Um Middleware Markoviano Incremental para Detecção de Anomalias em Sistemas de Controle de Acesso Físico

Lucas V. Morais[1], Vinícius P. Gonçalves[1], Fábio Lúcio L. de Mendonça[1]
Rodolfo I. Meneguette[2], Francisco A. Silva[3], Geraldo P. Rocha Filho[4]

[1]Universidade de Brasília (UnB)

[2]Universidade de São Paulo (USP)

[3]Universidade Federal do Piauí (UFPI)

[4]Universidade Estadual do Sudoeste Bahia (UESB)

vasconcelos.lucas@aluno.unb.br, vpgvinicius@unb.br

fabio.mendonca@redes.unb.br, meneguette@icmc.usp.br

faps@ufpi.edu.br, geraldo.rocha@uesb.edu.br

Abstract. *Behavioral anomaly detection in Physical Access Control Systems (PACS) is still predominantly based on static authorization rules, which creates a gap in identifying subtle movement deviations that do not violate explicit permissions but may indicate credential misuse or privilege abuse. To address this problem, this work proposes an unsupervised and incremental middleware for anomaly detection in PACS, designed to operate in real time over large volumes of sequential access logs. The middleware models each user's individual movement through Discrete-Time Markov Chains, in which states represent physical access points and transition probabilities capture legitimate spatial routines. The middleware was evaluated on more than five years of real corporate PACS data (≈13.9 million transitions) and, in a prospective evaluation with 44,329 previously unseen events, labeled approximately 1.75% of the records as anomalous, distinguishing partial from strong anomalies with low computational cost and quantitative support for operational alert prioritization.*

Resumo. *A detecção de anomalias comportamentais em Sistemas de Controle de Acesso Físico (PACS) ainda é predominantemente baseada em regras estáticas de autorização, o que cria uma lacuna na identificação de desvios sutis de deslocamento que não violam permissões explícitas, mas podem indicar uso indevido de credenciais ou privilégios. Para sanar esse problema, este trabalho propõe um middleware não supervisionado e incremental para detecção de anomalias em PACS, capaz de operar em tempo real sobre grandes volumes de registros sequenciais. O middleware modela o deslocamento individual de cada usuário por Cadeias de Markov em Tempo Discreto, nas quais os estados representam pontos de acesso físicos e as probabilidades de transição capturam rotinas espaciais legítimas. O middleware foi avaliado em mais de cinco anos de dados reais de um PACS corporativo (≈13,9 milhões de transições) e, em uma avaliação prospectiva com 44.329 eventos não vistos, rotulou cerca de 1,75% dos registros como anômalos, distinguindo anomalias parciais e fortes,*

com baixo custo computacional e suporte quantitativo à priorização operacional de alertas.

1. Introdução

Sistemas de Controle de Acesso Físico (*Physical Access Control Systems* – PACS) constituem a base da segurança predial moderna, regulando quem pode entrar, sair e se deslocar em instalações protegidas [Skopik et al. 2022]. Embora autentiquem credenciais e imponham permissões de forma eficaz, esses sistemas operam predominantemente sob lógicas estáticas, sem análise comportamental contínua dos padrões de deslocamento. Como resultado, atividades legítimas porém irregulares, como uso indevido de privilégios, compartilhamento de credenciais ou visitas não programadas, podem ocorrer sem violar regras explícitas e permanecer sem detecção [Geepalla and Asharif 2020]. Estudos com dados reais de PACS indicam que registros de acesso contêm informação comportamental suficiente para revelar tais desvios [Skopik et al. 2022].

De forma mais ampla, pesquisas em Sistemas Ciberfísicos (CPS) e IoT mostram que dados sequenciais operacionais permitem identificar desvios sutis em ambientes reais [Saheed and Sanjay 2025, Fernandes et al. 2026]. Esses estudos indicam que mecanismos baseados em regras fixas são frágeis em cenários não estacionários [Feng and Tian 2021], enquanto abordagens adaptativas fundamentadas em modelos probabilísticos [Huang et al. 2023] e em teoria da informação [Molina et al. 2022, Zamanzadeh Darban et al. 2024] são mais adequadas para capturar mudanças comportamentais. Em PACS, o comportamento de acesso manifesta-se naturalmente como sequências de transições entre pontos físicos, nas quais modelos probabilísticos e medidas entrópicas permitem distinguir rotinas usuais de deslocamentos inesperados de forma interpretável.

Salienta-se que o alto volume de eventos gerados por PACS inviabiliza inspeção manual contínua e torna impraticáveis abordagens dependentes de rotulagem prévia ou de reprocessamentos frequentes dos dados. Neste trabalho, anomalias são tratadas como desvios comportamentais sequenciais no deslocamento do usuário, caracterizados por transições raras ou por mudanças estruturais no padrão local de saídas a partir de um ponto de acesso, mesmo quando não há violação explícita de permissões. Nesse contexto, a combinação de modelagem Markoviana individual e medidas baseadas em entropia mostra-se promissora, pois Cadeias de Markov em Tempo Discreto (DTMCs) capturam rotinas espaciais como probabilidades de transição interpretáveis entre pontos físicos, enquanto a variação de entropia quantifica o impacto estrutural de novas observações sobre a distribuição local de transições, complementando a análise baseada exclusivamente em raridade estatística.

Diferentes abordagens têm sido propostas para a detecção de anomalias em PACS, em sua maioria baseadas em regras estáticas [Geepalla and Asharif 2020], perfilamento estatístico agregado [Skopik et al. 2022] ou modelos supervisionados treinados em cenários controlados [de Moura et al. 2024, Saheed and Sanjay 2025], o que limita sua aplicabilidade em ambientes reais. Embora alguns trabalhos explorem logs reais de PACS e evidenciem o potencial da análise comportamental, essas abordagens [Geepalla and Asharif 2020, Skopik et al. 2022] geralmente não modelam a dinâmica sequencial individual de deslocamento nem acompanham a evolução contínua

do comportamento legítimo. Ademais, métodos baseados em modelos complexos ou aprendizado profundo tendem a impor elevado custo computacional, dificultando sua adoção operacional em ambientes corporativos [Bitirgen and Basaran FILIK 2023, Saheed and Sanjay 2025]. Conforme apontado na literatura, mecanismos baseados em limiares fixos ou modelos estáticos são frágeis em cenários não estacionários [Feng and Tian 2021], evidenciando a necessidade de soluções não supervisionadas, incrementais e interpretáveis, lacuna explorada neste trabalho.

Diante desse lacuna, o objetivo deste trabalho é propor e avaliar um middleware não supervisionado e incremental para detecção de anomalias comportamentais em PACS. O middleware é capaz de modelar padrões individuais de deslocamento como Cadeias de Markov em Tempo Discreto e identificar desvios relevantes por meio de dois sinais complementares: (i) a raridade probabilística das transições; e (ii) a variação incremental de entropia associada à reorganização estrutural dos padrões de acesso. O middleware é modelado para operar sobre dados corporativos reais, sem necessidade de rotulação prévia, mantendo baixo custo computacional e aderência a requisitos operacionais de ambientes em produção.

Motivado por essas observações, este trabalho apresenta as seguintes contribuições: (i) a proposição de um middleware interpretável e em tempo real para detecção de anomalias comportamentais em PACS; (ii) a modelagem do deslocamento individual por DTMCs, nas quais estados correspondem a pontos de acesso físicos e as probabilidades de transição representam rotinas espaciais legítimas; e (iii) a incorporação de medidas entrópicas para monitorar variações estruturais nas distribuições de transição.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 apresenta a modelagem do middleware proposto. A Seção 4 apresenta os resultados alcançados para validar o middleware proposto. Por fim, a Seção 5 apresenta as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

A detecção de anomalias é uma área consolidada em domínios como Sistemas de Controle Industrial (ICS) e, de forma mais ampla, CPS, nos quais registros de sensores e séries temporais motivam modelos capazes de capturar dinâmicas não estacionárias e dependências sequenciais. Em contraste, PACS permanecem relativamente menos explorados, apesar de governarem o deslocamento físico em ambientes protegidos e gerarem logs ricos e carimbados no tempo. Na prática, PACS ainda são operados majoritariamente por autenticação e políticas estáticas, com limitada incorporação de análise comportamental contínua baseada em sequências de acesso.

Geepalla e Asharif [Geepalla and Asharif 2020] propuseram uma abordagem baseada em grafos para representar relações entre usuários, pontos de acesso e permissões, viabilizando a identificação de caminhos anômalos. De forma complementar, Skopik et al. [Skopik et al. 2022] apresentaram uma estrutura de detecção comportamental em logs reais de PACS, empregando perfilamento estatístico e agrupamento para identificar padrões como compartilhamento de credenciais e uso indevido de crachás. Embora demonstrem a viabilidade da analítica comportamental em PACS, essas abordagens tendem a operar com análises estatísticas ou representações estruturais que não modelam explicitamente a dinâmica sequencial individual de transições entre locais.

Em CPS/ICS, a literatura enfatiza a necessidade de mecanismos adaptativos para lidar com regimes operacionais em evolução. Feng et al. [Feng and Tian 2021] mostraram que limiares fixos são frágeis sob não estacionariedade e propuseram um arcabouço com identificação de espaço de estados e filtragem Bayesiana. Em linha semelhante, Bitirgen e Filik [Bitirgen and Basaran FILIK 2023] exploraram modelos híbridos CNN–LSTM informados por entropia para monitoramento de redes elétricas, enquanto Saheed e Misra [Saheed and Sanjay 2025] avançaram ao integrar explicabilidade e preservação de privacidade em arquiteturas profundas para CPS. Essas abordagens frequentemente demandam modelos mais custosos, calibração complexa e grande volume de dados, o que pode limitar sua aplicação direta em operações de segurança física.

Paralelamente, métodos baseados em teoria da informação têm sido utilizados para quantificar incerteza e mudanças estruturais em fluxos de dados. Cai et al. [Cai et al. 2023], Nevat et al. [Nevat et al. 2018] e Guo et al. [Guo et al. 2018] demonstraram a eficácia de métricas como entropia e divergências na detecção de mudanças sutis de distribuição. Em CPS, combinações de medidas entrópicas com estatísticas clássicas também foram exploradas para maior robustez [Moustafa et al. 2018]. Entretanto, a maior parte desses trabalhos concentra-se em anomalias de comunicação ou de processos físicos, e não no comportamento sequencial de mobilidade humana característico dos logs de PACS.

Modelos sequenciais probabilísticos, incluindo Cadeias de Markov e suas variações, constituem outro eixo recorrente na literatura, associando desvios a transições raras ou a perturbações em matrizes de transição [Alhakami et al. 2019, Kwon et al. 2020]. Em paralelo, estratégias híbridas que combinam múltiplos sinais são empregadas para reduzir falsos alarmes e aumentar a confiabilidade da detecção [Han and Woo 2022, Li et al. 2019, Franze' et al. 2022, Dutta et al. 2020]. No contexto de PACS, contudo, essas abordagens aparecem de forma fragmentada, seja focadas em perfis estatísticos agregados, em grafos de relacionamento ou em modelos inspirados em domínios de sensores.

Apesar dos avanços, observa-se uma lacuna metodológica na modelagem do comportamento de acesso em PACS, pois as abordagens existentes, em geral, não capturam simultaneamente a natureza sequencial, individual e incremental do deslocamento dos usuários entre pontos de acesso físicos. Adicionalmente, há uma lacuna operacional, uma vez que muitas soluções não são projetadas para operar em tempo real, apresentam custo computacional elevado ou dependem de dados rotulados e reprocessamentos frequentes, o que limita sua adoção em ambientes corporativos reais. Este trabalho endereça essas lacunas ao propor um middleware, não supervisionado e de baixo custo, que modela o deslocamento individual por Cadeias de DTMCs e quantifica desvios por raridade probabilística de transições e variação incremental de entropia, preservando interpretabilidade e adequação à operação contínua de PACS.

3. Modelagem do Comportamento de Acesso com Cadeias de Markov

Esta seção apresenta o middleware proposto para detecção de anomalias comportamentais em PACS, no qual o deslocamento dos usuários é modelado por DTMCs e os desvios são quantificados a partir da raridade probabilística das transições e da variação incremental de entropia.

3.1. Visão Geral do Middleware

O middleware organiza o processamento dos registros de acesso em um fluxo estruturado que combina uma fase de aprendizado *offline* com análise incremental em tempo real, conforme apresentado na Figura 1. Seu objetivo é capturar padrões sequenciais individuais de deslocamento em PACS e identificar desvios comportamentais por meio de métricas probabilísticas e entrópicas interpretáveis.

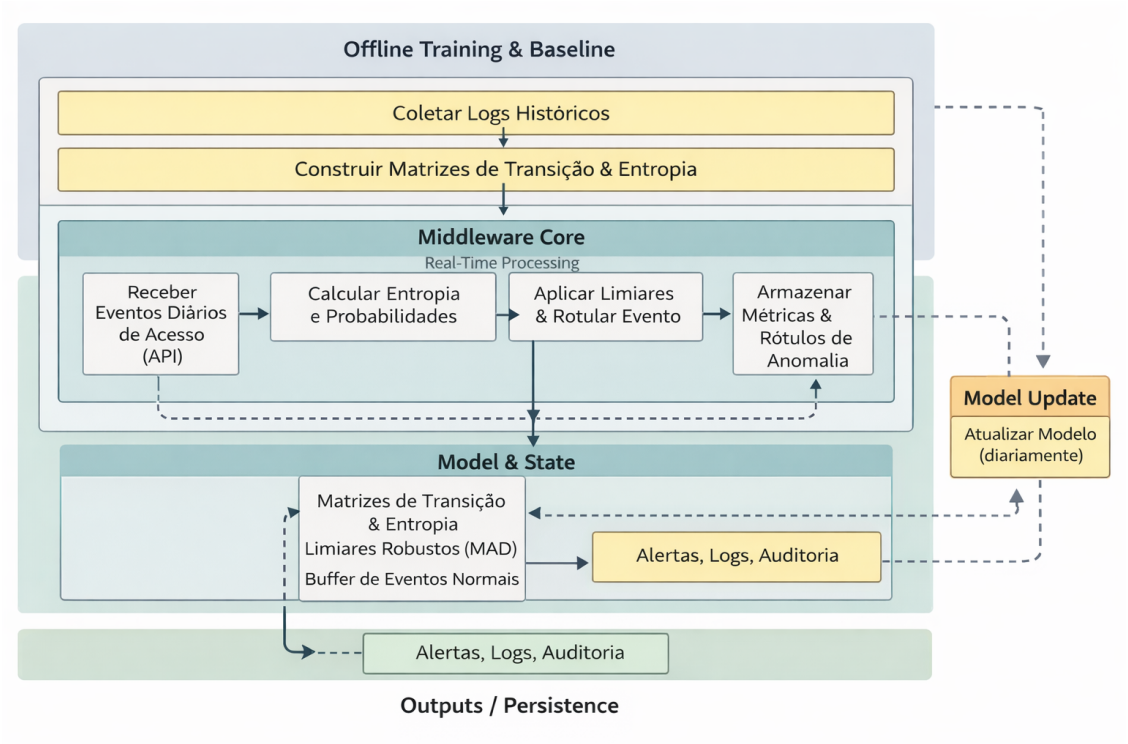


Figura 1. Visão geral do middleware proposto para detecção de anomalias em PACS.

Conforme apresentado na Figura 1, o funcionamento do middleware é composto por etapas complementares que refletem seu ciclo de vida operacional, desde a construção da linha de base comportamental até a análise contínua de eventos em produção. Na fase de treinamento *offline*, logs históricos de acesso são utilizados para construir, para cada usuário, matrizes de transição Markovianas individualizadas e métricas iniciais de entropia. Essas estruturas definem uma linha de base estatística do comportamento de deslocamento, que serve como referência para a detecção de desvios futuros.

O núcleo do middleware opera em tempo real, recebendo continuamente eventos de acesso por meio de uma API. Cada novo evento atualiza incrementalmente as probabilidades de transição e as métricas entrópicas associadas ao usuário correspondente. Em seguida, critérios de decisão baseados em limiares globais são aplicados para rotular o evento como normal ou anômalo, considerando simultaneamente a raridade probabilística da transição observada e o impacto estrutural medido pela variação de entropia. As métricas calculadas, os rótulos atribuídos e os registros de auditoria são então armazenados para análise posterior e para a atualização contínua do middleware.

3.2. Formalização do Modelo Markoviano de Deslocamento

Seja $\mathcal{S} = \{s_1, \ldots, s_{|\mathcal{S}|}\}$ o conjunto finito de estados discretos, no qual cada estado $s_i \in \mathcal{S}$ representa um ponto de acesso físico (catraca, porta controlada ou terminal de visitantes). Para cada usuário $u \in \mathcal{U}$, o PACS gera uma sequência temporalmente ordenada de estados observados $\boldsymbol{s}^{(u)} = (s_1^{(u)}, s_2^{(u)}, \ldots, s_{T_u}^{(u)})$, com $s_t^{(u)} \in \mathcal{S}$.

Modelamos o deslocamento individual por uma Cadeia de Markov de primeira ordem. Seja $X_t^{(u)}$ a variável aleatória que representa o estado do usuário u no instante t. Então, para quaisquer $s_i, s_j \in \mathcal{S}$,

$$\mathbb{P}\Big(X_{t+1}^{(u)} = s_j \mid X_{1:t}^{(u)}\Big) = \mathbb{P}\Big(X_{t+1}^{(u)} = s_j \mid X_t^{(u)} = s_i\Big) \triangleq P_u(s_j \mid s_i), \tag{1}$$

onde $P_u(s_j \mid s_i) \in [0,1]$ e $\sum_{s_j \in \mathcal{S}_u(s_i)} P_u(s_j \mid s_i) = 1$ para todo s_i, sendo $\mathcal{S}_u(s_i)$ o conjunto de sucessores observados a partir de s_i no histórico do usuário. Definimos P_u como a matriz de transição do usuário, cujas entradas são $[P_u]_{ij} = P_u(s_j \mid s_i)$.

A estimação de P_u é baseada em contagens de transições observadas. Para cada par $(s_i, s_j) \in \mathcal{S} \times \mathcal{S}$, definimos

$$N_u(s_i, s_j) \;=\; \sum_{t=1}^{T_u - 1} \mathbb{I}\Big[s_t^{(u)} = s_i,\; s_{t+1}^{(u)} = s_j\Big], \tag{2}$$

e o total de saídas do estado s_i como $N_u(s_i) = \sum_{s_k \in \mathcal{S}} N_u(s_i, s_k)$.

Para explicitar o suporte efetivamente observado no histórico do usuário, definimos

$$\mathcal{S}_u(s_i) = \{s \in \mathcal{S} \;:\; N_u(s_i, s) > 0\}. \tag{3}$$

Para evitar probabilidades nulas e permitir atualização incremental estável, adotamos suavização de Laplace ($\alpha = 1$) sobre esse suporte observado, isto é, considerando apenas as saídas já registradas a partir de s_i:

$$P_u(s_j \mid s_i) = \frac{N_u(s_i, s_j) + 1}{N_u(s_i) + |\mathcal{S}_u(s_i)|}, \qquad s_j \in \mathcal{S}_u(s_i). \tag{4}$$

No regime *online*, ao observar uma nova transição consecutiva ($s_t^{(u)} = s_i \rightarrow s_{t+1}^{(u)} = s_j$), as contagens são atualizadas por

$$N_u(s_i, s_j) \leftarrow N_u(s_i, s_j) + 1, \qquad N_u(s_i) \leftarrow N_u(s_i) + 1, \tag{5}$$

o que induz a atualização da distribuição de saída a partir de s_i em P_u via (4). A Tabela 1 ilustra um exemplo de transições observadas, suas contagens acumuladas e as probabilidades estimadas para um usuário u_1.

Usuário	**Estado** s_i	**Próximo Estado** s_j	**Contagem** $N_u(s_i, s_j)$	**Probabilidade** $P_u(s_j \mid s_i)$
u_1	s_1	s_1	n_{11}	p_{11}
u_1	s_1	s_2	n_{12}	p_{12}
u_1	s_2	s_1	n_{21}	p_{21}
u_1	s_2	s_3	n_{23}	p_{23}
u_1	s_3	s_1	n_{31}	p_{31}

Tabela 1. Exemplo de transições observadas para um usuário em um modelo DTMC.

3.3. Pontuação de Anomalias por Probabilidade e Entropia

Dado um usuário u e uma transição observada $s_i \rightarrow s_j$, o middleware quantifica desvio comportamental a partir de dois sinais complementares: (i) a raridade probabilística da transição e (ii) o impacto estrutural da atualização do middleware, medido por variação de entropia no estado de origem.

A probabilidade empírica de transição é estimada a partir das contagens históricas observadas, utilizando o estimador de máxima verossimilhança (MLE):

$$\widehat{P}_u(s_j \mid s_i) = \frac{N_u(s_i, s_j)}{N_u(s_i)}, \quad \text{quando } N_u(s_i) > 0, \tag{6}$$

e $\widehat{P}_u(s_j \mid s_i) = 0$ quando a transição $s_i \rightarrow s_j$ ainda não foi observada no histórico do usuário. Adotamos MLE neste critério por refletir diretamente a frequência observada de transições no histórico individual. A suavização de Laplace é aplicada apenas no componente entrópico, com o objetivo de garantir estabilidade numérica em regimes de baixa amostragem. A raridade probabilística é avaliada diretamente a partir de valores baixos de $\widehat{P}_u(s_j \mid s_i)$, os quais indicam transições empiricamente incomuns em relação ao padrão individual aprendido.

Para quantificar a estabilidade do comportamento a partir de um estado s_i, consideramos a entropia de Shannon da distribuição de saídas observadas a partir desse estado. Seja

$$\mathcal{S}_u(s_i) = \{s \in \mathcal{S} \ : \ N_u(s_i, s) > 0\} \tag{7}$$

o conjunto de estados que já foram efetivamente observados como sucessores de s_i no histórico do usuário u. A entropia é calculada sobre esse suporte local observado, utilizando suavização de Laplace para garantir estabilidade numérica em regimes de baixa amostragem:

$$\widetilde{P}_u(s \mid s_i) = \frac{N_u(s_i, s) + 1}{N_u(s_i) + |\mathcal{S}_u(s_i)|}, \qquad s \in \mathcal{S}_u(s_i). \tag{8}$$

A entropia local associada ao estado s_i é então definida como

$$H_u(s_i) = -\sum_{s \in \mathcal{S}_u(s_i)} \widetilde{P}_u(s \mid s_i) \, \log_2 \widetilde{P}_u(s \mid s_i). \tag{9}$$

Quando uma nova transição $s_i \rightarrow s_j$ ocorre no fluxo *online*, as contagens $N_u(s_i, s_j)$ são atualizadas incrementalmente, induzindo uma nova distribuição $\widetilde{P}_u(\cdot \mid s_i)$

e, consequentemente, uma nova entropia local. Definimos a variação incremental de entropia associada a essa transição como

$$\Delta H_u^{(t)}(s_i \to s_j) = \left| H_u^{(t+1)}(s_i) - H_u^{(t)}(s_i) \right|, \tag{10}$$

onde $H_u^{(t)}(s_i)$ denota a entropia imediatamente antes da incorporação da transição no instante t, e $H_u^{(t+1)}(s_i)$ a entropia após a atualização. Valores elevados de $\Delta H_u^{(t)}$ indicam reorganizações estruturais no padrão de saída de s_i, mesmo quando a transição isolada não é completamente inédita.

3.4. Limiarização e Rotulagem em Tempo Real

Para reduzir sensibilidade a caudas, outliers e não estacionariedade, adotamos limiares *globais* obtidos por estatísticas (mediana e desvio absoluto mediano, MAD) calculadas a partir das distribuições históricas agregadas do sistema.

Considere o conjunto de probabilidades históricas de transição $p \in (0, 1)$ armazenadas na matriz de transição. Aplicamos a transformação logit $L = \mathrm{logit}(p) = \log\left(\frac{p}{1-p}\right)$ e definimos

$$K_{\text{PROB}} = \max\left\{ \mathrm{logit}^{-1}(\tilde{\mu}_L - 3\,\mathrm{MAD}_L),\ \varepsilon \right\}, \tag{11}$$

onde $\tilde{\mu}_L$ e MAD_L são, respectivamente, a mediana e o desvio absoluto mediano (MAD) de L no histórico agregado, e $\varepsilon > 0$ é um piso numérico adotado para evitar a degeneração do limiar probabilístico em regimes de cauda extrema. No experimento, utilizou-se $\varepsilon = 10^{-3}$, valor suficientemente pequeno para não interferir na discriminação entre transições usuais e raras, mas adequado para garantir estabilidade numérica e evitar limiares próximos de zero.

Para o critério entrópico, construímos uma distribuição histórica agregada de variações incrementais ΔH computadas a partir das contagens de transição (com suavização de Laplace) e definimos

$$K_{\Delta H} = \tilde{\mu}_{\Delta H} + 3\,\mathrm{MAD}_{\Delta H}, \tag{12}$$

onde $\tilde{\mu}_{\Delta H}$ e $\mathrm{MAD}_{\Delta H}$ são calculados sobre a amostra agregada de ΔH.

Uma transição $s_i \to s_j$ é rotulada por:

$$\text{label}_{\text{prob}} = \mathbb{I}\left[\widehat{P}_u(s_j \mid s_i) < K_{\text{PROB}} \right], \tag{13}$$

$$\text{label}_{\text{entropy}} = \mathbb{I}\left[\Delta H_u^{(t)}(s_i \to s_j) > K_{\Delta H} \right]. \tag{14}$$

Para reduzir instabilidades em perfis com histórico insuficiente, os critérios de rotulagem são aplicados apenas quando o usuário possui ao menos $N_{\min}$ transições acumuladas; caso contrário, o evento é marcado como não avaliável. No experimento, adotou-se $N_{\min} = 10$ como um limiar mínimo prático, suficiente para evitar estimativas degeneradas de probabilidade e entropia em regimes de amostragem muito esparsos, sem postergar excessivamente a ativação do monitoramento para novos usuários. Essa escolha reflete um compromisso operacional entre estabilidade estatística e resposta rápida, mantendo baixo custo computacional e interpretabilidade em operação contínua.

4. Avaliação de Desempenho

Nesta seção avaliamos o middleware proposto em dados operacionais reais provenientes do sistema corporativo de controle de acesso físico *Global Access*. O objetivo é verificar se a combinação entre raridade probabilística de transições e variação incremental de entropia é capaz de distinguir rotinas usuais de deslocamento de desvios comportamentais relevantes em um ambiente real, caracterizado por alto fluxo, heterogeneidade de usuários e não estacionariedade natural dos padrões de acesso.

4.1. Cenário de Avaliação

A avaliação foi conduzida em um edifício corporativo em operação contínua, no qual o controle de acesso é realizado por meio do sistema *Global Access*, implantado em ambiente de produção. No período analisado, o sistema operava com 182 equipamentos ativos de controle de acesso, distribuídos entre áreas internas e externas, atendendo fluxos regulares de funcionários, prestadores de serviço e visitantes. Os dados utilizados consistem em registros históricos coletados entre janeiro de 2020 e outubro de 2025, totalizando aproximadamente 13,9 milhões de transições entre pontos de acesso físicos, empregados tanto na construção das linhas de base comportamentais individualizadas por usuário, modeladas como DTMC, quanto na derivação das estatísticas globais utilizadas nos critérios de decisão do middleware. A avaliação foi realizada de forma prospectiva, utilizando eventos ocorridos entre 1º e 5 de novembro de 2025, período não utilizado na modelagem inicial do sistema, no qual o volume diário de solicitações foi de $\approx$ 16,979 eventos, sendo que os dias com menor volume de eventos correspondem a dias não úteis (fins de semana), com uma média de $\approx$ 10,7 solicitações de eventos.

Antes da análise dos resultados operacionais, apresentamos os parâmetros globais estimados a partir do conjunto de treinamento histórico, os quais definem os critérios de decisão do middleware durante a avaliação prospectiva. Esses parâmetros são aprendidos exclusivamente com dados anteriores ao período de teste, garantindo que a rotulagem dos eventos não dependa de ajustes *a posteriori*. O limiar probabilístico global K_{PROB} foi estimado a partir da distribuição agregada das probabilidades empíricas de transição observadas nos modelos individuais, utilizando estatísticas (mediana e desvio absoluto mediano – MAD) após transformação logit. De forma análoga, o limiar entrópico global $K_{\Delta H}$ foi obtido a partir da distribuição histórica das variações incrementais de entropia associadas às atualizações dos modelos durante o treinamento. A Tabela 2 apresenta os parâmetros globais adotados no experimento, bem como estatísticas descritivas das distribuições utilizadas em sua estimação.

Tabela 2. Parâmetros globais e estatísticas de referência estimados no conjunto de treinamento.

Parâmetro	Símbolo	Valor
Limiar probabilístico global	K_{PROB}	0,0010
Limiar entrópico global	$K_{\Delta H}$	0,0485
Histórico mínimo para avaliação	$N_{\min}$	10

Durante o período de avaliação prospectiva, após procedimentos de limpeza e deduplicação, foram processados 44,329 eventos de acesso. A limpeza removeu registros

incompletos ou inconsistentes, enquanto a deduplicação eliminou eventos redundantes decorrentes de retransmissões ou registros múltiplos do mesmo acesso em janelas temporais curtas. Cada evento foi avaliado segundo dois critérios independentes: (i) violação do limiar probabilístico global K_{PROB}; e (ii) violação do limiar entrópico global $K_{\Delta H}$. Ambos estimados a partir do conjunto de treinamento histórico. Os eventos foram classificados em três classes operacionais: *Normal*, *Anomalia Parcial* (violação de exatamente um critério) e *Anomalia Forte* (violação simultânea de ambos).

4.2. Impacto dos Resultados

A distribuição dos eventos rotulados nas classes operacionais *Normal*, *Anomalia Parcial* e *Anomalia Forte* ao longo do período de avaliação é apresentada na Tabela 3, em termos de contagem total de eventos (valores absolutos) e percentual relativo ao conjunto avaliado. Observa-se que 98,25% dos eventos permanecem consistentes com os padrões históricos de deslocamento aprendidos pelo middleware, enquanto aproximadamente 1,75% dos registros são rotulados como anômalos sob ao menos um critério. A distinção entre *anomalias parciais* e *anomalias fortes* permite separar desvios associados à violação isolada de um critério daqueles que são simultaneamente raros e estruturalmente disruptivos, fornecendo uma base objetiva para priorização de alertas em operação.

Tabela 3. Distribuição das classes operacionais rotuladas durante o período de avaliação.

Classe	Contagem	Percentual (%)
Normal	43 554	98,2517
Anomalia Parcial	391	0,8820
Anomalia Forte	384	0,8663

Embora a rotulagem dependa exclusivamente da comparação com os limiares globais, estatísticas descritivas calculadas *a posteriori* permitem caracterizar quantitativamente os regimes comportamentais associados a cada classe operacional. As médias da probabilidade empírica de transição e da variação incremental de entropia observadas em cada classe são apresentadas na Figura 2. Eventos classificados como *Normais* apresentam, em média, probabilidades de transição elevadas e variações entrópicas praticamente nulas, indicando preservação da estrutura sequencial aprendida pelo modelo. As *Anomalias Parciais* ocupam um regime intermediário, caracterizado por redução significativa da probabilidade empírica de transição ou aumento moderado da entropia local, sem ruptura simultânea de ambas as dimensões. Em contraste, a classe *Anomalia Forte* concentra eventos com probabilidade empírica de transição nula, acompanhados por aumentos expressivos da entropia local, evidenciando reorganizações estruturais abruptas no padrão de deslocamento.

A complementaridade entre os critérios probabilístico e entrópico manifesta-se de forma consistente quando os eventos são analisados conjuntamente no espaço probabilidade–entropia. Essa interação pode ser observada sob duas perspectivas visuais complementares, apresentadas na Figura 3, que explicitam tanto o impacto estrutural da atualização do modelo Markoviano individual quanto a convergência entre raridade estatística e variação de entropia.

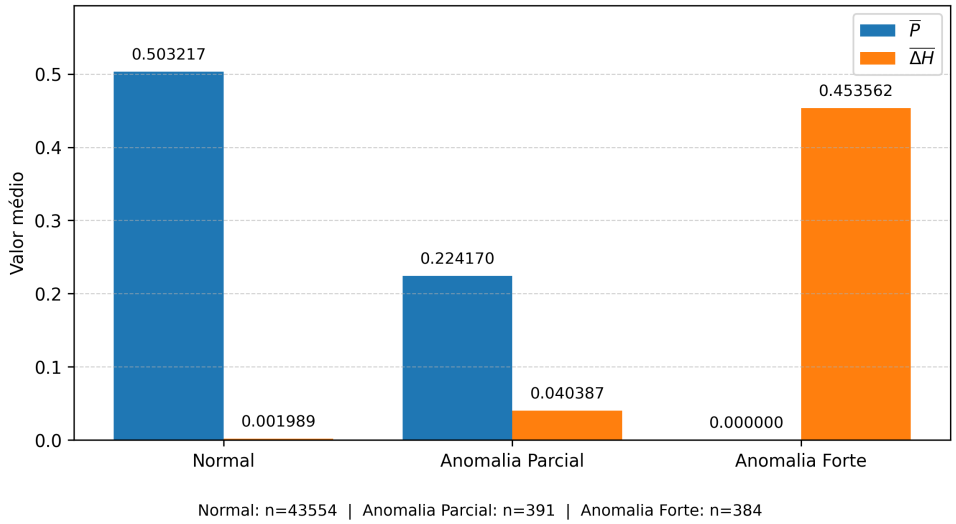
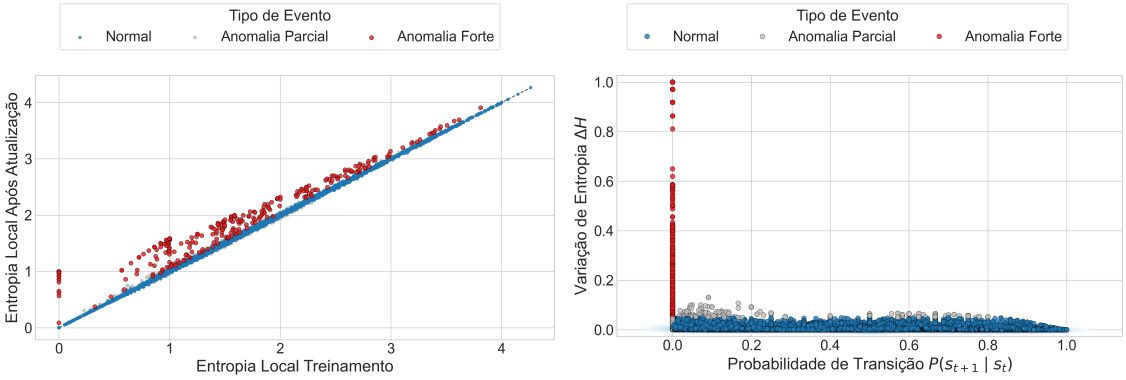


Figura 2. Valores médios de $\overline{P}$ e $\overline{\Delta H}$ por classe operacional (calculados *a posteriori*).



(a) Entropia local treino versus após atualização.

(b) Probabilidade empírica versus ΔH.

Figura 3. Avaliação empírica dos critérios entrópico e probabilístico para detecção de anomalias em PACS.

Na Figura 3(a) , observa-se a relação entre a entropia histórica do estado corrente (H_t) e a entropia após a incorporação de um novo evento (H_{t+1}), evidenciando o impacto estrutural da atualização incremental do modelo Markoviano individual. Eventos normais concentram-se próximos à diagonal $H_t \approx H_{t+1}$, indicando preservação da estrutura local de incerteza ao longo da sequência, enquanto eventos classificados como *Anomalia Forte* localizam-se predominantemente acima dessa região, refletindo aumentos abruptos da entropia associados à reorganização estrutural do padrão sequencial de deslocamento.

De forma complementar, na Figura 3(b) a interação entre raridade estatística e impacto entrópico ao relacionar a probabilidade empírica da transição $P(s_{t+1} \mid s_t)$ com a variação incremental de entropia (ΔH). Nesse espaço, as *anomalias fortes* concentram-se sistematicamente na região de baixa probabilidade empírica e alto ΔH, enquanto as *anomalias parciais* distribuem-se ao longo dos eixos, refletindo violações isoladas de um único critério.

Essa separação visual encontra respaldo quantitativo na distribuição dos eventos detectados por cada critério individualmente e por sua interseção, apresentada na Tabela 4. Observa-se que 49,55% dos eventos anômalos violam simultaneamente os critérios probabilístico e entrópico, caracterizando as anomalias fortes, enquanto os demais se distribuem entre violações isoladas do critério probabilístico (21,55%) e do critério entrópico (28,90%). Esses resultados ratificam que os sinais probabilístico e entrópico não são redundantes, mas capturam dimensões complementares do desvio comportamental. Desta forma, a raridade probabilística destaca transições pouco frequentes no histórico individual, ao passo que a variação incremental de entropia evidencia reorganizações estruturais no padrão local de deslocamento. A convergência entre ambos define, assim, um subconjunto mais restritivo e operacionalmente prioritário de eventos, associado às anomalias fortes.

Tabela 4. Distribuição dos eventos anômalos segundo os critérios probabilístico e entrópico.

Classe de evento	Quantidade	Percentual (%)
Violação apenas do critério probabilístico	167	21,55 %
Violação apenas do critério entrópico	224	28,90 %
Violação simultânea (anomalias fortes)	384	49,55 %

4.3. Discussão dos Resultados

Os resultados demonstram que o middleware proposto atua como um mecanismo eficaz de filtragem operacional, reduzindo o universo de eventos a serem inspecionados para cerca de 1,75% do total processado. Essa taxa emerge diretamente da aplicação de limiares globais, aprendidos a partir do histórico agregado, sem ajuste manual ou calibração a posteriori. Em ambientes corporativos de PACS, caracterizados por alto volume, heterogeneidade de usuários e não estacionariedade dos padrões de acesso, essa redução é particularmente relevante, pois torna viável a análise humana e a integração com fluxos de auditoria e resposta, ao mesmo tempo em que evita o excesso de alertas associado a abordagens excessivamente sensíveis ou baseadas em regras fixas.

A distinção entre anomalias parciais e fortes introduz uma estratificação objetiva do risco, associando maior criticidade a eventos que violam simultaneamente os critérios probabilístico e entrópico. As anomalias fortes concentram transições raras ou inéditas acompanhadas por aumentos expressivos da entropia local, indicando reorganizações abruptas no padrão individual de deslocamento e fornecendo um critério interpretável para priorização de alertas. Do ponto de vista computacional, o middleware baseia-se em atualizações Markovianas incrementais de baixa complexidade, com custo constante por evento e impacto mínimo no tempo de processamento, sendo adequado à operação em tempo real. Em contraste com métodos supervisionados ou modelos mais complexos, que exigem dados rotulados e reprocessamento periódico, a abordagem opera de forma contínua, leve e adaptativa, favorecendo sua adoção em ambientes de produção.

5. Conclusão e Trabalhos Futuros

Este trabalho propôs um middleware interpretável e não supervisionado para detecção de anomalias em PACS, modelando o deslocamento dos usuários por DTMCs individuali-

zadas e avaliando desvios por dois sinais: raridade probabilística da transição e variação incremental de entropia. Os resultados indicam que os critérios não são redundantes: a probabilidade de transição capta a raridade no histórico individual, enquanto a variação de entropia mede mudanças no padrão local. A combinação de baixa probabilidade e alto impacto entrópico define um subconjunto mais restritivo de eventos, associado às *anomalias fortes*, reforçando a utilidade da decomposição. Além disso, por usar atualizações incrementais e métricas de baixo custo, o middleware é compatível com cenários corporativos, onde interpretabilidade e estabilidade são essenciais. Como limitação, o modelo prioriza a dimensão espacial, podendo não destacar desvios temporais (como acessos em horários atípicos com trajetórias usuais) quando não há transições raras ou impacto entrópico relevante.

Como trabalhos futuros, pretende-se incorporar a dimensão temporal ao middleware e refinar os critérios de decisão com limiares mais adaptativos por perfil/usuário. Também pretende-se integrar sinais contextuais e de outros subsistemas de segurança (por exemplo, calendários, vínculos funcionais e eventos operacionais), mantendo a interpretabilidade, para aumentar o poder discriminativo e a utilidade prática do middleware em ambientes de produção.

Referências

Alhakami, W., Alharbi, A. I., Bourouis, S., Alroobaea, R. S., and Bouguila, N. (2019). Network anomaly intrusion detection using a nonparametric bayesian approach and feature selection. *IEEE Access*, 7:52181 – 52190. Cited by: 120; All Open Access; Gold Open Access.

Bitirgen, K. and Basaran FILIK, U. (2023). A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. *International Journal of Critical Infrastructure Protection*, 40. Cited by: 81.

Cai, T., Jia, T., Adepu, S., Li, Y., and Yang, Z. (2023). Adam: An adaptive ddos attack mitigation scheme in software-defined cyber-physical system. *IEEE Transactions on Industrial Informatics*, 19(6):7802 – 7813. Cited by: 54.

de Moura, A. C., Caetano, M. F., Gondim, J. J., Araujo, A., Marotta, M. A., Bondan, L., et al. (2024). Anomaly detection in logs: A comparative analysis of unsupervised algorithms. In *13th Symposium on Languages, Applications and Technologies (SLATE 2024)*, pages 12–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

Dutta, V., Choraś, M., Pawlicki, M., and Kozik, R. (2020). A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors*, 20(16):1 – 20. Cited by: 147; All Open Access; Gold Open Access; Green Final Open Access; Green Open Access.

Feng, C. and Tian, P. (2021). Time series anomaly detection for cyber-physical systems via neural system identification and bayesian filtering. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, KDD '21, page 2858–2867, New York, NY, USA. Association for Computing Machinery.

Fernandes, R., Dalmazo, B. L., Riker, A., Rocha Filho, G. P., Meneguette, R., Júnior, L. P., and Immich, R. (2026). A computational intelligence-driven reference architecture for anomaly detection in software-defined networking (sdn). In *Simpósio Brasileiro de Sistemas de Informação (SBSI)*, pages 811–830. SBC.

Franze', G., Lucia, W., and Tedesco, F. (2022). Resilient model predictive control for constrained cyber-physical systems subject to severe attacks on the communication channels. *IEEE Transactions on Automatic Control*, 67(4):1822 – 1836. Cited by: 60.

Geepalla, E. and Asharif, S. (2020). Analysis of physical access control system for understanding users behavior and anomaly detection using neo4j. In *Proceedings of the 6th International Conference on Engineering & MIS 2020*, pages 1–6.

Guo, Z., Shi, D., Johansson, K. H., and Shi, L. (2018). Worst-case stealthy innovation-based linear attack on remote state estimation. *Automatica*, 89:117 – 124. Cited by: 277.

Han, S. and Woo, S. S. (2022). Learning sparse latent graph representations for anomaly detection in multivariate time series. In *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, KDD '22, page 2977–2986, New York, NY, USA. Association for Computing Machinery.

Huang, X., Hu, Z., and Yun, P. (2023). A survey of collective anomaly detection on sequence dataset. *Int. J. Data Warehous. Min.*, 19(1):1–22.

Kwon, S., Yoo, H., and Shon, T. (2020). Ieee 1815.1-based power system security with bidirectional rnn-based network anomalous attack detection for cyber-physical system. *IEEE Access*, 8:77572 – 77586. Cited by: 83; All Open Access; Gold Open Access.

Li, D., Chen, D., Jin, B., Shi, L., Goh, J., and Ng, S. K. (2019). Mad-gan: Multivariate anomaly detection for time series data with generative adversarial networks. *Lecture Notes in Computer Science*, 11730 LNCS:703 – 716. Cited by: 987.

Molina, A. L., Gonçalves, V. P., De Sousa, R. T., Pividal, M., Meneguette, R. I., and Rocha Filho, G. P. (2022). A lightweight unsupervised learning architecture to enhance user behavior anomaly detection. In *2022 IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6. IEEE.

Moustafa, N., Adi, E., Turnbull, B., and Hu, J. (2018). A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access*, 6:32910 – 32924. Cited by: 131; All Open Access; Gold Open Access.

Nevat, I., Divakaran, D. M., Nagarajan, S. G., Zhang, P., Su, L., Ko, L., and Thing, V. L. (2018). Anomaly detection and attribution in networks with temporally correlated traffic. *IEEE/ACM Transactions on Networking*, 26(1):131 – 144. Cited by: 68.

Saheed, Y. K. and Sanjay, M. (2025). Cps-iot-ppdnn: A new explainable privacy preserving dnn for resilient anomaly detection in cyber-physical systems-enabled iot networks. *Chaos, Solitons and Fractals*, 191. Cited by: 42.

Skopik, F., Wurzenberger, M., Höld, G., Landauer, M., and Kuhn, W. (2022). Behavior-based anomaly detection in log data of physical access control systems. *IEEE Transactions on Dependable and Secure Computing*, 20(4):3158–3175.

Zamanzadeh Darban, Z., Webb, G. I., Pan, S., Aggarwal, C., and Salehi, M. (2024). Deep learning for time series anomaly detection: A survey. *ACM Comput. Surv.*, 57(1).