UNIVERSIDADE SÃO JUDAS TADEU

– Engenharia de Software –

Sistema Inteligente de Monitoramento Urbano com Inteligência Artificial e IoT para Prevenção de Violência contra Mulheres

Ana Carolina da Silva Guedes

Bruno Alves Tuckmantel Silva

Caio Henrique Martins dos Santos

Enzzon Gusttavo Oliveira Nascimento

Fernando Porto Estevão

Francibelde da Silva Lima

Grazielli Gomes S. Cardoso

Leonardo de Castro Ferreira

Thiago Cordeiro de Oliveira

São Paulo – SP

2025

Sumário

Resumo

Este artigo propõe um sistema inteligente de segurança urbana para prevenir a violência contra mulheres nas ruas. A solução combina visão computacional, redes neurais (YOLOv8 e OpenPose) e IoT para identificar riscos em tempo real.

Câmeras urbanas transmitem imagens via RTSP, que são analisadas pela inteligência artificial. Após análise rápida, em caso de detectar perigo, o sistema aciona luzes, sirenes (via ESP32 e MQTT) e notifica autoridades.

A metodologia envolve a coleta de dados audiovisuais rotulados, desenvolvimento do modelo IA, implementação dos dispositivos IoT e validação no ambiente urbano. Espera-se que o sistema atinja um nível de maturidade e escalabilidade no qual seja acessível e confiável.

Abstract

This article proposes an intelligent urban security system to prevent violence against women in public spaces. The solution integrates computer vision, neural networks (YOLOv8 and OpenPose), and IoT technologies to identify risks in real time. Urban surveillance cameras stream video via RTSP, which is analyzed by the artificial intelligence backend. Upon detecting a potential threat, the system automatically activates deterrent mechanisms such as lights, sirens (via ESP32 and MQTT), and notifies law enforcement. The methodology includes collecting labeled audiovisual data, developing AI models, implementing IoT devices, and validating the system in real urban environments. The goal is to achieve a mature and scalable solution that is both accessible and reliable.

1. Introdução

A violência contra a mulher constitui uma realidade alarmante no Brasil, manifestando-se de diversas formas, especialmente nos espaços públicos urbanos. Nas ruas, mulheres são frequentemente vítimas de assédio verbal, perseguições, tentativas de abuso e agressões físicas, situações que refletem a persistente desigualdade de gênero presente na sociedade.

De acordo com o Fórum Brasileiro de Segurança Pública (2023), aproximadamente 28% das mulheres brasileiras relataram ter sofrido algum tipo de violência no último ano, sendo que uma em cada quatro mulheres com mais de 16 anos afirma ter sido vítima nos últimos doze meses. Esses dados mostram a urgência de soluções para a segurança da mulher.

Nesse contexto, o desenvolvimento de uma tecnologia baseada na integração de câmeras com IA e IOT tem como objetivo identificar comportamentos suspeitos e acionar patrulhas preventivamente, mesmo na ausência de flagrante, uma abordagem que visa suprir a falta de mecanismos inteligentes de prevenção da violência, reduzindo a incidência.

A justificativa para esta proposta baseia-se na sensação de insegurança nas cidades e na necessidade urgente de políticas públicas e ferramentas inovadoras que garantam a segurança e dignidade da mulher no Brasil. O uso de tecnologias emergentes visa tornar as cidades mais seguras e promover justiça e igualdade para as mulheres.

Palavras-chave: IoT, Redes Neurais Convolucionais, Segurança Urbana, Inteligência Artificial, Violência Contra a Mulher.

Keywords:

Urban security; Internet of Things; Convolutional neural networks; Artificial intelligence; Violence prevention against women.

2. Objetivo Geral

Desenvolver um sistema inteligente de vigilância urbana baseado em inteligência artificial e IoT, capaz de detectar comportamentos suspeitos contra mulheres em tempo real e acionar, de forma automática, mecanismos de alerta e comunicação com autoridades locais.

3. Objetivos Específicos

- Realizar uma revisão técnica aprofundada sobre métodos de visão computacional aplicados à segurança urbana;
- Construir uma base de dados anotada com comportamentos suspeitos e normais em vídeos de ambientes urbanos;
- Implementar um modelo de IA baseado em redes neurais convolucionais (CNNs) para análise de vídeo em tempo real;
- Integrar o sistema de IA com dispositivos físicos de IoT utilizando microcontroladores ESP32 e protocolo MQTT;
- Validar o sistema em ambiente urbano controlado, avaliando tempo de resposta, precisão da detecção e eficácia das ações preventivas;
- Avaliar o desempenho do sistema em relação à escalabilidade, robustez e possibilidade de adoção por órgãos públicos de segurança.

4. Metodologia

A metodologia proposta envolve o desenvolvimento de um sistema inteligente de vigilância baseado em visão computacional e redes neurais convolucionais (CNNs). Inicialmente, será realizada a coleta e o tratamento de um banco de dados extenso contendo imagens e vídeos supervisionados, simulando comportamentos suspeitos em ambientes urbanos. Esses dados serão utilizados para treinar e validar os modelos de detecção de posturas corporais e padrões de movimento associados a situações de risco contra mulheres.

Para a operação em tempo real, o sistema integrará microcontroladores ESP32 conectados a câmeras de vigilância, responsáveis por transmitir o fluxo de vídeo via protocolo RTSP. A comunicação entre dispositivos e atuadores ocorrerá pelo protocolo MQTT, permitindo a ativação automática de luzes de alerta e sirenes sonoras em situações detectadas como suspeitas. O backend

de inteligência artificial, hospedado em servidor dedicado, processará as imagens e emitirá comandos de intervenção instantâneos.

Por fim, serão conduzidos testes experimentais em ambientes urbanos controlados para validar a eficácia da solução. As métricas avaliadas incluirão a precisão da detecção, o tempo de resposta do sistema e o impacto das intervenções automatizadas na prevenção de possíveis atos de violência. A metodologia adotada visa garantir a robustez e aplicabilidade do sistema no contexto real de segurança pública em cidades inteligentes.

4.1. Tipo de pesquisa

Este trabalho caracteriza-se como uma pesquisa aplicada e exploratória, com abordagem qualitativa e quantitativa, voltada ao desenvolvimento experimental de um sistema inteligente de vigilância para segurança urbana.

4.2 Etapas da Pesquisa

a) Revisão Bibliográfica e Documental

Relevância: Esta etapa garante a fundamentação teórica do projeto, orientando as decisões técnicas a partir do estado da arte em visão computacional, segurança pública, estudos sobre violência de gênero e infraestrutura urbana inteligente. Também permite identificar lacunas de pesquisa e oportunidades de inovação.

b) Coleta e Preparação de Dados

Serão utilizados datasets audiovisuais públicos e privados, contendo interações urbanas reais. senas serão rotuladas manualmente com comportamentos considerados normais e anômalos (como perseguição, aproximação agressiva etc.).

Relevância: A qualidade e diversidade dos dados são essenciais para o bom desempenho de modelos de aprendizado profundo. A anotação precisa dos vídeos permite que o modelo aprenda a distinguir padrões contextuais de risco com maior acurácia.

c) Desenvolvimento do Modelo de IA

Será implementado um sistema baseado em Redes Neurais Convolucionais (CNNs), com uso de arquiteturas como YOLOv8 (You Only Look Once) para detecção de objetos em tempo real, e OpenPose, para análise de posturas corporais. O sistema será treinado para reconhecer comportamentos suspeitos com base na movimentação e interação entre indivíduos.

Relevância: As CNNs são atualmente o padrão-ouro em visão computacional, sendo capazes de identificar padrões complexos em imagens e vídeos, essencial para a detecção automática de ameaças.

d) Integração com Dispositivos IoT

A plataforma será conectada a dispositivos físicos por meio de módulos ESP32, que controlam luzes de alerta, sirenes sonoras e painéis informativos, integrados via protocolo MQTT. A comunicação entre câmeras e o sistema ocorrerá via RTSP (Real Time Streaming Protocol).

Relevância: Essa integração permite ação imediata e automatizada em tempo real, essencial para prevenir ou interromper atos violentos enquanto ocorrem. A arquitetura IoT facilita a escalabilidade e a instalação em diferentes pontos da cidade.

e) Validação em Ambiente Real

A última etapa prevê a instalação piloto do sistema em um espaço urbano delimitado. Serão monitorados os indicadores de desempenho da IA (acurácia, tempo de resposta, taxa de falsos positivos) e a eficácia das intervenções automáticas (luz, som, acionamento policial).

Relevância: A validação prática garante a aderência do sistema às condições reais da cidade, verificando sua viabilidade técnica, social e ética.

4.3. **Justificativa**

O crescimento das zonas urbanas e a multiplicação das câmeras de segurança oferecem uma oportunidade inédita para o desenvolvimento de sistemas autônomos voltados à prevenção da violência. No entanto, o potencial dessas infraestruturas tem sido subutilizado devido à limitação da supervisão humana contínua e à falta de mecanismos inteligentes de interpretação de contexto.

A violência contra a mulher, em especial em espaços públicos com baixa movimentação, configura uma realidade complexa, difícil de ser combatida apenas com medidas tradicionais de policiamento. A utilização de algoritmos de visão computacional e redes neurais convolucionais (CNNs) pode suprir a necessidade de vigilância em larga escala, com monitoramento permanente e detecção de comportamentos anômalos em tempo real.

Além disso, a integração com uma rede de dispositivos IoT permite ao sistema tomar decisões autônomas, como acionar luzes, alarmes e enviar notificações à polícia, ampliando a eficácia e o tempo de resposta frente a situações de risco. Portanto, este projeto não apenas propõe uma inovação tecnológica, mas também contribui com soluções aplicáveis à segurança pública urbana, com forte impacto social, replicabilidade e baixo custo relativo.

4.4 Problema de pesquisas e hipóteses

4.4.1 Problema de pesquisa

É possível desenvolver um sistema baseado em inteligência artificial e IoT, capaz de detectar em tempo real comportamentos suspeitos contra mulheres em áreas urbanas, e acionar mecanismos de resposta automatizados com acurácia e baixo índice de falsos positivos?

4.4.2 Hipóteses

- H1: É possível treinar um modelo de IA com base em CNNs capaz de identificar, com acurácia superior a 85%, situações de risco iminente contra mulheres, a partir de vídeos de câmeras públicas.
- H2: A integração com dispositivos IoT permite uma resposta automática em tempo real, com latência inferior a 1,5 segundo, garantindo maior dissuasão de possíveis agressores, e mais rápida resposta.
- H3: O sistema é replicável em diferentes contextos urbanos com necessidade mínima de reconfiguração do modelo, desde que respeitada a homogeneidade de iluminação e ângulos de visão.

5. Referencial Teórico

A violência contra a mulher é uma das problemáticas sociais mais urgentes da atualidade. Segundo a pesquisa “Visível e Invisível: a vitimização de mulheres no Brasil”, do Fórum Brasileiro de Segurança Pública (FBSP), mais de 21 milhões de brasileiras com 16 anos ou mais relataram ter sofrido algum tipo de violência nos últimos 12 meses. Esses dados alarmantes revelam a urgência de soluções inovadoras que promovam ambientes urbanos mais seguros para as mulheres.

Destaca-se a importância de um planejamento urbano e social sensível ao gênero aliado à tecnologia propõe-se o uso de Inteligência Artificial aplicada à infraestrutura urbana existente, como câmeras de segurança. Essa tecnologia permite a detecção em tempo real de violência contra a mulher. Além de identificar comportamentos suspeitos, possibilita respostas automáticas ou imediatas. Assim, o sistema contribui para a prevenção e atuação rápida das autoridades competentes.

O Brasil é atualmente o quinto país do mundo com mais redes de câmeras de vigilância das marcas Hikvision e Dahua, ambas reconhecidas por suas soluções de reconhecimento facial e monitoramento inteligente. Essa infraestrutura preexistente pode ser reaproveitada no projeto proposto, denominado SafeCity, para garantir mais segurança às mulheres em espaços públicos. Tal tecnologia reforça a possibilidade do projeto se concretizar.

5.1. Violência Contra a Mulher e Tecnologia

A violência contra a mulher em espaços públicos é uma preocupação nas cidades, especialmente em horários e locais considerados de risco, buscando-se por diversas iniciativas aplicar tecnologia para proteger mulheres e dissuadir agressores.

Estudos como o de Garcia et al. (2020) demonstram que a integração entre tecnologia e políticas públicas pode ser decisiva na proteção de mulheres em ambientes urbanos, precisam ser inseridas em estratégias governamentais estruturadas para gerar impacto real.

5.2. IoT e Segurança Urbana

A Internet das Coisas (IoT) conecta objetos físicos à internet, permitindo a coleta e troca de dados em tempo real. ela viabiliza a automação e o monitoramento inteligente de diversos processos.é usado no controle de tráfego, iluminação pública, segurança e etc.

No contexto da segurança pública, a IoT permite a criação de sistemas de vigilância integrados, com câmeras, sensores de movimento, microfones e atuadores que interagem para detectar situações de risco e responder automaticamente a eventos.

Segundo Al-Fuqaha et al. (2015), o uso de IoT em cidades inteligentes tem se mostrado eficiente na prevenção de crimes e no aumento da sensação de segurança, especialmente quando combinado com inteligência artificial.

5.3. Visão Computacional e IA

A Inteligência Artificial (IA), é usada em sistemas de monitoramento automatizado.Algoritmos de detecção e reconhecimento analisam vídeos em tempo real e identificam comportamentos suspeitos, como perseguições e gestos agressivos.

Modelos como YOLO (You Only Look Once), OpenCV e redes neurais convolucionais (CNNs) são comuns nesse tipo de aplicação. Eles processam os dados de vídeo capturados por câmeras para tomar decisões automatizadas ou alertar operadores humanos.

De acordo com Huang et al. (2017), o uso de IA para análise de vídeo urbano tem potencial para reduzir o tempo de resposta a emergências e coibir atos de violência em áreas públicas.

5.4. Iluminação Inteligente e Respostas Automatizadas

A automação de dispositivos urbanos — como postes de iluminação — é promissora na prevenção de crimes. A proposta é que o ambiente “reaja” a comportamentos suspeitos, aumentando a luz, acionando alarmes ou comunicando as autoridades.

Tecnologias como sensores de presença, câmeras, e alarmes com IA estão sendo criados, testados ou implementados em projetos-piloto em diversas cidades e países ao redor de todo o mundo.

Segundo Lee et al. (2019), essas soluções têm alto potencial de dissuasão e são particularmente eficazes quando direcionadas a grupos vulneráveis, como mulheres e crianças.

6. Proposta de Solução

A proposta é criar o SafeCity, um sistema inteligente de vigilância urbana focado na prevenção da violência contra mulheres em espaços públicos. Assegurando o direito fundamental à liberdade de ir e vir, garantido pelo artigo 5º da Constituição Federal.

Com uso de tecnologias como Inteligência Artificial, Visão Computacional e Internet das Coisas, o projeto busca aumentar a segurança e reduzir a violência de gênero, especialmente em locais e horários com pouca movimentação.

6.1. Estrutura Geral do Sistema

O SafeCity terá câmeras inteligentes conectadas a um servidor de IA, que processará continuamente as imagens para identificar comportamentos de risco.

A análise será em tempo real, com modelos avançados de visão computacional treinados em dados reais e simulados de situações perigosas.

Os algoritmos utilizados serão capazes de reconhecer padrões como:

- Perseguição insistente;
- Aproximações agressivas e não solicitadas;
- Tentativas de toque físico sem consentimento.

6.2 Ações Automatizadas de Resposta

Ao identificar um comportamento suspeito, o sistema adotará medidas automatizadas em tempo real para prevenir a violência e acionar as autoridades.

Entre as ações previstas estão:

- Ativação de luzes de LED de alta intensidade, com o objetivo de inibir o agressor e chamar a atenção de pessoas próximas;
- Emissão de alarmes sonoros localizados, que funcionam como alerta público e dissuasor imediato;
- Notificação automática às autoridades públicas, como Guarda Civil ou Polícia Militar, integrando-se aos sistemas de monitoramento urbano já existentes;
- Envio opcional de alerta ao celular da possível vítima, caso ela esteja cadastrada no aplicativo SafeCity.

6.3 Aplicativo Móvel Integrado

Será desenvolvido um aplicativo complementar ao sistema, que permitirá às usuárias o acesso a funcionalidades como:

- Botão de pânico virtual;
- Compartilhamento de localização com contatos de confiança;
- Recebimento de alertas em tempo real sobre ocorrências próximas;
- Acompanhamento de rotas e histórico de deslocamentos.
- O uso do aplicativo será opcional e terá como base os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a segurança e privacidade das usuárias.

6.4 Painel de Controle e Monitoramento

O SafeCity contará com um painel de controle centralizado, operado por agentes capacitados, permitindo:

- Monitoramento em tempo real das câmeras instaladas;
- Registro de alertas e ocorrências;
- Geração de mapas de calor e estatísticas sobre áreas de maior risco;
- Ajustes nos parâmetros do sistema de IA com base em novas evidências e feedbacks.

6.5 Módulo de Aprendizado Contínuo

O sistema será projetado com um mecanismo de autoaprendizado baseado em feedback supervisionado, que permitirá a atualização constante dos algoritmos utilizados, otimizando cada dia mais a eficácia do sistema.

Através da incorporação de dados revisados por operadores humanos, o sistema se tornará mais eficaz ao longo do tempo, com redução de falsos positivos e adaptação ao contexto sociocultural de cada região.

6.6 Desenvolvimento Inicial: MVP

Como etapa inicial, será desenvolvido um Mínimo Produto Viável (MVP), a ser instalado em uma área urbana piloto com histórico relevante de violência contra mulheres. O MVP contará com:

- Aproximadamente 10 câmeras inteligentes interligadas;
- Infraestrutura de rede e servidor local para processamento de dados;
- Central de monitoramento básica;
- Funcionalidades automatizadas de luzes e alarmes;
- Primeira versão funcional do aplicativo.

Essa fase permitirá a validação técnica, social e operacional do sistema, com coleta de indicadores de desempenho como tempo de resposta, número de alertas registrados, e percepção de segurança das usuárias.

7. Conclusão

Este trabalho consistiu em uma investigação teórica aprofundada sobre o uso de tecnologias emergentes, como visão computacional, inteligência artificial e Internet das Coisas (IoT) aplicadas à segurança urbana com foco na prevenção da violência contra a mulher. A partir de uma revisão técnica e conceitual do estado da arte, foi concebida a proposta do sistema SafeCity, um modelo integrado que visa detectar comportamentos suspeitos em tempo real e acionar mecanismos de resposta automática, como luzes de alerta, alarmes sonoros e notificações às autoridades.

Embora o estudo não tenha incluído a implementação prática ou testes de campo, foram detalhadas todas as etapas técnicas, desde a coleta e rotulagem de dados até a arquitetura do sistema e os protocolos de comunicação envolvidos. A proposta abrange ainda uma abordagem escalável e replicável, alinhada aos princípios de cidades inteligentes e às demandas urgentes de segurança pública voltada ao público feminino.

Como próximos passos, recomenda-se a realização de uma prova de conceito (PoC) ou desenvolvimento de um protótipo funcional em ambiente controlado, seguido por testes em pequena escala em áreas urbanas específicas. Também seria relevante aprofundar os estudos sobre

viabilidade ética, privacidade de dados (LGPD) e parcerias com órgãos públicos para validação social e institucional da proposta. Com isso, espera-se que futuras iniciativas possam transformar essa base teórica em soluções práticas, eficazes e socialmente impactantes.

8. Dicionário Técnico

Redes Neurais Convolucionais (CNNs): Arquiteturas de aprendizado profundo projetadas para reconhecer padrões em imagens e vídeos, amplamente utilizadas em visão computacional.

• RTSP (Real Time Streaming Protocol): Protocolo de controle utilizado para transmissão contínua de dados audiovisuais em tempo real, comum em câmeras IP.

• ESP32: Microcontrolador de baixo custo e alta performance, utilizado em projetos de IoT para controle de sensores, LEDs, e comunicação sem fio.

• MQTT (Message Queuing Telemetry Transport): Protocolo leve de mensagens utilizado para comunicação entre dispositivos IoT de forma rápida e eficiente.

• YOLOv8: Algoritmo de detecção de objetos em tempo real baseado em deep learning, capaz de identificar múltiplos elementos em imagens com alta precisão.

• OpenPose: Biblioteca open-source para análise de postura corporal e esqueleto humano, utilizada em reconhecimento de movimentos.

• IoT (Internet das Coisas): Paradigma tecnológico que conecta dispositivos físicos à internet para troca de dados em tempo real.

• Edge Computing: Estratégia de processamento de dados próximo da origem (ex: na própria câmera), reduzindo latência e tráfego de rede.

9. Referencial Bibliográfico

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Visível e Invisível: a vitimização de mulheres no Brasil – 2025*. Disponível em: https://fontesegura.forumseguranca.org.br/mais-de-21-milhoes-de-brasileiras-sofreram-algum-tipo-de-violencia-nos-ultimos-12-meses-revela-pesquisa-do-forum-brasileiro-de-seguranca-publica. Acesso em: 16 maio 2025.

AGÊNCIA BRASIL. *Pesquisa aponta alta nos números de violência contra mulheres no país. 2025.* Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/direitos-humanos/audio/2025-03/pesquisa-aponta-alta-nos-numeros-de-violencia-contra-mulheres-no-pais. Acesso em: 16 maio 2025.

Fórum Brasileiro de Segurança Pública (FBSP). Visível e invisível: a vitimização de mulheres no Brasil. Disponível em: https://publicacoes.forumseguranca.org.br/items/b04fc1a7-990f-4875-8e8c-f34a377b2b83

Olhar Digital. Brasil é o 5º país do mundo com mais redes de câmeras de vigilância. Disponível em: https://olhardigital.com.br/2021/11/25/seguranca/brasil-cameras-reconhecimento-facial/

AL-FUQAHA, A. et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials.

HUANG, J. et al. (2017). Speed/Accuracy Trade-Offs for Modern Convolutional Object Detectors. IEEE CVPR.

GARCIA, R. et al. (2020). Smart Cities and Gender Violence: Technological Solutions for Safer Urban Spaces. Journal of Urban Safety.

LEE, S. et al. (2019). IoT-Based Smart Lighting Systems for Crime Prevention in Urban Areas. Sensors Journal.

O uso da tecnologia com aplicativos digitais: prevenção à violência doméstica e familiar contra mulheres. Disponível em: *https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/5241*