**Information Management and Business Review (ISSN 2220-3796)**
**Vol. 18, No. 4(S), pp. 181-195, 2026**

# Hybrid Face Detection for Business Access Control: A Conceptual Implementation Framework

Wan Zulaikha Wan Yaacob[1], *Noor Faizah Mohd Lajin[2], Nur Ain Ahmad Yatim Mustafa[1], Zulkarnaen Bin Mohd Lajin[3]
[1]Universiti Kuala Lumpur Business School, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia
[2]Faculty of Business and Management, Universiti Teknologi MARA, Malaysia
[3]Politeknik Sultan Idris Shah, Selangor, Malaysia
Email: wanzulaikha@unikl.edu.my, *noorfaizah@uitm.edu.my, ain.mustafa@unikl.edu.my, zulkarnaen.lajin@staff.psis.edu.my
Corresponding Author: Dr Noor Faizah Mohd Lajin

**Abstract:** Business access control decides who may enter which part of an organization's premises, under what conditions, and with what record, and organizations increasingly turn to biometric technology to make it more secure and less dependent on transferable credentials. Face detection is the first step of any facial access-control pipeline, and earlier research developed a hybrid Viola-Jones and Multi-Block Local Binary Pattern (MB-LBP) detector that copes better with faces rotated at several angles. Technical accuracy alone, however, does not show that such a detector can be introduced responsibly into a business. This paper therefore proposes a conceptual implementation framework for applying the hybrid detector to employee access control. Drawing on literature on face detection, biometric access control, technology adoption, privacy and employee acceptance, the framework identifies six dimensions: business need alignment, technical readiness, organisational readiness, security and privacy governance, employee acceptance, and business value. Together they shape implementation readiness, the outcome that determines whether an organization should proceed to a controlled pilot. A five-stage implementation process and seven propositions are offered for future empirical testing. No new face-detection experiment is reported. The paper links an established technical capability to the organizational conditions of its use and gives managers a structured basis for deciding whether, where and how to pilot facial access control.

**Keywords:** *Hybrid Face Detection, Viola-Jones, Multi-Block LBP, Business Access Control, Implementation Readiness, Biometric Technology*

## 1. Introduction

Business access control is the combination of policies, hardware and software that decides who may enter an organisation's buildings, rooms and information-bearing areas, records when they do so, and withdraws permission when roles change. It protects people, physical assets, confidential information and operating continuity, and it now overlaps with information security because door controllers, identity databases and audit logs are networked. Conventional credentials such as keys, PINs and proximity cards are easy to administer, but they can be lent, lost, copied or stolen, which loosens the link between the credential and the person who presents it (Lee et al., 2020; Temoshok, Proud-Madruga, et al., 2025).

Biometric systems address this weakness by verifying people through physical or behavioural characteristics. Facial technology is an especially visible example because it needs little physical contact, can run on inexpensive cameras and fits naturally into entrance routines. Reviews describe its use in attendance recording, entry to secured areas, payment and identity verification (Lazarini et al., 2022; Li et al., 2020) and studies in Malaysia have examined workplace attendance tracking (Khan et al., 2023) and facial payment (Lim et al., 2025). For businesses, the practical question is no longer only whether faces can be processed by a computer, but whether a facial system can improve access control without creating new security, privacy and organisational problems (Downie et al., 2025; Guleria et al., 2024).

Face detection differs from face recognition. Detection decides whether a face is present in an image and where it is, whereas recognition decides whose face it is (Hjelmås & Low, 2001; Li et al., 2020). A facial access-control transaction therefore passes through image capture, face detection, face recognition, identity verification, authorisation checking and an access decision. Errors made at the detection stage are carried into every later stage, so detection quality is a precondition of reliable recognition (Hasan et al., 2021; Li et al., 2020). Detection methods are usually grouped into feature-based approaches, which look for edges, facial parts, skin colour or

texture, and image-based approaches, which rely on statistical models, machine learning and neural networks (Hasan et al., 2021; Hjelmås & Low, 2001). Whatever the approach, rotation, lighting variation, noise, blur, cluttered backgrounds and occlusion remain persistent difficulties.

The Viola-Jones detector remains one of the most widely used methods because Haar-like features, integral images, AdaBoost and a cascade of classifiers together deliver fast detection (Viola & Jones, 2001). It works best on frontal faces and becomes less dependable when faces are rotated, partly covered, poorly lit or captured at low quality (Obaida et al., 2022; Taunk et al., 2020). Multi-Block Local Binary Pattern (MB-LBP) adds a texture description based on the intensity relationships between rectangular blocks (Zhang et al., 2007). Ali et al. (2025) combined the two methods into a hybrid detector for faces rotated through multiple angles and evaluated it experimentally using image-quality and detection measures.

A technically successful detector, however, is not yet a working business access-control system. An organisation must still ask whether the technology solves a real security or operational problem, whether its cameras, network and databases can support it, whether biometric data can be protected, whether employees will accept it, and whether the benefits justify the cost. This is the technology-to-business implementation gap. Technical studies show whether a method can perform its computational task; they say little about whether a business is technically, operationally, financially, legally and socially prepared to use it.

This paper therefore aims to develop a conceptual implementation framework for the hybrid Viola-Jones and MB-LBP method in business access control. Two research questions guide the work. First, which organisational conditions should be examined before the hybrid detector is introduced into an employee access-control environment? Second, how can those conditions be arranged into a staged process that leads to a justified decision to pilot, redesign or discontinue? Business access control is the focal domain of the study. Implementation readiness, meaning an organisation's preparedness to move from assessment to a controlled pilot, is the outcome that the framework seeks to explain.

The paper does not propose a new detection algorithm and does not repeat the earlier experiments. It treats the hybrid method as an established technical capability and examines what must be in place for that capability to be used responsibly. Section 2 reviews the literature on business access control, face detection, the hybrid method, organisational adoption and the research gap, and then develops the conceptual framework and propositions. Section 3 explains the research approach. Section 4 sets out the implementation process. Sections 5 to 9 present the discussion, theoretical contribution, managerial implications, limitations and conclusion.

## 2. Literature Review

### Business Access Control

Access control can be described as four linked functions: identifying a person, authenticating the claimed identity, authorising the person for a specific location or resource, and keeping an auditable record of the event. Digital identity guidance treats these as separate assurance questions and stresses that the strength of each depends on the technical and management controls around it (Temoshok, Fenton, et al., 2025; Temoshok, Proud-Madruga, et al., 2025). In businesses, physical and logical access are increasingly managed through the same identity infrastructure, so a weakness at the door can become a weakness in the information system and the reverse.

The effectiveness of an access-control system is multidimensional. Security effectiveness concerns how rarely unauthorised people are admitted. Usability concerns how rarely authorised people are rejected and how long entry takes. Auditability concerns whether events can be reconstructed. Cost and compliance concern the full cost of ownership and the legal duties attached to the data processed. The trade-off between acceptance and rejection errors is central to biometric access control, and reported error rates depend strongly on lighting, distance, user cooperation and population (Grother et al., 2019; Lee et al., 2020).

Biometrics change this picture in two ways. They tie the credential to the person, which reduces card sharing and loss, but they also create sensitive, hard-to-replace data and probabilistic decisions that can fail for legitimate users. Digital identity guidance therefore treats biometric comparison as a probabilistic process and

generally pairs it with another authenticator in digital authentication (Temoshok, Fenton, et al., 2025). These characteristics explain why the introduction of facial technology cannot be judged by detection accuracy alone, and why this paper treats the preparedness of the organisation, rather than the accuracy of the algorithm, as the outcome of interest.

**Face Detection**

Face detection locates human faces in an image and is the entry point to facial recognition, identity verification and authentication (Hasan et al., 2021; Hjelmås & Low, 2001; Li et al., 2020). At an employee entrance, the system captures an image, finds the face region, passes it to a matching module, verifies the employee's identity, checks authorisation and either releases the door or refuses entry. Poor localisation reduces the quality of the features available for matching, and a face that is not found cannot be matched at all.

Techniques are commonly divided into feature-based methods, which detect facial parts, skin regions, boundaries and texture, and image-based methods, which use statistical classification, neural networks and other learned representations of image regions (Hjelmås & Low, 2001; Li et al., 2020). Practical performance is affected by facial rotation, which shifts the positions of landmarks, by illumination, which changes brightness and contrast, by noise and motion blur, and by occlusion from masks, glasses or hair. These problems intensify when a system moves from controlled laboratory photographs to real entrances where people approach at different speeds, distances and angles (Lazarini et al., 2022; Lee et al., 2020).

**Viola-Jones Algorithm**

The Viola-Jones algorithm combines four ideas: Haar-like features that measure intensity differences between adjacent rectangles, integral images that make these features cheap to compute, AdaBoost selection of the most discriminative features, and a cascade that rejects non-face regions early (Viola & Jones, 2001). Its low computational cost is valuable in access control, where employees should not wait at a door while an image is analysed, and it is still widely used as the detection stage in attendance and access systems (Lazarini et al., 2022).

Its weakness is sensitivity to pose and image quality. Detection performance falls when faces are rotated, taken from unusual angles, poorly lit, partly obscured or captured at low resolution (Ali et al., 2025; Obaida et al., 2022; Taunk et al., 2020). Employees cannot be expected to stand squarely in front of a camera, so this limitation has direct operational consequences.

**Multi-Block Local Binary Pattern**

The Local Binary Pattern (LBP) describes texture by comparing each pixel with its neighbours, and its rotation-invariant and multiresolution forms made it a standard texture descriptor (Ojala et al., 2002). Applied to faces, LBP histograms proved to be a compact and effective description for face recognition (Ahonen et al., 2006), and comparative studies continue to include LBP among the established local descriptors (Kortli et al., 2018).

Multi-Block LBP extends the idea from single pixels to rectangular blocks. Zhang et al. (2007) compare the average intensity of a block with that of its neighbouring blocks, encode the result as a compact code and compute it quickly with integral images, so that features describing larger local structures can be used inside a boosted cascade for face detection. Later work applied multi-scale block LBP to face recognition (Liao et al., 2007). The practical significance of MB-LBP is that it supplies local texture and structure information that does not depend entirely on the large contrast patterns captured by Haar-like features. That information is useful when pose and illumination vary, which is precisely where the original Viola-Jones detector is weakest.

**Hybrid Viola-Jones and MB-LBP Face Detection**

The hybrid method integrates two complementary strengths. Viola-Jones contributes efficient cascade-based localisation, and MB-LBP contributes richer local texture information. In the processing flow described by Ali et al. (2025), the input image is preprocessed, for example resized and converted to grayscale; MB-LBP features are extracted to describe local texture; and the Viola-Jones cascade then determines the probable face region, which is passed on to recognition or authentication.

Ali et al. (2025) showed that the combination is technically feasible and evaluated it on faces rotated through different angles. Their evaluation concerned detection and image-quality measures, not the conditions of a working business entrance. The present study therefore takes the hybrid architecture as given and does not claim it as new. Its contribution lies in examining what must happen after technical development before the method can reasonably be considered for organisational use.

**Impact of Hybrid Face Detection on Business Access Control**

Because the available experimental evidence is technical, the effect of hybrid face detection on business access control has to be reasoned from how the detection stage interacts with the rest of the access-control system. Four channels can be distinguished. These are conceptual expectations to be tested, not established findings. The first channel is capturing tolerance and throughput. A detector that finds faces at several rotation angles should reduce failed captures when people approach a camera without perfect alignment. Fewer failed captures mean fewer repeated attempts and shorter queues, which matters because user cooperation and lighting are known constraints on standalone access-control devices (Lee et al., 2020). The benefit is expected to be greatest at busy entrances and in walk-up situations where people cannot be asked to pose.

The second channel is the quality of what is passed downstream. Detection errors propagate to recognition (Lazarini et al., 2022; Li et al., 2020), so better localisation of rotated faces can improve the crop and alignment supplied to the matcher. This is an indirect effect: the hybrid detector does not itself identify anyone, and any gain in false rejection depends on the recognition module that follows it. The third channel is computational footprint. The cascade structure keeps Viola-Jones inexpensive (Viola & Jones, 2001), and MB-LBP features are computed from integral images (Zhang et al., 2007). A hybrid of the two is therefore a plausible candidate for edge devices at doors, where processing power and network connectivity are limited (Lee et al., 2020). Whether the added MB-LBP processing remains within the latency tolerated at a particular entrance is an empirical question for each site.

The fourth channel concerns what the hybrid detector does not change. It does not provide identity matching, and it does not by itself resist photographs, videos or masks presented to the camera, which are assessed through presentation-attack testing (ISO/IEC, 2023; Temoshok, Fenton, et al., 2025). It does not remove differences in error rates between demographic groups that have been documented for face recognition algorithms (Grother et al., 2019). And because capturing and processing facial images can already involve personal data, governance duties begin at capture rather than at matching (Government of Malaysia, 2024).

Taken together, these channels suggest that hybrid face detection can improve the usability and robustness of facial access control at the front of the pipeline, but that the effect on security, cost and employee experience at enterprise level is mediated by infrastructure, integration, governance and acceptance. This is the reasoning on which the framework in Section 2.10 is built.

**Facial Technology in Business Environments**

Facial technologies have been proposed for many organisational activities. In attendance management they can reduce reliance on cards, badges or manual registers (Khan et al., 2023; Lazarini et al., 2022). In physical access control they can help decide whether an employee may enter offices, server rooms, laboratories, warehouses, financial processing areas or other restricted facilities (Lee et al., 2020). They can support visitor management, although the governance of visitor data differs from that of employee data, and they have been studied for identity verification and payment (Lim et al., 2025; Shiau et al., 2024).

These applications also raise concerns that go beyond technical performance. The literature identifies privacy, fairness, transparency, trust, organisational justice, surveillance and acceptance as recurring issues (Ciftci et al., 2024; Downie et al., 2025; Fu & Lyu, 2025; Guleria et al., 2024). Introducing facial technology into a business therefore has both technological and organisational consequences, which is the premise of the framework developed here.

**Organisational Adoption of Biometric Access Control**

Whether a business can use a technology successfully depends on more than the technology. The Technology-Organisation-Environment (TOE) perspective captures this by distinguishing the technological context (for

example compatibility, complexity and infrastructure), the organisational context (for example management support, skills and financial resources) and the environmental context (for example regulation, competition and external partners). A recent meta-review of more than 80 information systems studies that used TOE found that factors are often placed in different contexts from study to study and that some sub-categories are poorly measured (Thomas & Yao, 2023). This argues for defining each factor carefully rather than relying on the three headings alone. Recent applications of TOE to artificial intelligence adoption consistently find that readiness, top-management support, human and financial resources, technical compatibility and external conditions influence implementation (Badghish & Soomro, 2024; Hughes et al., 2026; Yang et al., 2024). These findings support the claim that a technically functioning detector is not automatically ready for organisational use. TOE is nonetheless a general adoption perspective. Biometric access control involves identifiable individuals and sensitive data, so the framework in this paper extends TOE with security and privacy governance, employee acceptance and business value.

Security and privacy are central because a face is linked to a person's identity and cannot be reissued like a card. An organisation must decide why it collects facial data, how much it needs, where it is stored, who may access it, how long it is kept and when it is deleted. The security architecture must also address unauthorised access, administrator privileges, network protection, incident response and attempts to deceive the system. Digital identity guidance and presentation-attack testing standards emphasise that biometric systems need technical and management controls because biometric measurements vary and can be attacked (ISO/IEC, 2023; Temoshok, Fenton, et al., 2025; Temoshok, Proud-Madruga, et al., 2025), and AI risk-management guidance adds that governance should cover the whole system life cycle (Tabassi, 2023). In Malaysia, the Personal Data Protection (Amendment) Act 2024 expressly includes biometric data within sensitive personal data (Government of Malaysia, 2024), so accountability and privacy governance must be addressed from the start of design.

Employee acceptance is the human side of the same problem. Workers may ask why facial data is collected, whether it will be used for purposes beyond access, who can see it and whether the system will increase monitoring. Studies of employee reactions to biometric and facial technologies point to trust, organisational justice, perceived benefit, transparency and privacy concern as influential factors (Carpenter et al., 2018; Ciftci et al., 2024; Downie et al., 2025; Fu & Lyu, 2025). A survey of employees in Malaysia found generally favourable views of the usefulness and ease of use of facial attendance tracking, together with concerns about privacy, data security and accuracy (Khan et al., 2023). Acceptance therefore depends not only on ease of use but also on whether employees consider the system necessary, proportionate, secure and fairly governed.

Combining these strands, an enterprise access-control system is best understood as a socio-technical system. A detector affects the organisation through its fit with infrastructure and existing systems, through the capability of the people who operate it, through the legal and security obligations attached to the data it handles, through the reactions of the people who pass through the door, and through its cost relative to the value it adds. Table 1 maps these channels to the framework dimensions developed in Section 2.10.

**Table 1: Mapping of TOE contexts and biometric-specific considerations to the framework dimensions**

| Framework Dimension | TOE context/extension | Illustrative focus | Key sources |
|---|---|---|---|
| Business needs alignment | Technological context (relative advantage) | Whether facial access control is better than cards, PINs or mobile credentials for the identified problem | (Guleria et al., 2024; Lee et al., 2020; Lim et al., 2025) |
| Technical readiness | Technological context (compatibility, complexity, infrastructure) | Cameras, lighting, processing location, integration, site testing | (Ali et al., 2025; Grother et al., 2019; Lee et al., 2020; Zhang et al., 2007) |
| Organisational readiness | Organisational context (support, skills, resources) | Management commitment, IT and security skills, budget, training | (Badghish & Soomro, 2024; Hughes et al., 2026; Weiner, 2009; Yang et al., 2024) |

| Framework Dimension | TOE context/extension | Illustrative focus | Key sources |
|---|---|---|---|
| Security and privacy governance | Environmental context (regulation, standards), extended | Lawful purpose, data minimisation, retention, presentation-attack testing, accountability | (Government of Malaysia, 2024; ISO/IEC, 2023; Tabassi, 2023; Temoshok, Proud-Madruga, et al., 2025) |
| Employee acceptance | Human extension to the organisational context | Trust, transparency, perceived fairness, surveillance concerns | (Carpenter et al., 2018; Ciftci et al., 2024; Downie et al., 2025; Fu & Lyu, 2025; Khan et al., 2023) |
| Business value | Outcome of technology and organisation together | Security, operational and economic value against total cost | (Downie et al., 2025; Lim et al., 2025; Shiau et al., 2024) |

**Research Gap**

Existing literature falls into two streams. The first examines the technical development and evaluation of face detection and recognition, including algorithm performance, feature extraction, image quality, detection accuracy, efficiency and robustness (Ali et al., 2025; Hasan et al., 2021; Hjelmås & Low, 2001; Kortli et al., 2018; Li et al., 2020; Obaida et al., 2022; Taunk et al., 2020; Viola & Jones, 2001; Zhang et al., 2007). The second examines technology adoption and its organisational consequences through readiness, management support, acceptance, privacy, trust, organisational justice, governance and business performance (Badghish & Soomro, 2024; Ciftci et al., 2024; Downie et al., 2025; Fu & Lyu, 2025; Guleria et al., 2024; Hughes et al., 2026; Lim et al., 2025; Shiau et al., 2024; Yang et al., 2024).

Little work connects the two. Technical studies, including the earlier hybrid Viola-Jones and MB-LBP study (Ali et al., 2025), ask whether a method can detect rotated faces effectively and contribute mainly to computer vision research. Adoption studies ask what influences willingness to adopt a technology, usually without reference to a specific detection capability. Businesses, however, need a structured way to decide whether and how an established detection capability can be introduced into access control.

The present paper addresses this gap by proposing a conceptual implementation framework for hybrid face detection in business access control. It takes the earlier algorithm as an existing capability, does not reproduce its experimental results, and asks a different question: what is required for responsible organisational implementation. In doing so it moves the contribution from computer vision towards technology management, organisational readiness, biometric governance and business access control.

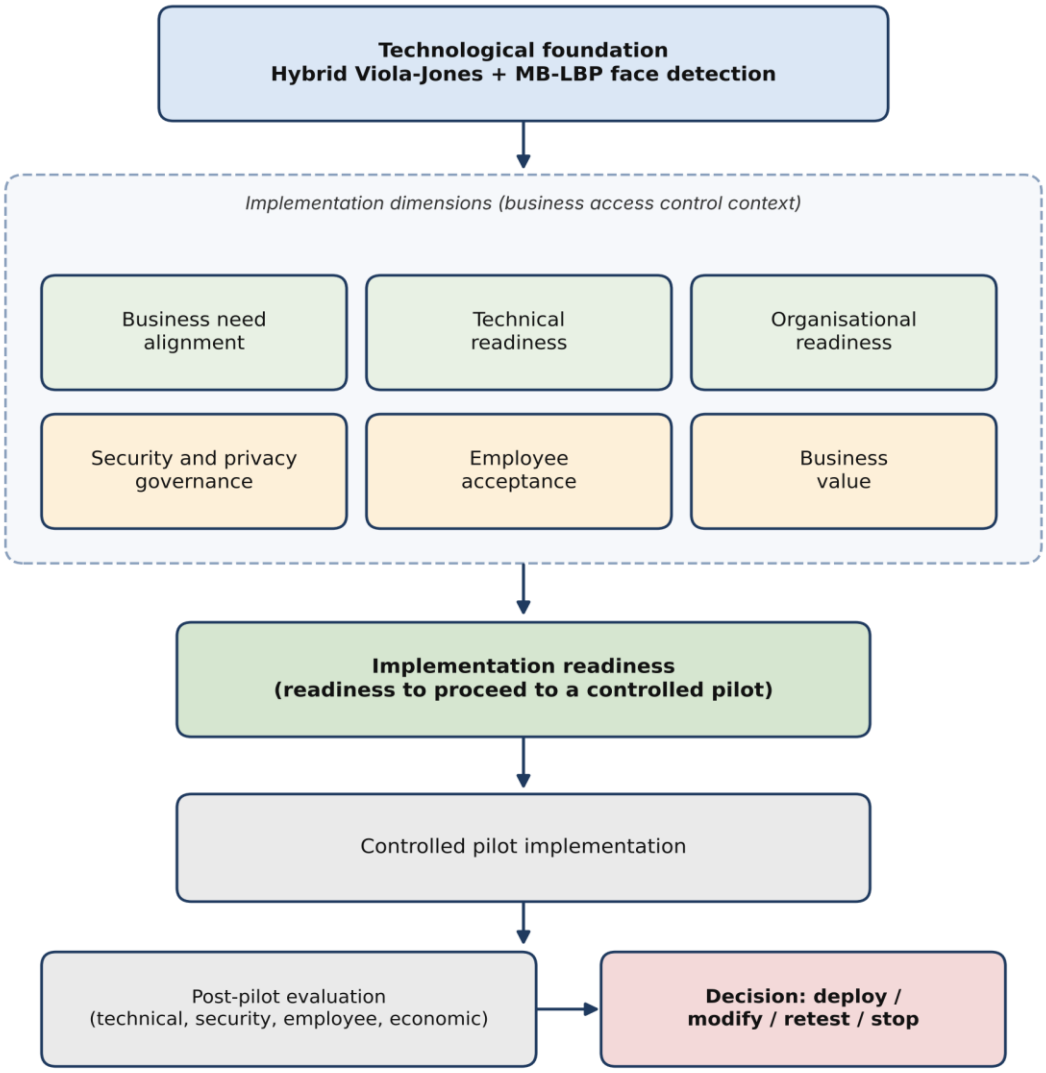
## 3. Proposed Conceptual Framework

***Overview of the Framework***

The framework starts from the technical capability established in earlier work, namely hybrid Viola-Jones and MB-LBP detection of faces at multiple rotation angles (Ali et al., 2025). Implementation requires further assessment along six dimensions. Business needs alignment asks whether the technology solves a real organisational problem. Technical readiness asks whether the technical and physical environment can support it. Organisational readiness examines the financial, managerial, technological and human resources available. Security and privacy governance asks whether biometric data can be handled and protected responsibly. Employee acceptance examines the attitudes, trust and concerns of the people affected. Business value asks whether the expected benefits outweigh the cost, risk and organisational burden.

Together these six dimensions shape implementation readiness, defined as the organisation's preparedness to move from conceptual evaluation to a controlled pilot. The pilot produces technical, organisational, user, security and economic evidence on which a later decision to deploy, modify, retest or stop is based. Figure 1 presents the framework.

**Figure 1: Conceptual Framework Diagram**




***Business Need Alignment***

Business needs alignment concerns how well facial access control addresses a specific organisational problem, such as securing entry to a building, restricting access to sensitive areas, preventing card sharing, simplifying attendance procedures or reducing repeated manual identity checks. Implementation should start from the problem, not from the technology. Studies of facial technology adoption stress perceived benefit and need as influences on acceptance and use (Downie et al., 2025; Lim et al., 2025), and standalone facial access systems have been justified by specific weaknesses of cards and PINs (Lee et al., 2020).

The organisation should compare facial technology with alternatives such as cards, fingerprints, mobile credentials, QR codes or manual checks (Guleria et al., 2024). If an existing method gives adequate security at lower cost and with fewer privacy concerns, adopting facial technology is not justified. Where secure facilities need stronger identity assurance, it may be. Business need alignment is therefore the first decision gate in the framework.

***Technical Readiness***

Technical readiness is the extent to which the physical and information-technology environment supports facial access control. Image quality depends on camera resolution, angle, placement, frame rate and capture distance. Lighting, shadows, movement, face direction, occlusion and background complexity affect detection (Lazarini et al., 2022; Lee et al., 2020). The organisation must also decide where processing takes place, whether on the device, at the edge or on internal servers, and whether processing power, memory, network capacity and availability can support that choice.

Integration is equally important. The detector must interface with recognition software, identity databases, employee records, authorisation rules, door hardware and security logs. Laboratory results such as those reported by Ali et al. (2025) evidence technical capability, but they cannot be assumed to transfer to every site, and demographic and environmental variation in performance has been documented for face recognition systems (Grother et al., 2019). Technical readiness therefore implies site testing, not reliance on published results alone.

***Organisational Readiness***

Organisational readiness is the enterprise's capability to implement, operate and sustain the technology. Readiness has been described as members' shared commitment to change and shared belief in their collective capability to carry it out (Weiner, 2009), and studies of AI adoption identify management support, skills and resources as consistent contributors (Badghish & Soomro, 2024; Hughes et al., 2026; Yang et al., 2024). Management support matters because implementation may require policy change, cross-department cooperation, new security procedures and employee communication.

Information technology capability is also required, covering installation, software administration, database maintenance, cybersecurity, performance monitoring, failure handling and updating of access rights. Human resource capability matters because IT staff, security officers, HR personnel, facility managers and administrators each have a role and need training. The organisation must also be able to meet the full cost of cameras, servers or edge devices, integration, security, networking, maintenance, training, upgrades and governance.

***Security and Privacy Governance***

Security and privacy governance refers to the policies and controls used to protect facial and identity data. Organisations should define the purpose of collecting biometric data, limit collection to what is necessary, restrict access to authorised personnel, apply cybersecurity controls, and set retention and deletion rules (Government of Malaysia, 2024; Temoshok, Proud-Madruga, et al., 2025). Responsibility should be assigned for system administration, privacy compliance, incident handling, employee queries and access authorisation. Testing against presentation attacks and a risk-management approach covering the system life cycle further strengthen governance (ISO/IEC, 2023; Tabassi, 2023).

In Malaysia, biometric data is treated as sensitive personal data under the Personal Data Protection framework (Government of Malaysia, 2024), so privacy and security requirements should be satisfied before a pilot begins. Employees' privacy concerns about biometric systems are themselves a reason for visible governance (Carpenter et al., 2018).

***Employee Acceptance***

Employee acceptance is the willingness of employees to use the system and their views on its necessity, legitimacy, usefulness, security and privacy. Workers may fear surveillance beyond access control, and may worry about where data is kept, who sees it, how long it is retained and what happens after a breach (Carpenter et al., 2018; Khan et al., 2023). Perceived fairness and organisational justice have been shown to shape reactions to facial recognition in organisational settings (Downie et al., 2025; Fu & Lyu, 2025), and privacy attitudes can shift with the context of use (Ciftci et al., 2024).

Employees may also worry about errors. If the system repeatedly fails to recognise legitimate users, it will be experienced as inconvenient and may be rejected. Communication is therefore part of implementation: the organisation should explain why it is introducing facial access control, what data is collected, how it is used and

protected, who can access it and what happens when authentication fails. Feedback gathered during a pilot can reveal usability, trust, fairness and privacy concerns before wider rollout.

***Business Value***

Business value assesses whether the benefits of facial access control justify its cost. Security value includes better identity verification, less unauthorised entry, tighter control of restricted areas and the removal of transferable credentials. Operational value includes less manual identification, faster entry, more efficient attendance processing and better records. Economic value requires comparing these benefits with total cost, including acquisition, infrastructure, integration, cybersecurity, maintenance, training, governance and replacement (Lim et al., 2025; Shiau et al., 2024).

Business value is not only a matter of cost saving. A high-cost system can be justified when the assets protected are valuable enough, and an advanced system can be unjustified when it offers few advantages over existing access procedures. Studies of facial technology adoption likewise treat perceived benefits and risks together rather than separately (Downie et al., 2025; Lim et al., 2025; Shiau et al., 2024).

***Implementation Readiness***

Implementation readiness is the framework's integrating outcome. It refers to the organisation's preparedness to move from concept-level assessment to pilot implementation, in line with the view that readiness concerns capability and commitment rather than certainty (Weiner, 2009). It does not mean that all risk has been removed. It means that the organisation has recognised an appropriate business need, judged the technical feasibility, secured the necessary resources, put security and privacy arrangements in place and considered employees' views. The concept separates technical capability from operational deployment: the existence of a functioning detector does not imply that an organisation is ready to deploy it.

***Conceptual Propositions***

Seven propositions are derived from the framework for future empirical testing.

The first concerns business need. When facial access control addresses a clearly identified security or operational requirement, organisations are more likely to allocate resources and obtain management support.

**P1:** Greater business need alignment is positively associated with implementation readiness.

The second concerns technical readiness. Suitable infrastructure, environmental conditions, processing capacity and integration capability should lower technical uncertainty and raise confidence in a pilot.

**P2:** Greater technical readiness is positively associated with implementation readiness.

The third concerns organisational readiness. Management support, technical capability, financial resources, trained personnel and operating procedures should leave an organisation better prepared.

**P3:** Greater organisational readiness is positively associated with implementation readiness.

The fourth concerns governance. Strong security and privacy governance should reduce uncertainty about biometric data handling and increase confidence that implementation can be conducted responsibly.

**P4:** Stronger security and privacy governance is positively associated with implementation readiness.

The fifth links governance to acceptance. Employees are expected to be more confident when organisations explain purpose, processing, security controls, retention and accountability transparently.

**P5:** Stronger security and privacy governance is positively associated with employee acceptance.

The sixth concerns acceptance and readiness. An organisation with adequate technical and financial capability may still struggle if employees regard the system as intrusive, unnecessary, unfair or insecure.

**P6:** Greater employee acceptance is positively associated with implementation readiness.

The seventh concerns business value and progression beyond the pilot. Even when a pilot is technically successful, organisation-wide deployment requires evidence that the benefits justify the financial and organisational burden.

**P7:** Greater anticipated business value is positively associated with the decision to progress from a controlled pilot towards broader organisational deployment.

## 4. Methodology

### Research Design

This study adopts a conceptual framework-development approach. It does not conduct another experimental comparison of Viola-Jones and MB-LBP face detection. It uses the existing hybrid method as the technological foundation and integrates it with literature on business access control, organisational technology adoption, biometric implementation, organisational readiness, security, privacy, employee acceptance and business value.

A conceptual approach is appropriate because the research questions concern the conditions an organisation should examine before deployment, not the accuracy a newly developed algorithm achieves. The study therefore extends from technical feasibility to organisational implementation, and its outputs are a framework, an implementation process and testable propositions.

### Framework Development Process

The framework in Section 2.10 was developed in four stages. The first stage identified the technical foundation established in the earlier hybrid Viola-Jones and MB-LBP research, including preprocessing, texture feature representation, face localisation and the place of detection in a wider facial authentication process. The second stage separated technical performance from organisational implementation. Factors not normally part of computer vision evaluation, such as management support, infrastructure readiness, system integration, privacy governance, employee acceptance and economic justification, were treated as candidate implementation requirements.

The third stage integrated these factors with the literature reviewed in Section 2. The sources comprised peer-reviewed studies of face detection and recognition, studies of technology adoption using the TOE perspective, studies of biometric privacy and employee acceptance, and standards and legislation relevant to biometric data. The resulting considerations were organised into six dimensions. The fourth stage specified relationships between these dimensions and implementation readiness and linked implementation readiness to controlled pilot deployment and post-pilot evaluation rather than to immediate full deployment.

### Scope of the Framework

The framework concerns employee physical access management in corporate settings. The hybrid Viola-Jones and MB-LBP method supplies only the face-detection component of a larger biometric identification architecture.

A complete access-control system needs further components. Once a face has been found, a recognition or identity-matching module is needed to identify the employee. The identity must be linked to an employee repository holding access rights, and an authorisation engine must decide whether the person may enter the requested location. Door-control hardware, system management, security and audit recording, incident handling, privacy controls and fallback procedures for failed authentication are also required. The framework therefore does not claim that Viola-Jones and MB-LBP alone provide a complete access-control solution.

### Proposed Technology Implementation Process

The framework is operationalised as a five-stage process that moves from assessment to a deployment decision. Each stage produces evidence for the next, and the process can stop at any stage.

### Business Assessment

The process begins with a business assessment. The organisation identifies the specific security or operational problem the technology is expected to address, where it would be deployed, which employees would be affected, which access-control mechanism is currently used and what improvement is expected. Alternative technologies should be considered at this stage, because the purpose is not to justify facial technology automatically but to test whether it is a suitable response to the problem (Guleria et al., 2024). The output is a documented business case covering the problem, intended use, potential advantages, major risks and alternatives.

**Readiness Assessment**

The second stage assesses technical, organisational, security, privacy and employee readiness. The technical assessment examines camera infrastructure, lighting, computing capacity, the physical environment, networking, software compatibility and integration requirements. The organisational assessment examines budget, management support, technical expertise, security resources, maintenance capability and staff availability (Weiner, 2009).

The security and privacy assessment examines what biometric information would be processed, how it would be protected, how long it would be kept, who may access it and which unit would be accountable (Government of Malaysia, 2024; Temoshok, Proud-Madruga, et al., 2025). Employee considerations should begin in this stage: employees should be told the proposed purpose, and major concerns should be identified before installation. The combined output indicates whether the organisation has sufficient implementation readiness to proceed.

**System Design and Integration**

The third stage integrates the hybrid detector into a complete employee access-control architecture. An employee approaches the camera, an image is captured and preprocessed, MB-LBP processes local facial texture and Viola-Jones identifies the facial region (Ali et al., 2025). The detected region is supplied to a separate recognition or identity-matching system. The identity is compared with an employee database, and an authorisation engine decides whether the employee may enter the requested location.

If authorisation is confirmed, the door device allows entry. If recognition or authorisation fails, access is denied or an alternative verification process starts. Every transaction is recorded in the security and audit systems. The architecture shows that hybrid detection is one component of a wider business system and not the access-control application as a whole.

**Controlled Pilot Implementation**

The fourth stage is a controlled pilot, not immediate organisation-wide implementation. A pilot may involve a single entrance, one restricted room, one department or a limited group of participants. Its purpose is to learn whether the system performs satisfactorily in real operating conditions before large investment is made.

The pilot should collect technical and non-technical information. Technical monitoring covers missed detections, processing time, availability, camera performance and behaviour in difficult conditions. Organisational monitoring covers staff workload, integration problems, security incidents and maintenance. Employee experience should also be documented, including feedback on usability, privacy, trust, waiting time, false rejection and inconvenience, because these issues may not appear in technical indicators (Khan et al., 2023).

**Post-Pilot Evaluation**

After the pilot, the organisation evaluates whether broader deployment is justified. Technical evaluation considers detection performance, processing time, false detections, reliability and availability, and environmental assessment examines lighting, facial position, movement, camera distance and partial obstruction. Security evaluation considers unauthorised access attempts, spoofing or presentation attacks, unauthorised access to biometric records, vulnerabilities and incidents (ISO/IEC, 2023). Employee evaluation examines acceptance, perceived usefulness, privacy concerns, trust, complaints and experience of failed authentication. Operational evaluation examines entry processing time, administrative and security workload, failed access events and integration with existing processes.

Economic evaluation compares implementation and operating costs with the security and operational benefits. The resulting evidence should support one of four decisions: wider deployment, modification followed by further testing, continuation of a limited pilot, or discontinuation.

**Discussion**

**From Technical Performance to Organisational Viability**

The framework argues that technical feasibility and organisational viability are different dimensions of technology implementation. The earlier hybrid study addressed whether the combination improves detection

of rotated faces, which is an image-processing question (Ali et al., 2025). The present study addresses what should be considered before an established technical method is transferred into a business. A technically effective detector can still be unsuitable if infrastructure is inadequate, integration is difficult, privacy risks are poorly managed, employees reject it or costs exceed expected value. Technical capability is therefore a necessary but insufficient condition for deployment.

**Organisational Context and Implementation**

Organisations differ substantially in what implementation requires. A small business with one secure entrance may need little infrastructure, whereas a large organisation with several buildings may need many cameras, centralised identity management, complex access privileges, high availability and integration with several systems. Industry context matters as well: a data centre, laboratory, financial institution, warehouse, university and general office have different security requirements. The business case for facial access control therefore cannot be judged independently of its environment, and the framework avoids assuming one configuration suits all organisations.

**Employee Acceptance as an Implementation Requirement**

Facial technology differs from conventional access technologies because it uses characteristics that belong to the employee. A card can be cancelled and replaced, but a face cannot. This may heighten sensitivity about the collection, storage and use of biometric information, especially if the purpose is unclear or employees suspect that access data could later be used for unrelated monitoring (Carpenter et al., 2018; Downie et al., 2025). Acceptance therefore requires transparency about purpose, data processed, security controls and procedures for errors. Strong communication and credible governance may raise confidence and reduce resistance, although this relationship needs empirical validation.

**Privacy by Design**

The framework supports a privacy-by-design approach in which privacy is considered during business assessment, architecture, database design, operating policy and pilot evaluation, not added after implementation. The organisation first defines the purpose of processing, then determines the minimum data required, designs security controls, restricts access, and sets retention and deletion rules (Government of Malaysia, 2024; Tabassi, 2023). This sequence of purpose definition, data requirement, data minimisation, protection, access control, retention and deletion is particularly relevant to biometric information because unauthorised disclosure creates risks different from those of conventional credentials.

**Security Considerations**

Business access control should not be evaluated by detection accuracy alone. A complete security evaluation should eventually include false acceptance, false rejection, attempts to deceive the system, unauthorised access to biometric information, authentication fallback, logging, system failure and identity management (ISO/IEC, 2023; Temoshok, Fenton, et al., 2025). High-security environments may combine facial verification with another factor instead of relying on it alone, and the appropriate architecture depends on the organisation's risk and business requirements.

**Business Value and Technology Selection**

The framework does not assume that facial technology should replace existing systems. For some organisations, cards, mobile credentials or fingerprints may give sufficient security at lower cost and with fewer privacy implications. In others, stronger identity verification may justify the added complexity of facial authentication. The decision should begin with the business problem and end with an assessment of business value, which prevents adoption from being driven by technological novelty.

**Moving from Pilot to Wider Deployment**

A pilot is an important intermediate stage between conceptual readiness and organisation-wide deployment. It tests actual operating conditions instead of relying on laboratory evidence or theoretical assumptions, and it shows whether the technology has unexpected organisational consequences. A technically successful pilot should not automatically lead to wider deployment. The final decision should weigh technical performance, employee acceptance, privacy and security outcomes, operating requirements, financial impact and business value.

## 5. Theoretical Contribution

The first contribution extends hybrid face detection research from algorithmic capability to technology implementation. Earlier technical research establishes the method's ability to perform a computational task, while the present framework considers how that capability could progress towards organisational application. The second contribution introduces implementation readiness as the outcome that connects technical capability with controlled pilot deployment, which avoids treating adoption as a binary choice between acceptance and rejection. It also responds to the observation that TOE factors are inconsistently categorised and measured (Thomas & Yao, 2023) by defining each dimension and its place in the process explicitly.

The third contribution integrates six implementation dimensions into one framework. Business need alignment, technical readiness, organisational readiness, security and privacy governance, employee acceptance and business value are frequently studied separately. The fourth contribution is the framework's staged character: deployment is conceptualised as a process that runs from business assessment through readiness assessment, integration, pilot and post-pilot evaluation to a final decision.

### Practical and Managerial Implications

The framework has several implications for managers considering facial access control. Management should first determine whether an identifiable organisational problem requires stronger identity verification; the availability of facial technology is not itself sufficient justification for investment. Managers should then assess whether infrastructure, technical resources and the operating environment can support the system. Camera placement, lighting, integration, processing capability, door hardware and databases must work together. Cross-functional involvement is likely to be needed: information technology may manage infrastructure, security teams may define access requirements, human resources may coordinate employee communication, legal or compliance functions may address data-protection duties and finance may evaluate costs and benefits.

A pilot is a managerial risk-control mechanism. Rather than committing to organisation-wide deployment, management can test the system in a limited setting and collect evidence before a larger investment. Finally, evaluation should concentrate on organisational value rather than technical success, because a system may reach high detection accuracy and still add little over existing access technologies.

### Limitations and Future Research

The framework has limitations. It is conceptual and has not been validated in a real organisation. No new face-detection experiment was conducted, since the hybrid method rests on previous technical research, and the discussion of how hybrid detection affects access control is therefore reasoned from the literature rather than measured. Employee acceptance and business value may differ across organisations and industries. The framework also concentrates on employee physical access and on the detection stage of a complete biometric system.

Future research should validate the framework through expert review, organisational case studies and workplace pilot testing. Technical testing may examine lighting, camera distance, facial orientation, movement and partial obstruction. Employee acceptance can be assessed through surveys or interviews, and business value by comparing security and operational benefits with implementation cost. The proposed relationships may also be tested quantitatively, for example with structural equation modelling. Collaboration with industry partners operating real access-control installations would allow pilots to be run in realistic conditions.

### Conclusion

This paper proposed a conceptual framework for applying hybrid Viola-Jones and Multi-Block Local Binary Pattern face detection in business access control. Earlier research showed that the hybrid method can detect faces at different rotation angles. This study extends that work by focusing on the organisational factors that should be considered before the technology is used in a real business environment.

The framework rests on six factors: business need alignment, technical readiness, organisational readiness, security and privacy governance, employee acceptance and business value. These factors determine implementation readiness, that is, how prepared an organisation is to run a pilot. The framework shows that

technical performance alone does not guarantee successful business implementation. A detector may work well technically, but the organisation also needs suitable infrastructure, system integration, sufficient resources, proper protection of biometric data, employee support and clear business benefits.

The implementation process starts with identifying the business need and continues through readiness assessment, system integration, pilot implementation and post-pilot evaluation, after which the organisation can decide whether to deploy, improve, retest or discontinue. The framework thus shifts attention from simply having the technology to asking whether the organisation is ready and whether the technology provides real business value. Future research can validate the framework through expert review, case studies, workplace pilots, employee surveys and business value assessment.

**References**

Ahonen, T., Hadid, A., & Pietikäinen, M. (2006). Face description with local binary patterns: Application to face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 28*(12), 2037–2041. https://doi.org/10.1109/TPAMI.2006.244

Ali, W. S. M. M., Basari, A. S. H., Yaacob, W. Z. W., & Doheir, M. (2025). Hybrid of Viola-Jones and multi-block local binary pattern based on machine learning method for multiple-angle rotation face detection. *International Journal of Engineering Trends and Technology, 73*(6), 8–16. https://doi.org/10.14445/22315381/IJETT-V73I6P102

Badghish, S., & Soomro, Y. A. (2024). Artificial intelligence adoption by SMEs to achieve sustainable business performance: Application of technology–organization–environment framework. *Sustainability, 16*(5), Article 1864. https://doi.org/10.3390/su16051864

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2018). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers, 20*(1), 91–110. https://doi.org/10.1007/s10796-016-9667-5

Ciftci, O., Berezina, K., & Soifer, I. (2024). Exploring privacy-personalization paradox: Facial recognition systems at business events. *Computers in Human Behavior, 159*, Article 108335. https://doi.org/10.1016/j.chb.2024.108335

Downie, L. A., Pachidi, S., Huysman, M., & Hafermalz, E. (2025). On the right track? Studying the use of biometric data to manage people in organizations. *Academy of Management Discoveries, 11*(2), 152–179. https://doi.org/10.5465/amd.2023.0037

Fu, H., & Lyu, Y. (2025). Implementing facial recognition technology in a university setting: An organizational justice perspective. *International Journal of Human–Computer Interaction, 41*(15), 9248–9261. https://doi.org/10.1080/10447318.2024.2423352

Government of Malaysia. (2024). *Personal Data Protection (Amendment) Act 2024* (Act A1727). Laws of Malaysia.

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Guleria, A., Krishan, K., Sharma, V., & Kanchan, T. (2024). Global adoption of facial recognition technology with special reference to India—Present status and future recommendations. *Medicine, Science and the Law, 64*(3), 236–244. https://doi.org/10.1177/00258024241227717

Hasan, M. K., Ahsan, M. S., Abdullah-Al-Mamun, Newaz, S. H. S., & Lee, G. M. (2021). Human face detection techniques: A comprehensive review and future research directions. *Electronics, 10*(19), Article 2354. https://doi.org/10.3390/electronics10192354

Hjelmås, E., & Low, B. K. (2001). Face detection: A survey. *Computer Vision and Image Understanding, 83*(3), 236–274. https://doi.org/10.1006/cviu.2001.0921

Hughes, L., Davies, F., Li, K., Gunaratnege, S. M., Malik, T., & Dwivedi, Y. K. (2026). Beyond the hype: Organisational adoption of generative AI through the lens of the TOE framework—A mixed methods perspective. *International Journal of Information Management, 86*, Article 102982. https://doi.org/10.1016/j.ijinfomgt.2025.102982

ISO/IEC. (2023). *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting* (ISO/IEC Standard No. 30107-3:2023). International Organization for Standardization.

Khan, S. S., Ujir, H., Razali, M. Q., & Othman, S. (2023). Facial recognition technology on attendance tracking. *Journal of Computing and Social Informatics, 2*(2), 9–26. https://doi.org/10.33736/jcsi.5541.2023

Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2018). A comparative study of CFs, LBP, HOG, SIFT, SURF, and BRIEF techniques for face recognition. In M. S. Alam (Ed.), *Pattern Recognition and Tracking XXIX* (Proceedings of SPIE Vol. 10649, Article 106490M). SPIE. https://doi.org/10.1117/12.2309454

Lazarini, M. A., Rossi, R., & Hirama, K. (2022). A systematic literature review on the accuracy of face recognition algorithms. *EAI Endorsed Transactions on Internet of Things, 8*(30), Article e5. https://doi.org/10.4108/eetiot.v8i30.2346

Lee, H., Park, S.-H., Yoo, J.-H., Jung, S.-H., & Huh, J.-H. (2020). Face recognition at a distance for a stand-alone access control system. *Sensors, 20*(3), Article 785. https://doi.org/10.3390/s20030785

Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. *IEEE Access, 8*, 139110–139120. https://doi.org/10.1109/ACCESS.2020.3011028

Liao, S., Zhu, X., Lei, Z., Zhang, L., & Li, S. Z. (2007). Learning multi-scale block local binary patterns for face recognition. In S.-W. Lee & S. Z. Li (Eds.), *Advances in biometrics: ICB 2007* (Lecture Notes in Computer Science, Vol. 4642, pp. 828–837). Springer. https://doi.org/10.1007/978-3-540-74549-5_87

Lim, H. T., Vafaei-Zadeh, A., Hanifah, H., & Nikbin, D. (2025). Evaluating the benefits and risks of facial recognition payment systems adoption in Malaysia. *International Journal of Bank Marketing, 43*(2), 292–320. https://doi.org/10.1108/IJBM-05-2024-0300

Obaida, T., Hassan, N. F., & Jamil, A. S. (2022). Comparison of Viola-Jones and YOLO v3 for face detection in real time. *Iraqi Journal of Computer, Communication, Control and System Engineering, 22*(2), 63–72. https://doi.org/10.33103/uot.ijccce.22.2.6

Ojala, T., Pietikäinen, M., & Mäenpää, T. (2002). Multiresolution grayscale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 24*(7), 971–987. https://doi.org/10.1109/TPAMI.2002.1017623

Shiau, W.-L., Liu, C., Cheng, X., & Yu, W.-P. (2024). Employees' behavioral intention to adopt facial recognition payment to service customers: From SQB and value-based adoption perspectives. *Journal of Organizational and End User Computing, 36*(1), 1–32. https://doi.org/10.4018/JOEUC.359894

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

Taunk, P., et al. (2020). Face detection using Viola-Jones with Haar cascade. *TEST Engineering & Management, 80*(6), 19146–19149.

Temoshok, D., Fenton, J. L., Choong, Y.-Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. P. (2025). *Digital identity guidelines: Authentication and authenticator management* (NIST Special Publication 800-63B-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4

Temoshok, D., Proud-Madruga, D., Choong, Y.-Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2025). *Digital identity guidelines* (NIST Special Publication 800-63-4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-4

Thomas, D., & Yao, Y. (2023). Technology-organization-environment meta-review and construct analysis: Insights for future research. In *Proceedings of the 56th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2023.707

Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. In *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2001)* (Vol. 1, pp. I-511–I-518). IEEE. https://doi.org/10.1109/CVPR.2001.990517

Weiner, B. J. (2009). A theory of organizational readiness for change. *Implementation Science, 4*, Article 67. https://doi.org/10.1186/1748-5908-4-67

Yang, J., Blount, Y., & Amrollahi, A. (2024). Artificial intelligence adoption in a professional service industry: A multiple case study. *Technological Forecasting and Social Change, 201*, Article 123251. https://doi.org/10.1016/j.techfore.2024.123251

Zhang, L., Chu, R., Xiang, S., Liao, S., & Li, S. Z. (2007). Face detection based on multi-block LBP representation. In S.-W. Lee & S. Z. Li (Eds.), *Advances in biometrics: ICB 2007* (Lecture Notes in Computer Science, Vol. 4642, pp. 11–18). Springer. https://doi.org/10.1007/978-3-540-74549-5_2