

Implementação de Sistemas de Segurança e Prevenção de Perdas em Smart-Markets

Carlos E. C. Silva¹, Wagner W. Á. Bombardelli², Mateus L. R. da Silva³, Lucas E. Negrini⁴,
Evandro F. Silva⁵, Kevin V. P. dos Santos⁶, Paola C. Carvalho⁷,
Bruno C. G. Pawlak⁸

¹Curso de Tecnologia em Ciência de Dados – Faculdade Donaduzzi
Toledo – PR – Brasil

Abstract. *The expansion of autonomous markets, or smart-markets, has revolutionized retail by offering 24/7 availability and reducing operational costs. However, the absence of on-site human supervision introduces significant security challenges, specifically theft and vandalism. These issues directly impact the financial viability and scalability of the business model. This paper explores the implementation of technological solutions designed to mitigate these risks. By integrating intelligent monitoring and automated access control, the project aims to reduce losses and enhance the security infrastructure of unmanned retail environments.*

Resumo. *A ascensão dos mercados autônomos (smart-markets) representa uma evolução significativa no varejo, impulsionada pela automação e conveniência. No entanto, a ausência de supervisão humana introduz vulnerabilidades críticas, como furtos e vandalizações, que impactam a viabilidade do modelo de negócio. Este trabalho apresenta a implementação de uma solução tecnológica para mitigar esses riscos. Ao integrar monitoramento inteligente e controle de acesso, o projeto visa reduzir perdas e fortalecer a segurança em ambientes varejistas desassistidos.*

1. Introdução

O modelo de *smart-markets* fundamenta-se na conveniência e na automação extrema, permitindo que o consumidor realize compras de forma autônoma. Apesar do crescimento acelerado deste setor, a vulnerabilidade patrimonial permanece como um dos principais entraves operacionais. A inexistência de barreiras físicas tradicionais e de fiscalização humana em tempo real cria um ambiente propício para delitos que comprometem a rentabilidade das unidades.

Atualmente, o principal desafio para a sustentabilidade desse modelo reside na dificuldade de mitigar atos de vandalismo e furtos. A ausência de monitoramento reativo cria uma percepção de anonimato que favorece condutas ilícitas. Tais ocorrências geram prejuízos financeiros diretos e demandam elevados investimentos em manutenção e reposição de estoque. Neste contexto, este trabalho propõe uma arquitetura tecnológica focada na identificação e dissuasão de condutas ilícitas através de monitoramento inteligente.

2. Descrição da Solução e Integração de Módulos

A solução proposta consiste em um sistema de monitoramento inteligente operando como uma camada de Segurança Patrimonial Ativa. O fluxo de integração real baseia-se em uma arquitetura orientada a eventos para correlacionar a identidade do usuário com suas ações na gôndola.

A comunicação entre os módulos ocorre em três etapas sequenciais:

1. **Autenticação e Inicialização:** O cliente realiza o acesso ao estabelecimento via verificação facial. A validação compara o descritor facial do usuário com a base cadastrada por meio do cálculo de distância euclidiana. Após o reconhecimento, o sistema registra a sessão ativa. No estágio atual, a comunicação com o módulo de processamento local (*edge computer*) ocorre via requisições HTTP (API), consolidando os dados de presença.
2. **Auditoria Visual Redundante:** Enquanto o usuário interage com o inventário, as câmeras registram a ação. O modelo YOLOv8 realiza a inferência em tempo real para identificação e contagem volumétrica dos produtos. O sistema foca na contagem direta dos itens presentes na área de cobertura, enviando periodicamente o quantitativo consolidado para o servidor central.
3. **Conciliação Lógica:** No momento do fechamento da compra, a Inteligência Artificial não realiza sugestões de preenchimento ou inserções automáticas no carrinho do cliente; sua função restringe-se a verificar de forma passiva se os itens faturados no ponto de venda (POS) batem rigorosamente com os produtos detectados visualmente pelas câmeras, gerando alertas de discrepância caso os valores não coincidam.

Para sustentar o rastreamento, o modelo YOLOv8n opera de forma otimizada com 3,2 milhões de parâmetros, permitindo inferências de baixa latência em hardware limitado e garantindo precisão mesmo sob iluminação variável.

3. Ferramentas e Tecnologias Utilizadas

A arquitetura fundamenta-se na integração entre hardware embarcado e um fluxo de processamento otimizado. O núcleo físico utiliza a plataforma Raspberry Pi para computação local, que, em conjunto com módulos de câmera de alta definição, realiza a captura contínua de dados visuais no local da captura (*edge computing*).

O gerenciamento desses dados utiliza a biblioteca OpenCV para a recepção dos fluxos de vídeo e tratamento prévio dos quadros. Na sequência, as informações são transferidas para o motor de processamento baseado em PyTorch e Ultralytics, onde o modelo YOLOv8n realiza a detecção de objetos. O sistema identifica as coordenadas espaciais e a classificação dos itens, cruzando os dados visuais com a identidade do usuário para assegurar a conformidade da transação.

4. Resultados Práticos e Análise de Confiabilidade

O desempenho do modelo foi mensurado através de métricas padrão de visão computacional, conforme consolidado na Tabela 1.

No nosso repositório do GitHub, você pode acompanhar melhor nossos resultados práticos obtidos:
<https://github.com/EngMateus/ZenixSeguranca/blob/master/README.md>

Tabela 1. Métricas de Desempenho do Modelo YOLOv8n

Sensibilidade (Recall)	mAP50	mAP50-95
80%	81%	75%

No contexto da segurança patrimonial ativa, a análise minuciosa dos erros do sistema e o desenho de estratégias de mitigação são vitais para medir a usabilidade prática da solução:

- **Falsos Negativos (Furtos não detectados):** Atrelados ao limite de 80% de Sensibilidade Recall, ocorrem quando o modelo falha em registrar uma retirada devido a oclusões físicas severas. Para mitigar essa falha, o sistema adota uma cobertura de câmeras complementares e redundantes no local, que cobrem os pontos cegos umas das outras. Um veredito de inconformidade só é gerado após uma quantidade significativa de positivos ser fornecida pelo pipeline de visão e, mesmo diante do alerta do sistema, a decisão final de aplicar qualquer penalidade ou auditoria interna é obrigatoriamente tomada por um operador humano.
- **Falsos Positivos (Alarmes falsos):** Representados pela margem de erro do mAP50 (81% de precisão), acontecem quando o modelo confunde produtos com embalagens semelhantes. O impacto desse erro é mitigado diretamente pela regra de negócio adotada: a IA não faz nenhuma sugestão ativa de compra e não interfere no fechamento do carrinho. O sistema apenas verifica se o faturamento confere com o que foi retirado. Caso haja divergência persistente confirmada por múltiplas câmeras, o caso é repassado para a triagem e decisão de um supervisor humano, eliminando atritos ou cobranças indevidas geradas por decisões autônomas do modelo.

O rigor do mAP50-95 em 75% comprova a precisão espacial das caixas delimitadoras, essencial para auxiliar o monitoramento ao separar produtos sobrepostos em prateleiras compactas.

5. Escalabilidade, Lições Aprendidas e Limitações

O desenvolvimento do projeto evidenciou os desafios de implementar visão computacional no *edge computing*. A principal lição reside em equilibrar a eficiência do modelo com a restrição de hardware local.

No que tange à escalabilidade, a arquitetura descentralizada mostra-se altamente viável. Como o processamento pesado do YOLOv8n e do OpenCV ocorre localmente em cada nó, a expansão para novas unidades não sobrecarrega um servidor central. O tráfego de rede para a nuvem restringe-se a metadados textuais leves (JSON contendo a identificação do produto e a contagem de itens) e logs de quebra de conformidade (alertas de fraude), reduzindo drasticamente custos com banda e infraestrutura de servidores em nuvem.

Entretanto, o projeto atual possui limitações claras: a validação restringe-se a ambientes controlados e domésticos; o treinamento inicial da rede neural exige hardware robusto fora da borda (GPUs dedicadas); e o volume reduzido de imagens do *dataset* inicial exige o uso intensivo de técnicas de *data augmentation* para blindar o modelo contra variações do ambiente comercial real.

Referências

Jocher, G., Chaurasia, A., and Qiu, J. (2023). **Ultralytics YOLOv8**. Disponível em: <https://github.com/ultralytics/ultralytics>.

OpenCV (2024). **Open Source Computer Vision Library**. Disponível em: <https://opencv.org>.

Paszke, A. et al. (2019). **PyTorch: An Imperative Style, High-Performance Deep Learning Library**. In Advances in Neural Information Processing Systems 32.