INSTITUTO DE PESQUISAS TECNOLÓGICAS

COMUNICAÇÃO TÉCNICA

Nº 178936

Aumentando a segurança cibernética em casas inteligentes: uma revisão sistemática das tendências e desafios orientados por AI.

Mauro César dos Santos Leite
Adriano Galindo Leal
Otávio Kiyatabe Nicesio

Palestra apresentada INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT, 20., CONTECSI, São Paulo. 10 slides.

Instituto de Pesquisas Tecnológicas do Estado de São Paulo S/A - IPT
Av. Prof. Almeida Prado, 532 | Cidade Universitária ou
Caixa Postal 0141 | CEP 01064-970
São Paulo | SP | Brasil | CEP 05508-901
Tel 11 3767 4374/4000 | Fax 11 3767-4099

www.ipt.br

AUMENTANDO A SEGURANÇA CIBERNÉTICA EM CASAS INTELIGENTES: UMA REVISÃO SISTEMÁTICA DAS TENDÊNCIAS E DESAFIOS ORIENTADOS POR IA

Mauro César dos Santos Leite

Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Adriano Galindo Leal

Instituto de Pesquisas Tecnológicas do Estado de São Paulo

Otavio Kiyatake Nicesio

Instituto de Pesquisas Tecnológicas do Estado de São Paulo

1 - Introdução

O aumento do uso de dispositivos inteligentes sem qualquer controle dentro do ambiente doméstico representa um risco aos seus habitantes e o uso da inteligência artificial para garantia da segurança deve ser considerado.

A baixa capacidade de processamento dos dispositivos e baixo conhecimento dos moradores em relação às tecnologias no geral são grandes obstáculos para a implantação de soluções de proteção.

Atualmente a automação residencial não se restringe mais a entusiastas e poder contar com ferramentas que aprendem os comportamentos dos moradores e detectam anomalias é um benefício a ser considerado.

2 - Referencial Teórico

Cibersergurança e Inteligência Artificial

IA usa algoritmos para processar imensas quantidades de dados e aprender padrões, classificando-os e podendo realizar previsões, permitindo seu uso na área de cibersegurança:

- Detecção de intrusão;
- Detecção de malware;
- Detecção de phishing.

Cibersegurança no ambiente doméstico

- Danos aos dispositivos
- Interrupção dos serviços
- Vazamento de informações

3 - Metodologia

Utilização do método PICO para elaboração das perguntas de pesquisa

Population	Pesquisa em Segurança Cibernética para Casas Inteligentes.
Intervention	Frameworks ou técnicas para detectar e prevenir ameaças cibernéticas.
Control	Lista de referências obtidas por meio de pesquisa exploratória sobre o tema, servindo de base para a seleção de palavras-chave e fontes, como (Chong, Sandberg, & Teixeira, 2019) e (Heartfield R., Loukas, Bezemskij, & Panaousis, 2021) .
Outcome	Segurança contra ameaças cibernéticas no ambiente doméstico.

3 - Metodologia

As bases de dados elencadas abaixo foram utilizadas para busca dos materiais de pesquisa

Database	Web Address
ACM Digital Library	dl.acm.org/
IEEE Xplore	ieeexplore.ieee.org/xplore/
Scopus Digital Library	www.scopus.com/
ISI Web of Science	www.webofscience.com/

E as strings de busca foram:

framework AND Cybersecurity AND artificial intelligence AND smart home

3 - Metodologia

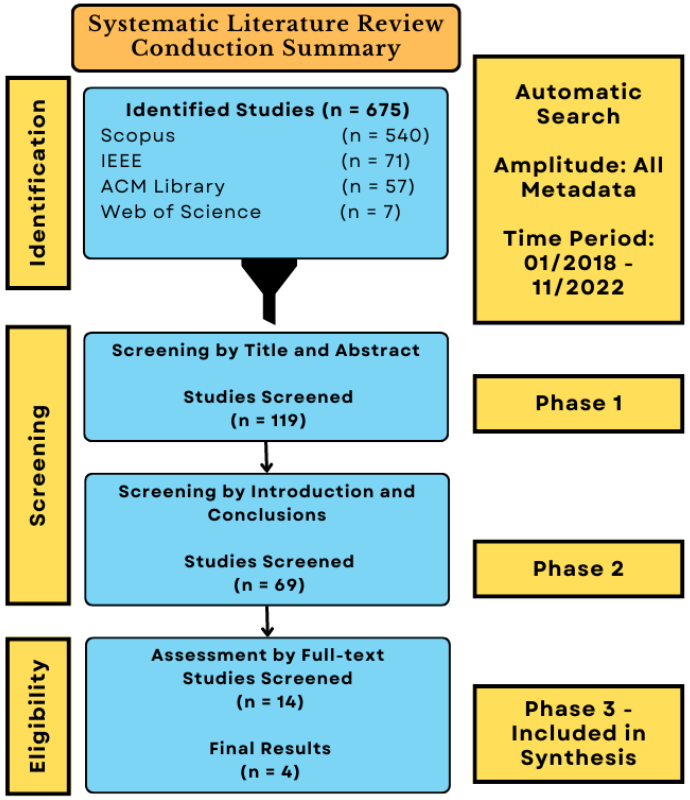
Critério de inclusão:

- I1) Artigos ou materiais de estudo disponíveis em texto completo, com foco de segurança cibernética aplicadas a casas inteligentes.
- I2) Estudos com foco na detecção e prevenção de ameaças em ambientes domésticos inteligentes.

Critério de exclusão:

- E1) Materiais de estudo em outros idiomas além do inglês.
- E2) Precisão do modelo inferior a 90%.
- E3) Materiais não relacionados com a aprendizagem comportamental dos residentes para prevenção de riscos.
- E4) Materiais que não têm aplicabilidade em residências inteligentes.
- E5) Estudos duplicados.

3 - Metodologia



#	Title	Author	Year	Selection Criteria	Status
1	Aegis+: A Context-aware Platform-independent Security Framework for Smart Home Systems (Sikder, Babun, & Uluagac, 2021)	Sikder et al.	2021	I1	Accepted
2	Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning (Heartfield R. , Loukas, Bezemskij, & Panaousis, 2021)	Heartfield et al.	2021	I2	Accepted
3	Jarvis: Moving Towards a Smarter Internet of Things (Mudgerikar & Bertino, 2020)	Mudgerikar and Bertino	2020	I1	Accepted
4	Haunted House: Physical Smart Home Event Verification in the Presence of Compromised Sensors (Birnbach, Eberz, & Martinovic, 2022)	Birnbach et al.	2022	I1	Accepted

4- Resutados

1. Aegis+: A Context-aware Platform-independent Security Framework for Smart Home Systems (Sikder, Babun, & Uluagac, 2021)

Correlaciona os eventos ocorridos com as ações dos habitantes, a partir dos padrões aprendidos, para identificar anomalias. Para isso usa os eventos registrados, analisa-os e usa um modelo de aprendizagem por reforço com funções de recompensa.
Utiliza a cadeia de Markov para realizar o treinamento das matrizes.

2. Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning (Heartfield R. , Loukas, Bezemskij, & Panaousis, 2021)

Dividido em 3 etapas, ele coleta os eventos dos dispositivos, em seguida aplica a aprendizagem por reforço sob diferentes cenários e por último utiliza os metadados para aplicar técnicas de aprendizagem e apresentar soluções para os eventos analisados.

4- Resutados

3. Jarvis: Moving Towards a Smarter Internet of Things (Mudgerikar & Bertino, 2020)

Esse framework usa um modelo de aprendizagem por reforço Deep-Q e é alimentado por dados coletados em um ambiente doméstico e também com dados simulados.

4. Haunted House: Physical Smart Home Event Verification in the Presence of Compromised Sensors (Birnbach, Eberz, & Martinovic, 2022)

Este modelo além de tratar os logs dos dispositivos, também utiliza os dados coletados por sensores espalhados pelo ambiente doméstico para determinar com mais precisão a interferência humana.

5 - Conclusões

- Há muitos desafios a serem superados, o que torna necessário a realização de novas pesquisas nesta área;
- A importância de pesquisar soluções que considerem a interferência humana nos padrões comportamentais;
- Incorporar o comportamento humano nas soluções de segurança desde a concepção dos sistemas.