American Journal of Applied Sciences

Original Research Paper

A Data-Sharing Model to Secure Borders using an Artificial-Intelligence-Based Risk Engine and Big-Data Concepts

Mohammad S. Al Rousan and Benedetto Intrigila

Department of Enterprise Engineering, University of Rome "Tor Vergata", Italy

Article history
Received: 08-11-2021
Revised: 16-03-2022
Accepted: 21-03-2022

Corresponding Author:
Mohammad S. Al Rousan
Department of Enterprise Engineering, University of Rome "Tor Vergata", Italy
Email: Moh.rousan1983@gmail.com

Abstract: The primary aim of this research is to develop a framework for data management and sharing that will enable countries to share complex data about known and unknown high-risk passengers to streamline border-control security processes through the use of big data analytics and Artificial Intelligence (AI). A total of 15 semi-structured interviews were used to gather qualitative data. A thematic analysis approach was used to analyze the data and the interview data were coded using NVivo 11 qualitative-data-analysis software. Five aggregate dimensions were developed, comprising nine themes and nine sub-themes, based on 39 codes that emerged from the data. This research has several theoretical and practical contributions. Primarily, the development of an AI-based risk engine will not only improve how borders are enforced but will also lead to the integration of new technology for border control, thus boosting securitization, decreasing human factors/error, minimizing border-related crime, and helping to manage healthcare issues.

Keywords: Risky Passengers, Border Security, Biometrics, Big Data, Artificial Intelligence

Introduction

The research issue highlighted and addressed in this study is the proposition of a framework for data sharing between nations to improve border security via the use of technologies such as big data and Artificial Intelligence (AI). The current research proposes the development of an artificial intelligence-based risk engine that will not only speed border control operations but will also address the problem of identifying known and unknown dangerous travelers. The study's relevance may also be observed in the increased security, elimination of human error, a decrease in border-related crimes, and a more positive view on travel. Processes for border control have grown more complicated, requiring significant operational and financial resources. Additionally, it has been shown that these rigorous procedures have a detrimental effect on passenger experience and satisfaction. However, security measures must be improved to avoid malevolent actions and to guarantee the passengers' safety. Many of the existing procedures are manual and depend on the judgment of border-control-security personnel. These procedures, however, are imprecise and may result in discriminating behavior.

A lot has been written concerning how professionals should handle discretionary decision-making and its consequences (Gelsthorpe and Padfield, 2014; Lipsky, 2010; Spader, 1984). One of the major problems with discretion is potential prejudices or discriminatory attitudes. The same applies to police decision-making and profiling. In parallel to the argument concerning discretionary decision-making, the increasing use of proactive profiling by security professionals has sparked fierce controversy regarding its validity (Delsol and Shiner, 2015; Gelman *et al*., 2012). Profiling is praised by security services and their supporters (Engel *et al*., 2002; Glaser *et al*., 2014). Others, however, argue that proactive profiling is detrimental since it unfairly targets minorities and erodes public confidence in the police and society (Baker, 2002; Delsol and Shiner, 2015; Engel and Cohen, 2014; Gabbidon *et al*., 2012; Gonzales, 2002; Harcourt, 2006; Harris, 2002). Most of the profiling research has been undertaken in Anglo-Saxon nations with distinct police-citizen interactions and discourse surrounding police–race relations (cf. Bonnet and Caillaut, 2015). Profiling is used by companies in a wide range of sectors and nations, with varying histories and language conventions. Thus, current findings may not be generalizable. For example, migration control remains mostly unexplored (Pratt, 2010). While border and migration studies are rife with normative discussion and critical theoretical work, empirical studies on border

practices such as profiling are rare (Côté-Boucher *et al*., 2014). In the words of Hirsch and Kornrich (2008, p. 1397), "In reality, discriminating and fair behavior is difficult to distinguish. The definition of discrimination is fluid and susceptible to change." Thus, it is critical to remove the human factor from profiling.

The issue of false positives and negatives also affects passenger security, safety, and enjoyment. Some research has been done on passenger profiling and its subsequent use for security checks (Cavusoglu *et al*., 2010). Other research has focused on detecting passenger security concerns (McLay *et al*., 2010). Previous research has examined passenger preferences for full-body scanners over pat-downs (Mitchener-Nissen *et al*., 2012). These studies found that informing passengers about the science underlying airport scanners and multispectral imaging equipment improved the acceptability of full-body scanning procedures. Other research has examined the impact of and need for, procedural fairness in passenger screening, as well as the reactions of passengers selected for secondary screening (Hasisi and Weisburd, 2011).

Furthermore, Basuchoudhary and Razzolini (2006) found that selective passenger screening based on appearance and behavior is neither effective nor desirable. As a result, travelers are increasingly being classified based on their risk profile. In this context, Persico and Todd (2005) developed an algorithm to show that screening high-risk groups more thoroughly than low-risk groups reduces the likelihood of negative outcomes. However, these authors noted that not screening low-risk groups might increase their chance of conducting terrorist actions. While this is true, Babu *et al*. (2006, p. 633) stated that "passenger grouping is beneficial even when the threat probability is assumed constant." These authors found that classifying passengers increases efficiency even when all passenger categories are checked equally. The effectiveness of passenger profiling has also been examined (Reddick, 2011).

Jackson *et al*. (2012) examined the benefits of an approach comparable to profiling, but one that is focused on identifying a low-risk group. Frequent travelers may be classified as a low-risk group and tested on an as-needed basis (Jackson *et al*., 2012). This enables the deployment of additional resources for the screening of high-risk passengers. Additional studies have been undertaken to determine ways to improve the efficiency of passenger screening. For example, Nie *et al*. (2012) demonstrated that allocating people to various lanes increases the efficiency of the passenger screening process when utilizing simulation-based modeling.

Moreover, numerous prior studies have shown the utility of predicting infectious diseases using information concerning transportation networks (Hwang *et al*., 2012; Nicolaides *et al*., 2012). The likelihood of an infectious illness emerging, as well as its time of emergence, may be calculated using several methods, including model simulations, extreme computations, and mathematical formulas based on complex Poisson-network topologies (Gautreau *et al*., 2008; Tomba and Wallinga, 2008; Wang and Wu, 2018). Thus, border screening is used in conjunction with isolating individuals diagnosed with suspected cases of disease and quarantining contacts to delay or prevent infectious individuals from entering the country/geographical region or to prevent the global spread of a disease from a source country. Border screening is intended to identify infected people on or near the border to segregate or prevent them from moving and spreading the disease to another country; however, this technique is successful only when the stated objective is accomplished efficiently (Selvey *et al*., 2015). According to Wagner (2021, p. 171), "New research activities may achieve this through ensuring an intelligent and risk-analysis-based approach to minimize risks and threats and challenges of balancing the two opposing ideals of mobility and security through the development of innovative tools, smoothly functioning work-flow procedures and solutions by using the latest technology." Thus, the primary aim of this research is to develop a framework for data management and sharing that will enable countries to share complex data about known and unknown high-risk passengers to streamline border-control security processes through the use of big data analytics and AI. Based on the above discussion, the following research questions will be answered by the researcher.

RQ1. How is border security being enacted currently?
RQ2. What are some of the main data-sharing challenges that prevent the identification of known and unknown risky passengers?
RQ3. How can data sharing be facilitated across borders, while avoiding data-sharing laws from being violated, facilitating the identification of known and unknown passengers, and strengthening borders?

Literature Review

Border Security

Borders are no longer seen as immutable lines in the sand but rather as a process that entities go through. This paradigm shift has resulted in the realization that boundaries are processes rather than fixed lines. The power of Balibar's comments to evoke a fresh viewpoint is remarkable "We are living in a period of border vacillation-both in terms of layout and function-which is also a vacillation of the fundamental concept of boundary, which has become very ambiguous" (Balibar, 1998, p. 217). The significance of Balibar's assumption is that the vacillation of a boundary does not entail its destruction. According to current geopolitical thinking, borders are not where they are supposed to be in today's globe. On the

contrary and perhaps most importantly, boundaries are becoming "multiplied and diminished in their localization, thinned out and doubled, no longer the beaches of politics, but the area of the political itself" (Balibar, 1998, p. 220).

Strong gates and walls, on the other hand, offer a controlled situation in which the binary divide between "us here" and "them there" is easier to manage for the governing elites (Newman, 2006). Even the most ardent globalization supporters would admit that the basic structure of society requires categories and boundaries and that borders provide order (see Albert *et al*., 2001; van Houtum and van Naerssen, 2002). Borders are state instruments in this reasoning and therefore serve as a sign of state power and identity (Anderson and Bort, 1998). This is not to argue that state boundaries are always only lines of demarcation. Anderson and Bort (1998) criticized the concept of boundaries as hard (geographical) lines, stating that political action is so complex that it is difficult to determine where one jurisdiction ends and another begins. He argued that boundaries are not inherent in the natural order of sovereign nation-states, but that "other notions of the boundary as an institution existed before the modern sovereign state and others will emerge after its extinction" (Anderson, 2004, p. 319).

As a consequence of new techniques that are less concerned with the physical position of the boundary and more concerned with what the border means to the various groups of people who encounter it, new views on border studies have arisen (Newman and Paasi, 1998; van Houtum, 2000). We may obtain a better understanding of how borders are created, maintained, and reproduced if we concentrate on the bordering process. In this context, the groundwork has been laid for the establishment of genuine and efficient border security measures. As a result, rather than focusing on the territorial dividing line, there is a tendency to concentrate on how people create their boundaries via the creation of their own "insides" and "outsides," and to view the border as a location where these identities dynamics may play out. Paasi (2005), for example, focused on the relationship between boundaries/borders and identity development.

Newman and Paasi (1998, p 188) agreed with (Anderson and Bort, 1998), in that "borders and their meanings are historically contingent and even if they are arbitrary lines between states, they may have profound symbolic, cultural, historical and religious significance for social communities, which are frequently contested. They express themselves in a wide range of social, political, and cultural activities." Borders, in this sense, are social constructs. van Houtum's results illustrate critical, post-structural approaches to border studies; van Houtum is especially interested in how boundaries organize social space and create a difference. Bordering, for example, was described by van Houtum and van Naerssen (2002, p. 134) as "related to practices of othering." Bordering, ordering, and othering (constructing difference), according to van Houtum and van Naerssen (2002), are all "intrinsically territorial" behaviors. As a result, otherness is a fundamental prerequisite for border construction and is constantly reproduced to maintain the stability of a territorially bounded society. According to van Houtum and Struver (2002), "overcoming boundaries" is mainly concerned with overcoming socially constructed ideas of belonging to a certain place and the need for geographical fixity. This spatial fixity reflects traditional views on border security.

Data-Sharing Challenges

Initiatives to exchange data have been enthusiastically welcomed by some but viewed with mistrust by others. According to Feingold (2011, p. 27), "governments in most of the world are often hesitant to share data within their ministries, much less with outsiders... [Governments] are especially hesitant to disclose data that they believe will reflect negatively on them and be used against them." Strong data protection, according to Castro and McQuin (2015), is counterproductive for countries' interests and they urged international organizations to pursue the free flow of data across borders. Furthermore, these authors asserted that data security is influenced less by the location of data storage and more by the data-storage methods used.

Border-control power is being eroded from the border, absorbed by the state, or transformed into a distant process. Borders are no longer simply fixed geographical limits, as Balibar (2002) succinctly stated. Borders are, instead, omnipresent, limitless, and effortlessly integrated into regular bureaucratic procedures. E-borders and strict visa rules at developing-country consulates are two ways that may deter poor immigrants and asylum seekers from seeking to gain entry to developing nations. Big data and related tools are among the most recent technologies being studied to enhance the monitoring of potentially "risky" visitors.

However, as Bollier (2010) noted, greater data collection does not imply more information. Situational awareness is an important component of border security since it influences decision-makers' policies. AI is the next game-changing technology in the border services ecosystem. Border services will be able to respond more quickly to the changing nature of travel and trade, identify illegal activity and facilitate passage in a more automated way when new data environments are created, and smarter systems are deployed. Border security, on the other hand, has received little attention, and resources devoted to border security AI initiatives are minimal.

Potential of Artificial Intelligence (AI) and Big Data in Border Security

Big Data

Data is processed and sent in real-time or in the past using big data analytics techniques. The volume, velocity, and diversity of big data must be kept in mind while analyzing it, as outlined by McAfee *et al*. (2012) and Davis (2012) (2014). Decision-oriented and action-oriented data analysis may be used by companies to make strategic decisions for the organization (Kumar and Kumar, 2015). It may be said that big data analysis is an essential part of the bigger framework within which employees work with the information they have to make it more valuable (Kumar and Kumar, 2015). A variety of tools and approaches may be used to analyze the volume, kind, and speed of data generated, enabling enterprises to realize their full potential and goals. Many approaches are used to analyze vast amounts of data, including predictive modeling, social network analysis, computational linguistics, audio analysis, and video processing. These methods may be used to investigate and draw conclusions from a broad variety of data.

"V" concepts are used by Gartner (2012) to describe big data. All of these V's signify volume, velocity, and variety (McAfee *et al*., 2012; Davis, 2014; Sun *et al*., 2015). When a large amount of data is gathered, a broad variety of variables may be analyzed and conclusions are drawn more often (George *et al*., 2016). Concepts such as 'terabytes of data and 'petabytes' show just how swiftly data storage capacity is increasing (Akter *et al*., 2016). It's also important to think about how rapidly this data is acquired, altered, and analyzed and how soon it loses its usefulness (Davis, 2014; George *et al*., 2016). When decision-makers have access to fast, 'innovative' information, as well as the ability to grasp a wide range of data, real-time decision-making, and implementation may increase (White, 2011; Boyd and Crawford, 2012). "variety" contains a broad range of streaming data kinds, both organized and unstructured, therefore it's crucial to keep this in mind (Constantiou and Kallinikos, 2015; George *et al*., 2016).

Authenticity and variability were revealed to be important factors of large-scale data. The correctness of huge datasets is widely agreed upon (Akter *et al*., 2016; Abbasi *et al*., 2016). Veracity in Big Data includes the concepts of trust, validity, and safeguards against unauthorized entry and modification (Demchenko *et al*., 2013). Management needs accurate data to make well-informed decisions and gain a competitive edge (Akter *et al*., 2016). Data must be thoroughly validated and submitted to stringent protocols before any analysis can be performed to assure its accuracy (Dong and Strivastana, 2013; Gandomi and Haider, 2015). Large amounts of data may be turned into useful information and this fact is well-known (Gandomi and Haider, 2015). Adding value was a fundamental part of Oracle's definition of big data. The low density of large data is another characteristic of this kind of data. There is a strong correlation between their length and the amount of data being analyzed, according to Oracle (2012). In addition to the two previously mentioned factors, Seddon and Currie (2017) added the following two Unpredictability and visibility. Big data interpretation may take various forms, but visualization is the act of displaying meaningful data via the use of artificial intelligence algorithms (Seddon and Currie, 2017).

Artificial Intelligence

To use the phrase "artificial intelligence," one must be able to analyze and interpret external factors. The computer or operator decides how to employ these acquired abilities and knowledge to perform certain tasks and fulfill specific goals (Kaplan and Haenlein, 2019). According to this definition, A computer attempts to emulate human thinking. Machine intelligence has increased the negative impact on human employment in various areas, including construction, shipping, healthcare, customer service, decision-making, and many more (information systems) (Huang and Rust, 2018). Artificial intelligence is making gadgets, computers, and networks more efficient. Connectivity and self-learning are two of the most important characteristics of artificial intelligence, which allow computers to improve and grow themselves based on previous work (Huang and Rust, 2018). Siri, Alexa, and Google Assistant are examples of AI technology that can carry out the orders of their users (Kaplan and Haenlein, 2019). Technology advances have been made possible due to a better knowledge of the process.

Since its inception some 60 years ago, Artificial Intelligence (AI) has grown into a multidisciplinary and cross-disciplinary area of study (Dosilovic *et al*., 2018). The use of artificial intelligence in specialized industrialization and monetization initiatives suggests new growth patterns. Deep Learning and Big Data have become the standard in AI development. As a result of the development of Artificial Neural Networks (ANNs), machines are now capable of doing activities that were previously thought impossible for machines to perform. Research and development, as well as industrialization, in Artificial Intelligence (AI) have progressed from prototype to sophisticated levels. Commercially accessible voice and image recognition, computational linguistics, and predictive modeling. Artificial Intelligence (AI) is becoming more generally understood and available as its use expands beyond commercial and industrial sectors to include manufacturing and agriculture. Al (Doshi-Velez and Kim, 2017; Doilovi *et al*., 2018; Mata *et al*., 2018). Research into artificial intelligence has been easy from the start because of the promising results (Russell and Norvig, 2016).

Because AI's advancement has been slower than projected and is reliant on shifting research paths, new techniques and enhancements to old ones have been required (Russell and Norvig, 2016). Technology innovation has increased dramatically over the last decade owing to a massive rise in data collected at a quicker pace than ever before, necessitating the development of emerging technologies, such as increasing processing capacity and inventing new AI techniques (Brynjolfsson and McAfee, 2017). Organizations like Netflix and Google may now utilize Artificial Intelligence (AI) to analyze large quantities of data and use the findings to promote their services with new goods, markets, and utility services (Iansiti and Lakhani, 2020; Venkatraman, 2017).

Due to the competitive nature of the global marketplace, many organizations are forced to employ AI technology because of the large volumes of data they collect, limited resources, and the necessity for speedy decision-making (Davenport, 2018). Entrepreneurial innovation is driving CEOs to rethink their long-term goals (Davenport, 2018). Pappas, Mikalef, Giannakos, Krogstie, and Lekakos (2018) urge more research on the impact of AI on firm strategy development and implementation. The dearth of theoretical and practical information on how to create a distinctive selling proposition with sophisticated AI technology is true (Duan *et al.*, 2018; Pappas *et al*., 2018; Mikalef *et al*., 2019).

Big Data and Artificial Intelligence (AI) in Border Control

An explosion of data and algorithm optimization have resulted in a fresh wave of success in AI research during the past 15 years, especially in the area of Machine Learning (ML) and its subset, deep learning. Since then, several AI applications created in business and university labs have entered daily usage (Bughin *et al*., 2017). AI applications have found use in areas such as intelligence, defense, and military policy, international security (arms control), and domestic security (state security, police and border protection, disaster management, and the protection of critical infrastructures). But understanding how AI affects national and global security now and, in the future, is not easy. Although certain military organizations were interested in AI during the Cold War (Roland and Shiman, 2002), the US government released three strategic studies on AI in 2016. (Allen and Kania, 2017). As a consequence, 29 countries have developed national AI strategies, demonstrating AI's wide potential across disciplines (Horowitz *et al*., 2020). While these approaches differ in focus, they all aim to help their countries profit from recent AI breakthroughs (Horowitz *et al*., 2020). The revolutionary nature and wide application of AI are expected to drive economic growth. Simultaneously, AI technologies are becoming more secure, with implications for national and international security. Due to state actors' linkages between new technologies and power politics, AI is increasingly receiving attention from security experts. But, like the policy discourse, the scholarly discourse on AI in international relations is still young (Horowitz *et al*., 2020). Some neo-realist articles discuss the systemic power-altering element of AI, but the academic community has not sufficiently addressed its dynamic and emergent character. Furthermore, considering technology as an exogenous and "black-boxed" element does not provide the field with the necessary analytical tools, especially because global technology companies and research institutions actively shape AI design.

Academics have already highlighted the need to rethink our concept of human agency in light of AI's increasing capacity to do tasks that previously needed human intelligence (Hoijtink and Leese, 2019). These characteristics will gain importance as AI develops. The nature of AI challenges ideas about human and technical agency, necessitating a closer look at how AI technologies, society, and security politics interact to influence future security perceptions.

Ratcliffe (2008, p. 267) defines information as "data that has been given meaning and structure." Thus, information technologies are utilized to not only collect data but also to give it meaning and structure. The development and use of information technology in Europe have increased dramatically during the last two decades (Besters and Brom, 2010; Bigo *et al*., 2012; Dijstelbloem *et al*., 2011). Schengen Information Systems (SIS), Visa Information Systems (VIS) holding asylum applicants' fingerprints and the European Border Surveillance System (EUROSUR) have all been deployed, resulting in a huge network of information and information technology (Broeders, 2007). Words like "digital fortress," "e-borders," and "the migratory machine" have been invented to describe these developments (Besters and Brom, 2010; Dijstelbloem *et al*., 2011). Others have referred to the deployment of border technology as border dispersion, suggesting that borders are scattered geographically. Thus, denying visas should be utilized to keep people away from the border (Tsianos and Karakayali, 2010; Weber, 2007). Despite the increasing reliance on IT to restrict movement, data on border processes is scarce. According to Côté-Boucher *et al.* (2014), critical theoretical and legal perspectives have historically dominated border studies but competing discourses and rationalities of border control intersect in complex ways with the daily professional routines and administrative procedures of those involved in border governance. Theoretical and legal modifications may not be enough to grasp the border's complexity. They called for a "practice turn" to allow empirical validation of border-practices research.

Healthcare Overview

COVID-19 outbreaks, containment efforts, and eventual dissemination have been documented globally in recent months. In a little over two months, the virus traveled from Wuhan, China, to 33 additional nations. Currently, airlines and cruise/ferry companies give API and PNR data to various governments to assist maintain border controls, with a focus on anti-terrorism and severe organized crime. API is the core information contained in machine-readable zones of passports, ID cards, and other travel documents. Some details are present throughout every traveler's journey, but only at the moment. We could track a traveler's trip even if it was booked in one transaction. For example, a traveler's API for a flight from London to Sydney through Hong Kong will be regarded as a single trip.

Infectious illness prediction using transport network information has been shown in many studies (Hwang *et al*., 2012; Nicolaides *et al*., 2012). Emergence probability and time may be estimated via modeling simulations, thorough computation, or analytical expressions based on complicated Poisson-network topologies (Gautreau *et al*., 2008; Tomba and Wallinga, 2008; Wang and Wu, 2018).

Border screening, isolation of suspected instances of illness, and quarantine of contacts are all done to delay or dissuade infected persons from entering the country/geographical area. The goal of border screening is to detect infectious individuals at or near the border so they may be separated or prevented from transmitting the illness to another nation (Selvey *et al*., 2015).

Methodology

The current study employs a qualitative method to address the research questions and goals. An ontological presupposition by the researcher is rendered actual by the study's social actors. A person's diverse views and experiences are exclusively accountable for publicly acknowledged knowledge, which cannot be externally generalized in the current research setting. The interpretivism paradigm aims to use these fundamental principles to offer new insights into reality and knowledge. The researcher chose an interpretative method over a positivist approach as it is more suited to quantitative research (Cohen *et al*., 2000). Semi-structured interviews were used to complement the phenomenological method. To obtain high-quality, in-depth information, the researcher believes this technique is appropriate (Easterby-Smith *et al*., 2015).

In general, an inductive method was considered the most appropriate. First, the researcher can compress and synthesize large amounts of raw text data. Second, it enables the researcher to connect the study's goals to the raw data findings (Easterby-Smith *et al*., 2015). Third, it enables the researcher to build a model from the data's underlying structure. The inductive method is characterized by commonly used motifs in the qualitative data processing. According to Saunders *et al*. (2018), most inductive investigations result in a model with three to eight important categories.

This technique is widely used to analyze qualitative data for a variety of research objectives. Inductive data gathering leads to theory development (Bryman and Bell, 2018). To be more exact, highly subjective data are gathered first, followed by discerning patterns, which results in discovery and theory refinement (Saunders *et al*., 2018). The inductive approach is also flexible, while the deductive method requires a lengthy investigation with potentially subjective evidence (Easterby-Smith *et al*., 2015). Regarding the use of big data analytics and AI, this study aims to develop a framework for data management and sharing that allows countries to share complex data on known and unknown risky passengers. In other words, the current study's objective is to create a new theory for border-control process optimization. To this end, a qualitative approach was used, resulting in 15 semi-structured interviews being conducted. Thematic analysis was used to examine these interviews, with data being coded using NVivo software. Five aggregate dimensions were created, encompassing nine themes and nine sub-themes based on 39 codes extracted from the data.

Findings and Discussion

The dimensions and themes that have emerged from the thematic analysis are depicted in the Fig. 1 concept map.

Aggregate Dimension 1: Multi-Tiered

Process of Data Identification and Investigation

The research found that, despite border-control officers' competence, many data identification and investigation processes are performed manually across international and local boundaries. Agents at the border do not have access to data and may only confirm or deny a match. Pre-clearance may detect unknown hazardous travelers or people whose healthcare condition has to be confirmed (without access to data), but it is not a comprehensive system and is prone to mistakes for people carrying "invisible" items such as infectious diseases or other risks to other passengers; a more comprehensive approach is therefore needed. The results also showed that, although some nations are moving towards more sophisticated and automated systems, others are still clinging to decades-old methods.

Biometrics is widely seen as the future of border security. A one-to-one match of the passenger's biometrics is used for biometric identification. The first stage involves manually comparing the participant's faces to the picture on their papers. Some border-control data investigation and identification techniques use iris

scanning, which yields highly accurate findings but is much more costly than other types of biometric identification. Iris-recognition technology can identify a person in a couple of seconds.

Because the iris is visible from a few yards away, iris scanning is less intrusive than retina scanning. Biometrics has improved border security, reduced operating expenses, and streamlined passenger passage. The study's participants believe that biometrics offers a better degree of accuracy in passenger identification and inspection than the manual method, which is prone to human error. Biometrics outperform manual data identification and inquiry methods by orders of magnitude. The amount of human error that occurred before has been substantially decreased through biometrics.

Iris biometric technology has helped in passenger identification. Therefore, security is being improved and the manual approach is being phased out. This eliminates the prospect of border-security officials enabling dangerous people to enter or leave the nation. Participants also said that fingerprinting is an often utilized and popular identification technique.

Making passenger trips simpler has been identified as one of the main advantages of Automated Border Control (ABC) gates as a means of guaranteeing border security. Using one of the border-securing automatic identification systems, travelers may enter or leave the nation via ABC gates. These gates have been developed and built-in line with International Civil Aviation Organization (ICAO) standards; they can clear individuals in part based on iris and fingerprint recognition. There is a growing trend to combine ABC gates with biometrics, which improves border-control system operations. ABC gates are electronic gates that enable travelers to enter or leave the country by using their fingerprint and identification card.

These gates may use biometric information, and, in the future, a single biometric-based token may be used, eliminating the requirement for a passport. Such technology reduces peak-time strain on border-control personnel, reduces costs, and provides a better level of security via biometric matching without human interaction at the gate. The main goal of ABC gates is to enhance anti-spoofing techniques, system compatibility, biometric scalability, and e-gate access for those with restricted mobility or vision. The raw data from which the above discussion has been derived is presented in Table 1.

Aggregate Dimension 2: Identification of Known and Unknown Risky Passengers

One of the methods used to detect high-risk passengers is biometric identification. Passengers trying to enter or leave the country are checked against criminal databases using their biometric information. Border-control officials collect data ahead of time, such as from airlines, and cross-check passenger information. Border officers search all nation's wanted-list databases for such information to identify possibly risky travelers. These methods are only useful for known risky travelers whose information is already available. As a consequence, identifying unknown hazards necessitates the use of a more sophisticated system. The raw data from which the above discussion has been derived is presented in Table 2.

Aggregate Dimension 3: Data Sharing

Data transmission between countries is often facilitated by Interpol or regional data-sharing agreements. Another development in the data related to known risky passengers is the exchange of information by law enforcement agencies. Unknown risky passengers are people that authorities are ignorant of and who may be risky, but about whom they have no information. They may not be recognized if the authorities in their home country have not registered them on any of the international/regional systems to which border-security officers have access.

Participants emphasized that there are regional data-sharing agreements in existence but that they do not function on a global scale. There is no mechanism in place for directly transferring data across nations; only one-to-one or regional agreements exist, and they do not span the whole globe. However, it is recognized that an agreed-upon integration model is required for the cross-national interchange of data and basic information. What makes things more complicated is that each nation has its own set of data-sharing techniques and structures that are governed by its privacy laws. In other words, the way data are exchanged varies by country. Several countries have advanced systems that transmit data directly through integration services. Others send them through e-mail, fax, or directly input data into foreign websites. Furthermore, in some countries, procedures are manual, making data sharing problematic. Participants emphasized the absence of a suitable framework for cross-border data sharing. The main problem is the potential of breaching each country’s data-privacy regulations. Cross-border data exchange lacks cutting-edge technologies, such as AI and big-data models, which prevents the real-time sharing of complicated data. Not only are the data-sharing techniques outdated, but there is no one entity capable of facilitating cross-border data interchange. Thus, data exchange across countries requires a uniform global framework. organization, or paradigm. The raw data from which the above discussion has been derived is presented in Table 3.

Aggregate Dimension 4: Optimizing Healthcare-Information Sharing

The COVID-19 pandemic has caused tremendous harm owing to a lack of integration and collaboration across countries. One participant stated that, if nations had exchanged passenger data in advance, it would have aided

both the home country and the destination in restricting the spread of the virus and boosted passengers' trust in travel. As a result of this lack of data sharing, health-related concerns have had a significant impact on the tourism business. Future data-sharing platforms should incorporate passengers' healthcare information, according to participants. A procedure for communicating at least the passenger overview and risk-engine results must include the passenger's healthcare record.

Along with the flight ticket, healthcare data should be shared between nations. Participants highlighted the importance of future data-sharing platforms, including passenger health information. At the border check, each traveler must carry and present a healthcare passport or a digital healthcare certificate. The raw data from which the above discussion has been derived is presented in Table 4.

Aggregate Dimension 5: Potential for using Big Data and Artificial Intelligence (AI)

The usage of big data and AI is fragmented, with no common application accessible across borders, which creates integration challenges. For example, there is no worldwide platform for big data and AI use. While some countries are adopting comprehensive big data analysis plans, this is inadequate since it should be done globally. However, creating a global AI framework and technical standards would be challenging. Participants highlighted the absence of a global platform for using big data and AI, which poses next-generation integration difficulties. In this context, the current study's participants highlighted the necessity for an AI-based risk engine that utilizes big data for data sharing. The raw data from which the above discussion has been derived is presented in Table 5.

The Solution for Data Sharing Between Countries using Artificial Intelligence (AI) and Big Data

The creation of an AI-based risk engine was one of the main proposals made by participants for addressing data-sharing problems, reinforcing borders, simplifying passenger trips, and detecting unknown risky individuals. Participants highlighted the need to have a platform based on AI and big data to solve these issues. One participant provided an example, stating that it is difficult to identify potentially dangerous passengers who are not already in the database. Today, each airport needs big data to assist in cost reduction and value maximization for all airport stakeholders, with passengers as the cornerstone. Border control authorities must now develop a risk engine that will use AI technology to detect potentially dangerous individuals. The most critical component, according to participants, is the inclusion of an AI-based risk engine within, or alongside, the Interpol platform. A big-data platform that all countries may feed directly with information on passengers' status is thought to be sufficient since it may include information about passengers' status as determined by law enforcement and health authorities in the country in which they live. A worldwide AI-based passenger risk engine is the panacea for the world's problems. Implementing a risk engine based on AI and big data analysis methods may help overcome these obstacles. It is simpler and more cost-effective to deploy a new platform that combines an AI risk engine with healthcare and big data analytics. However, one of the difficulties is in developing a well-designed risk-engine platform that complies with each country's requirements.

A risk engine's primary benefit is that it allows data sharing while complying with privacy regulations. In other words, countries may share data without revealing or utilizing personal information about passengers. According to the participants, AI should be utilized as a worldwide platform for developing an AI-based risk engine without giving governments direct access to the data. Additionally, participants stated that countries may share a short history of the traveler's health information to ensure the passenger does not represent a danger to the destination country. This may be accomplished by immediately transferring healthcare data from the departing nation to the new platform. The incoming nation may then be allowed to conduct medical examinations of tourists before their arrival to guarantee they would not cause harm. Developing a secure AI platform that does not exchange personal data across countries but instead exchanges a result, a color, or an indication may be a viable solution. Eventually, every nation will benefit from this, which will improve border security. Notably, this may be done without violating any data-sharing regulations.

Passenger data will be used by the risk engine, which will determine whether an individual is a threat to overall border security. The results of the risk engine's analysis may be shown graphically or numerically to border security agents, who can then use the information to determine the passenger's degree of danger without revealing any personal information that isn't previously known to them. Because XAI aims to provide explainable methodologies that enable end-users to understand, trust and manage the future generation of AI systems, explainable AI is offered here. Black-box models are the primary problem with these AI systems. In other words, we comprehend abstract mathematical principles, but we have no idea how AI goes about making judgments (Gunning, 2017). As a result of this

uncertainty in ordinary AI models, constitutional, moral, and security issues are emerging. A person's consent to a choice made entirely on their own accord is also prohibited under GDPR. As a result, the need for systems that offer robots with obvious and understandable characteristics is increasing in economic, interpersonal, and geopolitical situations. User requests for real-time viewing of findings and suggestions for revisions are the goal of this project. Holzinger and colleagues, 2017. Furthermore, XAI serves as a way for humans to comprehend why a certain action has been taken. Because of the application of Artificial Intelligence (XAI), border security agents may learn why an individual was marked as a hazardous person, along with any relevant data points, before making a final judgment on whether to accept or reject that conclusion. Learning curves for AI-based risk engines may also help them improve their ability to make more accurate decisions, resulting in fewer false negatives and false positives.

The capacity to ease data sharing is one of the main advantages of using AI and big data. In other words, the future of border control will be dependent on the use of cutting-edge technologies like big data and AI. We can enhance border security while simultaneously enhancing the passenger experience by using AI and big data. Airports and border-control authorities must work in close collaboration to enhance border security procedures. Sharing data without violating current data-privacy rules is also important; this may be done by using big data concepts and AI to share data with other countries without compromising existing data-privacy laws. In other words, the use of AI and big data may assist countries in resolving issues related to their data privacy laws.

Additionally, airports will eventually be able to enable smooth passenger journeys via the use of AI, video analytics, and biometrics, with AI and big data playing a key role in fulfilling the world's strictest security standards and simplifying passenger processes. Additionally, to maximize the value of AI algorithms, they must be integrated throughout all countries. In other words, all countries' data must be used to run AI algorithms, with the results sent to each through an integration hub.

In short, participants agreed that using AI and big data may enhance border security while also improving the passenger experience. Additionally, the use of AI and big data may help governments in overcoming roadblocks connected with their data privacy laws. Additionally, it was noted that by integrating AI and big data, it may be possible to simplify passenger identification and pattern recognition. Additionally, the participants emphasized the importance of big data and AI in today's travel industry for evaluating data and detecting passenger trends. We already use big data analysis on all data to identify connections between passenger behavior and time spent duty-free, as well as to offer a more customized experience for travelers. For governments, the most critical component in detecting potentially dangerous passengers who may endanger their country. In response to the above recommendations and insights, a data-sharing paradigm is proposed in Fig. 1 and the proposed system development is presented in Fig. 2 and 3.

The AI risk engine shown in the figures allows the border security agent to acquire findings on the passenger's danger in an encrypted manner. More precisely, the border security agent will be able to see the outcome in three categories (in a coded format that is only accessible by the border security agent): Dangerous passenger, unknown risk, and no risk. When the passenger information successfully matches a record in the blacklists, watchlists, and other databases against which the passenger details were verified, the dangerous passenger result is produced. Without disclosing more passenger information to the border security agent, the agent will be able to determine the traveler's risk level. When there is no obvious evidence of passenger danger and the passenger cannot be classed as a "no risk" passenger or is deemed to be a potentially problematic passenger, the person is classified as "an unknown risk." Such travelers may be moved for additional investigation, during which a border security official might conduct an interview and conduct a detailed examination of their possessions. Finally, the third category will be "risk-free," in which the traveler will be permitted to cross the border freely. With XAI at the heart of decision-making, authorized border security agents (such as those with a high-level security clearance) may request an explanation from the AI-risk engine on why this choice was made. This implies that the human agent will have ultimate decision-making power, particularly in the event of dangerous and unknown passengers. From the minute a person booked a flight or starts the visa application procedure, the risk engine is triggered. The risk engine will gather passenger data that is both publicly accessible and contributed by the passengers. This data will be compared and evaluated against an encrypted dataset that includes travel documents, stop lists, visa management systems, Interpol data, and healthcare data, as well as the databases of each of the countries associated with the risk engine (which will essentially be local databases). This will occur at the process's back end, in a system like the one described below.

Table 1: Aggregate dimension 1: The multi-tiered process of data identification and investigation

Theme 1: Manual processes are conducted	
Code 1: Passenger checks in with valid ticket and details are evaluated manually	Participant 1: "As a start, the process starts with a passenger booking a ticket with an airline and then the basic data will be collected by the airline. Such as (full name, sex, date of birth, … etc.). At this stage, we are not aware as a government authority of the data unless it's passed to us through the hub that we have developed to collect all the passenger's information from the airline before their arrival or departure in a certain period. However, at this stage data are not very accurate because it depends on the passenger to fill the information directly"
Code 2: Evaluation of travel	Participant 7: "The officer will check the travel document using his hands, officers are well documentation trained to identify forged documents. Yet, it's not fully accurate since it's a human process. The officer then either scans the travel document and retrieves the passenger profile from the civil registry database, or visa management system, depending on the passenger type."
Code 3: Passenger data are matched with a pre-existing database	Participant 4: "We do the business and criminal checks based on the airline information and ensure the passenger is not part on any the criminal lists or is not violating any of the visa or business rules we have in place. We conduct random checks from the operational point of view on all passengers. the random checks are to ensure the passenger's identity, documents, and boarding pass."
Code 4: Physical and luggage security checks are performed	Participant 12: "Eventually, the passenger is allowed to proceed to the next step, which is the security check of associated bags. Once nothing is found, the passenger can proceed to the boarding gate, which is managed by airport staff or the airline company agents."
Code 5: Pre-clearance facilitates border-security operations	Participant 6: "72 h before the date and time of the travel, the data (which includes name, sex, nationality, date of birth, travel document number, and travel document type) is pushed to our pre-clearance system through which we match between the passenger details and the core systems in the country (civil and criminal)."
Theme 2: Biometrics	
Sub-theme 1: Biometric identification is carried out	
Code 6: Process: matching 1:1	Participant 7: "The passenger will stand in front of a camera or fingerprint scanner where the biometrics will be scanned. Then, it will be checked against a biometric template stored on the card chip in the case of biometric travel documentation."
Code 7: Process: matching 1: *N*	Participant 8: "Matching 1: N between the passenger's captured image at the gate or the counter and the image/templates stored in the engine is carried out. Our biometric database is not huge and it's divided in a way that we can retrieve matching results in less than a couple of seconds."
Code 8: Facial identification is carried out	Participant 9: "Identification of passengers at the counters or gates happens using a facial a camera and passport scanner. We retrieve the image on the passport and compare it with the passenger's facial image captured through the facial camera. Once the result is above a certain threshold, then we allow the passenger to proceed to the next steps."
Code 9: Fingerprinting is accurate but not reliable	Participant 11: "Fingerprint also comes with high accuracy in general, but for certain types of individuals it does not work."
Code 10: Iris identification is the most accurate but is expensive	Participant 11: "Iris modality has the highest accuracy according to international certification bodies. However, it's relatively more expensive compared to other modalities."
Sub-theme 2: Biometrics are the future of border control	
Code 11: Biometrics are more	Participant 9: "Biometrics today have increased border-control security, reduced the cost of the efficient and cost-effective operation and facilitated passengers' movement. Also, it is one step towards smart border control that we aim to achieve in the future."
Code 12: Biometrics provide higher security	Participant 10: "Biometrics have increased and strengthened the security of border control. It's way better than the manual process used before."
Code 13: Biometrics reduce human errors	Participant 9: "We were the first to implement [biometrics] in the region and we have successfully upgraded our biometric system multiple times. Before biometrics, we used to face multiple human errors coming from errors which caused incorrect data sometimes."
Theme 3: Automated control gates are employed and are important	
Code 14: ABC gates integrated biometrics	Participant 7: "In Europe, the border-control gates are based on facial biometrics that is stored on the travel document. The gate will do matching [1:1]. In other countries, it's based on biometric services with the biometric engine to do the matching [1: N]."
Code 15: ABC gates secure the borders	Participant 8: "Operations errors are very minimal compared to before, plus the data captured are of a higher percentage of accuracy compared to before. So, looking at the gates' value today, I can assure you the security has increased, and throughput is way better."
Code 16: ABC Gates facilitate passenger journeys	Participant 2: "We also have ABC for pre-registered passengers; passengers need to register their fingerprint and document in the ABC gates system to be able to use the border-control gates once they leave or enter the country. Today there is a lot of competition between airports around the world, and passengers are demanding easier and faster processes. They want to have a process that facilitates their journey, and we try to provide them with that always. ABC gates are an automated process, with no human interaction, and work 24 hours a day. The process has helped us reduce the pressure on border-control officers during peak hours and helped us in having fewer costs and supported us in having higher security rates because of biometric

Table 1: Continue

	matching without any human interaction at the gate."
Code 17: Border-control gates are outdated	Participant 14: "Also, we will install gates in the coming months. Today, the process is run without biometrics and border-control gates."
Code 18: Reduced operational costs	Participant 5: "For governments, it's achieving the security demanded and reducing the operational costs for them."

Table 2: Aggregate dimension 2: Identification of known and unknown risky passengers

Theme 4: Identification of known risky passengers	
Sub-theme 3: Current process of identifying risky passengers	
Code 19: Based on biometrics	Participant 6: "Identification of passengers based on biometrics happens through an the algorithm on our local criminal biometric database where we conduct 1:1 or 1: *N* matching using a NIST-certified algorithm."
Code 20: Cross-checking passenger details against a database	Participant 8: "We identify risky passengers who are registered in our database through the well-known channel, which are: Criminal databases, which are usually filled by a decision from the court, international criminals, which are usually filled through Interpol. Once the passenger comes to the border-control counter, the officer will retrieve the data and the system will provide the result to the officer or the gate. Based on the result, the passenger will be escorted to the passenger's affairs office to handle their situation [if one arises]."
Code 21: Use of stop lists	Participant 13: "If the passenger is listed in the system as a blacklisted passenger, then we will be able to catch the passenger once they arrive at the border-control gate."
Code 22: Using an algorithm connected to a database	Participant 6: "Identification of passengers based on data happens through an algorithm on our combined criminal database. This database collects data directly from criminals within the country [automated integration], regional criminals [manual entry], and international criminals such as Interpol [semi-automated process]".
Sub-theme 4: Data-privacy laws make identification challenging	
Code 23: Data-privacy laws make identification challenging	Participant 2: "I believe the main challenge today regarding sharing data with other countries as each country has different rules about risky passengers. So, there is no clear agreed model on data sharing and what kind of data should be shared. Also, do not forget about data-privacy rules. Also, some countries cannot share data regarding their citizens even if they are known to be risky."
Sub-theme 5: Known data are shared through international law-enforcement authorities	
Code 24: Known data are shared through international law-enforcement authorities	Participant 1: "Data are shared through well-known channels through the law-enforcement authorities, i.e., Interpol or any regional authority."
Sub-theme 6: Lack of appropriate data sharing between countries leads to free travel for risky passengers	
Code 25: Lack of appropriate data sharing between countries leads to free travel of risk passengers	Participant 5: "Some well-known criminals in country X can travel, and country Y has no idea if this passenger is risky or not because this person is allowed to travel, yet there is a possibility that this passenger is risky. There is no clear agreement to share extra information about passengers who are previously considered risky in their own countries or the countries they reside in."
Theme 5: Identification of unknown risky passengers	
Code 26: Identification of unknown risky passengers	Participant 3: "Risky passengers that we have no information about are difficult to identify. Because, in general, no one knows there are risks at least in our records. So, we rely so much on regional and international well-known platforms for that such as Interpol. And we identify them either through the data we receive or through the biometrics if they are enrolled in our systems."

Table 3: Aggregate dimension 3: Data sharing

Theme 6: Lack of data-sharing agreements between countries	
Code 27: Data-sharing agreements exist between countries regionally but not internationally	Participant 1: "It's not easy for any government or authority to share their risky passengers but at least there should be a channel to share the data using the modern technologies to handle such an issue."
Code 28: Potential violation of data-sharing laws of different countries	Participant 10: "I believe there are other challenges such as having a framework for data sharing between countries, while observing the data-privacy laws."
Theme 7: No framework or model exists for sharing data	
Code 29: Data sharing processes are outdated	Participant 13: "They are shared today using manual process by e-mail, letters, or fax. In certain international systems, there are advanced integration services in a place where we utilize them indirectly."
Code 30: No single organization for sharing data	Participant 7: "In addition, there is no one organization handling all these activities among countries in the world."

Table 4: Aggregate dimension 4: Optimizing healthcare-information sharing

Theme 8: Optimizing healthcare-information sharing	
Code 31: Data-sharing challenges have worsened during the pandemic	Participant 3: "Today if the countries had shared the data in advance about passengers, that would have helped both [home country and destination] in stopping the spread of the virus and would have increased passenger trust in traveling."
Code 32: No appropriate framework or channel to share healthcare-related information	Participant 4: "Today, we do not have an automated process for sharing the healthcare status of passengers between domestic airports. All airports within the country check the data directly with the government databases for such cases. Yet, there is no direct integration between the systems, so we rely more on a manual process where passengers present documents once requested by officers."
Code 33: Future data sharing should include healthcare status	Participant 5: "I believe the best way is through a clear data-sharing model that also includes the healthcare status of passengers. This will be the best future collaboration and integration between countries under one international organization."
Code 34: Use of vaccination cards or digital passports for known test for infectious diseases	Participant 13: "We used to have a manual process before the pandemic; for specific countries, passengers must present vaccination card. Today, we ask every passenger to provide a PCR and a vaccination card before they enter the country. Many countries stopped accepting foreign passengers, which was very harmful to the economy."

Table 5: Aggregate dimension 5: Potential for using big data and Artificial Intelligence (AI)

Theme 9: Potential for using big data and artificial intelligence (AI)	
Sub-theme 7: Scattered use of big data and AI technologies	
Code 35: Scattered use of big data and AI technologies	Participant 6: "There is no worldwide platform today to use big data and AI on a global scale. Some countries are using in-depth big-data analysis approaches within the country. however, it's not enough because it should be on an international level."
Sub-theme 8: An AI-based risk engine needs to be developed	
Code 36: A risk engine can allow sharing of data while maintaining privacy laws	Participant 10: "Having a platform based on AI and big data will solve the challenges here. As an example, there is a challenge in identifying risky passengers who are not part of our database. They might be part of the databases of other countries though. Therefore, pushing data in a very high manner might be the solution in this situation, where countries can push data to an AI engine. The AI risk engine can include the healthcare results or records about passengers, where each country will push the list of vaccinations or contiguous diseases to this dashboard. This requires to pull data from the health organizations of each country as well."
Code 37: A risk engine can provide color-coded information without revealing details about the passenger	Participant 7: "Imagine traveling from a country where the risk engine advises the border-control agency about the passenger. The advice should not be detailed. It can be color-coded, where the result is an automated result about the passenger. Each country can benefit from this eventually and this will help in securing the borders."
Sub-theme 9: AI and big data can help in securing and strengthening border control	
Code 38: Data sharing can be facilitated using AI and big data	Participant 1: "Utilization of modern technologies such as big data and AI is the future of border control. We can utilize them to increase border-control security and enhance the passenger experience as well. Airports and border-control authorities are working closely together to enhance the process to secure the borders. Sharing the data without violating the data-privacy laws is important as well; this can be done using big-data concepts and AI."
Code 39: Passenger identification and pattern recognition can be streamlined using AI and big data	Participant 5: "Big data and AI implementation is the future for securing borders through the implementation of big data concepts for identifying patterns among passengers and for predicting passengers' risk factors based on prediction models".

The data will be sent via safe and encrypted layers created specifically for this AI-ris engine, ensuring that no passenger data is compromised and that the greatest standards of data security are maintained. To secure passenger information and privacy, encryption will guarantee that the data is unreadable by other parties such as hackers. However, this encryption may be decrypted when a passenger is flagged or at the request of a senior border security official with a security clearance. The encryption and decryption keys will be

DOI: 10.3844/ajassp.2022.51.67

provided through private servers to border security personnel strategically located at a specific border. These persons must have a senior management position and possess a high degree of security clearance.

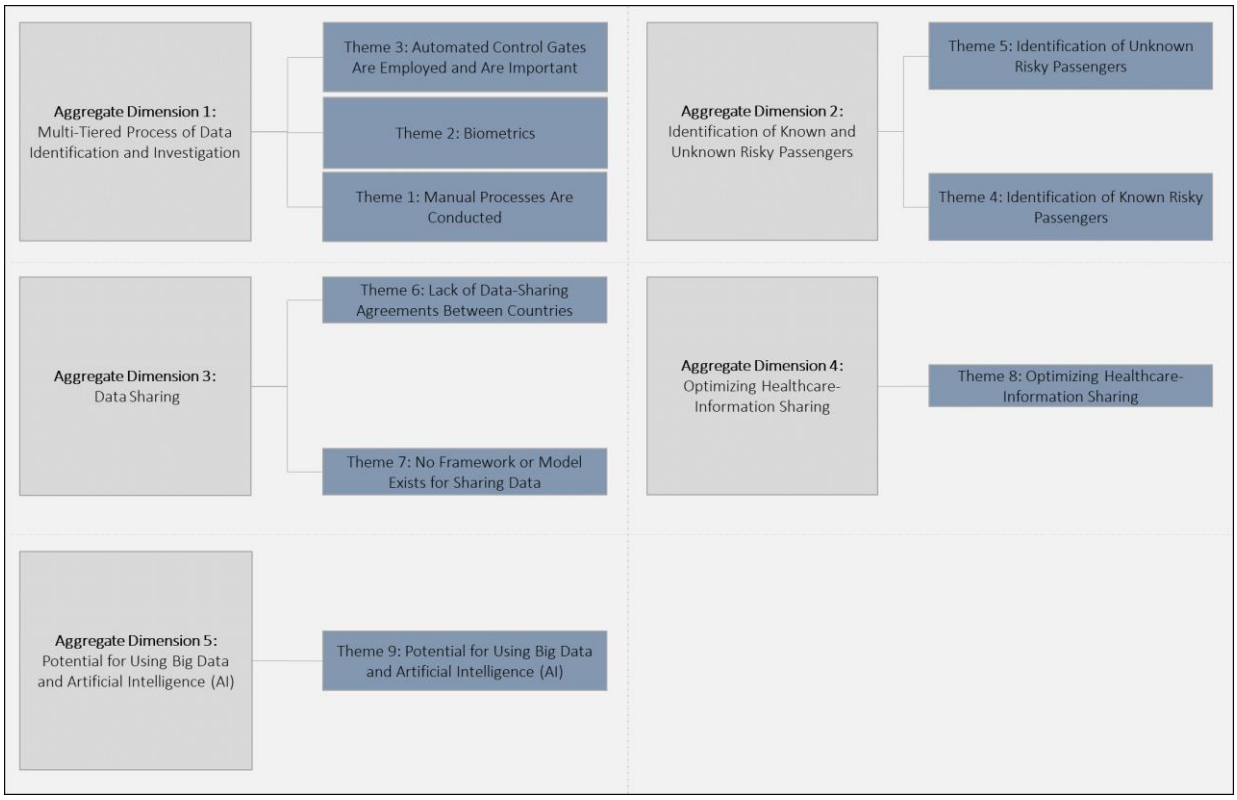

Fig. 1: Concept Map

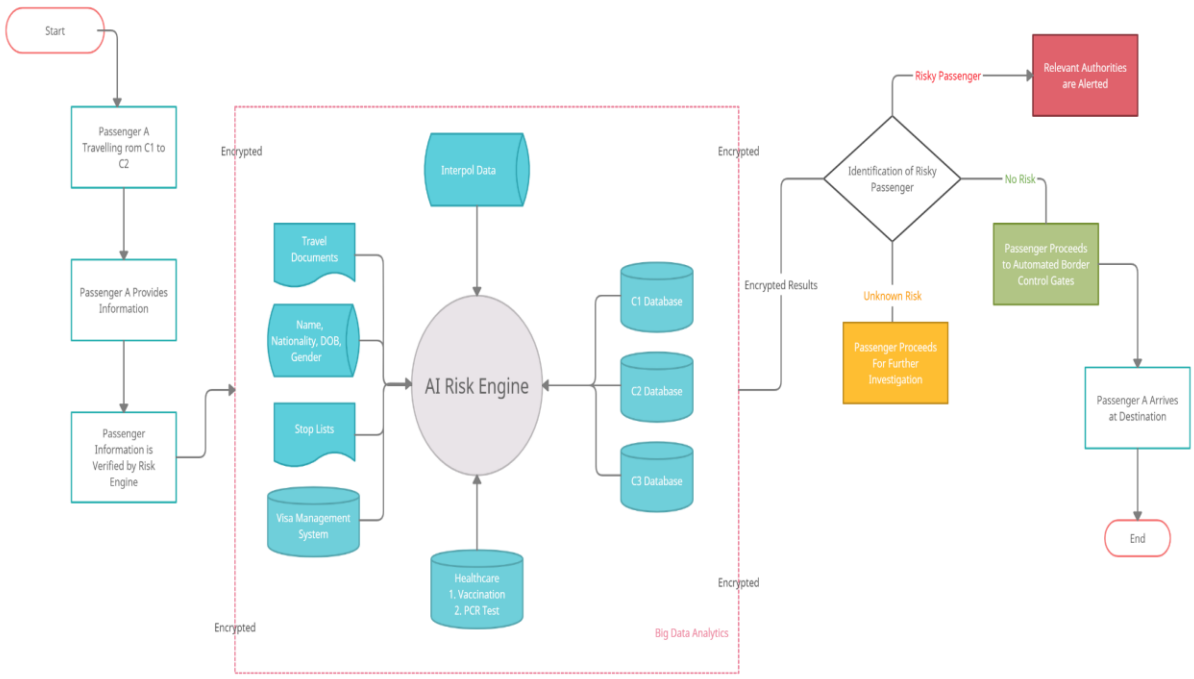

Fig. 2: AI risk engine diagram

DOI: 10.3844/ajassp.2022.51.67

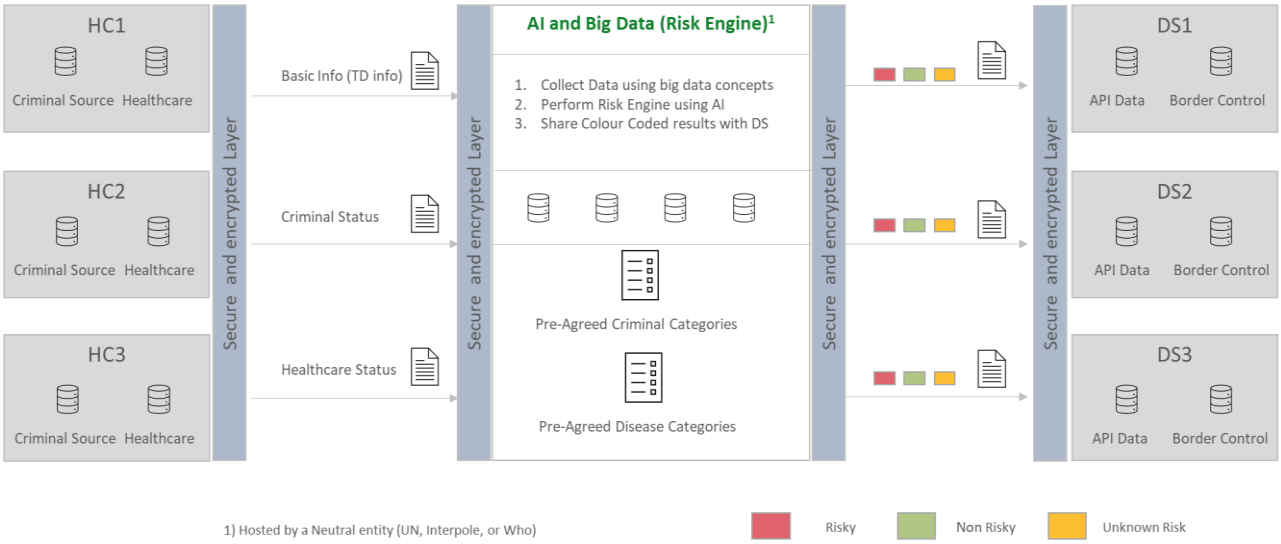

Fig. 3: AI and big data risk engine data-sharing model

Conclusion and Contributions

Theoretical Contributions

The current research makes several theoretical contributions. First, this research bridges the divide between border security and advanced technology research. Accordingly, typical barriers to border research and practice may be addressed and further research can be undertaken. More precisely, border-security research has not yet incorporated AI and big data concepts into its reasoning. As a result, this study not only improves knowledge of border security but also offers a better grasp of the possibilities for integrating ideas from AI and big data research into the border-security research field.

Second, this study fills a critical theoretical gap since no previous research has established a framework or offered a solution for resolving typical risk-management-related border security and control problems. One of the main reasons for this is that nations face similar data-sharing difficulties, with one country lacking the legislative structure necessary to exchange data about its people without infringing their fundamental human right to privacy. Additionally, these data-sharing difficulties are among the typical theoretical concerns identified in previous studies as impeding global border strengthening.

Third, this study contributes to a better understanding of how boundaries are enacted globally and provides a coherent theoretical framework for commonly employed security measures. There was a gap in the literature since previous studies had failed to provide a clear understanding of what happens presently in terms of border security and what might be done to improve the process.

Finally, this study has examined border security and control as a holistic process, rather than concentrating only on one scenario. Much prior research has been performed in a contextual setting (either the US or the UK) or in a context that confines the debate to a specific geographical area, thus constraining theory development. In comparison, this study not only examines the broader holistic context but also creates a generic border-control framework that takes into account sea, land, and air boundaries. This is a new addition to science made by this study.

Managerial Contributions

The current research makes many practical contributions and has significant managerial consequences. First, the research has outlined and created a practical framework for facilitating data exchange in a complicated legal context while adhering to all applicable privacy regulations. The second practical benefit of this study is the simplification of border processes. For example, by using an AI-based risk engine at the border, long procedures that certain crossings entail may be avoided, ensuring a smoother trip for passengers. The consequences are comparable to those of pre-clearance, in which previously selected non-risky individuals or regular travelers are exempt from rigorous border-security inspections. This also has cost implications, as more resources may be devoted to security to identify undiscovered high-risk individuals. Finally, the development of an AI-based risk engine will not only improve border enforcement but will also enable the integration of new technology into borders, thereby increasing securitization, reducing human factors, mitigating border-related crime, and assisting in the management of healthcare situations.

Potential Policy Changes and Organizational Impact

The possible deployment of an AI-based risk engine will have both policy and organizational consequences for border-security agencies responsible for air, sea, and land crossings. In other words, developing an AI risk engine is a resource-intensive process that will require substantial technical knowledge and financial resources. Additionally, integrating an AI risk engine across several borders would be a difficult task requiring modifications to existing operational procedures. Finally, incorporating an AI risk engine into nations' data-sharing frameworks would need significant legislative reforms, particularly in the EU, owing to the strict requirements of the General Data Protection Regulation (GDPR).

Limitations of the Study

Due to the study's qualitative nature and the researcher's participation in data gathering, it is prone to researcher bias. Bias in research arises when the researcher, either directly or indirectly, influences the study's findings. While the researcher may have had no conscious or direct influence on the research's results, the researcher may have contributed subconsciously to the presence of researcher bias. While the researcher took many precautions to prevent this, including thematic analysis, verbatim transcriptions of the interviews, and member verification to ensure the transcripts were accurate, one cannot be confident that researcher bias was not present in the study.

Additionally, qualitative research must address issues of the power imbalance between the interviewer and the respondent. It is conceivable that participants see the interviewer as superior to themselves, resulting in restricted answers as a consequence of the perceived divide between the researcher and the participant. The converse is also true, with the researcher feeling fearful of the participant's authority, especially if she/he has a position higher than the researcher. Numerous techniques have been used to mitigate this issue. First, no participant was selected from the researcher's place of employment to rule out the potential of a power imbalance due to rank and experience differences. Second, all volunteers (who were deliberately selected) shared the researcher's general rank, which avoided any possible rank conflicts. Third, to strengthen the researcher–interviewee interaction, the researcher engaged participants before the interview by explaining the study project, talking about work, and ensuring that participants felt comfortable during the interview.

Authors Contributions

Mohammad S. Al Rousan: Design and development of the research plan, participated in all experiments, coordinated the data analysis, and contributed to the writing of the manuscript.

Benedetto Intrigila: Designed the research and organized the study.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues are involved.

References

Albert, M., Jacobson, D., & Lapid, Y. (2001). Identities, Borders, Orders: Rethinking international relations theory. U of Minnesota Press.

Allen, G., & Kania, E. B. (2017). China is using America's own plan to dominate the future of artificial intelligence. Foreign Policy, September 8. https://foreignpolicy.com/2017/09/08/china-is-using-americas-own-plan-to-dominate-the-future-of-artificial-intelligence/

Anderson, M. & Bort, E. (1998). The frontiers of Europe. A&C Black.

Babu, V. L. L., Batta, R., & Lin, L. (2006). Passenger grouping under constant threat probability in an airport security system. European Journal of Operational Research, 168 (2), 633–644. doi.org/10.1016/j.ejor.2004.06.007

Baker, E. (2002). Flying while Arab-Racial profiling and air travel security. Journal of Air Law and Commerce, 67 (4), 1375-405.

Balibar, E., Cheah, P., & Robbins, B. (1998). Cosmopolitics: Thinking and Feeling Beyond the Nation.

Balibar, E. (2002). World borders, political borders. PMLA, 117 (1), 68–78. doi.org/10.1632/003081202x63519

Bonnet, F., & Caillault, C. (2015). The invader, the enemy within, and they-who-must-not-be-named: How police talk about minorities in Italy, the Netherlands, and France. Ethnic and racial studies, 38(7), 1185-1201. https://www.tandfonline.com/doi/abs/10.1080/01419870.2014.970566

Bigo, D. (2012). Security, surveillance, and democracy. Routledge handbook of surveillance studies, 27, pp, 277-84

Basuchoudhary, A., & Razzolini, L. (2006). Hiding in plain sight–using signals to detect terrorists. Public Choice, 128(1), 245-255. https://link.springer.com/article/10.1007/s11127-006-9052-x

Brom, F. W., & Besters, M. (2010). 'Greedy'information technology: The digitalization of the European migration policy. European Journal of Migration and law, 12(4), 455-470. https://brill.com/view/journals/emil/12/4/article-p455_4.xml

Bollier, D. (2010). The Promise and Peril of Big Data. Aspen Institute, Communications and Society Program, Washington, DC.

Broeders, D. (2007). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. International Sociology, 22 (1), 71–92.

Bryman, A. & Bell, E. (2018). Business Research Methods. Oxford University Press, New York, NY.

Bughin, J., Laberge, L. & Mellby, A. (2017). The case for digital reinvention. McKinsey Quarterly, February 9. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-case-for-digital-reinvention

Cavusoglu, H., Koh, B., & Raghunathan, S. (2010). An analysis of the impact of passenger profiling on transportation security. Operations Research, 58 (5), 1287-1302.

Cohen, L., Manion, L., & Morrison, K. (2000). Research Methods in Education. 8th Ed. Routledge, London.

Côté-Boucher, K., Infantino, F., & Salter, M. B. (2014). Border security as practice: An agenda for research. Security Dialogue, 45 (3), 195–208. doi.org/10.1177/0967010614533243

Castro, D. & McQuinn, A. (2015). Cross-border data flows enable growth in all industries. Information Technology and Innovation Foundation, 2, pp.1-21.

Delsol, R. & Shiner, M. (2015). The politics of the powers. In: Stop and Search: The Anatomy of a Police Power, Delsol, R. and M. Shiner (Eds.), Palgrave Macmillan, London, pp, 31-56.

Dijstelbloem, H., Meijer, A., & Besters, M. (2011). The migration machine. In: Migration and the New Technological Borders of Europe, Dijstelbloem, H. and A. Meijer (Eds.), Palgrave Macmillan, London, pp, 1-21.

Easterby-Smith, M., Thorpe, R., Jacksonm, P. R., & Jaspersen, L. J. (2015). Management and Business Research. Sage, Thousand Oaks, CA.

Engel, R. S., Calnon, J. M., & Bernard, T. J. (2002). Theory and racial profiling: Shortcomings and future directions in research. Justice Quarterly, 19 (2), 249–273. doi.org/10.1080/07418820200095231

Engel, R. & Cohen, D. M. (2014). Racial profiling. In: The Oxford Handbook of Police and Policing, Reisig, M.D. and R.J. Kane (Eds.), Oxford University Press, Oxford. doi.org/10.1093/oxfordhb/9780199843886.013.024

Feingold, D. A. (2011). 3. Trafficking in Numbers: The social construction of human trafficking data. In Sex, Drugs and Body Counts (pp. 46-74). Cornell University Press.

Hirsh, C. E. & Kornrich, S. (2008). The context of discrimination: Workplace conditions, institutional environments and sex, and race discrimination charges. American journal of sociology, 113(5), pp.1394-1432.

Gabbidon, S. L., Higgins, G.E. & Nelson, M. (2012). Public support for racial profiling in airports: Results from a statewide poll. Criminal Justice Policy Review, 23 (2), 254–269.

Gautreau, A., Barrat, A. & Barthélemy, M. (2008). Global disease spread: Statistics and estimation of arrival times. Journal of Theoretical Biology, 251 (3), 509-522. doi.org/10.1016/j.jtbi.2007.12.001

Gelman, A., Hill, J., & Yajima, M. (2012). Why we (usually) don't have to worry about multiple comparisons. Journal of Research on Educational Effectiveness, 5 (2), 189–211. doi.org/10.1080/19345747.2011.618213

Gelsthorpe, L., & Padfield, N. (2014). Exercising Discretion: Decision-making in the Criminal Justice System and Beyond. Routledge, London.

Glaser, J., Spencer, K., & Charbonneau, A. (2014). Racial bias and public policy. Policy Insights from the Behavioral and Brain Sciences, 1 (1), 88–94.

Gonzales, J. V. (2002). Flying while Arab: Passenger profiling in the aftermath of the September 11th terrorist attacks. International Travel Law Journal, 2: 76–86.

Harcourt, B. E. (2006). Behavioral Profiling at US Airports. U.S. Government Printing Office, Washington DC.

Harris, D. H. (2002). How to improve airport security. Ergonomics in Design, 10 (1), 17–22.

Hasisi, B. & Weisburd, D. (2011). Going beyond ascribed identities: The importance of procedural justice in airport security screening in Israel. Law and Society Review, 45 (4), 867–892.

Hoijtink, M., & Leese, M. (2019). Technology and Agency in International Relations. Routledge, London.

Horowitz, M. C., Kahn, L., & Mahoney, C. (2020). The future of military applications of artificial intelligence: A role for confidence-building measures? Orbis, 64 (4), 528–543. doi.org/10.1016/j.orbis.2020.08.003

Hwang, G. M., Mahoney, P. J., James, J. H., Lin, G. C. Berro, A. D., Keybl, M. A., Goedecke, D. M., Mathieu, J. J. & Wilson, T. (2012). A model-based tool to predict the propagation of infectious disease via airports. Travel Medicine and Infectious Disease, 10 (1), 32-42. doi.org/10.1016/j.tmaid.2011.12.003

Jackson, B. A., Chan, E. W., & LaTourrette, T. (2012). Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise. Journal of Transportation Security, 5 (1), 1–34.

Lipsky, M. (2010). Street-level Bureaucracy: Dilemmas of the Individual in Public Services. Russell Sage Foundation, New York, NY.

McLay, L. A., Lee, A. J., & Jacobson, S. H. (2010). Risk-based policies for airport security checkpoint screening. Transportation science, 44(3), pp.333-349

Mitchener-Nissen, T., K. Bowers, and K. Chetty. 2012. Public attitudes to airport security: The case of whole-body scanners. Security Journal, 25 (3), 229–243.

Newman, D., 2006. Borders and bordering: Towards an interdisciplinary dialogue. European journal of social theory, 9(2), pp.171-186.

Newman, D. & Paasi, A. (1998). Fences and neighbors in the postmodern world: Boundary narratives in political geography. Progress in Human Geography, 22 (2), 186-207. doi.org/10.1191/030913298666039113

Nicolaides, C., Cueto-Felgueroso, L., González, M. C., & Juanes, R. (2012). A metric of influential spreading during contagion dynamics through the air transportation network. PLoS ONE, 7 (7), e40961. https://doi.org/10.1371/journal.pone.0040961

Nie, X., Parab, G., Batta, R., & Lin, L. (2012). Simulation-based Selectee Lane queueing design for passenger checkpoint screening. European Journal of Operational Research, 219 (1), 146–155.

Paasi, A. (2005). The changing discourses on political boundaries. Mapping the backgrounds, contexts, and contents. In: B/ordering Space, Van Houtum. H., O. Kramsch and W. Zierhofer (Eds.), Ashgate, Burlington, VT, pp, 17–31.

Persico, N. and Todd, P. E. (2005). Passenger profiling, imperfect screening, and airport security. American Economic Review, 95 (2) 127–131.

Pratt, A. (2010). Between a hunch and a hard place: Making suspicion reasonable at the Canadian border. Social and Legal Studies, 19 (4), 461–480. doi.org/10.1177/0964663910378434

Ratcliffe, J. H. (2008). Knowledge management challenges in the development of intelligence-led policing. In: The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions, Williamson, T. (Ed.), Wiley, Chichester, pp, 205-220.

Reddick, S. R. (2011). Point: The case for profiling. International Social Science Review, 79 (3/4), 154-156.

Roland, A. & Shiman, P. (2002). Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983–1993. MIT Press, Cambridge, MA.

Saunders, M., P. Lewis, and A. Thornhill. 2018. Research Methods for Business Students. Pearson Education, London.

Selvey, L. A., Antão, C., & Hall, R. (2015). Evaluation of border entry screening for infectious diseases in humans. Emerging Infectious Diseases, 21 (2), 197-201.

Spader, D. J. (1984). Rule of law v. rule of man: The search for the golden zigzag between conflicting fundamental values. Journal of Criminal Justice, 12 (4), 379–394. doi.org/10.1016/0047-2352(84)90050-3

Tomba, G. S. & Wallinga, J. (2008). A simple explanation for the low impact of border control as a countermeasure to the spread of an infectious disease. Mathematical Biosciences, 214 (1-2), 70-72.

Tsianos, V. & Karakayali, S. (2010). Transnational migration and the emergence of the European border regime: An ethnographic analysis. European Journal of Social Theory, 13 (3), 373–387. doi.org/10.1177/1368431010371761

van Houtum, H. (2000). III European perspectives on borderlands. Journal of Borderlands Studies, 15 (1), 56-83. doi.org/10.1080/08865655.2000.9695542

Wang, L. & Wu, J. T. (2018). Characterizing the dynamics underlying the global spread of epidemics. Nature Communications, 9 (1), e218. doi.org/10.1038/s41467-017-02344-z

Van Houtum, H. & Van Naerssen, T. (2002). Bordering, ordering and othering. Tijdschrift voor economische en sociale geografie, 93(2), pp.125-136.

Wagner, J. (2021). Border Management in Europe. In Border Management in Transformation (pp. 171-194). Springer, Cham.

Weber, L. (2007). Policing the virtual border: Punitive pre-emption in Australian offshore migration control. Social Justice, 34 (2), 77-93.