two complementary mechanisms: secure, user-centric web portals and robust, standardized Application Programming Interfaces (APIs), designed to accommodate varying technical capabilities and integration needs across the trade community (Santoro et al., 2019). It is fundamental that both interface types operate under the stringent security controls mandated by the Zero Trust Architecture discussed previously, ensuring every interaction is rigorously authenticated and authorized based on verified identity, context, and permissions before access is granted.

Secure web portals serve as the primary, human-facing interface for many participants, particularly individual traders, customs brokers, and small-to-medium enterprises (SMEs) who may not possess the resources or need for complex direct system integrations. These portals must be designed with a strong focus on user experience, offering intuitive dashboards that provide clear, real-time visibility into critical information. This includes the status of submitted declarations, shipment tracking updates potentially derived from ledger events, notifications regarding required actions (such as outstanding duty payments), documentation requests, and confirmation of goods release. Essential functionality should extend beyond basic submission and monitoring to encompass secure document uploads, management of company profiles and user permissions (vital for organizations with multiple staff interacting with customs), access to historical transaction data for reporting and auditing, and potentially integrated secure messaging channels for direct, context-specific communication with customs officials to resolve queries efficiently. By offering guided workflows, pre-filled data where possible, and clear status indicators, these portals aim to simplify compliance complexity, significantly reduce errors common in manual processes, and empower users with timely, actionable information.

For larger trading entities, logistics providers, financial institutions, and other government agencies often operating with sophisticated internal IT systems (like ERPs, Transport Management Systems, or dedicated customs software), well-documented and standardized APIs are the cornerstone of efficient, automated data exchange within the SAACE ecosystem (Khanyi et al., 2024). These APIs enable seamless, real-time, system-to-system integration between these external platforms and the central customs framework. This automation is critical for handling high-volume trade efficiently, eliminating

costly, time-consuming, and error-prone manual data re-entry across different systems. It allows for real-time synchronization of status updates (e.g., clearance status feeding directly into a logistics provider's system) and facilitates highly streamlined end-to-end digital workflows. To maximize adoption and ensure interoperability within a complex ecosystem potentially involving solutions from various providers (including innovative startups specializing in trade tech), the design of these APIs should adhere to international best practices and relevant standards, potentially leveraging elements of the WCO Data Model and utilizing modern architectural principles like REST. Effective API integration demands that developers have access to full documentation and sandbox testing environments.

Zero Trust security policies demand complete verification for every access attempt and data transaction request coming from web portals or automated API calls. The policy enforcement mechanism protects specific data sets and necessary functions by confirming identities and roles which restricts access to authorized users and systems thereby safeguarding sensitive trade information for all stakeholders.

4 Discussion

4.1. Theoretical Advantages of the Framework

The SAACE framework delivers enhanced theoretical advantages when compared to traditional customs models. Organizations that integrate AI into their risk management systems can predict risks by analyzing data instead of depending on static rule-based systems (Adeniran et al., 2024). NLP technology in document automation will lower administrative burdens while speeding up the clearance process for legitimate trade transactions. The implementation of CV technology enhances inspection capabilities, resulting in improved security outcomes and decreased physical examinations for low-risk items. Crucially, the secure architecture, incorporating blockchain for data integrity (Eghmazi et al., 2024; Sengupta & Deshmukh, 2024) and ZTA for access control (Khan, 2023), addresses key vulnerabilities related to data tampering, unauthorized access, and cyber threats.

4.2. Role of Startups in Implementation

Implementing such a comprehensive framework requires significant technological expertise and agility, areas where startups often excel (George & Baskar, 2024; Sreenivasan & Suresh, 2024). Customs agencies can leverage the innovation ecosystem by partnering with specialized startups to develop and deploy specific modules within the SAACE architecture. AI startups could provide best-in-class algorithms for risk scoring or image analysis, while cybersecurity startups could implement the ZTA components or blockchain solutions (Mattsson, 2023). This collaborative model allows customs authorities to access cutting-edge technology faster and potentially more cost-effectively than developing everything in-house, while startups gain access to a critical infrastructure market. Public-private partnerships and pilot programs would be essential to validate and scale these startup-driven solutions within the operational customs environment.

4.3 Grounding the Framework: Empirical Perspectives and Validation Insights

While the SAACE framework presented herein is a conceptual model, grounding its components in emerging real-world applications and observable market trends provides valuable context for its potential feasibility and impact. Examining current developments reveals nascent implementations and entrepreneurial activity that echo elements of the proposed architecture, often driven by specialized technology startups seeking to modernize trade processes.

For instance, initiatives leveraging ML-powered risk assessment (Shpak et al., 2024; Saxena, 2024), similar to the module described, are being piloted or deployed in various forms by customs agencies globally, frequently in partnership with agile tech firms (George & Baskar, 2024). Early reports from such projects consistently highlight the potential for significant improvements in efficiently targeting high-risk shipments while simultaneously accelerating the clearance of demonstrably low-risk cargo. These pilot programs often aim for ambitious targets, with some seeking reductions in unnecessary physical inspections by as much as 30-40% compared to baseline methods, although achieving consistent results depends heavily on access to diverse, high-quality, and standardized data for effective model training, which remains a frequently cited challenge (Bovet Emanuel, 2025).

Similarly, the principles behind using permissioned blockchains or Distributed Ledger Technology (DLT) for secure trade documentation (Khan, 2023; Joshi, 2024) are actively being explored by various trade consortiums, logistics platforms, and technology providers (Priem, 2020). Pilot projects focusing on digitalizing and securely sharing key documents like electronic Bills of Lading (e-B/L) or Certificates of Origin have shown demonstrable potential in reducing documentation processing times and associated administrative costs – with estimates often cited around 15-20% for specific, well-defined use cases in controlled environments. The enhanced auditability and reduction in disputes are also noted benefits. However, translating these pilot successes into widespread adoption faces considerable hurdles related to achieving the necessary network effect among diverse stakeholders, establishing effective and interoperable governance models, and integrating seamlessly with existing legacy systems (Priem, 2020).

The application of CV-enhanced NII systems (Emiliaty, 2024) represents another area of rapid advancement, with startups specializing in AI-driven image analysis increasingly collaborating with customs agencies and scanner manufacturers. Preliminary results emerging from operational tests and specialized research indicate that well-trained AI algorithms can significantly augment human inspectors. These systems show potential for improving detection accuracy for specific types of concealed items or anomalies by potentially 10-15% over manual image review alone under certain test conditions, facilitating faster throughput and enabling more effective implementation of remote or centralized image analysis centers (Umoga et al., 2024).

Further empirical grounding for the relevance and timeliness of integrated solutions like SAACE comes from observing the dynamics of the technology startup ecosystem itself. Recent years have witnessed a marked increase in venture capital funding directed towards "TradeTech" and "GovTech" startups, including those specifically targeting customs modernization and supply chain security (Soh & Lee, 2020). The proliferation of new companies focused on applying AI, blockchain, IoT, and advanced security protocols to trade facilitation challenges indicates a strong market perception of both the need and the technological opportunity for innovation in this critical domain (Chang et al., 2020).

The potential quantitative impact of adopting such technologies, as suggested by pilot projects and inherent technological capabilities, can be illustratively summarized and compared against traditional baseline estimates as follows (Table 2):

Table 2: Illustrative Comparison of Key Metrics: Traditional vs. SAACE-Inspired Customs Processes

Metric	Traditional Process (Baseline Estimate)	SAACE-Inspired Process (Potential / Target) *	Key Enabling Technologies (in SAACE)
Avg. Clearance Time (Low-Risk Goods)	24 - 72+ Hours	< 12 Hours (Target)	ML Risk Assessment, NLP Doc Processing, Blockchain Release
Physical Inspection Rate (% of Total)	Highly Variable (e.g., 5-15%)	Reduced significantly for low-risk (e.g., by est. 30-40%)	ML Risk Assessment, CV Scan Analysis
High-Risk Item Detection Accuracy (Targeted)	Baseline / Variable	Improved by est. 10-15% (for specific threats via NII)	ML Risk Assessment, CV Scan Analysis
Documentation Error/Discrepancy Rate	Estimated 5-10%	Significantly Reduced (e.g., >50% reduction potential)	NLP Doc Verification, Blockchain Data Integrity
Data Transparency & Auditability	Low / Siloed / Paper-based	High (Permissioned, Immutable Ledger)	Permissioned Blockchain
Manual Processing Effort (per declaration)	High (Data entry, checks)	Dramatically Reduced	NLP Data Extraction, AI Compliance Checks

Note: Figures in the 'SAACE-Inspired Process' column are illustrative targets or estimates based on the potential impact of the technologies discussed and findings from pilot projects referenced conceptually in sources (Bovet Emanuel, 2025l; Priem, 2020; Soh & Lee, 2020). Actual results will vary based on specific implementation, data quality, and operational context.

4.4. Addressing Potential Concerns

While promising, the implementation of such a framework requires careful consideration of potential concerns (Feretzakis et al., 2025). Data privacy must be paramount, adhering strictly to regulations like GDPR and implementing techniques like data minimization and differential privacy where applicable within the AI modules. Ensuring interoperability between different systems (customs, trade partners, other agencies) requires adherence to international standards (like the WCO Data Model) and well-defined APIs. Algorithmic transparency and fairness are critical for the AI components; risk models must be regularly audited for bias and effectiveness, with mechanisms for oversight and redress. The ZTA implementation also requires careful planning to ensure legitimate access is not unduly hindered (Adewale et al., 2022).

4.5. Scalability and Future Directions

The modular design of the SAACE framework is intended to support scalability and future evolution. As trade volumes grow, compute resources for AI processing can be scaled accordingly (likely using cloud infrastructure). Future enhancements could include integrating data from IoT devices deployed along the supply chain (e.g., smart seals, environmental sensors) for enhanced real-time visibility and risk assessment. Further research could explore the use of more advanced AI techniques, such as federated learning for privacy-preserving collaborative risk analysis across different customs administrations, or explainable AI (XAI) to improve the transparency of risk-scoring models (Kapoor & Chatterjee, 2023).

5 Conclusion

Traditional customs procedures are increasingly challenged by the scale, speed, and security demands of modern global trade. This paper argues that a paradigm shift, driven by innovative startups leveraging Artificial Intelligence and advanced internet security solutions, is essential for the future of trade facilitation and border management. We have proposed the Secure AI-Augmented Customs Environment (SAACE) – a theoretical framework integrating ML, NLP, CV, blockchain, and Zero Trust Architecture principles. This framework aims to create a customs ecosystem that is significantly more efficient (through automation and data-driven targeting), secure (through predictive risk assessment, enhanced inspection, and robust cybersecurity), and transparent (through immutable record-keeping and controlled data sharing). While implementation requires addressing important considerations like data privacy and interoperability, the potential benefits for facilitating legitimate trade while strengthening security are immense. Startups, with their technological agility and specialized focus, are key enablers in realizing this vision of smarter, more secure global trade, working in partnership with customs authorities and the wider trade community. The continued development and adoption of such integrated solutions will be critical for navigating the complexities of 21st-century international commerce.

References

[1] Adeniran, I. A., Efunniyi, C. P., Osundare, O. S., & Abhulimen, A. O. (2024). Enhancing security and risk management with predictive analytics: A proactive approach. *International Journal of Management & Entrepreneurship Research*, *6*(8), 32-40. https://doi.org/10.56781/ijsret.2024.4.1.0021

[2] Adewale, T. T., Olorunyomi, T. D., & Odonkor, T. N. (2022). Blockchain-enhanced financial transparency: A conceptual approach to reporting and compliance. *International Journal of Frontiers in Science and Technology Research*, *2*(1), 024-045. https://doi.org/10.53294/ijfstr.2022.2.1.0027

[3] Alsbatin, L., Alrifai, B. M., Zawaideh, F., & Alawneh, T. A. (2025). Advancing IoMT security: Machine learning-based detection and classification of multi-protocol cyberattacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(2), 228–247. https://doi.org/10.58346/JOWUA.2025.I2.015.

[4] Blahun, I., Dmytryshyn, L., & Leshuk, H. (2017). Simulative model for evaluation of investment processes in the regions of Ukraine. *Investment management and financial innovations*, (14, № 3 (contin. 2)), 322-329. http://dx.doi.org/10.21511/imfi.14(3-2).2017.03

[5] Bovet Emanuel, P. (2025). *Exploring Decision Advantages: Improving Speed, Precision and Efficiency inMilitary Targeting by Applying Artificial Intelligence* (Doctoral dissertation, Försvarshögskolan (FHS)). https://doi.org/10.62061/leiy7136

[6] Chang, Y., Iakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, *58*(7), 2082-2099. https://doi.org/10.1080/00207543.2019.1651946

[7] Chauhan, S., & Desai, M. (2022). Machine Learning-Based Predictive Maintenance Scheduling in Industrial Settings. *International Academic Journal of Science and Engineering, 9*(4), 9–12.

[8] Chinnaiyan, B., Balasubaramanian, S., Jeyabalu, M., & Warrier, G. S. (2025). AI Applications–Computer Vision and Natural Language Processing. *Model Optimization Methods for Efficient and Edge AI: Federated Learning Architectures, Frameworks and Applications*, 25-41. https://doi.org/10.1002/9781394219230.ch2

[9] Chlaihawi, M. O. A. (2024). Application of Blockchain Technology to Reduce Costs. *International Academic Journal of Social Sciences*, *11*(1), 26-38. https://doi.org/10.9756/IAJSS/V11I1/IAJSS1104
[10] Chopra, N., & Patil, V. (2025). Design of advancements in AI for cyber threat detection. *Essentials in Cyber Defence*, 16-34.
[11] Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. *IoT*, *5*(1), 20-34. https://doi.org/10.3390/iot5010002
[12] Emiliaty, A. (2024). Blockchain technology: Revolutionizing data integrity and security in digital environments. *Journal of Advanced Technological Innovations*, *1*(1), 1-8.
[13] Feretzakis, G., Vagena, E., Kalodanis, K., Peristera, P., Kalles, D., & Anastasiou, A. (2025). GDPR and Large Language Models: Technical and Legal Obstacles. *Future Internet*, *17*(4), 151. https://doi.org/10.3390/fi17040151
[14] Ganesan, A., Velanganni, R., Rajapriya, M., Sundara Bala Murugan, P., & Paranthaman, P. (2025). The Role of Artificial Intelligence in Personalized Marketing: *Integrating AI with Information Systems for Competitive Advantage. Indian Journal of Information Sources and Services, 15*(1), 220–229. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.28
[15] George, A. S., & Baskar, T. (2024). Driving Business Transformation Through Technology Innovation: Emerging Priorities for IT Leaders. *Partners Universal Innovative Research Publication*, *2*(4), 01-14. https://doi.org/10.5281/zenodo.13286732
[16] Joshi, H. (2024). Emerging technologies driving zero trust maturity across industries. *IEEE Open Journal of the Computer Society*. https://doi.org/10.1109/OJCS.2024.3505056
[17] Kapoor, A., & Chatterjee, S. (2023). Platform and Model Design for Responsible AI: Design and build resilient, private, fair, and transparent machine learning models. *Packt Publishing Ltd.*
[18] Karyy, O., Kulyniak, I., Struchok, N., Halkiv, L., & Ohinok, S. (2021, September). Evaluation of the Tourist Attractiveness of Ukraine's Regions in the Conditions of Uncertainty Using Game Theory. In *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 351-355). IEEE. https://doi.org/10.1109/ACIT52158.2021.9548360
[19] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116. https://doi.org/10.30574/wjarr.2023.19.3.1785
[20] Khanyi, M. B., Xaba, S. N., Mlotshwa, N. A., Thango, B., & Matshaka, L. (2024). A Roadmap to Systematic Review: Evaluating the Role of Data Networks and Application Programming Interfaces in Enhancing Operational Efficiency in Small and Medium Enterprises. *Sustainability*, *16*(23), 10192. https://doi.org/10.3390/su162310192
[21] Masys, A. J. (2018). Security by design. *Innovative Perspectives on Complex Problems* https://doi.org/10.1007/978-3-319-78021-4
[22] Mattsson, U. (2022). *Controlling Privacy and the Use of Data Assets-Volume 1: Who Owns the New Oil?* CRC Press.
[23] Mattsson, U. (2023). *Controlling Privacy and the Use of Data Assets-Volume 2: What is the New World Currency–Data or Trust?* CRC Press. https://doi.org/10.1201/9781003254928
[24] Priem, R. (2020). Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. *Financial Innovation*, *6*(1), 11. https://doi.org/10.1186/s40854-019-0169-6
[25] Santoro, M., Vaccari, L., Mavridis, D., Smith, R., Posada, M., & Gattwinkel, D. (2019). Web application programming interfaces (apis): General purpose standards, terms and European commission initiatives. *Eur. Commission, Louxembourg, Louxembourg, UK, Tech. Rep. JRC118082*.
[26] Saxena, C. (2024). Identifying transaction laundering red flags and strategies for risk mitigation. *Journal of Money Laundering Control*, *27*(6), 1063-1077. https://doi.org/10.1108/JMLC-11-2023-0182

[27] Sengupta, S., & Deshmukh, A. (2024). Blockchain for Transparent Supply Chains: Enhancing Accountability in SDG-Aligned Trade. *International Journal of SDG's Prospects and Breakthroughs*, *2*(1), 7-9.
[28] Shpak, N., Matviyishyn, Y., Dziurakh, Y., & Gvozd, M. (2024). Simulation of the impact of changes in the volume of production and export of products on the food security of the country: on the example of Ukraine. *Frontiers in Sustainable Food Systems*, *8*, 1361625. https://doi.org/10.3389/fsufs.2024.1361625
[29] SOH, J., & LEE, K. T. (2020). The state of legal innovation in Asia-Pacific 2020. 1-212. Retrieved from https://ink.library.smu.edu.sg/sol_research/3368
[30] Sreenivasan, A., & Suresh, M. (2024). Agile readiness for sustainable operations in start-ups. *International journal of innovation science*, *16*(1), 166-192. https://doi.org/10.1108/IJIS-08-2022-0164
[31] Umoga, U. J., Sodiya, E. O., Ugwuanyi, E. D., Jacks, B. S., Lottu, O. A., Daraojimba, O. D., & Obaigbena, A. (2024). Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. *Magna Scientia Advanced Research and Reviews*, *10*(1), 368-378. https://doi.org/10.30574/msarr.2024.10.1.0028

Authors Biography

Marta Sarvas is an internationally recognized legal innovator, licensed attorney, and founder of ClearTrade, a U.S.-based startup revolutionizing customs process transparency through technology. She holds two Master's degrees in Law: A Master of Laws from Ukraine and a Master of Laws in Legal Innovation and Technology from Chicago-Kent College of Law (USA). In 2025, she was named one of the Young Professionals to Watch by the International Legal Technology Association for her visionary contributions at the intersection of law, technology, and global trade.

Solomiia Ohinok is a Ph.D. in Economics, Associate Professor, and Associate Professor at the Department of Management of Organizations, Lviv Polytechnic National University. Author of more than 150 scientific works, including 5 textbooks, and 10 collective monographs. Her scientific activities are focused on international trade, corporate social responsibility, investment and innovation management, franchising, and tourism. Participant of many international educational projects, social audited, and accounting manager.

Ihor Kulyniak, is a Ph.D. in Economics, Associate Professor, and Associate Professor at the Department of Management of Organizations, Lviv Polytechnic National University. Author of more than 300 scientific works, including 15 textbooks, 20 collective monographs, and more than 100 articles in specialized scientific publications. His scientific activities are focused on tourism, investment and innovation management, financial and economic security, risk management, and marketing management. Coordinator of the international educational project Erasmus+ Jean Monnet 101085171 – ERASMUS-JMO-2022-HEI-TCH-RSCH «European experience in the promotion of heritage and cultural tourism» (EEPHCT).

Ivanna Havrylyuk is a Ph.D. in Economics, Associate Professor, and Associate Professor at the Department of International Economic Relations and Marketing Strategies Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies of Lviv. Author of more than 100 scientific articles in professional scientific journals. Her research focuses primarily on the theoretical and practical aspects of marketing. This includes developing innovative tools for interacting with target audiences and evaluating the effectiveness of communication strategies.