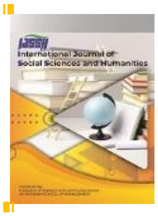

International Journal of Social Sciences and Humanities
Vol. 4 No. 2, Juni 2026, pages: 415-430
e-ISSN: 2985-6469
https://ejournal.45mataram.ac.id/index.php/ijssh

Evolutions, Risks, and Future Directions of Automated Border Control at International Airports: A Bibliometric Analysis

Ary Rezqy Hakim[1], **Palupi Lindiasari Samputra**[2], **Ridwan Arifin**[3]

Corresponding Author's e-mail : *ary.rezqy@ui.ac.id*

Article History

Manuscript submitted:
13 March 2026
Manuscript revised:
19 April 2026
Accepted for publication:
18 May 2026

Keywords

Automated Border Control;
Autogate;
Biometrics;
Airport Security;
Facial Recognition;
Smart Border;

Abstract

Digital transformation in border management has accelerated the implementation of Automated Border Control (ABC) systems, commonly known as autogates, as part of efforts to strengthen national security. These systems utilize biometric technologies, facial recognition, and artificial intelligence (AI) to enhance the efficiency of immigration inspections. However, their implementation introduces various challenges, including cybersecurity threats, data privacy concerns, human error, and digital border governance issues. This study aims to examine the development of Automated Border Control research and identify emerging risk trends associated with autogate implementation. A bibliometric analysis was conducted on 664 publications indexed in the Scopus database. Using VOSviewer, the study mapped the conceptual structure, thematic clusters, and evolution of the ABC research field. The findings reveal that the literature has evolved from a primary focus on operational efficiency toward more complex issues such as AI-driven surveillance, cybersecurity, and governance risks. Biometrics, facial recognition, security, and e-gates emerged as the dominant research themes. The study concludes that ABC systems represent a strategic socio-technical infrastructure that requires adaptive governance and multidimensional risk management to support digital national security.

Contents

[1] National Resilience Studies Program, The Graduate School of Sustainable Development, Universitas Indonesia, Depok, Indonesia
[2] National Resilience Studies Program, The Graduate School of Sustainable Development, Universitas Indonesia, Depok, Indonesia
[3] National Resilience Studies Program, The Graduate School of Sustainable Development, Universitas Indonesia, Depok, Indonesia

e-ISSN : 2985-6469

Introduction

Digital transformation in border management has accelerated the adoption of Automated Border Control (ABC) systems, commonly referred as autogates, across international airports worldwide. These systems utilize biometric technologies, including facial recognition, fingerprint recognition, and iris recognition, to perform automated identity verification without direct interaction between travelers and immigration officers (Chaki & Ashour, 2021). The integration of biometric technologies is widely regarded as a means of enhancing service efficiency while improving identification accuracy, given that biometric characteristics are unique to individuals and relatively difficult to falsify (Labati et al., 2015).

The global expansion of ABC systems has been closely associated with heightened international security concerns following the September 11, 2001 terrorist attacks. In response, many countries have invested in biometric- and artificial intelligence (AI)-based smart border systems as part of broader strategies to strengthen national security and border surveillance capabilities (Amoore, 2006). Consequently, Automated Border Control has evolved beyond its role as a technology-enabled public service tool and has become an integral component of border governance and mobility control within contemporary national security frameworks (van der Ploeg, 2003).

The growing implementation of ABC has also been driven by the need to improve operational efficiency at international airports. Rapid growth in global air passenger traffic has placed increasing pressure on immigration inspection capacity, making conventional manual procedures insufficient to meet modern service demands. Previous studies have demonstrated that Automated Border Control systems can significantly reduce processing times and alleviate congestion at immigration checkpoints (MacLeod & McLindin, 2011). As a result, ABC have become a key element of the smart airport ecosystem, supporting service automation, operational efficiency, and enhanced passenger experience.

From a public service perspective, autogates are widely recognized as a digital innovation capable of enhancing the quality of immigration services. Empirical studies in Indonesia indicate that system quality, service quality, and ease of use significantly influence user satisfaction with autogate services (Pinaring & Indriasari, 2025; Muzakkir et al., 2025). Furthermore, these systems can reduce immigration processing times to approximately 15–25 seconds per passenger while minimizing human error during identity verification. Such developments highlight the role of autogates as a key component of digital transformation in public service delivery, emphasizing efficiency, accuracy, and user-centered service.

Despite these benefits, the implementation of Automated Border Control systems is accompanied by a range of multidimensional risks arising from increasing reliance on biometric technologies and AI-based authentication systems. Biometric risks, including false acceptance rates and false rejection rates, may result in inaccurate identification outcomes during immigration inspections. Sanchez del Rio et al. (2016) note that facial recognition systems continue to face challenges related to lighting conditions, facial pose variations, and biometric manipulation, all of which may affect system reliability and verification accuracy.

Cybersecurity vulnerabilities constitute another critical challenge. The integration of cloud databases, e-passports, and interconnected digital networks positions autogates as part of a country's critical digital infrastructure, making them susceptible to cyberattacks, data breaches, and identity theft (Gudavalli et al., 2012). Data security incidents reported at Soekarno–Hatta International Airport in 2024 further illustrate the strategic importance of cybersecurity in the implementation of border automation systems in Indonesia (Pinaring & Indriasari, 2025). Such threats may undermine the legitimacy, effectiveness, and resilience of digital border management systems.

Recent scholarship suggests that autogates should not be understood solely as technological innovations but rather as socio-technical systems involving complex interactions among technology, institutions, regulations, and human actors. Oostveen et al. (2014) demonstrate that system usability and interface design significantly influence the effectiveness of Automated Border Control systems. Similarly, Kulju et al. (2019) argue that border automation transforms the role of immigration officers from manual inspectors into supervisors of automated systems, requiring new competencies, organizational adaptation, and revised operational practices.

Although research on Automated Border Control has expanded considerably, existing studies remain largely concentrated on technical aspects such as biometrics, facial recognition technologies, and AI algorithm performance. Comparatively less attention has been devoted to governance capability, adaptive policy frameworks, human and AI collaboration, and the broader implications of autogate systems for national resilience and digital border governance (Robertson et al., 2017). This limitation reveals an important research gap, particularly in the context of developing countries such as Indonesia, where digital transformation in immigration and border management is progressing rapidly.

To address this gap, the present study seeks to answer two research questions. First, how has the thematic landscape of research on ABC evolved within the international literature? Second, what types of risks have been identified, and how have risk-related research themes developed in the context of digital border systems? Addressing these questions is essential for understanding the evolution of ABC research and identifying future directions for scholarship on autogates, smart border governance, and national resilience.

This study aims to map the development of Automated Border Control research using a bibliometric analysis approach based on the Scopus database. VOSviewer is employed to identify thematic clusters, research trends, and emerging knowledge gaps within the field. This study contributes to the theoretical advancement of Automated Border Control research while providing a comprehensive overview of the evolving landscape surrounding digital border governance. The existing literatures focus has moved from operational efficiency to advanced issues including AI surveillance, cybersecurity, and governance risks. Core themes now center on biometrics, facial recognition, security, and e-gates. The ABC systems serve as key socio-technical infrastructure, demanding adaptive governance and comprehensive risk management to enhance national digital resilience.

Literature Review

ABC has emerged as a technology-enabled border inspection system designed to enhance both efficiency and security in the management of international mobility. According to Chaki and Ashour (2021), ABC systems facilitate automated identity verification through the integration of e-passports, facial recognition, fingerprint recognition, and digital immigration databases. The development of these systems reflects a broader transformation in border governance, shifting from labor-intensive manual inspections toward digitally enabled and automated identity management.

Biometric technologies constitute the core foundation of modern autogate systems. Existing studies suggest that facial recognition and iris recognition technologies provide higher levels of accuracy than conventional inspection methods because they rely on unique biological characteristics that are difficult to forge or manipulate (Labati et al., 2015). Furthermore, advances in artificial intelligence (AI) and deep learning have enhanced the capabilities of ABC systems in image analysis, identity matching, and presentation attack detection, thereby improving their ability to identify fraudulent identities and unauthorized access attempts (Sanchez del Rio et al., 2016).

e-ISSN : 2985-6469

The development of ABC systems has also been closely associated with the pursuit of operational efficiency in international airports. Growing volumes of international air travel have placed increasing pressure on immigration checkpoints, creating a need for automated solutions capable of processing travelers more efficiently. MacLeod and McLindin (2011) demonstrated that autogates can significantly reduce passenger processing times and alleviate congestion at border control points. Consequently, Automated Border Control has become an integral component of the smart airport ecosystem, supporting service automation, operational efficiency, and enhanced passenger experience.

Empirical studies conducted in Indonesia similarly indicate that autogate implementation contributes positively to the quality of immigration services. Research by Pinaring and Indriasari (2025) and Muzakkir et al. (2025) found that system quality, service quality, and ease of use significantly influence user satisfaction with autogate services. In addition to improving inspection efficiency, these systems help reduce human error in identity verification processes. Despite these benefits, however, the implementation of Automated Border Control also introduces a range of multidimensional risks.

Biometric risk has emerged as one of the most prominent concerns in the ABC literature. Facial recognition systems continue to face challenges associated with false acceptance rates, false rejection rates, variations in facial pose, and biometric spoofing attacks (Nguyen et al., 2019). These challenges become increasingly complex when biometric technologies are integrated into AI-driven surveillance and automated border management systems, where identification errors may have significant security and operational consequences.

Cybersecurity has also become a critical issue in the development of smart border systems. The integration of cloud-based databases, e-passports, and interconnected digital networks positions autogates as part of a nation's critical digital infrastructure, exposing them to risks such as cyberattacks, data breaches, and identity theft (Gudavalli et al., 2012). As border control systems become increasingly digitized, cybersecurity is no longer merely a technical concern but a strategic prerequisite for the sustainability and resilience of digital border infrastructures.

Recent scholarship further highlights growing concerns regarding surveillance risks and ethical governance in the deployment of Automated Border Control systems. The use of facial recognition and AI-powered surveillance technologies has raised important questions concerning privacy protection, state surveillance legitimacy, algorithmic accountability, and the potential misuse of biometric data (Kindt, 2013). In this context, autogates should be understood not only as technical security tools but also as components of broader digital governance systems that require adaptive regulatory frameworks and institutional accountability mechanisms.

Human factors constitute another critical dimension of ABC effectiveness. Oostveen et al. (2014) demonstrated that system usability and interface design significantly influence the successful adoption and operation of autogates. Many operational failures stem from suboptimal human–machine interactions, including document scanning errors and improper biometric positioning by travelers. These findings suggest that technological performance alone is insufficient to guarantee effective border automation, as user interaction remains a key determinant of system success.

The digital transformation of border control has also fundamentally altered the role of immigration officers. According to Kulju et al. (2019), immigration personnel are increasingly transitioning from manual inspectors to supervisors of automated systems responsible for monitoring system performance and managing exceptions generated by AI-based border control technologies. This transformation requires new digital competencies, enhanced technical expertise, and the ability to oversee complex automated decision-making processes.

The evolution of Automated Border Control reflects a broader paradigm shift toward smart border governance driven by biometric technologies, artificial intelligence, and digital surveillance. Nevertheless, the existing literature remains heavily concentrated on technical issues such as biometric performance and AI algorithm accuracy. Comparatively less attention has been devoted to governance capability, institutional readiness, adaptive policy frameworks, and socio-technical risk management (Robertson et al., 2017). This imbalance highlights the need for a multidimensional perspective that conceptualizes autogates as adaptive socio-technical border infrastructures whose effectiveness depends not only on technological sophistication but also on governance capacity, organizational readiness, and institutional resilience

Methods

This study employs a bibliometric analysis to examine the development of research on Automated Border Control (ABC) systems in immigration checkpoints and international airports. Bibliometric analysis is widely used to systematically map the intellectual structure, thematic evolution, and knowledge domains within a particular research field through quantitative analysis of bibliographic metadata (Donthu et al., 2021). This approach enables researchers to identify research trends, emerging themes, and gaps in the existing literature through transparent and replicable procedures.

The dataset was retrieved from the Scopus database and analyzed using VOSviewer software. Scopus was selected because it provides extensive international coverage of peer-reviewed publications and is recognized as one of the most comprehensive databases for research in technology, security studies, transportation, public administration, and border governance. Furthermore, Scopus offers rich bibliographic metadata, including titles, abstracts, keywords, authors, affiliations, publication years, source titles, citations, and references, which are essential for bibliometric mapping. A search was conducted using the keyword “Automated Border Control” within the title, abstract, and keyword fields, covering publications from 2005 to 2025. The initial search yielded 664 documents.

A screening process was subsequently conducted based on predefined inclusion and exclusion criteria. The inclusion criteria comprised: (1) publications addressing Automated Border Control (ABC) or autogate systems in the context of immigration inspection and border management at international airports; (2) journal articles, conference papers, and proceedings published in English; and (3) publications containing complete abstracts and bibliographic metadata. The exclusion criteria included: (1) studies focusing solely on biometric technologies without explicit relevance to ABC systems; (2) research conducted in non-immigration domains such as banking, healthcare, or general security applications; (3) duplicate records; and (4) publications deemed irrelevant following title and abstract screening.

Following the screening and eligibility assessment, 59 publications were retained for analysis. These documents constitute the final dataset used to map the conceptual structure and thematic landscape of Automated Border Control research. The analysis was conducted using VOSviewer to generate co-occurrence networks, thematic clusters, and research trend visualizations. Attention was given to identifying dominant research themes, emerging topics, and evolving risk dimensions associated with the implementation of Automated Border Control systems. The resulting bibliometric maps provide insights into the intellectual development of the field and highlight future research opportunities in smart border governance, digital border infrastructure, and border security management.

e-ISSN : 2985-6469

.

Results and Discussions

1. Thematic Landscape of Research on ABC within the International Literature

The VOSviewer mapping results show that research on Automated Border Control (ABC) in airports is dominated by themes related to biometrics, facial recognition, and digital security. The network visualization indicates that the keyword “biometrics” is the most central node and exhibits the strongest connections with other themes, including security, facial recognition, e-passport, identity, and airport automated border control. This finding suggests that biometrics serves as the primary foundation of modern autogate systems and acts as a key link between security, digital identity verification, and automated border inspection. In addition, the emergence of clusters such as deep learning, iris recognition, feature extraction, and image analysis demonstrates that the research landscape is increasingly shifting toward the application of artificial intelligence and computer vision technologies to improve the accuracy of identity verification systems.

The co-occurrence keyword analysis identified ten major clusters representing the development of Automated Border Control (ABC) research within the context of digital border management at international airports. Each cluster reflects a distinct research focus while remaining interconnected within the broader smart border ecosystem characterized by biometric technologies, artificial intelligence, and automated surveillance systems.

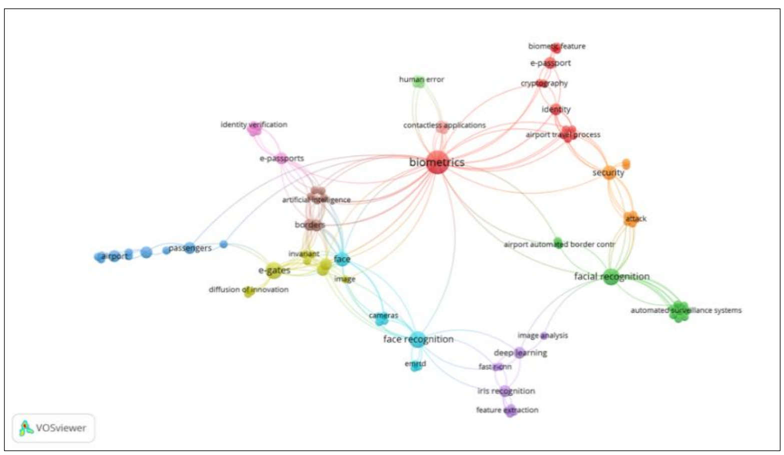

Figure 1. Network Visualization of Automated Border Control Research Based on Author Keyword Co-occurrence (VOSviewer, 2026)

Cluster 1 (Red) represents the theme of Biometric Identity Management, characterized by dominant keywords such as biometrics, identity, e-passport, biometric feature, cryptography, airport travel process, and contactless applications. This cluster indicates that a substantial portion of ABC research focuses on biometric-based digital identity authentication and the protection of electronic travel data. Previous studies suggest that the adoption of biometrics in modern border systems has evolved alongside the growing demand for secure and efficient digital identification mechanisms (Labati et al., 2015). The presence of keywords such as cryptography and contactless applications further reflects the emergence of contactless travel systems integrated with biometric data protection and digital security measures (Gudavalli et al., 2012).

Cluster 2 (Green) represents the theme of AI-Based Surveillance and Border Automation, with key terms including facial recognition, automated surveillance systems, and airport automated border

.

control. This cluster highlights the increasing role of facial recognition technologies as the core component of automated surveillance within the smart border ecosystem. Sanchez del Rio et al. (2016) identified facial recognition as a key enabling technology for e-gates and automated border systems due to its ability to enhance identification accuracy and support AI-driven real-time monitoring. The prominence of automated surveillance systems also reflects the growing integration of artificial intelligence into contemporary migration and border management practices.

Cluster 3 (Blue) focuses on Passenger Flow and Airport Operations, represented primarily by the keywords airport and passengers. This cluster indicates that part of the literature remains concerned with improving airport operational efficiency and user experience through the implementation of autogates. MacLeod and McLindin (2011) demonstrated that Automated Border Control systems can increase passenger throughput while reducing congestion at immigration checkpoints. Consequently, research within this cluster positions autogates as a component of digital transformation initiatives aimed at enhancing public service delivery within international air transportation systems.

Cluster 4 (Purple) represents Advanced AI and Computer Vision, comprising keywords such as deep learning, iris recognition, feature extraction, image analysis, and Fast R-CNN. This cluster reflects the increasing technical sophistication of ABC research, particularly in the application of computer vision and deep learning techniques to improve biometric accuracy. Nguyen et al. (2019) found that integrating biometrics with AI-driven image analysis significantly improves identification performance in Automated Border Control systems. The appearance of models such as Fast R-CNN further demonstrates advancements in AI methodologies for facial detection and biometric image processing.

Cluster 5 (Yellow) represents E-Gate Adoption and Technological Diffusion, characterized by the keywords e-gates, diffusion of innovation, face, image, and invariant. This cluster highlights scholarly attention to the implementation and diffusion of automated inspection technologies in airport environments. Oostveen et al. (2014) emphasized that usability and user acceptance are critical determinants of successful e-gate implementation. The inclusion of the term diffusion of innovation suggests an emerging research interest in technology adoption processes and institutional acceptance of automated border control systems.

Cluster 6 (Cyan) focuses on Facial Authentication Infrastructure, represented by the keywords face recognition, cameras, and eMRTD. This cluster underscores the importance of technical infrastructure in supporting facial authentication within ABC systems. Robertson et al. (2017) demonstrated that the effectiveness of face recognition systems depends heavily on camera quality, interoperability of electronic Machine Readable Travel Documents (eMRTDs), and the operational performance of biometric authentication technologies. These findings indicate that successful autogate deployment requires robust integration between hardware and software components.

Cluster 7 (Orange) represents Cybersecurity and Threat Mitigation, with dominant keywords including security and attack. This cluster reflects growing scholarly concern regarding cybersecurity threats within border automation systems. Gudavalli et al. (2012) emphasized the importance of biometric data protection and digital security enhancement in preventing cyberattacks and identity theft. Research within this cluster increasingly conceptualizes autogates as part of a nation's critical digital infrastructure, requiring resilient cybersecurity frameworks to ensure operational continuity and data integrity.

Cluster 8 (Pink) focuses on Digital Identity Verification, represented by the keywords e-passports and identity verification. This cluster examines digital identity validation and the interoperability of electronic travel documents within automated inspection systems. Research on e-passports suggests that data interoperability and standardized digital identity frameworks are essential for effective cross-border

e-ISSN : 2985-6469

verification processes (van der Ploeg, 2003). The prominence of this cluster highlights the central role of digital identity integration in contemporary border management systems.

Cluster 9 (Brown) represents AI Governance and Border Management, characterized by the keywords artificial intelligence and borders. This cluster indicates a growing research interest in the integration of AI technologies into border governance and digital migration management systems. Amoore (2006) argued that the use of AI in border management extends beyond technical efficiency to encompass governance arrangements, mobility surveillance, and algorithmic decision-making. These developments suggest that autogates are increasingly being conceptualized as components of broader smart border governance frameworks.

Cluster 10 (Light Green) represents Human Factors in Automation, with human error as its dominant keyword. Although relatively small in size, this cluster highlights the continuing importance of human factors in the implementation of Automated Border Control systems. Kulju et al. (2019) demonstrated that border automation transforms the role of immigration officers from manual inspectors into supervisors of automated systems, requiring new competencies and oversight capabilities. These findings suggest that the effectiveness of autogates depends not only on technological sophistication but also on workforce readiness and the quality of interaction between human operators and automated systems.

Table 1. Thematic Clusters Identified from Keyword Co-Occurrence Analysis

Cluster	Keywords	Main Theme	Description	References
Cluster 1 (Red)	biometrics, identity, e-passport, biometric feature, cryptography, airport travel process, contactless applications	Biometric Identity Management	Focuses on digital identity authentication, e-passports, and the protection of biometric data in automated air travel processes.	Labati et al. (2015); Gudavalli et al. (2012); van der Ploeg (2003)
Cluster 2 (Green)	facial recognition, automated surveillance systems, airport automated border control	AI-Based Surveillance and Border Automation	Highlights the evolution of facial recognition as the core technology underpinning automated surveillance and smart border ecosystems.	Sanchez del Rio et al. (2016); Amoore (2006); Vizitiu et al. (2024)
Cluster 3 (Blue)	airport, passengers	Passenger Flow and Airport Operations	Focuses on airport operational efficiency and passenger experience in the implementation of automated border systems.	MacLeod & McLindin (2011); Pinaring & Indriasari (2025); Muzakkir et al. (2025)

Cluster 4 (Purple)	deep learning, iris recognition, feature extraction, image analysis, Fast R-CNN	Advanced AI and Computer Vision	Emphasizes the application of deep learning and computer vision techniques to optimize biometric identification accuracy.	Nguyen et al. (2019); Schuckers et al. (2006); Sanchez del Rio et al. (2016)
Cluster 5 (Yellow)	e-gates, diffusion of innovation, invariant, face, image	E-Gate Adoption and Technological Diffusion	Describes the implementation of e-gates and the diffusion of automated border control innovations across airport environments.	Oostveen et al. (2014); MacLeod & McLindin (2011); Jane's Airport Review (2005)
Cluster 6 (Cyan)	face recognition, cameras, eMRTD	Facial Authentication Infrastructure	Focuses on the technical infrastructure supporting facial recognition and the integration of electronic Machine Readable Travel Documents (eMRTD) within ABC systems.	Robertson et al. (2017); Labati et al. (2015); Sanchez del Rio et al. (2016)
Cluster 7 (Orange)	security, attack	Cybersecurity and Threat Mitigation	Highlights concerns related to cybersecurity threats, cyberattacks, and vulnerabilities in border automation systems.	Gudavalli et al. (2012); Kindt (2013); Milbredt et al. (2022)
Cluster 8 (Pink)	e-passports, identity verification	Digital Identity Verification	Focuses on digital identity validation and the interoperability of electronic travel documents in automated border inspection systems.	van der Ploeg (2003); Labati et al. (2015); Robertson et al. (2017)
Cluster 9 (Brown)	artificial intelligence, borders	AI Governance and Border Management	Highlights the integration of artificial intelligence into governance frameworks and digital border management systems.	Amoore (2006); Broeders (2007); Vizitiu et al. (2024)

e-ISSN : 2985-6469

Cluster 10 (Light Green)	human error	Human Factors in Automation	Highlights issues related to human error and human involvement in automated border control systems.	Kulju et al. (2019); Oostveen et al. (2014); Robertson et al. (2017)

The overlay visualization further reveals the evolution of Automated Border Control (ABC) research from an initial focus on operational efficiency toward broader concerns related to digital surveillance and AI-enabled security systems. Keywords displayed in blue to green shades, such as e-gates, security, airport travel process, and identity, indicate that earlier studies primarily concentrated on inspection efficiency, identity verification, and the implementation of automated border inspection systems at airports. During this phase, research was largely concerned with the integration of basic biometric technologies and the enhancement of passenger throughput at immigration checkpoints. The following table summarizes the characteristics and thematic focus of each research cluster.

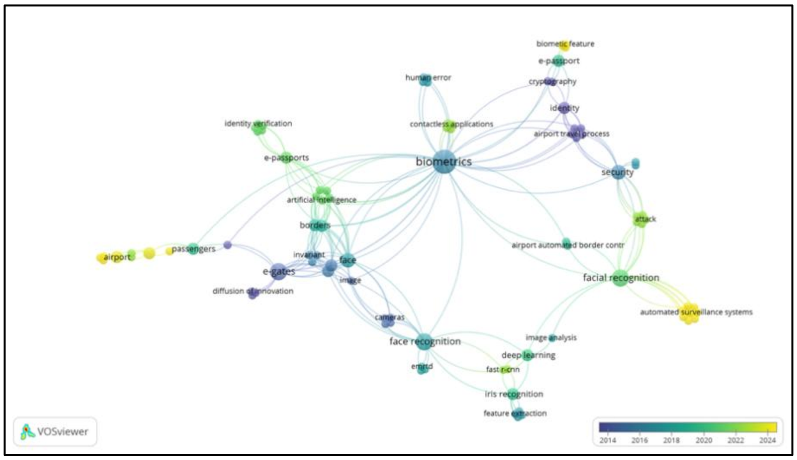

Figure 2. Overlay Analysis (Source: VOSViewer, 2026)

The analysis reveals a significant increase in Automated Border Control (ABC) research after 2016, coinciding with the rapid advancement of AI-based facial recognition technologies and smart airport systems. The evolution of ABC research demonstrates a clear shift from a predominantly technical focus toward the development of smart border ecosystems supported by artificial intelligence and integrated digital surveillance. During the period 2005–2010, research primarily focused on the application of basic biometric technologies to support automated identity verification through fingerprint recognition and e-passport systems. Studies conducted during this phase emphasized identification accuracy and passenger processing efficiency as key objectives in international border security management (van der Ploeg, 2003; Jane's Airport Review, 2005).

Subsequent developments expanded the scope of research beyond basic biometric authentication toward more sophisticated approaches incorporating facial recognition, machine learning, and automated surveillance technologies. This transition reflects growing interest in leveraging artificial intelligence to enhance the effectiveness, reliability, and scalability of border control operations. As a result, Automated Border Control systems have increasingly been conceptualized not only as tools for identity verification but also as integral components of digitally enabled border governance frameworks.

Table 2. Research Evolution Automated Border Control

Period	Research Focus	Research Characteristics
2005–2010	Basic Biometric Verification	Research primarily focused on the application of basic biometric technologies, such as fingerprint recognition and e-passport systems, to support automated identity verification and enhance border inspection efficiency.
2011–2015	E-Passport and E-Gate Development	Studies emphasized the development of automated gate systems, interoperability of electronic travel documents, and the integration of e-passports into border control processes.
2016–2020	Facial Recognition and AI Integration	Research increasingly explored the integration of facial recognition, artificial intelligence, machine learning, and image analysis technologies to improve identification accuracy and strengthen border security systems.
2021–2025	Smart Border Ecosystems and Surveillance Automation	Research expanded toward AI-driven surveillance, contactless border control, smart border governance, cybersecurity, digital identity management, and the automation of border security operations.

The period from 2011 to 2015 witnessed the expansion of research toward e-gate implementation and the interoperability of automated inspection systems based on e-passports. Studies during this phase increasingly examined the integration of biometric technologies with automated gate systems, while also evaluating usability and user experience in airport autogate operations (MacLeod & McLindin, 2011; Oostveen et al., 2014). A significant shift occurred between 2016 and 2020, when research began to focus on facial recognition, artificial intelligence (AI), and image analysis as core components of AI-driven border security systems (Sanchez del Rio et al., 2016). Entering the period 2021–2025, the research agenda expanded further toward the development of smart border ecosystems characterized by automated surveillance systems, deep learning applications, contactless border control, and digital governance frameworks for contemporary border management (Vizitiu et al., 2024; Pinaring & Indriasari, 2025).

Beyond technological developments, the literature indicates that the implementation of Automated Border Control involves a range of interconnected and multidimensional risks. Biometric risk remains one of the most prominent concerns, particularly regarding the reliability of facial recognition and iris recognition systems in accurately identifying individuals. Nguyen et al. (2019) noted that biometric systems continue to face challenges related to lighting conditions, facial pose variations, and identity manipulation, all of which may result in false acceptance or false rejection outcomes. Such risks become increasingly critical when biometric authentication serves as the primary mechanism for cross-border identity verification.

Cybersecurity has also emerged as a strategic issue within smart border systems. The integration of cloud databases, e-passports, and interconnected digital networks exposes autogates to vulnerabilities such as cyberattacks, identity theft, and data breaches (Gudavalli et al., 2012). The prominence of keywords such as attack, security, and cryptography in the network visualization further confirms the growing scholarly attention devoted to cybersecurity challenges. In addition, the literature highlights governance risks associated with regulatory readiness, institutional capacity, and policy harmonization in the management of cross-border digital surveillance systems.

Human and ethical dimensions constitute another important area of concern. Oostveen et al. (2014) demonstrated that system usability and human–machine interaction significantly influence the effectiveness of autogate operations. At the same time, the increasing deployment of AI-based surveillance and facial recognition technologies has raised concerns regarding privacy protection, the legitimacy of digital surveillance practices, and the potential misuse of biometric data (Kindt, 2013). These findings suggest that the successful implementation of Automated Border Control requires an adaptive governance approach, as the associated risks extend beyond technical issues to encompass social, ethical, and institutional dimensions.

The evolution of the literature indicates that Automated Border Control has gradually transformed from a technology-oriented innovation into a complex socio-technical infrastructure. While early research primarily emphasized operational efficiency and biometric performance, recent studies increasingly address governance challenges, cybersecurity resilience, and the broader implications of AI-enabled border management. This shift reflects the growing recognition that the effectiveness of smart border systems depends not only on technological sophistication but also on institutional readiness, regulatory capacity, and multidimensional risk management.

2. Risk-Related Research Themes Developed in the Context of Digital Border Systems

The findings indicate that the implementation of Automated Border Control (ABC) systems requires an adaptive governance approach, as the risks associated with border automation are multidimensional, interconnected, and continuously evolving. The bibliometric analysis reveals that the existing literature remains predominantly focused on technological aspects, particularly biometric authentication, facial recognition, and AI-based identity verification systems. Research in this domain has largely concentrated on improving identification accuracy, image analysis techniques, and the operational efficiency of automated gate systems (Labati et al., 2015; Sanchez del Rio et al., 2016). This dominance is clearly reflected density visualization, where keywords such as biometrics, facial recognition, and security exhibit the highest levels of density and connectivity within the research network.

Table 3. Major Risks Associated with Automated Border Control Implementation

Risk Type	Description
Biometric Risk	False acceptance and false rejection
Cybersecurity Risk	Hacking and data breach
Governance Risk	Regulation and institution readiness
Operational Risk	System downtime and bottleneck
Human Risk	Human error and skill gap
Ethical Risk	Privacy and surveillance concern

In contrast, research on governance capability, institutional readiness, and socio-technical risk management remains relatively underdeveloped. Existing studies have paid limited attention to how immigration institutions adapt to AI-driven border systems or how human–AI collaboration influences the effectiveness and legitimacy of digital border governance. Robertson et al. (2017) observed that most evaluations of ABC systems continue to emphasize technical performance indicators rather than organizational preparedness, governance arrangements, and institutional adaptation. This imbalance suggests that the development of border automation technologies has progressed more rapidly than the governance mechanisms required to manage their broader implications.

These findings highlight important opportunities for advancing the literature on smart border governance and adaptive socio-technical systems. The emergence of themes such as cybersecurity, automated surveillance systems, and contactless applications in the overlay visualization suggests that the research agenda is gradually shifting toward issues of cyber resilience, governance adaptation, and institutional capability in managing digital border infrastructures. Consequently, future research on Automated Border Control should move beyond a purely technological perspective and incorporate broader considerations of national resilience, digital governance, and adaptive governance mechanisms to address the emerging risks associated with smart border ecosystems.

Conclusion

This study demonstrates that Automated Border Control (ABC) should no longer be understood merely as a technological innovation designed to improve the efficiency of immigration inspections. Rather, the evolution of the literature indicates that ABC has developed into a strategic socio-technical infrastructure that integrates biometric technologies, artificial intelligence, digital identity systems, and border governance mechanisms. In this context, the findings answer the first research question by showing that the intellectual trajectory of ABC research has evolved from a narrow focus on operational efficiency and biometric authentication toward a broader concern with digital surveillance, cybersecurity, governance, and institutional adaptation within smart border ecosystems.

The study also answers the second research question by demonstrating that the risks associated with Automated Border Control extend beyond technical vulnerabilities and encompass interconnected biometric, cybersecurity, governance, human, and ethical dimensions. These findings suggest that the effectiveness of ABC systems cannot be assessed solely through technological performance indicators such as accuracy, speed, or automation capability. Instead, successful implementation depends on the ability of institutions to develop adaptive governance arrangements capable of managing complex socio-technical risks in increasingly digitalized border environments. Consequently, the future of border automation is not only a technological challenge but also a governance challenge that requires organizational readiness, regulatory adaptability, and institutional resilience

These gaps present important opportunities for advancing the literature on smart border governance and adaptive socio-technical systems. The emergence of themes such as cybersecurity, automated surveillance systems, and contactless applications in the overlay visualization indicates that ABC research is increasingly moving toward issues of cyber resilience, governance adaptation, and institutional capability in managing digital border infrastructures. Consequently, future research on autogates should extend beyond a purely technological perspective and incorporate broader considerations of national resilience, digital governance, and adaptive governance mechanisms to address the emerging risks associated with smart border ecosystems.

e-ISSN : 2985-6469

Acknowledgments

We are grateful to two anonymous reviewers for their valuable comments on the earlier version of this paper.

References

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. Political Geography, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Broeders, D. (2007). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. International Sociology, 22(1), 71–92. https://doi.org/10.1177/0268580907070126

Butt, M., Marti, S., Nouak, A., Koplin, J., Raghavendra, R., & Li, G. (2013). Towards e-passport duplicate enrollment check in the European Union. In 2013 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1–5). IEEE. https://doi.org/10.1109/BIOSIG.2013.6679836

Carlos-Roca, L. R., Torres, I. H., & Tena, C. F. (2018). Facial recognition application for border control. Proceedings of SPIE - The International Society for Optical Engineering, 10618. https://doi.org/10.1117/12.2303719

Chaki, N. M., & Ashour, M. W. (2021). Automated border control systems: A literature review. In IET Conference Proceedings. Institution of Engineering and Technology.

Del Río, J. S., Conde, C., Tsitiridis, A., Gómez, J. R., Martín de Diego, I., & Cabello, E. (2015). Face-based recognition systems in the ABC e-gates. In Lecture Notes in Computer Science (Vol. 9319, pp. 340–349). Springer. https://doi.org/10.1007/978-3-319-24192-1_30

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Ferrara, M., Franco, A., & Maltoni, D. (2018). Face demorphing. IEEE Transactions on Information Forensics and Security, 13(4), 1008–1017. https://doi.org/10.1109/TIFS.2017.2777347

Ghali, A. A., Jamel, S., Mohamad, K. M., Yakub, N. A., & Deris, M. M. (2017). A review of iris recognition algorithms. Journal of Telecommunication, Electronic and Computer Engineering, 9(2-5), 15–18.

Gudavalli, M., Raju, S. V., & Kumar, K. S. M. V. (2012). A template protection scheme for multimodal biometric system with fingerprint, palmprint, iris and retinal traits. ACM International Conference Proceeding Series, 1–6. https://doi.org/10.1145/2461131.2461137

Gutin, M., Tsui, E. K., Gutin, O., Wang, X.-M., & Gutin, A. (2006). Thermal infrared panoramic imaging sensor. Proceedings of SPIE - The International Society for Optical Engineering, 6201. https://doi.org/10.1117/12.665778

Jane's Airport Review. (2005). Tougher security at Schiphol inflates fees. Jane's Airport Review, 17(6), 6–7.

Keshtgar, S., Keshtgar, A., Mistry, P., & Shakib, K. (2019). Assessing facial recognition after orthognathic surgery at automated border controls in airports. British Journal of Oral and Maxillofacial Surgery, 57(10), 1030–1034. https://doi.org/10.1016/j.bjoms.2019.08.014

Kindt, E. (2013). Privacy and data protection issues of biometric applications: A comparative legal analysis. Springer Dordrecht. https://doi.org/10.1007/978-94-007-7522-0

Kulju, M., Ylikauppila, M., Toivonen, S., & Salmela, L. (2019). A framework for understanding human factors issues in border control automation. In IFIP Advances in Information and

Communication Technology (Vol. 569, pp. 169–180). Springer. https://doi.org/10.1007/978-3-030-20497-6_15

Labati, R. D., Genovese, A., Muñoz, E., Piuri, V., Scotti, F., & Sforza, G. (2015). Automated border control systems: Biometric challenges and research trends. In Lecture Notes in Computer Science (Vol. 9319, pp. 281–291). Springer. https://doi.org/10.1007/978-3-319-24192-1_24

MacLeod, V., & McLindin, B. (2011). Methodology for the evaluation of an international airport automated border control processing system. In Studies in Computational Intelligence (Vol. 339, pp. 1–18). Springer. https://doi.org/10.1007/978-3-642-18354-6_1

Milbredt, O., Bringer, J., Chabanne, H., & Kindarji, B. (2022). Cybersecurity challenges in biometric border control systems. Computers & Security, 118, 102732. https://doi.org/10.1016/j.cose.2022.102732

Muzakkir, A. A. F., Seloatmodjo, F. A. B., Hartanto, M. M., Nursanto, G. A., & Putra, R. D. (2025). Factors influencing user satisfaction in using immigration autogate. In Proceedings of the 22nd International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2025).

Neo, H.-F., & Teo, C.-C. (2022). Biometrics in tourism: Issues and challenges. Tourism Review, 77(5), 1340–1355. https://doi.org/10.1108/TR-05-2021-0236

Nguyen, H. M., Rattani, A., & Derakhshani, R. (2019). Biometrics fusion with applications in passenger re-authentication for automated border control systems. In 2019 IEEE International Symposium on Technologies for Homeland Security (HST) (pp. 1–6). IEEE. https://doi.org/10.1109/HST47167.2019.9032972

Oostveen, A.-M. (2014). Non-use of automated border control systems: Identifying reasons and solutions. European Journal of Law and Technology, 5(3), 1–17.

Oostveen, A.-M., Kaufmann, M., Krempel, E., & Grasemann, G. (2014). Automated border control: A comparative usability study at two European airports. In Proceedings of the International Conferences on Interfaces and Human Computer Interaction 2014, Game and Entertainment Technologies 2014 and Computer Graphics, Visualization, Computer Vision and Image Processing 2014 (pp. 239–246).

Opitz, A., & Kriechbaum-Zabini, A. (2015). Evaluation of face recognition technologies for identity verification in an eGate based on operational data of an airport. In 2015 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1–5). IEEE. https://doi.org/10.1109/BIOSIG.2015.7314610

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Pinaring, B. P., & Indriasari, E. (2025). Evaluating user satisfaction of automated border control in smart airports: Case studies from Indonesia. In Proceedings of the 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT 2025).

Robertson, J. J., Guest, R. M., Elliott, S. J., & O'Connor, K. (2017). A framework for biometric and interaction performance assessment of automated border control processes. IEEE Transactions on Human-Machine Systems, 47(6), 987–998. https://doi.org/10.1109/THMS.2017.2700843

e-ISSN : 2985-6469

Sanchez del Rio, J., Moctezuma, D., Conde, C., Martín de Diego, I., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. Computers & Security, 62, 49–72. https://doi.org/10.1016/j.cose.2016.07.001

Sarkar, E., Benkraouda, H., Krishnan, G., Gamil, H., & Maniatakos, M. (2022). FaceHack: Attacking facial recognition systems using malicious facial characteristics. IEEE Transactions on Information Forensics and Security, 17, 2189–2204. https://doi.org/10.1109/TIFS.2022.3177585

Schreiber, D., Kriechbaum, A., & Rauter, M. (2013). A multisensor surveillance system for automated border control (eGate). In 2013 International Conference on Biometrics and Kansei Engineering (pp. 193–198). IEEE. https://doi.org/10.1109/ICBAKE.2013.53

Schuckers, S., Abhyankar, A., & Hornak, L. (2006). Multimodal biometric systems: Integration and performance analysis. IEEE Aerospace and Electronic Systems Magazine, 21(6), 5–10. https://doi.org/10.1109/MAES.2006.1642573

Spreeuwers, L. J., Hendrikse, A. J., & Gerritsen, K. J. (2012). Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport. In 2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (pp. 1–12). IEEE.

Stevens, C. (2021). Person identification at airports during passport control. Journal of Transportation Security, 14(1–2), 55–70. https://doi.org/10.1007/s12198-021-00233-z

van der Ploeg, I. (2003). Biometrics and the body as information: Normative issues of the socio-technical coding of the body. In D. Lyon (Ed.), Surveillance as social sorting: Privacy, risk, and digital discrimination (pp. 57–73). Routledge.

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Vizitiu, C., Preda, V., & Ionescu, R. (2024). Smart security and digital transformation in airport border systems. Journal of Transportation Security, 17(2), 155–173. https://doi.org/10.1007/s12198-024-00275-8

Wilson, D. (2006). Biometrics, borders and the ideal suspect. In Borders, mobility and technologies of control (pp. 87–109). Springer Netherlands. https://doi.org/10.1007/1-4020-4899-8_5