Segurança Cibernética em Automação Industrial: Um Modelo Baseado em Sistema Especialista para IoTT

Cândida Rosa Paraizo
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
candida.paraizo@aluno.ifsp.edu.br

Abstract

This article discusses expert systems, with a focus on those based on "production rules." Initially, it briefly presents the current landscape of increasingly sophisticated AI-driven cyberattacks and how they can affect Industrial Internet of Things (IIoT) devices. Next, it describes the fundamentals of an expert system and, finally, demonstrates a real-world application through a solution designed to classify vulnerabilities in IIoT devices.

Keywords: expert system, artificial intelligence, cybersecurity, industrial internet of things

Resumo

O presente artigo trata de sistemas especialistas, com enfoque para os do tipo “baseado em regras de produção”. Inicialmente será apresentado, de forma resumida, o cenário atual de ataques cibernéticos sendo sofisticados por inteligência artificial, e como isso pode afetar dispositivos de Internet das Coisas Industriail (IIoT). Em seguida haverá a descrição do que consiste um sistema especialista e, por fim, será mostrado uma aplicação real, através de uma solução que visa classificar vulnerabilidades de dispositivos de IIoT.

Palavras-chaves: sistema especialista, inteligência artificial, cibersegurança, internet das coisas industrial

1. Introdução

O objetivo desse artigo é apresentar um sistema especialista baseado em regras de produção voltado para identificar vulnerabilidades cibernéticas de dispositivos de Internet das Coisas Industrial (IIoT). Primeiramente será introduzido ao leitor a correlação entre Inteligência Artificial e o aumento de casos de crimes cibernéticos. Em seguida será explicado como dispositivos IIoT são vulneráveis e como sistemas especialistas (SE) podem auxiliar na identificação e mitigação de riscos. Após, será explicado como é o funcionamento dos SEs, em aspectos gerais. Por fim, através de um código desenvolvido especificamente para este artigo, haverá a aplicação dos conceitos mencionados para auxiliar no entendimento dos leitores.

2. Inteligência Artificial

O interesse e o uso por ferramentas, tecnologias e dispositivos que utilizam Inteligência Artificial (IA) cresceu nos últimos anos, não só por pessoas, como também por empresas. Segundo a CNN Brasil, em 2024, pelo menos 72% de instituições ao redor do mundo já a adotaram, um aumento de 17% em comparação com o ano anterior. Em relação ao investimento, houve um aumento para 65%, no qual era 33% em 2023. Apesar da boa impressão e dos diversos benefícios que o uso da inteligência artificial traz, há também o outro lado da moeda, como aumento da sofisticação de crimes cibernéticos através de seu uso.

De acordo com a pesquisa “The State of Cybersecurity in LATAM 2024”, 55% das empresas brasileiras sofreram com ataques cibernéticos alimentados por IA em 2023, um percentual 4% maior do que a média da junção dos demais países incluídos na pesquisa (51% para México, Colômbia e Argentina). Isso demonstra os riscos devido ao uso de IA por cibercriminosos e o quanto ainda há vulnerabilidades expostas que podem ser mais facilmente exploradas com os usos de IA.

3. Dispositivos IIoT

Engana-se quem pensa que somente computadores e celulares são alvos disso, os dispositivos classificados como Internet das Coisas são um dos com vulnerabilidades mais expostas. Engana-se quem pensa que os dispositivos por estarem isolados em uma rede, estão livres de ataques. Segundo a Gartner (empresa de pesquisa e consultoria americana especializada em tecnologia da informação e serviços empresariais), na América Latina, em 2024, as ocorrências de ataques cibernéticos e crimes aumentaram em 72%. Algumas das causas são credenciais fracas, falta de criptografia de dados, protocolos inseguros, dentre outros fatores, como elenca o blog do Instituto Brasileiro de Cibersegurança.

Devido a isso há a necessidade da implementação de sistemas e ferramentas que auxiliem na identificação, que seja de fácil implementação e entendimento para quem está entrando nesse mercado. E é nesse momento que surgem os sistemas especialistas.

4. Sistema Especialista

Sistemas especialistas (SE) são programas computacionais que usam tecnologias de inteligência artificial para simular o julgamento e comportamento de um ser humano que tenha experiência e conhecimento em um campo específico (TechTarget 2024), no caso da aplicação desse artigo, será para identificar vulnerabilidades e sugerir correções após análises de alguns aspectos de em dispositivos de Internet das Coisas Industriais.

Os baseados em regras de produção é um tipo de SE, no qual a representação do conhecimento está em conjuntos de regras que diz o que fazer e o que concluir em diferentes situações. Eles são compostos por três elementos:

Base de conhecimento: onde estão armazenadas as informações de domínio ou área de estudo específicos utilizados pelo sistema especialista.

Mecanismo de Inferência: sistema baseado em regras que extrai informações da base de conhecimento e toma decisões com base das informações de entrada.

Interface do Usuário: parte do sistema especialista no qual os usuários finais interagem para obter um retorno para suas perguntas ou problemas.

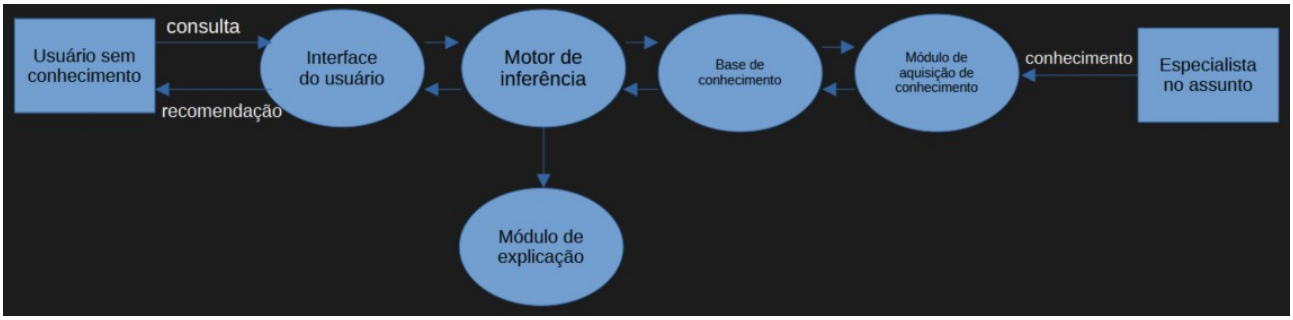

Figura 1: funcionamento de um sistema especialista

O conhecimento começa com um especialista humano (no lado direito do fluxograma) e flui pelo sistema especialista, onde é processado para que um usuário não especialista (lado esquerdo) possa consultar o sistema e receber uma resposta.

Abaixo há figuras de partes do código elaborado para implementação do sistema especialista voltando para identificar vulnerabilidades cibernéticas de dispositivos de Internet das Coisas Industrial (IIoT), com destaque para as três elementos que o compõem.

```python
perguntas = {
    1: {
        'pergunta': "A senha padrão foi trocada?",
        'resposta_vulneravel': "nao"
    },
    2: {
        'pergunta': "O dispositivo está atualizado com os patches de segurança mais recentes?",
        'resposta_vulneravel': "nao"
    },
    3: {
        'pergunta': "Há criptografia nos dados em trânsito e nos dados armazenados?",
        'resposta_vulneravel': "nao"
    },
    4: {
        'pergunta': "Há alguma ferramenta de monitoramento das atividades do seu dispositivo?",
        'resposta_vulneravel': "sim"
    },
    5: {
        'pergunta': "Há credenciais embutidas no código?",
        'resposta_vulneravel': "sim"
    },
    6: {
        'pergunta': "Seu dispositivo está desnecessariamente exposto na internet?",
        'resposta_vulneravel': "sim"
    }
}
```

Figura 2: base de conhecimento

```python
# Classificação de risco com pesos diferentes para cada vulnerabilidade
def classificar_risco(total_vulnerabilidades, total_perguntas):
    percentual = (total_vulnerabilidades / total_perguntas) * 100

    if percentual == 0:
        return "Baixo", "✅ Dispositivo seguro"
    elif percentual <= 30:
        return "Baixo", "ℹ️ Algumas melhorias recomendadas"
    elif percentual <= 60:
        return "Médio", "⚠️ Atenção necessária - risco moderado"
    elif percentual <= 80:
        return "Alto", "🔴 Ação imediata recomendada - risco elevado"
    else:
        return "Crítico", "❌ Risco extremo - medidas urgentes necessárias"
```

Figura 3: mecanismo de inferência

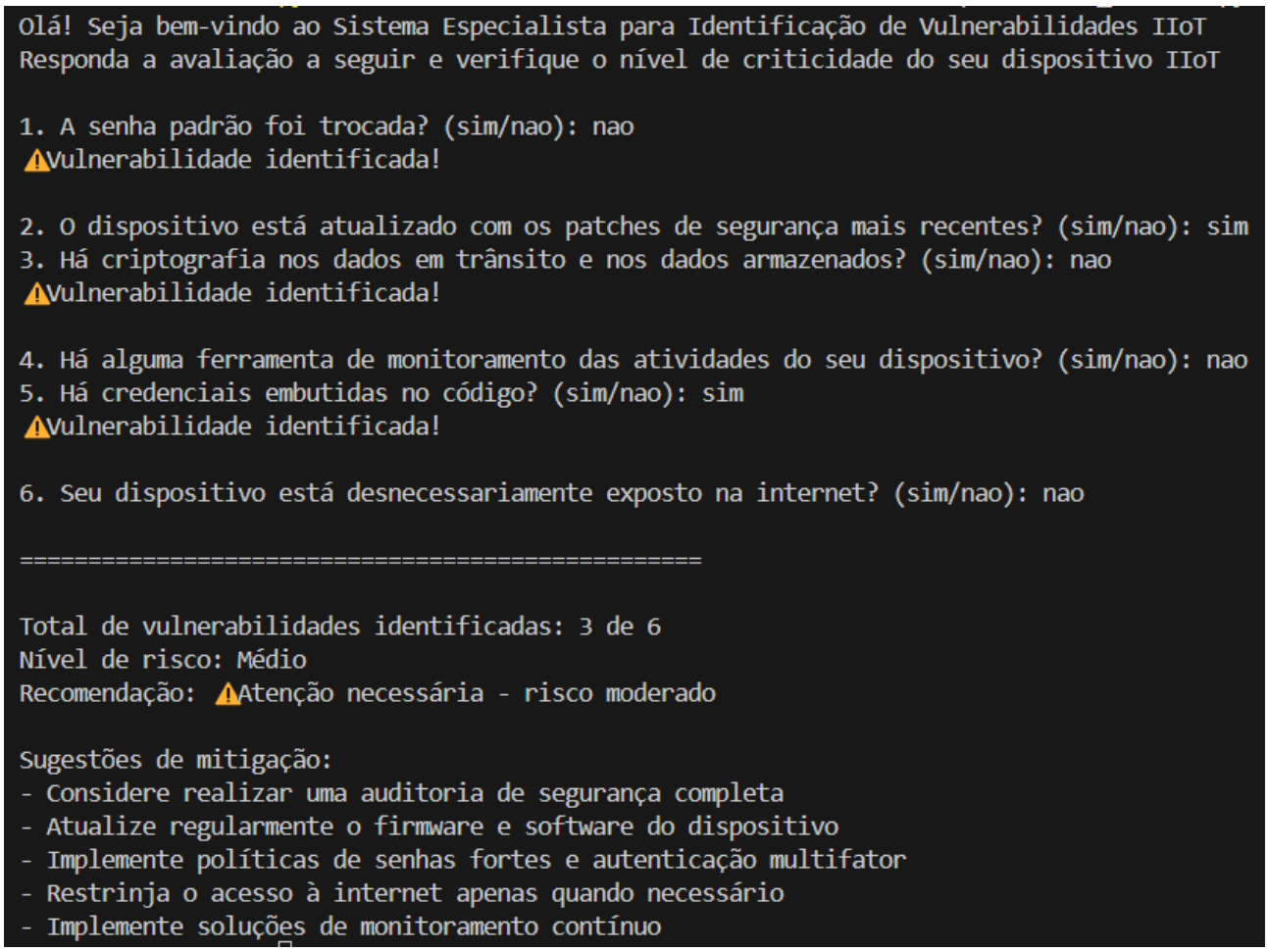

Figura 4: interface do usuário

O código completo pode ser encontrado em:
https://github.com/crparaizo/sistemaEspecialista_IFSP/blob/master/sistemaEspecialista_ARTIGO.py

Explicação do vídeo pode ser encontrada em (clique em “view raw”):
https://github.com/crparaizo/sistemaEspecialista_IFSP/blob/master/explicacaoSE.mkv

5. Conclusão

Os sistemas especialistas baseados em regra de produção representam o conhecimento de um especialista, através de um conjunto de regras, para direcionar no que deve ser feito ou concluído a depender da situação. Devido a isso, oferecem boa orientação para indivíduos que não possuem o domínio do assunto, mas que precisam atuar na identificação ou resolução de algum problema. Eles são compostos por três elementos principais: base de conhecimento, mecanismo de inferência e interface do usuário, mas periodicamente necessitam ser atualizados ou revisados para que o conhecimento armazenado reflita as mudanças da realidade, juntamento com as novas tecnologias que surgirem.

Referências Bibliográficas

CNN BRASIL. Uso de inteligência artificial aumenta e alcança 72% das empresas, diz pesquisa. CNN Brasil, 2025. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/uso-de-inteligencia-artificial-aumenta-e-alcanca-72-das-empresas-diz-pesquisa/. Acesso em: 12 mai 2025.

FORBES BRASIL. IA foi utilizada em mais de 50% dos ataques recentes contra empresas brasileiras. Forbes Brasil, 2024. Disponível em: https://forbes.com.br/forbes-tech/2024/05/ia-foi-utilizada-em-mais-de-50-dos-ataques-recentes-contra-empresas-brasileiras/. Acesso em: 12 mai 2025.

TI INSIDE. Ameaças digitais: como fugir da mira dos hackers? TI Inside, 2025. Disponível em: https://tiinside.com.br/12/03/2025/ameacas-digitais-como-fugir-da-mira-dos-hackers/. Acesso em: 15 mai 2025.

IBSEC. 10 vulnerabilidades críticas em dispositivos IoT. IBSEC, [ano]. Disponível em: https://ibsec.com.br/10-vulnerabilidades-criticas-em-dispositivos-iot/. Acesso em: 17 mai 2025.

IBSEC. 10 práticas para mitigar riscos em IoT e IIoT. IBSEC, [ano]. Disponível em: https://ibsec.com.br/10-praticas-para-mitigar-riscos-em-iot-e-iiot/. Acesso em: 17 mai 2025.

IBSEC. Explorando técnicas avançadas de segurança: do hacking de IoT ao gerenciamento de ameaças. IBSEC, [ano]. Disponível em: https://ibsec.com.br/explorando-tecnicas-avancadas-de-seguranca-do-hacking-de-iot-ao-gerenciamento-de-ameacas/. Acesso em: 22 mai 2025.

CEPEIN. Título do documento. CEPEIN, 2025. Disponível em: https://cepein.femanet.com.br/BDigital/arqPics/1911550412P960.pdf. Acesso em: 23 mai 2025.

GROSAN, Crina; ABRAHAM, Ajith. Rule-Based Expert Systems. In: Intelligent Systems. Berlin, Heidelberg: Springer, 2011. p. 149-185. (Intelligent Systems Reference Library, v. 17). Disponível em: https://doi.org/10.1007/978-3-642-21004-4_7. Acesso em: 30 mai 2025.

TECH TARGET. Expert system. TechTarget, 2024. Disponível em: https://www.techtarget.com/searchenterpriseai/definition/expert-system. Acesso em: 30 mai 2025.