Biometric Checkout

system's phase: use

Section 1 INFORMATION ON THE SYSTEM'S USE AND TEAMS

1.1 **System's Use.**

Purpose. Streamlining and securing the checkout process by using biometric identification.
Capability. Facial, iris, and fingerprint recognition.
Domain. Retail and customer services.
AI User. Supermarket managers and staff.
AI Subject. Customers of the supermarket.

1.2 **System Components.** The system uses a multi-model architecture to process:
(1) high-resolution facial images from a high-resolution infrared camera,
(2) high-resolution iris images from a high-resolution infrared camera,
(3) fingerprint images from an optical fingerprint reader,
(4) payment information from a digital transaction system,
(5) records of purchases from the supermarket's customer transaction database.

For real-time facial image processing (1), the system uses the Deep 3D Face Recognition Network (FR3DNet) model, version 3.0, which is a specialized Convolutional Neural Network (CNN) trained on 3.1 million 3D faces to produce detailed 3D facial recognition maps. Unlike 2D facial recognition models, which can be misled by photographs, FR3DNet accurately captures the geometry of the customer's face, inluding its depth, as well as the contours of the eye sockets, nose bridge, and chin line.
For iris image processing (2), the system uses the High-Resolution Iris Recognition with Infrared Illumination (HR-IRII) model, version 2.2. It improves customer identification by combining a conditional Generative Adversarial Network (cGAN) with support vector machine (SVM) optimization to capture the intricate patterns of the customers' irises, such as the unique fibrous structures, the detailed collarette region, and the distinct crypts and ridges.
For fingerprint image processing (3), the system uses Visual Geometry Group Network (VGGNet) model, version 1.1.1 with batch normalization. It captures unique fingerprint features such as whorls, loops, and arches, and then processes them through a CNN model to create a unique digital representation.
For payment information processing (4), the system uses a Random Forest Classifier (RFC) model, version 5.5. It analyzes transactions made with credit cards, debit cards, and digital wallets to identify unusual patterns in transaction data and flag potential fraudulent activities.
For processing records of purchases (5), the system uses an Autoregressive Integrated Moving Average (ARIMA) model, version 8.1. It tracks past customer purchase patterns and predicts future purchases to enables inventory level optimization.
The system is equipped with an alert mechanism that triggers notifications to both the customer and store personnel whenever any of the models detect an anomaly.

1.3 **System Data.** The system is built on a diverse and inclusive training and testing datasets of personally identifiable information (including biometric information from facial images, iris, and fingerprint images), and payment information, adhering to a 70/30 split. The training dataset of high-resolution facial images consisted of a diverse collection of 118 233 portrait photographs. The majority of them (96%) was sourced from the Flickr-Faces-HQ (70 000 images), CelebA-HQ (30 000 images), and Labeled Faces in the Wild (13 233 images) datasets. This dataset was then expanded with a custom set of 5 000 portraits that incorporated various conditions reflective of the supermarket environment, such as different lighting and obstructions. The training dataset of iris images (32 596) was based on the BATH Iris Database (16 000 images), CASIA-Iris-Lamp (16 212 images) and UPOL Iris Database (384 images). The training dataset of fingerprint scans (30 000 images) was obtained by filtering the NIST Special Database 302. The training dataset for payment information included anonymized transaction records comprising 100,000 instances collected from a leading financial institution's database in Country X. The training dataset for records of purchases consisted of 420 103 357 transaction logs obtained from the Tesco Grocery 1.0 dataset (420 000 000 logs), the Retail Data Analytics (99 457 logs), and the Consumer Behavior and Shopping Habits Dataset (3 900 logs). Both datasets are updated once a year.
The system will process in real-time the five aforementioned data types, all of which contain personally identifiable information. Additionally, facial images, payment information, and records of purchases may potentially be utilized for future purposes beyond biometric identification. Future plans involve combining this information with phone numbers from the customer database to offer personalized personalized discount coupons printed at the moment the customers complete their checkout. Paramount to the system's operation are stringent data protection protocols, which govern access to and use of the personally identifiable information. These include encrypted storage and handling by only authorized supermarket personnel, including managers and trained staff members. These measures are designed to protect individual privacy and ensure the system's compliance with both the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).

1.4 **System Evaluation.**

Evaluation at development stage. The evaluation of models for biometric identification encompassed a variety of scenarios to ensure robustness and accuracy. Benchmarks included diverse customer demographics, varying lighting conditions within the supermarket, customers wearing hats, glasses, and masks, and different levels of congestion at checkout lines. The system's accuracy was tested by comparing its ability to correctly identify individuals against a pre-registered database under these varying conditions. Facial image processing achieved an accuracy rate of 92%, while processing of iris and fingerprint images attained accuracy rates of 89% and 95%, respectively. Additionally, the evaluation measured the system's response time from biometric input to authentication completion, aiming for a seamless and fast checkout experience.
The evaluation of models for processing payment information and purchase records involved a combination of automated testing, manual verification, and real-world transaction simulation to ensure the system's robustness and accuracy. Simulated transactions were conducted under various conditions, including different payment methods, transaction amounts, and error scenarios, to gauge the system's accuracy and security in processing payments. Results indicated an accuracy rate of 94% for payment information, ensuring secure financial transactions. However, the system exhibited a lower accuracy rate of 45% in accurately predicting future purchases, highlighting a potential area for further improvement and optimization.

Evaluation at deployment stage. The system was piloted in 50 supermarkets and evaluated in collaboration with 350 end users, including individuals in various positions such as managers, cashiers, and customer service representatives, gathering vital feedback to refine usability and functionality in line with on-ground operational needs.

Evaluation at use stage. The system is consistently monitored for latency and downtime to maintain stable performance. Its accuracy is continually enhanced through the integration of new data, preserving relevance and precision. Moreover, the system is continually evaluated with feedback from supermarket managers, staff, and customers.

1.5 **Teams.** The system's design involved a diverse team of professionals. AI and machine learning engineers specializing in biometric technologies worked alongside cybersecurity experts to secure sensitive customer data. Retail technology specialists ensured the system's integration into supermarket workflows, enhancing user experience without infringing on privacy. Privacy and ethics consultants, alongside legal advisors, addressed regulatory compliance and ethical concerns, ensuring transparent customer consent mechanisms were in place. Consumer behavior researchers and supermarket staff provided insights into user preferences and operational efficiency.

Section 2 RISKS

The system is high risk due to its use of biometric identification (EU AI Act, Annex III, point 1(a)).

2.1 **Capability Risks.**

Customer data leak. For customers, the storage of personally identifiable data, including biometric information, raises concerns about privacy and security. In the event of a breach, such as unauthorized access or hacking, customers face long-term privacy issues as biometric data cannot be replaced or reset. This jeopardizes their personal information and may lead to identity theft or misuse. Additionally, for stores, a breach in the system could result in financial losses due to legal repercussions, fines, and potential lawsuits. It may also damage the stores' reputation and deter customers from engaging with the business, impacting revenue and growth. Institutions, including regulatory bodies, are also at risk, as a breach would undermine their efforts to enforce data protection laws, such as those outlined in the EU AI Act, leading to a loss of trust and credibility in their ability to safeguard customers' privacy rights. Moreover, improper handling of system's data could negatively imact the environment, contributing to electronic waste and carbon emissions through increased server usage and data storage.

Delays during power and network disruptions. For customers, such disturbances can create inconvenience, potentially affecting their satisfaction and loyalty. For stores, these disruptions result in missed sales opportunities, leading to direct financial losses and the potential for reputational harm.

2.2 **Human Interaction Risks.**

Unauthorized customer behaviour tracking. For customers, such tracking can result in invasive targeted advertising or discrimination based on purchasing habits, undermining individuals' rights to privacy and nondiscrimination. For stores, such tracking may lead to breaches of customer trust, potentially resulting in reputational damage and loss of business. Institutions, particularly regulatory bodies, may face challenges in enforcing privacy laws and protecting consumer rights against such invasive practices, undermining trust in the regulatory framework. From an environmental standpoint, excessive data collection and storage could contribute to digital pollution, exacerbating the carbon footprint of the system.

Customer unfamiliarity. Customers may face unfamiliarity with privacy and data security regarding how their biometric data is stored and utilized, along with technological skepticism and accessibility challenges, particularly among certain groups. Cultural sensitivities and individual resistance to change may further impede acceptance.

2.3 **Systemic Impact Risks.**

Digital exclusion. For customers, the implementation of biometric checkout systems could lead to marginalization among individuals who are less technologically literate or have diverse abilities, as well as those who opt out of biometric identification due to ethical, religious, or privacy concerns. This digital divide may result in unequal access to supermarket services, particularly affecting marginalized communities and exacerbating inequality (Sustainable Development Goal 10), contrary to efforts aimed at ensuring inclusive and equitable service provision for all (Sustainable Development Goal 16). For stores, the digital exclusion resulting from biometric checkout systems can lead to loss of business opportunities as segments of the population are unable or unwilling to engage with the technology. This can hinder revenue generation and customer retention efforts, ultimately impacting the store's profitability and competitiveness. For institutions, digital exclusion poses a risk of widening the gap in access to essential services, undermining efforts to promote social inclusion and economic empowerment. Additionally, it may lead to decreased trust in institutions perceived as prioritizing technological advancement over inclusivity and accessibility. For the environment, the reliance on biometric checkout systems without addressing digital exclusion can exacerbate electronic waste generation. Disenfranchised individuals may resort to outdated, less sustainable methods of transaction, contributing to environmental degradation.

Section 3 MITIGATION STRATEGIES

3.1 **Mitigations of the Capability Risks.**

Customer data leak. The system is undergoing regular updates with the latest security patches to ensure that vulnerabilities in the encryption algorithms are promptly addressed, minimizing the risk of unauthorized access to customer data. Additionally, these updates enhance firewall configurations, fortifying the system's defenses against potential cyberattacks.

Delays during power and network disruptions. By maintaining traditional, non-biometric payment methods and checkout methods, such as cash and manual checkout processes, supermarkets can continue to process transactions and serve customers effectively during instances of power outages or network disruptions. This approach ensures business continuity and customer satisfaction,

3.2 **Mitigations of the Human Interaction Risks.**

Unauthorized customer behaviour tracking. This risk can be mitigated in the future updates of the system by incorporating explicit opt-in consent mechanisms for using records of purchases.

Customer unfamiliarity. To mitigate this risk, supermarkets should provide assistance by deploying trained staff members who can guide unfamiliar customers through the biometric system's use.

3.3 **Mitigations of the Systemic Impact Risks.**

Digital exclusion. This risk can be mitigated in the future updates of the system by incorporating assistive technologies in the system, including voice-activated commands and adaptive interfaces. Voice-activated commands can help visually impaired customers navigate the interface of the self-checkout machines, while adaptive interfaces can adjust to the needs of those with motor impairments, ensuring that all customers have equal access to the shopping experience.

Section 4 BENEFITS

Reduction in checkout times. By implementing biometric technology for the checkout process, the system significantly reduces transaction times, offering customers a more convenient and streamlined shopping experience. For stores, this translates to increased customer satisfaction and loyalty. Furthermore, by making cutting-edge technology accessible to all customers, regardless of technological proficiency, stores uphold principles of inclusivity and cultural advancement (Article 27, UN Declaration of Human Rights).

Reduction of identity theft and fraudalent transactions. The use of biometric identification ensures a high level of accuracy in customer identification. This capability significantly reduces the risk of identity theft and fraud, offering a more secure transaction environment for both customers and stores. The reliability of biometric identification supports trust and safety in financial transactions, contributing to a secure digital economy.

Reduction in the need for human labor at checkout points. The adoption of biometric checkout systems can lead to significant improvements in operational efficiency for supermarkets, reducing labor costs associated with traditional checkout processes and minimizing transaction errors.

Optimization of inventory levels. By linking biometric identification with shopping histories and payment methods, the system enables the collection of valuable data on shopping behaviors and preferences. This capability allows retailers to gain insights into consumer trends, enabling personalized shopping experiences and improving inventory management

Reduction in the need for physical payment methods. The transition to digital transactions in checkout processes reduces reliance on physical payment methods such as paper receipts and plastic cards, benefiting different stakeholders. For customers, the shift enhances convenience by streamlining the checkout process, enabling quicker transactions. Stores benefit from reduced operational costs associated with managing physical payment methods, such as printing paper receipts and maintaining card readers. Institutions experience improved efficiency and data management through digital transactions, facilitating better financial tracking and analysis. Moreover, the environment benefits from reduced waste generation.

REPORTING RISKS

Helpline: 0XXX XXX XXX
Reporting portal: report-risk@com
Mail: XX Main Street,
XXX-XXX Contry X

Last update: 29 Feb 2024

REGISTERED OFFICE

Name of the company
XX Main Street,
XXX-XXX Contry Z

CERTIFICATES

GDPR Compliant

PCI DSS Compliant