Apoena Revista Eletrônica

A INTELIGÊNCIA ARTIFICIAL APLICADA NA PREVENÇÃO DE INVASÃO E ATAQUES CIBERNÉTICOS A CFTV

Elisson Novais Moreira de Souza

Fabio Fonseca Barbosa Gomes

Celso Barreto da Silva

Resumo:

Atualmente, a sociedade está buscando se adaptar às necessidades de diversos ramos, incluindo as pessoas com deficiência (PCD). Isso impulsionou o desenvolvimento de tecnologias assistivas no Brasil, resultando em avanços significativos, ampliando as capacidades humanas através de pesquisas e estratégias. Desta maneira, este trabalho tem como proposta o projeto de um aplicativo móvel operado pela câmera do *smartphone*, com o objetivo de ajudar as pessoas com deficiência auditiva a realizar os seus afazeres através deste recurso. Isto é possível com a utilização de uma plataforma remota universal, que funciona com os conceitos da Internet das Coisas (IoT) para conectar objetos eletrônicos de um ambiente.

Palavras-Chave: Automação, controle remoto, acessibilidade

INTRODUÇÃO

Atualmente, o uso generalizado de sistemas de Circuito Fechado de Televisão (CFTV) tem ampliado a segurança de instalações e propriedades em todo o mundo. No entanto, à medida que eles se tornam mais integrados e conectados, aumenta a vulnerabilidade a ataques cibernéticos. A segurança dos sistemas de CFTV é fundamental, pois eles desempenham um papel crítico na proteção de ativos, na prevenção de crimes e na obtenção de evidências para investigações. Nesse contexto, a Inteligência Artificial (IA) emerge como uma solução inovadora e eficaz para a prevenção de invasões e ataques cibernéticos em sistemas de CFTV (SISTEMA IRIS, 2023).

A IA oferece uma abordagem proativa para a segurança cibernética em sistemas de CFTV, permitindo uma análise em tempo real de fluxos de dados de vídeo e tráfego de dados, identificando comportamentos suspeitos e potenciais ameaças. A capacidade da IA de aprender com dados históricos e adaptar-se a novos tipos de ataques a torna uma ferramenta valiosa na detecção precoce de invasões. Além disso, a IA desempenha um papel essencial na automação de

respostas a incidentes, permitindo a mitigação de riscos em tempo real (RUSSELL e NORVIG, 2021).

Para isto acontecer, a segurança dos sistemas de CFTV exige a incorporação de técnicas de IA para aprimorar a detecção de ameaças cibernéticas vito que ela oferece uma abordagem abrangente e adaptável para enfrentar os desafios em constante evolução no cenário de segurança cibernética (DE SOUZA, 2019).

A vista disso, o presente projeto debruça sobre o seguinte questionamento: "Como desenvolver e implementar eficazmente soluções baseadas em IA para a prevenção de invasões e ataques cibernéticos em sistemas de CFTV, garantindo a integridade dos dados de vídeo e a segurança das instalações, em um ambiente de ameaças cibernéticas em constante evolução?"

Este problema de pesquisa aborda a necessidade crítica de proteger sistemas de CFTV contra invasões e ameaças cibernéticas, garantindo que eles continuem a ser uma ferramenta confiável na prevenção de crimes, segurança de propriedades e apoio a investigações, para isso acontecer a IA é fundamental, visto que esta hipótese sugere que a utilização desta tecnologia permitirá uma detecção proativa de ameaças, protegendo eficazmente contra invasões cibernéticas e assegurando a funcionalidade contínua e segura desses sistemas.

O objetivo geral deste projeto é aplicar a IA de maneira eficaz na prevenção de invasões e ataques cibernéticos a sistemas de CFTV. Isso será alcançado por meio do desenvolvimento de soluções de segurança baseadas em IA que permitirão a detecção proativa de ameaças, a proteção dos sistemas de CFTV contra invasões e a garantia da integridade dos dados de vídeo.

Já os objetivos específicos são: (i) compreensão dos conceitos básicos de IA e CFTV, (ii) pesquisar soluções existentes para segurança de dados em CFTV; (iii) esboçar uma solução para o problema da CFTV

3. INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial é uma disciplina da ciência da computação que tem a capacidade de fazer com que as máquinas tenham a capacidade de se comunicar como se fossem um ser humano, executando tarefas mais complexas. Basicamente, as IA são formadas por algoritmos e sistemas que podem “aprender” com dados, reconhecer padrões, tomar decisões e aprimorar

seu desempenho ao longo do tempo. Esta tecnologia subdividida em várias subáreas, incluindo aprendizado de máquina, processamento de linguagem natural, visão computacional e redes neurais artificiais. A capacidade de processar e analisar grandes volumes de dados é uma das principais vantagens da IA tornando-a uma ferramenta poderosa para uma ampla gama de aplicações, incluindo segurança cibernética (RUSSELL e NORVIG, 2021).

Com a evolução constante das ameaças digitais, as soluções tradicionais de segurança tornaram-se inadequadas para lidar com a complexidade e a sofisticação dos ataques cibernéticos. Com isso, a IA passou a ser empregada na segurança cibernética com o objetivo de identificar e responder a ameaças em tempo real.

Os algoritmos de aprendizado de máquina podem analisar o tráfego de rede, identificar comportamentos anômalos e antecipar possíveis ataques. Além isso, a IA pode ser usada para a detecção de malware, autenticação de usuários e fortalecimento de sistemas de segurança (ALPAYDIN, 2020).

3.1 Descrição dos sistemas de CFTV.

Os sistemas de Circuito Fechado de Televisão (CFTV) são sistemas de vigilância eletrônica projetados para capturar, monitorar e gravar imagens de vídeo em ambientes específicos. Eles consistem em câmeras de vídeo, sistemas de gravação, monitores e redes de transmissão. As câmeras de CFTV variam em tipos e características, como câmeras fixas, móveis, com infravermelho para visão noturna, e câmeras IP que podem se conectar à rede, conforme pode ser visualizado através da figura 1.

Figura 1: Tipos de câmeras usadas na CFTV

Fonte: TELECO (2023)

Os sistemas de gravação armazenam as imagens em unidades de disco rígido ou na nuvem. A capacidade de monitorar em tempo real e revisar as gravações posteriormente torna o CFTV uma ferramenta valiosa para a segurança e monitoramento de instalações, propriedades e áreas públicas (SILVA e MARCOLINO, 2018).

Esta tecnologia é muito utilizada na prevenção de crimes, no monitoramento de atividades, na identificação de incidentes e na coleta de evidências. A presença de câmeras de CFTV atua como um elemento dissuasor, desencorajando comportamentos criminosos (BAHIA, 2022). Além disso, esses sistemas fornecem uma visão detalhada de eventos e permitem que as autoridades e proprietários de propriedades ajam de forma rápida e eficaz em resposta a emergências. Com a capacidade de monitorar locais 24 horas por dia, 7 dias por semana, os sistemas de CFTV contribuem para um ambiente mais seguro (FIGUEIREDO *et al*., 2017).

Embora os sistemas de CFTV sejam essenciais para a segurança física, eles não estão isentos de ameaças cibernéticas. A crescente conectividade e a transição para sistemas de CFTV baseados em rede os tornaram suscetíveis a invasões cibernéticas. As ameaças incluem ataques que visam desativar câmeras, acessar *feeds* de vídeo sensíveis, ou controlar as câmeras remotamente.

Invadir um sistema de CFTV pode permitir que invasores monitorem atividades, obtenham informações confidenciais ou comprometam a segurança do local. Portanto, a proteção contra ameaças cibernéticas em sistemas de CFTV é de extrema importância para garantir que esses sistemas continuem sendo uma ferramenta eficaz de segurança (SOUZA e ALVES, 2019).

3.2 Diferentes ameaças cibernéticas que os sistemas de CFTV enfrentam

Os sistemas de CFTV estão sujeitos a diversas ameaças cibernéticas que podem comprometer a sua integridade e eficácia. As ameaças incluem ataques de força bruta, nos quais invasores tentam obter acesso não autorizado às câmeras e sistemas de gravação; ataques de negação de serviço (DoS) que podem sobrecarregar os sistemas e torná-los inoperantes; sequestro de *feeds*

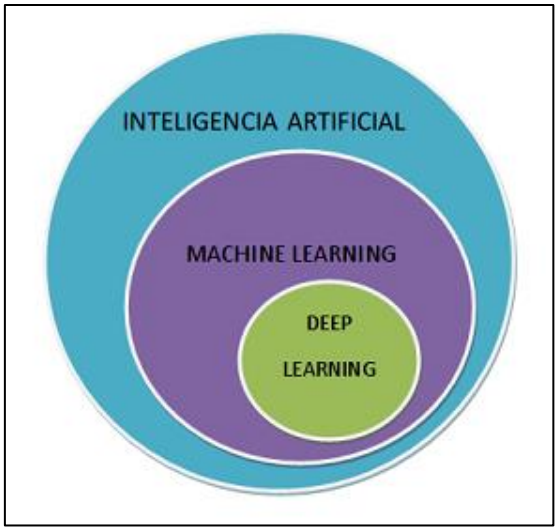
de vídeo, em que invasores interceptam os feeds para obter acesso a informações confidenciais; e ataques de injeção de código malicioso. Compreender essas ameaças é fundamental para proteger os sistemas de CFTV contra possíveis invasões (KREBS, 2016).

Um caso sobre ataques a sistemas de CFTV ocorreu em 2016, quando câmeras de CFTV mal configuradas foram exploradas por *hackers* para realizar ataques de negação de serviço distribuído (DDoS). Outros casos incluem a invasão de câmeras em ambientes empresariais para espionagem e o sequestro de *feeds* de vídeo para chantagem. Esses estudos de casos ressaltam a necessidade crítica de proteger sistemas de CFTV contra ameaças cibernéticas e demonstram as implicações significativas de invasões bem-sucedidas (GADIOT *et al*., 2019; AL-HAIQI *et al*., 2019).

4 COMO A IA PODE SER USADA PARA IDENTIFICAR AMEAÇAS CIBERNÉTICAS.

A IA desempenha um papel fundamental na identificação de ameaças cibernéticas em sistemas de CFTV. Ela pode analisar grandes volumes de dados em tempo real, identificar comportamentos suspeitos e prever possíveis ameaças. Técnicas de IA, como o aprendizado de máquina, permitem a criação de modelos preditivos que reconhecem padrões de tráfego de rede e atividades anômalas, conforme pode ser visualizado na figura 2.

Figura 2: Camadas para a Inteligência Artificial.



Fonte: MITARITONNA (2019)

Na figura 2 é possível perceber que a Inteligência Artificial é composta por *Machine Learning* (Aprendizado de Máquina), que irá buscar os dados para seu "aprendizado" através dos dados obtidos por grandes bases de dados na *Deep Learning* (Apredizado Profundo) (MITARITONNA (2019).

Além disso, a IA pode ser usada para correlacionar eventos aparentemente não relacionados e alertar sobre potenciais ameaças antes que elas se tornem um problema real. A detecção de ameaças cibernéticas em tempo real é essencial para a segurança de sistemas de CFTV, e a IA desempenha um papel crítico nesse processo (DE SOUZA, 2019).

O aprendizado de máquina e as redes neurais são técnicas de IA utilizadas na segurança cibernética, incluindo a proteção de sistemas de CFTV. O aprendizado de máquina permite que os sistemas se adaptem e aprendam com dados históricos, melhorando sua capacidade de identificar ameaças. As redes neurais, por sua vez, são modelos inspirados no funcionamento do cérebro humano, que são particularmente eficazes na detecção de padrões complexos em grandes conjuntos de dados. Além disso, outras técnicas de IA, como algoritmos de classificação e análise de dados em tempo real, são aplicadas para identificar comportamentos suspeitos e ameaças cibernéticas. A combinação dessas técnicas torna possível a prevenção de ataques cibernéticos em sistemas de CFTV (CANNADY, 1998)

A prevenção de ataques cibernéticos em sistemas de CFTV é uma prioridade crítica para garantir a segurança de instalações e propriedades. A IA desempenha um papel essencial nesse processo, pois pode identificar ameaças em tempo real e tomar medidas para mitigar o risco. Técnicas de aprendizado de máquina são usadas para criar modelos de detecção de intrusões que monitoram o tráfego de rede e identificam atividades suspeitas.

Além disso, a IA é empregada na autenticação de usuários e na aplicação de políticas de segurança rigorosas para impedir acessos não autorizados (RUSSEL e NORVIG, 2021). A combinação de técnicas de IA ajuda a fortalecer a segurança dos sistemas de CFTV, garantindo que eles continuem a desempenhar um papel vital na proteção de instalações

4.1 Estratégias de prevenção, como autenticação, autorização e criptografia.

A segurança cibernética em sistemas de CFTV depende de estratégias sólidas de prevenção. A autenticação é um dos pilares fundamentais, garantindo que apenas usuários autorizados tenham acesso aos sistemas.

Isso pode ser alcançado por meio de senhas robustas, autenticação de dois fatores e biometria. Além disso, a autorização define os níveis de acesso de cada usuário, garantindo que apenas pessoal autorizado possa visualizar ou controlar câmeras. Além disso, a criptografia é crucial para proteger a integridade dos dados, garantindo que as transmissões de vídeo e as informações armazenadas sejam inacessíveis a invasores (AXIS, 2023)

A Inteligência Artificial (IA) é usada de forma proativa na detecção de ameaças cibernéticas em sistemas de CFTV Ela é capaz de analisar o tráfego de rede e os padrões de atividade em tempo real. Ela pode identificar comportamentos suspeitos, como tentativas de acesso não autorizado, invasões de câmeras ou atividades anômalas, armazenar e processar dados históricos, adaptando-se a novos tipos de ameaças.

Todas essas ações podem fazer com que a inteligência artificial se torne uma tecnologia preventiva na detecção de ameaças emergentes e tome medidas para mitigar riscos antes que eles se tornem problemas reais (FILHO, 2023).

Os sistemas de detecção de anomalias utilizam algoritmos de IA para criar modelos de comportamento normal com base em dados históricos. Quando atividades anômalas são detectadas, como tentativas de acesso não autorizado ou padrões de tráfego incomuns, os sistemas emitem alertas.

Eles são eficazes na identificação de ameaças cibernéticas que podem passar despercebidas por sistemas de segurança convencionais. A integração desses sistemas em sistemas de CFTV é crucial para uma detecção proativa de ameaças e uma resposta rápida a incidentes (CASTANHEL *et al*, 2020).

Além disso, pode ser necessário o envolvimento de proprietários de sistemas de CFTV reais, desde que haja consentimento e conformidade com as regulamentações de privacidade, além de equipamentos e tecnologia (hardware, software e recursos de rede), dados e amostras (fatos de vídeo de CFTV e tráfego de rede).

5. CONSIDERAÇÕES FINAIS

A segurança dos dados está cada vez em pauta, visto que existem grandes perigos com as informações na rede. O CFTV é uma solução que veio para permitir grande capacidade na segurança da população, porém ela deve ser usada com responsabilidade e segurança. A inteligência artificial chega para ajudar no monitoramento das câmeras, impedindo seu uso de forma irresponsável e indiscriminada por parte de usuários mal-intencionados. Compreende-se que a solução de introdução de uma IA para prevenção de e invasão de ataques cibernéticos a CFTV é possível. Para trabalhos futuros, é necessário realizar um experimento prático com ataques a um sistema de CFTV em laboratório para analisar quais seriam as melhores formas de garantir a segurança do usuário, analisando o seu comportamento.

REFERÊNCIAS:

AL-HAIQI, A. et al. Novel clustering and classification algorithms for online websites to detect real-time XSS attack by using enhanced integration feature selection and feature weighting. Journal of King Saud University-Computer and Information Sciences, 2019.

ALPAYDIN, E. Introdução ao Aprendizado de Máquina. MIT Press, 2020.

AXIS. Vigilância por vídeo da Axis ajuda Kolhapur a se tornar uma cidade mais segura. Disponível em: https://www.axis.com/pt-br/customer-story/video-surveillance-kolhapur-safe-city. Acesso em 20 dez. 2023.

BAHIA. SSP dá Início à Operação de mais 1200 Câmeras Inteligentes. Disponível em http://www.dpt.ba.gov.br/2022/06/482/SSP-da-inicio-a-operacao-de-mais-1200-cameras-inteligentes.html. Acesso em 20 dez. 2023.

CANNADY, J. Redes neurais artificiais para detecção de uso indevido. In: Conferência de Segurança de Sistemas de Informação Nacional, 1998.

CASTANHEL, G. R. et al. Detecção de Anomalias: Estudo de Técnicas de Identificação de Ataques em um Ambiente de Contêiner. In: Workshop de Trabalhos de Iniciação Científica e de Graduação - Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG), 2020.

DE SOUZA, E. A. Aplicabilidade de Algoritmos de Aprendizado de Máquina para Detecção de Intrusão e Análise de Anomalias de Rede. Brasília, DF, 2019.

FIGUEIREDO, E.; SIQUEIRA, A. A. F.; BARBOSA, A. G. Análise de sistemas de CFTV e sua relação com o aumento da segurança em condomínios residenciais. Revista Brasileira de Engenharia de Segurança, v. 7, n. 1, p. 66-80, 2017.

FILHO, M. Sistemas Analíticos de CFTV com Inteligência Artificial, 2023.

GADIOT, G. et al. IoT malware em roteadores domésticos: Ameaças reais e insights práticos. Future Generation Computer Systems, v. 98, p. 176-189, 2019.

HAN, J. et al. A survey on security threats and defensive techniques in cognitive radio networks. IEEE Access, v. 7, p. 64275-64289, 2019.

KREBS, B. A tale of two botnets: dispositivos IoT sob ataque. KrebsOnSecurity, 2016.

MITARITONNA, A. ¿Cuál es la diferencia entre Inteligencia Artificial, Machine Learning y Deep Learning?. Disponível em: https://www.linkedin.com/pulse/cu%C3%A1l-es-la-diferencia-entre-inteligencia-artificial-y-mitaritonna/?originalSubdomain=es. Acesso em 20 dez. 2023.

RUSSELL, S. J.; NORVIG, P. Inteligência Artificial: Uma Abordagem Moderna. Pearson, 2021.

SILVA, R. M.; MARCOLINO, L. S. Avaliação da eficácia de sistemas de monitoramento de vídeo em ambientes de negócios no Brasil. Revista de Gestão da Tecnologia e Sistemas de Informação, v. 15, n. 1, p. 141-160, 2018.

SISTEMA IRIS. IA em Segurança: Como a IA está transformando a segurança. Disponível em: https://www.sistemairis.com.br/ia-em-seguranca-como-a-ia-esta-transformando-a-seguranca/#:~:text=O%20Sistema%20Iris%20oferece%20armazenamento,a%20partir%20dos%20dados%20coletados. Acesso em 20 dez. 2023

SOUZA, J. M.; ALVES, M. A. C. Desenvolvimento de sistemas de CFTV com tecnologias de código aberto para pequenas e médias empresas no Brasil. Revista Brasileira de Segurança Eletrônica, v. 9, n. 2, p. 91-104, 2019.

TELECO. CFTV: Captura de Imagem. Disponível em: https://www.teleco.com.br/tutoriais/tutorialcftv/pagina_2.asp. Acesso em 20 dez.