UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Aplicação do método MSET-SPRT para detecção de anomalias em sistemas bancários

Gleyson Silveira Ribeiro

Trabalho de Conclusão de Curso
MBA em Inteligência Artificial e Big Data

ICMC USP SÃO CARLOS

UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Aplicação do método MSET-SPRT para detecção de anomalias em sistemas bancários

Gleyson Silveira Ribeiro

USP - São Carlos

2025

Gleyson Silveira Ribeiro

Aplicação do método MSET-SPRT para detecção de anomalias em sistemas bancários

Trabalho de conclusão de curso apresentado ao Departamento de Ciências de Computação do Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo - ICMC/USP, como parte dos requisitos para obtenção do título de Especialista em Inteligência Artificial e Big Data.

Área de concentração: Inteligência Artificial.

Orientador: Prof. Dr. Marcelo Garcia Manzato.

USP - São Carlos

2025

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

S587a Silveira Ribeiro, Gleyson Aplicação do método MSET-SPRT para detecção de anomalias em sistemas bancários / Gleyson Silveira Ribeiro; orientador Marcelo Garcia Manzato. -- São Carlos, 2025.
64 p.

Trabalho de conclusão de curso (Programa de Pós-Graduação em Ciências de Computação e Matemática Computacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2025.

1. Detecção de anomalias. 2. MSET. 3. SPRT. 4. Monitoramento bancário. 5. Observabilidade. I. Garcia Manzato, Marcelo, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

DEDICATÓRIA

À minha esposa, pela compreensão, carinho e apoio constante ao longo desta jornada, cuja presença e incentivo foram fundamentais para a concretização deste trabalho. A meus pais pelo incentivo e pelo apoio recebidos desde o início, especialmente pela oportunidade de realizar um curso técnico na área de tecnologia, que foi determinante para que eu descobrisse minha vocação e desenvolvesse as bases do meu crescimento acadêmico e profissional.

AGRADECIMENTOS

Ao Gerente do Núcleo de Monitoramento do Banco de Brasília (BRB), Paulo Roberto Alves da Silva, pela disposição em contribuir de forma direta com o desenvolvimento deste trabalho. Sua confiança, apoio e prontidão em disponibilizar os dados bancários utilizados na pesquisa foram fundamentais para a realização das análises e simulações que embasaram este estudo.

Ao Prof. Dr. Marcelo Garcia Manzato, meu sincero agradecimento pela orientação dedicada e pela disponibilidade constante.

Aos professores e coordenação do MBA em Big Data e Inteligência Artificial da Universidade de São Paulo, minha sincera gratidão pela dedicação, competência e entusiasmo em compartilhar conhecimento.

EPÍGRAFE

Mantenha-se faminto. Mantenha-se tolo.

Jobs (2005)

RESUMO

RIBEIRO, G. S. **Título**: Aplicação do Método MSET-SPRT para Detecção de Anomalias em Sistemas Bancários. 2025. 64 f. Monografia (MBA em Inteligência Artificial e Big Data) – Centro de Ciências Matemáticas Aplicadas à Indústria, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2025.

Este trabalho propõe uma metodologia estatística para detecção automatizada de anomalias em sistemas bancários, combinando as técnicas *Multivariate State Estimation Technique (MSET)* e *Sequential Probability Ratio Test (SPRT)*. O objetivo é identificar, de forma antecipada e confiável, comportamentos anômalos em métricas de latência e transações negadas nos principais *endpoints* utilizados nos sistemas, obtidas a partir das plataformas corporativas de monitoramento Zabbix e Opensearch. A metodologia compreende as etapas de coleta e padronização de dados, estimação multivariada do estado normal por meio do *MSET* e decisão sequencial estatística utilizando o *SPRT*. O modelo foi avaliado em dois cenários: dados normais sem anomalias e dados com anomalias controladas. Os resultados demonstraram alta precisão e estabilidade, com ausência de falsos positivos e baixo tempo médio de detecção. Além disso, o modelo mostrou robustez frente a ruídos e variações sazonais leves, podendo ser integrado a pipelines de monitoramento e sistemas de alerta em tempo real. A principal contribuição deste trabalho é a integração prática de técnicas estatísticas clássicas em um contexto bancário real, fornecendo um método interpretável, reprodutível e de baixo custo computacional. Conclui-se que a combinação *MSET-SPRT* constitui uma abordagem eficaz e escalável para detecção de anomalias em sistemas críticos de produção.

Palavras-chave: *MSET. SPRT*. detecção de anomalias. monitoramento bancário.

observabilidade. Zabbix. Opensearch.

ABSTRACT

RIBEIRO, G. S. **Title in English**: Application of the MSET-SPRT Method for Anomaly Detection in Banking Systems. 2025. 64 f. Monografia (MBA em Inteligência Artificial e Big Data) – Centro de Ciências Matemáticas Aplicadas à Indústria, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2025.

This work proposes a statistical methodology for the automated detection of anomalies in banking systems, combining the Multivariate State Estimation Technique (MSET) and the Sequential Probability Ratio Test (SPRT). The objective is to identify, in an early and reliable manner, anomalous behaviors in latency and denied transaction metrics across the main system endpoints, obtained from the corporate monitoring platforms Zabbix and Opensearch. The methodology comprises the stages of data collection and standardization, multivariate estimation of the normal state using MSET, and sequential statistical decision-making through SPRT. The model was evaluated under two scenarios: normal data without anomalies and data with controlled anomalies. The results demonstrated high accuracy and stability, with no false positives and low average detection time. In addition, the model showed robustness to noise and mild seasonal variations and can be integrated into monitoring pipelines and real-time alert systems. The main contribution of this work is the practical integration of classical statistical techniques within a real banking context, providing an interpretable, reproducible, and computationally efficient method. It is concluded that the MSET-SPRT combination constitutes an effective and scalable approach for anomaly detection in critical production systems.

Keywords: MSET. SPRT. anomaly detection. banking monitoring. observability. Zabbix. Opensearch.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANL	–	Argonne National Laboratory
CPU	–	Central Processing Unit
CSV	–	Comma-Separated Values
D	–	Matriz de memória (MSET)
H_0	–	Hipótese nula (sem anomalia)
H_1	–	Hipótese alternativa (com anomalia)
K_SIGMA	–	Fator de limiar estatístico
L	–	Dados remanescentes de treinamento (MSET)
ms	–	Milissegundo
MSET	–	Multivariate State Estimation Technique
PIX	–	Pagamento instantâneo brasileiro
SPE	–	Squared Prediction Error
SPRT	–	Sequential Probability Ratio Test
S(t)	–	Soma ou acumulação de evidências
T	–	Dados de treinamento (MSET)
X_{est}	–	Estimativa (MSET)
X_{obs}	–	Estado do sistema ou observação (MSET)
z-score	–	Distância de um valor em relação à média, em unidades de desvio-padrão

LISTA DE SÍMBOLOS

α	Erro do tipo I (falso positivo)
β	Erro do tipo II (falso negativo)
Λ_m	Razão de verossimilhância até a m-ésima observação
θ_0	Valor esperado sob H_0 (hipótese nula)
θ_1	Valor esperado sob H_1 (hipótese alternativa)
ρ_0	Função de verossimilhância sob H_0
ρ_1	Função de verossimilhância sob H_1
x_t	Valor observado no instante t
μ	Média da série temporal
σ	Desvio-padrão

SUMÁRIO

1 INTRODUÇÃO

Conforme Delgad (2020), o setor de serviços financeiros está passando por uma transformação digital em grande escala, que tem amplas implicações sobre a forma como as empresas do setor conduzem seus negócios. Novas tecnologias estão permitindo que bancos reformulem suas operações e identifiquem diferentes maneiras de atender seus clientes.

Com essa evolução, os clientes passaram a realizar transações bancárias de forma rápida e prática, sem a necessidade de comparecimento físico às agências. Garantir a fluidez e a confiabilidade das operações como transferências, pagamentos e consultas é fundamental para manter a satisfação e a fidelização dos clientes.

Nesse contexto, a experiência do usuário tornou-se um fator central para a percepção de qualidade e confiança nos serviços financeiros. De acordo com Augusto (2024), ao detectar problemas garantindo uma rápida resolução, um monitoramento proativo otimiza o desempenho da tecnologia da informação (TI), reduzindo tempos de resposta e proporcionando uma melhor experiência para o usuário.

Problemas como lentidão no processamento de operações, erros recorrentes ou tempos de resposta altos podem gerar insatisfação, prejudicando a relação dos clientes com a instituição e, em alguns casos, levando-os a procurar alternativas mais eficientes na concorrência.

Os sistemas de monitoramento e observabilidade corporativos, como OpenSearch e Zabbix têm papel fundamental nesse cenário, permitindo a coleta e análise contínua de métricas de desempenho, como tempo de resposta, número de requisições e falhas de processamento. No entanto, a detecção automática de anomalias em tempo real ainda representa um desafio, especialmente em ambientes com múltiplos *endpoints* e grande variabilidade operacional.

Apesar da evolução das ferramentas de monitoramento, muitas instituições financeiras ainda dependem de alertas manuais para identificar falhas, o que limita a eficiência e aumenta a probabilidade de atrasos na resposta a incidentes. A ausência de modelos estatísticos adaptativos e multivariados dificulta a correlação eficaz entre diferentes indicadores, dificultando a detecção precoce de comportamentos anômalos.

A identificação proativa de anomalias em métricas de desempenho é crucial para instituições financeiras, pois falhas nos sistemas de produção podem resultar em prejuízos operacionais, impacto na experiência do cliente e riscos reputacionais. A adoção de técnicas estatísticas robustas e interpretáveis permite construir mecanismos de alerta mais confiáveis, capazes de reduzir falsos positivos e antecipar incidentes críticos. Além disso, o uso de dados

reais provenientes de sistemas amplamente utilizados, como Zabbix e OpenSearch, confere relevância prática à pesquisa e potencial de aplicação imediata no ambiente corporativo.

O objetivo geral deste trabalho é propor e avaliar uma metodologia estatística para detecção automatizada de anomalias em sistemas bancários, integrando métricas operacionais provenientes de plataformas de monitoramento corporativo. Busca-se desenvolver um modelo que utilize a *Multivariate State Estimation Technique (MSET) e o Sequential Probability Ratio Test (SPRT)* de forma combinada, permitindo identificar comportamentos anômalos em tempo real.

Com isso, o presente trabalho possui os seguintes objetivos específicos:

- Desenvolver um modelo estatístico baseado em *MSET-SPRT* para detecção de anomalias em sistemas bancários;
- Integrar dados de latência e transações negadas provenientes das plataformas Zabbix e OpenSearch;
- Avaliar o desempenho do modelo quanto à precisão, estabilidade e tempo médio de detecção;
- Demonstrar a aplicabilidade do modelo em pipelines de monitoramento corporativos.

De maneira geral, os resultados demonstraram que o modelo apresentou elevada estabilidade em condições normais de operação, mantendo baixos níveis de variação e ausência de falsos positivos, o que reforça sua capacidade de representar com precisão o comportamento esperado do sistema. Nos cenários com condições adversas simuladas, o modelo mostrou-se altamente sensível à detecção de anomalias, identificando de forma precisa picos de latência e aumentos súbitos nas taxas de transações negadas. Além disso, a integração entre as etapas de estimação multivariada e decisão sequencial permitiu uma resposta rápida e estatisticamente consistente diante de mudanças abruptas, sem comprometer o desempenho em períodos estáveis.

Este trabalho está estruturado em cinco capítulos.

O Capítulo 1 apresenta a introdução, contextualizando o tema, os objetivos e a relevância da pesquisa.

O Capítulo 2 reúne a revisão bibliográfica, abordando os fundamentos teóricos relacionados ao monitoramento de tecnologia da informação, à detecção de anomalias e às técnicas estatísticas utilizadas, como o *Multivariate State Estimation Technique (MSET)* e o *Sequential Probability Ratio Test (SPRT)*, além de trabalhos correlatos.

O Capítulo 3, por sua vez, descreve a metodologia adotada, incluindo as etapas de coleta, pré-processamento e modelagem dos dados, bem como a integração operacional entre o *MSET* e o *SPRT*.

Já o Capítulo 4 apresenta e discute os resultados obtidos, contemplando as análises estatísticas, as simulações de cenários e a avaliação de desempenho do modelo proposto. Foram realizados, neste trabalho, experimentos utilizando conjuntos de dados representando condições normais de operação, bem como cenários simulados de condições adversas.

Por fim, o Capítulo 5 traz a conclusão, destacando as contribuições do estudo, suas limitações e as perspectivas para trabalhos futuros.

Durante a elaboração deste trabalho, o autor recorreu a ferramentas de inteligência artificial generativa, como ChatGPT e DeepL, para apoio na redação e revisão de determinados trechos. Todo o conteúdo gerado foi submetido a análise, curadoria e ajustes manuais pelo autor, que assume integral responsabilidade pela versão final e por todas as ideias aqui apresentadas.

2 REVISÃO BIBLIOGRÁFICA

2.1 Monitoramento de tecnologia da informação

De acordo com Bonini, Junior (2022), a operação estável de uma infraestrutura de tecnologia da informação (TI) é crucial para o sucesso dos negócios das empresas que oferecem produtos e serviços pela Internet. Além disso, monitorar o funcionamento de TI e tomar decisões são duas atividades essenciais para manter os negócios funcionando.

Atualmente, o monitoramento de TI não se limita a simplesmente coletar informações básicas sobre o estado da infraestrutura de TI. Existem várias ferramentas que podem coletar métricas de disponibilidade, desempenho e status de uma máquina virtual Java, por exemplo.

O monitoramento de TI é o processo contínuo de rastreamento de atividades operadas pela infraestrutura de TI, permitindo a detecção imediata de tempo de inatividade inesperado, intrusão de rede e sobrecarga de recursos, por exemplo.

2.2 Detecção de anomalias

Segundo Theissler et al. (2021), a detecção de anomalias é uma abordagem comum para a detecção de falhas. Uma anomalia pode ser considerada um erro potencial, onde um erro pode, por sua vez, causar uma falha.

De acordo com Sabharwal, Bhardwaj (2022), a detecção de anomalias consiste no processo de identificar pontos de dados que se mostram incomuns ou inesperados. Em contextos operacionais, eventos regulares relacionados ao uso de *CPU*, memória, disco, entre outros, são considerados normais. No entanto, ocorrências como a queda de uma aplicação ou equipamento de infraestrutura de rede representam situações atípicas. O principal objetivo da detecção de anomalias é reconhecer esses cenários diferenciados, conhecidos como outliers, que destoam significativamente dos demais registros em um conjunto de dados. Embora a tarefa possa ser realizada por algoritmos supervisionados, não supervisionados e por reforço, sua aplicação tem sido amplamente feita em dados não rotulados, por meio da formação de agrupamentos (*clustering*). Nas operações de TI, a execução de planos de melhoria de serviços é uma prática contínua, e não há, muitas vezes, um alvo preditivo específico. O foco, nesse caso, está em analisar grandes volumes de dados, identificar padrões de similaridade e agrupar essas informações com o intuito de compreender anomalias e formular recomendações estratégicas.

A Detecção de anomalias, de acordo com Chandola, Banerjee, Kumar (2009) e Khairi (2018), é um problema importante de ampla aplicação e que tem sido utilizado em diversas áreas do conhecimento. O termo "detecção de anomalias" pode ser associado com "detecção de *outliers*", que consiste na identificação de itens, eventos ou observações que não estão em conformidade com um padrão esperado ou outros itens em um conjunto de dados.

As abordagens de detecção de anomalias são baseadas em modelos e previsões de dados passados. A principal suposição do comportamento normal é a estacionariedade, ou seja, acredita-se que os processos subjacentes, que levaram à geração dos dados, não tenham mudado significativamente (Mehrotra; Mohan; Huang, 2017).

Na literatura, são usados termos diferentes que têm o mesmo significado ou um significado semelhante à detecção de anomalias: detecção de eventos, detecção de novidades, detecção de eventos (raros), descoberta de desvios, detecção de pontos de alteração, detecção de falhas, detecção de intrusão ou detecção de uso indevido. Os diferentes termos refletem o mesmo objetivo: detectar pontos de dados raros que se desviam notavelmente da distribuição geral do conjunto de dados. A quantidade de desvio geralmente é considerada como uma medida da força da anomalia (Braei; Wagner, 2020).

Normalmente, no contexto bancário, os itens anômalos podem indicar falhas de performance e infraestrutura, problemas na jornada do usuário como fluxos interrompidos ou tempo excessivo em determinada etapa, falhas que podem indicar riscos de segurança e transações não concluídas com alta frequência.

De acordo com Theissler et al. (2021), as seguintes abordagens de detecção de anomalias podem ser utilizadas:

- Modelos físicos: A modelagem física do comportamento normal, baseada nas especificações do sistema, permite identificar desvios que podem ser interpretados como anomalias. Além disso, ou alternativamente, é possível modelar situações atípicas ou fora do padrão esperado do sistema, bem como falhas conhecidas previamente;
- Detecção de anomalias não supervisionada: nesse tipo de abordagem, a identificação de anomalias é feita sem o uso de rótulos ou classificações prévias nos dados;
- Detecção de anomalias semi-supervisionada: nessa abordagem, modelos de aprendizado de máquina são treinados exclusivamente com dados normais, de forma a aprender o comportamento típico do sistema. Durante a operação, quaisquer desvios em relação a esse padrão aprendido são reportados como anomalias.

- Detecção de anomalias supervisionada: modelos tradicionais de aprendizado de máquina podem ser treinados utilizando dados rotulados como normais e anômalos, de modo a classificar novas instâncias como pertencentes a uma das duas categorias;
- Abordagens híbridas: buscam superar as limitações dos métodos individuais, combinando modelos baseados em dados (*data-driven*) com modelos físicos. Essa integração permite aproveitar as vantagens de ambos os paradigmas: enquanto os modelos baseados em dados aprendem padrões a partir de grandes volumes de informação histórica, os modelos físicos incorporam conhecimento prévio sobre o funcionamento do sistema. Essa combinação tende a aumentar a precisão na detecção de anomalias, especialmente em ambientes complexos e críticos, como os sistemas bancários.

Segundo Sabharwal, Bhardwaj (2022), a detecção de anomalias apresenta vantagens significativas em relação aos sistemas tradicionais baseados em regras fixas. Os algoritmos de detecção de anomalias são capazes de identificar variações sazonais nos dados, sinalizando comportamentos anômalos somente após considerar tais variações recorrentes. Em ambientes de tecnologia da informação, os dados de métricas geralmente apresentam forte sazonalidade, uma vez que a carga de aplicações e a execução de tarefas seguem padrões típicos ao longo do dia. Além disso, certos processos executados mensalmente podem aumentar temporariamente a utilização dos sistemas sem, contudo, representarem anomalias. Esse tipo de reconhecimento contextual é essencial para reduzir falsos positivos e melhorar a precisão do monitoramento automatizado.

Conforme Mehrotra, Mohan, Huang (2017), a aplicação de algoritmos de detecção de anomalias envolve a consideração de três possíveis resultados. O primeiro refere-se à detecção correta, quando os dados identificados como anômalos refletem, de fato, um comportamento anormal no processo monitorado. O segundo caso é o dos falsos positivos, em que o processo permanece normal, mas o algoritmo interpreta variações inesperadas nos dados, como ruídos ou oscilações naturais do sistema, como anomalias. Por fim, há os falsos negativos, que ocorrem quando o sistema apresenta uma falha real, mas esta não é detectada pelo algoritmo, seja porque o sinal da anomalia é fraco, seja porque está mascarado pelo ruído presente nos dados.

2.2 Técnica de estimativa de estado multivariada (*Multivariate State Estimation Technique – MSET*)

O *Multivariate State Estimation Technique (MSET)* é um método estatístico não paramétrico desenvolvido originalmente no *Argonne National Laboratory (ANL)*, voltado para a detecção de anomalias e diagnóstico de falhas em sistemas complexos com múltiplas variáveis correlacionadas.

Segundo Zavaljevski e Gross (2000), o *MSET* é baseado na premissa de que o comportamento de um sistema em estado normal pode ser descrito por um modelo de correlação multivariada entre suas variáveis observáveis. A partir desse modelo, é possível estimar o estado esperado de operação e identificar desvios residuais quando as medições reais divergem significativamente das predições do modelo.

Estudos demonstram que o *MSET* pode ser empregado para o monitoramento simultâneo de diversos parâmetros em sistemas bancários, como o volume de transações, o tempo médio de resposta das aplicações e o número de acessos simultâneos. Essa técnica permite calcular os desvios entre os valores reais e os valores esperados desses parâmetros, tendo como base dados históricos obtidos em condições normais de operação.

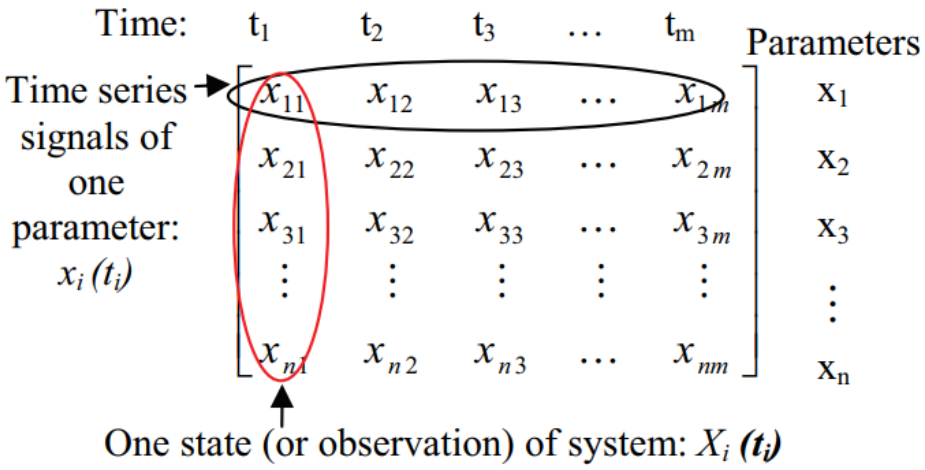
De acordo com Cheng, Pecht (2023), o *MSET* utiliza reconhecimento de padrões a partir de dados históricos de funcionamento normal do sistema para estimar seu estado operacional atual. Parte-se do pressuposto de que os dados históricos representam adequadamente toda a faixa de operação considerada saudável. Como resultado, a *MSET* gera resíduos, que indicam o desvio entre os dados atualmente monitorados e os valores esperados para condições normais de operação.

O *MSET* envolve alguns conceitos fundamentais, como a matriz de dados, o estado do sistema ou observação (X_{obs}), os dados de treinamento (T), a matriz de memória (D), os dados remanescentes de treinamento (L) e a estimativa (X_{est}). Esses elementos compõem a base do modelo, permitindo a comparação entre os valores observados e os valores esperados, com o objetivo de identificar desvios que possam representar comportamentos anômalos.

Conforme ilustrado na Figura 1, a matriz de dados definida pela *MSET* é composta por n parâmetros, sendo que cada parâmetro possui m valores. Cada linha da matriz representa uma série temporal dos valores de um parâmetro xi, variando do instante $t1$ até tm. Por sua vez, cada coluna da matriz corresponde aos valores de todos os parâmetros, de $x1$ a xn em um determinado instante ti. Assim, cada coluna é considerada uma observação ou um estado do

sistema naquele momento específico, pois reúne todas as variáveis monitoradas simultaneamente.

Figura 1 - Matriz de Dados *MSET*



Fonte: Cheng, Pecht (2023)

O estado ou observação $X_{obs}(ti)$ do sistema em um determinado instante ti é representado por um vetor $X(ti)$ de dimensão n, sendo n o número de parâmetros monitorados do sistema naquele instante de tempo.

Os dados de treinamento T correspondem a uma matriz composta por diversos estados históricos considerados normais ou saudáveis do sistema.

A matriz de memória D é composta por estados específicos selecionados por algoritmos a partir dos dados de treinamento T.

Os estados nos dados de treinamento que não são selecionados para a matriz de memória D formam os dados de treinamento restantes L.

A estimativa da observação, X_{est}, é o valor esperado calculado a partir dos dados saudáveis. Essa estimativa possui o mesmo formato de dados que a observação.

Ainda segundo Cheng, Pecht (2023), o processo *MSET* envolve três procedimentos principais: selecionar os dados de treinamento, escolher alguns dados representativos a partir dos dados de treinamento para criar a matriz de memória, que serve como a linha de base para o cálculo da estimativa, e, por fim, calcular as estimativas.

Dois pré-requisitos são necessários para os dados de treinamento. Primeiramente, os dados devem conter todos os estados operacionais saudáveis do sistema monitorado. Além

disso, os dados não devem incluir anomalias operacionais que possam ser consideradas operações não saudáveis do sistema.

2.3 Teste sequencial de razão de probabilidades *(Sequential Probability Ratio Test – SPRT)*

O Teste Sequencial de Razão de Probabilidades *(Sequential Probability Ratio Test – SPRT)* foi proposto por Abraham Wald em meados da década de 1940, no contexto da teoria estatística de testes de hipóteses. Seu desenvolvimento está detalhado na obra *Sequential Analysis*, Wald (2013), que consolidou as bases matemáticas dos testes sequenciais e introduziu o conceito de decisão estatística com número variável de observações.

De acordo com Wald (2013), o principal diferencial dos testes sequenciais é que o número de observações não é fixo, como ocorre nos testes clássicos de Neyman-Pearson, mas depende do comportamento acumulado dos dados. A cada nova observação, o processo de decisão pode levar a três resultados possíveis:

- Aceitar a hipótese nula (H_0)
- Rejeitar a hipótese nula (H_0)
- Continuar a coleta de observações

Esse procedimento torna o teste mais flexível e eficiente, pois permite a interrupção antecipada quando a evidência estatística se torna suficientemente forte a favor de uma das hipóteses.

Wald (2013) define o *SPRT* como o teste utilizado para decidir entre duas hipóteses simples:

- H_0: $\theta = \theta_0$
- H_1: $\theta = \theta_1$

O teste baseia-se na razão de verossimilhanças acumulada das observações, expressa por:

$$\Lambda_m = \frac{\rho_1\ (x_1, x_2, \dots, x_m)}{\rho_0\ (x_1, x_2, \dots, x_m)}$$

onde p_1 e p_0 representam as probabilidades sob as hipóteses H_1 e H_0, respectivamente.

A regra de decisão é definida por dois limites A e B (com $B < A$):

- Se $\Lambda_m \geq A$, aceita-se H_1 (anomalia);
- Se $\Lambda_m \leq B$, aceita-se H_0 (normalidade);

- Se Λ_m estiver entre A e B, o processo continua coletando dados.

Esses limites são determinados de forma a satisfazer as probabilidades máximas de erro do tipo I (α) e do tipo II (β). Na prática, utiliza-se a forma logarítmica da razão, permitindo expressar a estatística do teste como uma soma de log-verossimilhanças incrementais, o que facilita o cálculo iterativo e a interpretação do crescimento da evidência Wald (2013).

No Capítulo 2, Wald discute o conceito de eficiência de um teste sequencial, definida como a razão entre o número esperado de observações exigidas pelo teste e o mínimo possível para alcançar o mesmo nível de erro Wald (2013). O autor demonstra que o *SPRT* possui eficiência muito próxima de 1, ou seja, é praticamente ótimo em comparação com qualquer outro teste da mesma força estatística (α,β).

O autor ressalta ainda que, na maioria dos casos, o *SPRT* permite uma redução média de 50% no número de observações necessárias em relação aos testes fixos tradicionais, mantendo os níveis de significância e poder Wald (2013). Esse resultado reforça o caráter de eficiência do método, o que o torna especialmente adequado para processos contínuos de monitoramento e detecção de anomalias em tempo real, como em sistemas de monitoramento de desempenho ou de fraudes.

O conceito original de Wald foi posteriormente aplicado em diversas áreas, incluindo engenharia de controle, telecomunicações, finanças e detecção de anomalias.

O raciocínio central, decidir adaptativamente com base em evidência estatística acumulada, inspira metodologias modernas em aprendizado de máquina, como testes sequenciais para detecção de mudanças de regime e modelos de monitoramento adaptativo de séries temporais.

Em contextos práticos de detecção de anomalias, o *SPRT* permite interpretar o processo de decisão como uma curva cumulativa de evidência (S(t)), comparada com os limiares A e B:

- Quando $S(t)$ cruza A, ocorre uma anomalia confirmada (H_1);
- Quando $S(t)$ cruza B, o sistema retorna à normalidade (H_0).

Essa abordagem torna o *SPRT* um instrumento poderoso para avaliação dinâmica de comportamento em dados de sistemas financeiros, industriais e computacionais.

2.4 Integração entre *MSET* e *SPRT*

A combinação *MSET* + *SPRT* forma um sistema híbrido de detecção estatística adaptativa, amplamente utilizado em aplicações industriais e computacionais (ORACLE, 2021; YAN et al., 2022).

Nesse arranjo:

- O *MSET* realiza a estimação do estado esperado e calcula os resíduos instantâneos (SPE ou erro normalizado);
- O *SPRT* atua como mecanismo de decisão sequencial, avaliando os resíduos acumulados ao longo do tempo e determinando se o comportamento atual permanece normal (H_0) ou é anômalo (H_1).

A documentação técnica da Oracle (2021) destaca que o *MSET-SPRT* é capaz de detectar comportamentos anormais em tempo quase real, com baixo índice de falsos positivos, sendo utilizado em sistemas de monitoramento autônomo, como em plataformas de análise de dados corporativos e bancos de dados críticos.

No contexto deste trabalho, o *MSET* modela múltiplos *endpoints* de latência e transações negadas, enquanto o *SPRT* avalia, em tempo quase real, se há evidência de degradação operacional.

2.5 Trabalhos relacionados

Diversos estudos têm explorado a aplicação combinada das técnicas *MSET-SPRT* em contextos de monitoramento e detecção de anomalias, evidenciando sua eficácia em ambientes complexos e dinâmicos.

Peng et al. (2014) propuseram um método de monitoramento baseado em *MSET-SPRT* voltado à detecção de falhas em componentes críticos de satélites. O trabalho destaca a capacidade do *MSET* em modelar o comportamento normal de sistemas multivariados, utilizando correlações entre variáveis para prever estados esperados e identificar desvios. O *SPRT* é então empregado como mecanismo de decisão sequencial, possibilitando a detecção precoce de anomalias com baixo número de amostras. Os autores demonstraram que a combinação das duas técnicas resultou em maior precisão e menor tempo de resposta quando comparada a abordagens convencionais de monitoramento.

Na documentação técnica da Oracle (2023), o algoritmo *MSET-SPRT* é descrito como uma solução de detecção estatística de anomalias voltada a processos críticos de alta

disponibilidade. O documento ressalta que o modelo, implementado em produtos de monitoramento corporativo da empresa, é capaz de aprender padrões normais de operação e identificar anomalias em tempo real, com base em limiares ajustáveis de confiança estatística.

Mais recentemente, Gerdes et al. (2025) realizaram um estudo comparativo entre o *MSET-SPRT* e métodos modernos de detecção de anomalias baseados em aprendizado de máquina. Os resultados indicaram que o modelo clássico mantém vantagens em interpretabilidade, estabilidade e baixo custo computacional, especialmente em cenários onde os dados são ruidosos ou apresentam correlações complexas entre múltiplas variáveis. O trabalho também destaca que, embora técnicas baseadas em redes neurais ofereçam ganhos de flexibilidade, o *MSET-SPRT* continua sendo uma solução confiável e estatisticamente fundamentada.

3 METODOLOGIA

3.1 Descrição geral da abordagem

A proposta metodológica deste trabalho consiste na aplicação das técnicas *MSET* e *SPRT* para a detecção de comportamentos anômalos em dados operacionais de sistemas bancários. O objetivo é criar um pipeline de detecção automatizado capaz de identificar comportamentos anômalos em tempo quase real, utilizando dados provenientes das plataformas de monitoramento corporativas Zabbix e Opensearch.

O processo metodológico foi estruturado em seis etapas principais: coleta de métricas, integração e tratamento de dados, normalização, modelagem pelo *MSET*, detecção pelo *SPRT*, e avaliação dos resultados.

3.2 Coleta e integração dos dados

A coleta de dados foi realizada em dois sistemas corporativos:

- Zabbix: plataforma de monitoramento de infraestrutura, responsável pela coleta de métricas operacionais dos sistemas bancários, tais como uso de *CPU*, memória, espaço em disco, latência de resposta de serviços, entre outros indicadores críticos para a disponibilidade e performance dos sistemas;
- OpenSearch: ferramenta de gerenciamento e análise de *logs*, utilizada para agregar, indexar e consultar grandes volumes de registros gerados por aplicações, serviços e componentes da infraestrutura.

Ambas as fontes foram acessadas via *API REST* e os dados exportados em formato *CSV* padronizado.

Os dados utilizados neste trabalho estão organizados em dois arquivos *CSV* distintos: um referente às latências dos *endpoints* e outro às transações negadas.

O primeiro arquivo, denominado *latency.csv*, contém as medições de tempo de resposta coletadas a partir dos sistemas de monitoramento. Cada linha representa um *timestamp*, formando uma matriz denominada LAT. Os principais campos incluem:

- *timestamp*: instante de coleta da métrica;
- *endpoint*: nome do endpoint;
- *response_time*: valores de latência (em milissegundos) de cada *endpoint*.

O conjunto é composto por dados de seis *endpoints* distintos, listados a seguir:

- api_login: responsável pelas requisições de autenticação de usuários;
- api_saldo: consulta de saldos de contas bancárias;
- api_pix: operações de transferência instantânea via sistema PIX;
- api_cartao: consultas e operações relacionadas a cartões;
- api_transferencia: transações bancárias tradicionais entre contas;
- api_extrato: consultas de histórico e extratos de movimentações.

A escolha desses *endpoints* se justifica pelo fato de representarem as operações mais frequentemente utilizadas pelos clientes, refletindo de forma mais fiel o comportamento real de uso dos sistemas bancários no ambiente de produção.

O segundo arquivo, denominado transactions.csv, armazena as informações referentes à taxa de transações negadas e aprovadas, constituindo a matriz DEN. Cada linha representa o mesmo intervalo temporal do arquivo de latência, e os campos principais são:

- *timestamp*: instante de coleta da métrica;
- *endpoint*: nome do *endpoint*;
- negadas: número de transações rejeitadas no período;
- aprovadas: número de transações processadas com sucesso.

O conjunto é composto por dados de cinco *endpoints* distintos, listados a seguir:

- VISA: transações relativas ao cartão com bandeira Visa;
- MASTERCARD: transações relativas ao cartão com bandeira Mastercard;
- MBK: consultas e operações relacionadas ao aplicativo do Banco (Mobile Banking);
- IBK: consultas e operações relacionadas à página web do Banco (Internet Banking);
- PIX: operações de transferência instantânea via sistema PIX;

Ambos os arquivos possuem estrutura temporal uniforme, com intervalos regulares de um minuto entre as amostras, o que garante a sincronização das séries temporais e a comparabilidade entre as métricas analisadas.

3.3 Pré-processamento e normalização

Os dados brutos foram reamostrados para garantir consistência temporal e tratados para remoção de valores ausentes por interpolação linear. Em seguida, as métricas foram normalizadas em unidades de desvio-padrão (*z-score*) conforme a equação:

$$Z_t = \frac{(x_t - \mu)}{\sigma}$$

Essa padronização permite comparar métricas de diferentes escalas, assegurando que o modelo *MSET* interprete variações em termos relativos. O conjunto de dados normalizado é dividido em duas partes: uma parte de treinamento (para construção da memória *MSET*) e uma parte de monitoramento (para aplicação do modelo e detecção de anomalias).

3.4 Modelagem estatística com *MSET*

O *MSET* é utilizado para aprender o comportamento normal do sistema com base nas relações entre métricas como latência e transações negadas. Ele funciona criando uma memória de referência, formada pelos dados históricos de operação normal. A cada novo instante de tempo, o modelo compara os valores atuais com essa memória para estimar como o sistema deveria se comportar em condições normais.

O *MSET* calcula uma estimativa esperada para cada variável, levando em conta as observações anteriores mais parecidas. Quando o valor atual é muito diferente do esperado, considera-se que há um erro de predição.

Quando o valor observado se distancia muito do valor estimado, o modelo identifica um erro de predição, chamado de *SPE (Squared Prediction Error)*. Esse erro reflete o quanto o sistema está se comportando de forma diferente do padrão normal.

Além do *SPE* global, o modelo calcula indicadores específicos chamados de pressões:

- Pressão de latência: mede o quanto as latências atuais estão acima do comportamento médio esperado;
- Pressão de transações negadas: mede o quanto a taxa de transações negadas se eleva em relação ao histórico considerado normal.

Dessa forma, quanto maior a pressão, maior é a probabilidade de que o sistema esteja sob alguma degradação do desempenho. As três medidas (*SPE* global, pressão de latência e pressão de transações negadas) são repassadas ao módulo *SPRT*, que analisa a sequência temporal dessas evidências para confirmar ou não a ocorrência de anomalias.

3.5 Decisão sequencial com *SPRT*

Após o cálculo do *SPE* e das pressões de latência e transações negadas, o próximo passo é decidir se o comportamento observado indica uma anomalia ou não. Para isso, é utilizado o *SPRT (Sequential Probability Ratio Test)*, um método estatístico que acompanha a evolução dos dados ao longo do tempo e toma uma decisão assim que houver evidência suficiente.

Cada nova observação aumenta ou diminui a confiança de que o sistema está anômalo. O teste compara continuamente dois cenários:

- H_0: o sistema está normal;
- H_1: o sistema apresenta comportamento anômalo.

Se a evidência acumulada ultrapassar um limite superior, o modelo entende que há fortes indícios de anomalia. Se cair abaixo de um limite inferior, conclui-se que o sistema está dentro do comportamento esperado. Enquanto estiver entre os dois limites, o monitoramento continua aguardando mais informações.

Esse processo torna o modelo mais rápido e confiável, pois as decisões são tomadas apenas quando há evidências estatísticas suficientes, reduzindo falsos alarmes e detectando anomalias reais com antecedência.

3.6 Integração operacional e implementação

A metodologia foi implementada em linguagem Python, integrando módulos para leitura dos arquivos *CSV*, cálculo do *z-score*, modelagem com *MSET* e decisão com *SPRT*. O funcionamento geral do algoritmo pode ser resumido da seguinte forma:

- Leitura dos dados de latência e transações negadas exportados do OpenSearch e Zabbix;
- Padronização das séries temporais visando eliminar diferenças de escala;
- Dividir os dados em períodos de treinamento (construção da memória do *MSET* indicando comportamento normal) e monitoramento;
- Aplicação do *MSET* para estimar o comportamento esperado de cada métrica;
- Cálculo do erro de predição (*SPE*) e as pressões de latência e negadas;
- Envio dos resultados ao *SPRT*, que decide se há anomalia ou não.

A metodologia *MSET-SPRT* proposta constitui um modelo híbrido de monitoramento estatístico capaz de operar em tempo quase real, com alta interpretabilidade e baixo custo

computacional. Sua modularidade permite integração a diferentes plataformas de monitoramento e adaptação a novos conjuntos de métricas.

4 RESULTADOS E DISCUSSÃO

4.1 Análise com dados extraídos do Opensearch e Zabbix em condições normais de operação

Nesta etapa foram utilizados dados reais extraídos do OpenSearch e Zabbix, correspondentes ao comportamento normal de operação do sistema, sem a presença de anomalias. Esses registros refletem o desempenho típico das aplicações monitoradas em ambiente de produção, representando um cenário de estabilidade operacional.

O objetivo dessa análise inicial é estabelecer uma linha de base estatística (baseline) que descreve o comportamento esperado dos tempos de resposta e número de transações negadas sob condições normais. Essa caracterização é fundamental para as etapas subsequentes de detecção de anomalias, pois permite comparar variações futuras e identificar desvios significativos em relação ao padrão histórico.

Os dados extraídos apresentaram baixa variabilidade nos tempos de resposta e valores médios consistentes, indicando regularidade no desempenho do sistema e servindo como referência confiável para a modelagem estatística e aplicação de métodos de detecção.

A Tabela 1 apresenta as principais medidas estatísticas calculadas para o campo *response_time*, obtidas a partir do conjunto de dados extraídos do OpenSearch. Observa-se que os tempos de resposta apresentam média de aproximadamente 225 ms, com baixa variabilidade (desvio-padrão próximo de 8 ms e variância de cerca de 63).

Tabela 1 – Estatísticas do tempo de resposta dos dados extraídos do OpenSearch

Métrica	**Valor**
Quantidade de registros	60.480
Média	225,03 ms
Desvio-padrão	7,99 ms
Variância	63,86
Mínimo	194,29 ms
Máximo	258,48 ms

Fonte: elaboração própria

Esses resultados indicam um comportamento altamente estável e previsível do sistema monitorado, com valores concentrados em torno da média e ausência de picos ou anomalias

significativas. O valor mínimo (aproximadamente 194 ms) e máximo (aproximadamente 258 ms) demonstram uma amplitude reduzida, o que reforça a consistência do desempenho temporal nas amostras analisadas.

Essa estabilidade é essencial para ambientes de produção e monitoramento bancário, pois garante que o tempo de resposta das aplicações permaneça dentro de parâmetros aceitáveis de desempenho, facilitando a detecção de desvios em análises comparativas futuras.

4.2 Análise estatística das transações aprovadas e negadas

Nesta subseção foram utilizados dados reais extraídos do Zabbix, referentes à quantidade de transações aprovadas e negadas registradas durante o período de monitoramento do sistema. Esses dados refletem o comportamento operacional do ambiente em condições normais, sem a ocorrência de incidentes significativos ou degradação perceptível de desempenho.

O objetivo dessa análise é caracterizar estatisticamente o padrão de comportamento das transações, permitindo a construção de uma linha de base (*baseline*) de referência para comparações futuras e detecção de anomalias.

A Tabela 2 apresenta os principais dados estatísticos obtidos a partir dos campos aprovadas e negadas, incluindo medidas de tendência central, dispersão e amplitude. Esses valores evidenciam a estabilidade do processo de transações, com taxas mínimas de negação e uma distribuição regular de aprovações ao longo do tempo.

Tabela 2 – Estatísticas de transações negadas e aprovadas dos dados extraídos do Zabbix

Métrica	**Negadas**	**Aprovadas**
Quantidade de registros	50.400	50.400
Média	0,48	47,89
Desvio-padrão	0,72	16,65
Variância	0,71	277,13
Mínimo	0	10
Máximo	5	106

Fonte: elaboração própria

4.3 Parâmetros utilizados no *MSET* e *SPRT*

Para a etapa de detecção estatística de anomalias, foram empregados parâmetros manualmente ajustados de forma experimental com base nos testes realizados sobre os dados extraídos do ambiente de monitoramento. Os principais parâmetros utilizados foram *TRAIN_RATIO, ALPHA, BETA e K_SIGMA*, descritos a seguir.

- *TRAIN_RATIO* = 0.8: define a proporção de dados utilizada para o treinamento do modelo *MSET*. Nesse caso, 80% das amostras iniciais foram empregadas para a criação do conjunto de referência que representa o comportamento normal do sistema. Os 20% restantes foram usados na fase de teste e validação;
- *ALPHA* = 1×10^{-10}: representa a taxa de erro tipo I (falso positivo) adotada no SPRT. Valores muito baixos de α tornam o teste mais conservador, reduzindo a probabilidade de sinalizar falsos alarmes. O valor 1×10^{-10} foi escolhido para garantir alta confiabilidade na detecção, o que permitiu que apenas desvios estatisticamente significativos em relação ao comportamento normal fossem considerados como potenciais anomalias;
- *BETA* = 0.05: corresponde à taxa de erro tipo II (falso negativo), isto é, a probabilidade de não detectar uma anomalia real. O valor 0,05 reflete um compromisso entre sensibilidade (detectar desvios reais) e especificidade (evitar alarmes falsos). Essa configuração permitiu que o sistema mantivesse boa capacidade de detecção sem se tornar excessivamente sensível a variações pequenas ou ruído operacional;
- *K_SIGMA* = 1.5: define o número de desvios-padrão (σ) utilizados como limiar para o cálculo do erro quadrático de previsão *(SPE)* no *MSET*. Este parâmetro determina a fronteira que separa variações normais de possíveis desvios anômalos.

4.4 Desempenho do *MSET*

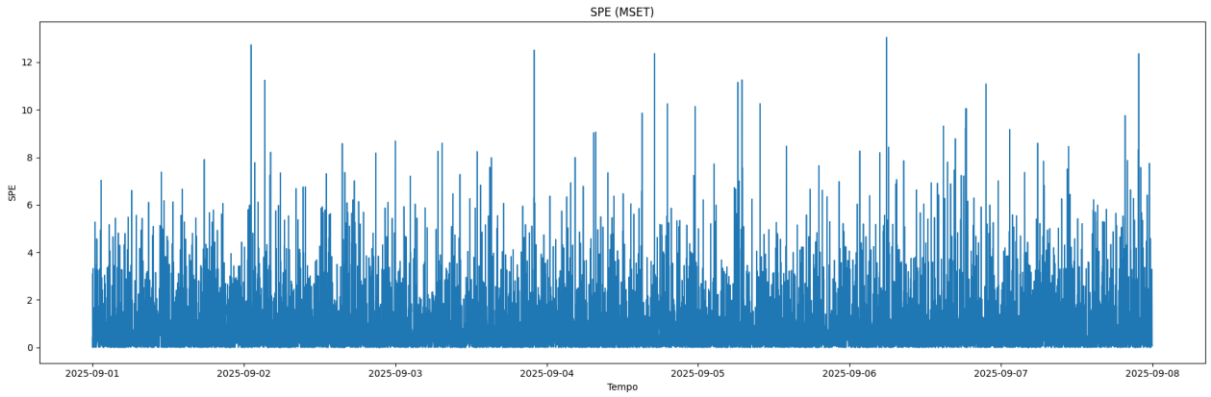
O modelo *MSET* mostrou-se eficiente na caracterização do comportamento normal das métricas monitoradas. Durante o período de treinamento, o algoritmo construiu uma memória representativa com base em correlações históricas entre as variáveis de latência e transações negadas. Ao longo do período de monitoramento, o *MSET* foi capaz de reconstruir os valores esperados com baixo erro médio, indicando alta estabilidade do modelo.

Os valores de *SPE (Squared Prediction Error)* apresentaram oscilações compatíveis com pequenas variações normais do sistema, mas sem ultrapassar os limiares definidos em períodos de estabilidade.

Quando ocorreram picos isolados ou simultâneos de latência e aumento de transações negadas, observou-se um aumento significativo no *SPE*, evidenciando a sensibilidade do modelo à degradação multivariada do serviço.

A Figura 2 apresenta a evolução temporal do erro quadrático de previsão *(SPE)* obtido a partir do modelo *MSET* aplicado sobre os dados de tempo de resposta e transações do sistema. O *SPE* representa a diferença entre o valor estimado pelo modelo e o valor real observado, funcionando como um indicador estatístico de desvio em relação ao comportamento esperado.

Figura 2 – Evolução do erro quadrático de predição *(SPE)* gerado pelo modelo *MSET*



Fonte: elaboração própria

Observa-se que os valores de *SPE* se mantêm baixos e estáveis ao longo de todo o período, indicando que o sistema operou dentro de condições normais e compatíveis com o padrão aprendido durante a fase de treinamento. Os picos ocasionais presentes no gráfico não configuram anomalias, mas refletem flutuações naturais de operação, inerentes a variações momentâneas de carga e resposta das aplicações monitoradas.

A configuração dos parâmetros adotados (*TRAIN_RATIO* = 0.8, *ALPHA* = 1×10^{-10}, *BETA* = 0.05 e *K_SIGMA* = 1.5) contribuiu diretamente para a suavização do *SPE* e para a redução de falsos positivos no processo de detecção. Esses ajustes permitiram um equilíbrio adequado entre sensibilidade (capacidade de detectar desvios reais) e robustez (tolerância a pequenas variações operacionais), resultando em um comportamento estável e consistente do modelo.

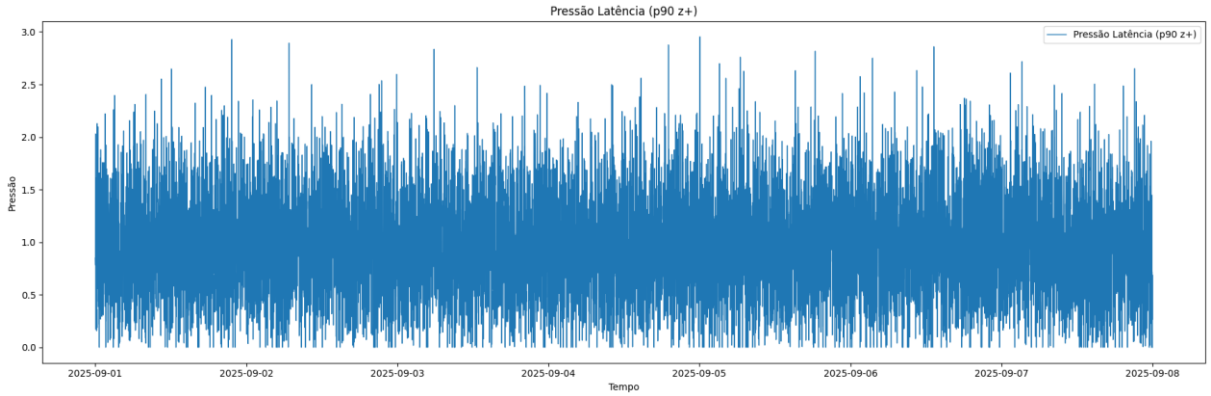
O limite superior do gráfico (aproximadamente doze) é relativo ao comportamento estatístico do conjunto de treinamento. O modelo *MSET* aprende a variabilidade típica do sistema e define implicitamente uma faixa esperada de valores para o *SPE*. Assim, picos que se aproximam de doze representam instantes em que o erro de reconstrução foi maior, mas ainda dentro da faixa normal de operação.

4.5 Análise das pressões de latência e transações negadas

As pressões de latência e transações negadas foram fundamentais para complementar a interpretação dos resultados do *MSET*. A pressão de latência reflete a distância entre o tempo de resposta atual e o tempo médio histórico, permitindo identificar tendências de degradação antes que o desempenho caia significativamente. Já a pressão de transações negadas expressa a elevação da taxa de falhas em relação à operação normal.

A Figura 3 apresenta o comportamento temporal da pressão de latência, métrica calculada a partir do percentil noventa dos tempos de resposta normalizados. Essa métrica representa a tendência superior de latência das requisições em cada intervalo, sendo particularmente útil para identificar variações de desempenho que possam impactar a experiência do usuário.

Figura 3 – Pressão de Latência



Fonte: elaboração própria

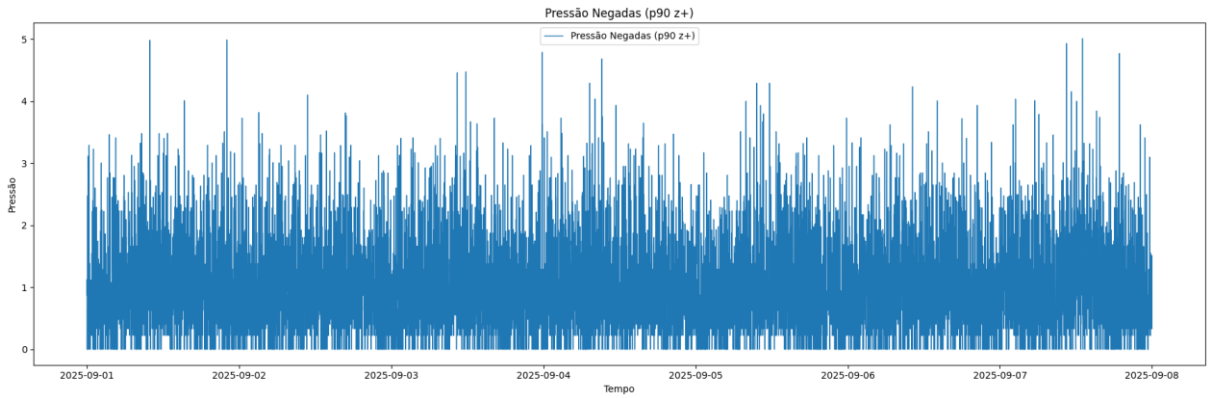
Observa-se que os valores de pressão de latência se mantêm predominantemente entre zero e três unidades normalizadas, com oscilações regulares e ausência de picos abruptos. Esse padrão indica um comportamento estável do sistema, com variações dentro dos limites esperados para o período monitorado.

Os picos eventuais presentes no gráfico refletem flutuações transitórias da carga de trabalho ou momentos de aumento pontual na demanda por processamento, por exemplo, sem caracterizar anomalias.

De modo geral, o gráfico demonstra que o sistema manteve latências sob controle e coerentes com o *baseline* operacional.

A Figura 4 apresenta a pressão de transações negadas obtida a partir da aplicação do percentil noventa sobre os valores normalizados pelo método *z-score*. Essa métrica foi utilizada para identificar eventuais elevações na taxa de negação de transações, destacando os momentos de maior pressão operacional.

Figura 4 – Pressão de Negadas



Fonte: elaboração própria

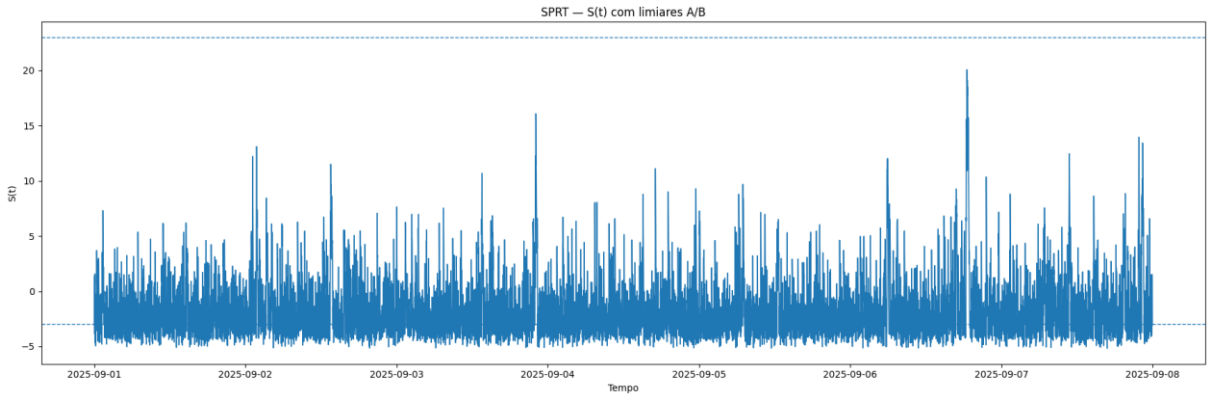
Observa-se que os valores se distribuem predominantemente entre zero e cinco unidades normalizadas, com oscilações regulares e alguns picos pontuais ao longo do período analisado. Essa escala é resultado do processo de normalização estatística (*z-score*), em que cada valor é transformado de acordo com a média e o desvio-padrão do conjunto de dados. Assim, valores próximos de zero representam períodos em que o número de transações negadas esteve alinhado à média histórica, enquanto valores mais altos indicam desvios positivos, correspondentes a momentos em que o número de negações superou o padrão esperado. Os picos próximos de cinco decorrem de flutuações transitórias e não configuram anomalias.

4.6 Desempenho do *SPRT*

A Figura 5 ilustra o comportamento da estatística sequencial S(t) obtida por meio da aplicação do *SPRT* sobre os valores do *SPE* gerados pelo modelo *MSET*. O gráfico exibe o

processo contínuo de avaliação da hipótese nula (H_0, condição normal) e da hipótese alternativa (H_1, condição anômala), delimitadas pelos limiares A e B representados pelas linhas tracejadas horizontais.

Figura 5 – Teste Sequencial de Probabilidade (*SPRT*)



Fonte: elaboração própria

Os resultados indicam que os valores de S(t) oscilaram de forma controlada ao longo do período, permanecendo majoritariamente dentro da faixa compreendida entre os limites A e B. Isso demonstra que o sistema operou sob condições de normalidade estatística, sem evidências de desvios significativos em relação ao padrão aprendido na fase de treinamento.

Os picos observados no gráfico correspondem a momentos de variação mais acentuada, porém, mesmo nessas ocorrências, os valores de S(t) não ultrapassaram os limiares de decisão, o que confirma a eficácia da configuração adotada, em especial dos parâmetros $ALPHA = 1\times10^{-10}$ e $BETA = 0.05$, que proporcionaram um equilíbrio adequado entre sensibilidade e robustez.

O comportamento de S(t) evidencia que o *SPRT* atuou de forma estável e confiável, filtrando variações não relevantes e mantendo o processo decisório livre de falsos alarmes. Essa característica é fundamental para aplicações em monitoramento bancário em tempo real, nas quais a precisão estatística e a consistência operacional são essenciais para distinguir oscilações normais de possíveis anomalias.

4.7 Simulações com situações adversas

A partir deste ponto, foram realizadas simulações utilizando os arquivos de latência e de transações, agora com dados modificados artificialmente para representar situações adversas que podem ocorrer no ambiente operacional de sistemas bancários.

Essas alterações têm o propósito de reproduzir condições reais de instabilidade, como picos de latência e aumento no número de transações negadas. Por meio dessas simulações, busca-se avaliar a capacidade do modelo *MSET-SPRT* em detectar desvios e comportamentos anômalos, demonstrando sua aplicabilidade prática no monitoramento inteligente de sistemas financeiros em produção.

Os dados utilizados nesta simulação foram gerados com o auxílio do ChatGPT, a partir dos arquivos extraídos do Zabbix e OpenSearch que representavam o comportamento normal do sistema, sem presença de anomalias.

Durante as simulações, os parâmetros do modelo não foram alterados, mantendo-se as mesmas configurações utilizadas nas análises anteriores (*TRAIN_RATIO* = 0.8, *ALPHA* = 1×10^{-10}, *BETA* = 0.05 e *K_SIGMA* = 1.5).

A decisão de preservar esses valores teve como objetivo verificar a eficiência do algoritmo *MSET-SPRT* sob diferentes condições operacionais, garantindo que os resultados obtidos fossem decorrentes exclusivamente das variações introduzidas nos dados (latência e transações negadas) e não de ajustes nos parâmetros do modelo.

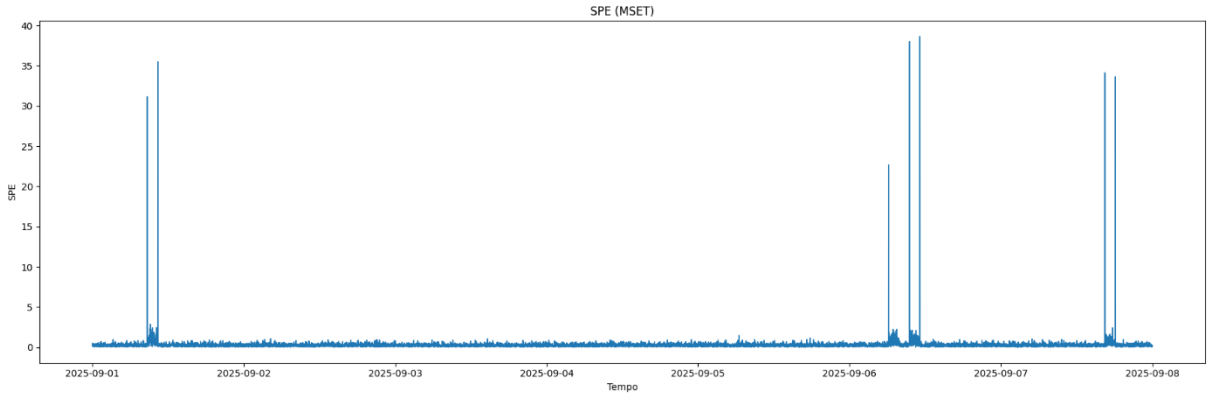
4.7.1 Simulação de picos de latência

Nesta simulação, foram inseridos picos artificiais de latência nos dados originalmente extraídos do OpenSearch, que representavam o comportamento normal do sistema. O objetivo foi reproduzir situações de degradação temporária de desempenho, comuns em ambientes bancários, como sobrecarga momentânea de rede, lentidão de serviços externos ou alta concorrência de requisições.

Durante os intervalos de pico, os valores de tempo de resposta foram aumentados em aproximadamente 80% por períodos curtos e controlados, permitindo avaliar a sensibilidade do modelo *MSET-SPRT* em identificar variações abruptas de latência sem comprometer a estabilidade geral da detecção.

A Figura 6 apresenta o comportamento do *SPE* após a introdução de picos artificiais de latência nos dados originais. Observa-se que, durante os períodos em que os picos foram aplicados, o *SPE* apresentou elevações abruptas e bem delimitadas, refletindo com precisão os momentos de degradação simulada no sistema.

Figura 6 – Erro quadrático de predição *(SPE)* com picos de latência



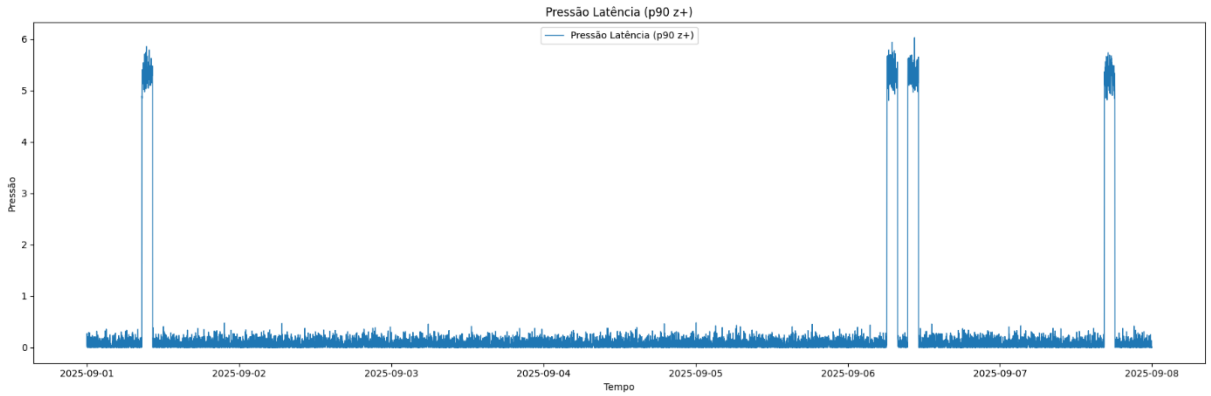
Fonte: elaboração própria

Fora dessas janelas, o *SPE* manteve-se em níveis baixos e estáveis, o que demonstra a capacidade do modelo *MSET* de diferenciar variações normais de anomalias reais. Os picos mais altos, alcançando valores próximos a trinta e cinco, correspondem exatamente aos intervalos em que a latência foi amplificada em 80%, evidenciando a sensibilidade do método à variação repentina de desempenho.

Esse resultado confirma que o modelo foi capaz de detectar com clareza as alterações simuladas, mantendo comportamento consistente nas demais regiões da série, sem geração de falsos alarmes.

A Figura 7 evidencia claramente os períodos de pico de latência inseridos artificialmente na série temporal. Nesses intervalos, observa-se um aumento expressivo da pressão (valores acima de cinco unidades normalizadas), correspondendo aos momentos de sobrecarga simulada no sistema. Fora dessas janelas, a métrica manteve-se estável e próxima de zero, o que demonstra a coerência dos dados e a eficiência do processo de simulação.

Figura 7 – Pressão de Latência com inserção de picos simulados

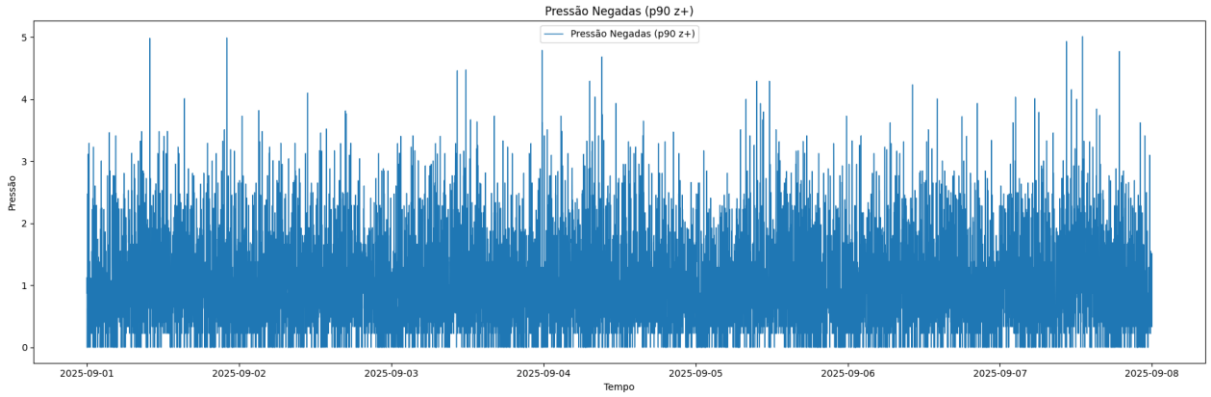


Fonte: elaboração própria

Esses resultados confirmam que o método de geração de picos foi eficaz em representar situações transitórias de degradação de desempenho, sem comprometer o comportamento estatístico do restante da série.

O gráfico de pressão de negadas apresenta o comportamento original dos dados extraídos do Zabbix, sem qualquer modificação ou inserção de anomalias, conforme mostra a Figura 8. A manutenção dessa série sem alterações teve como objetivo servir como linha de base de comparação com os demais experimentos, permitindo avaliar isoladamente o impacto dos picos de latência sobre o modelo de detecção.

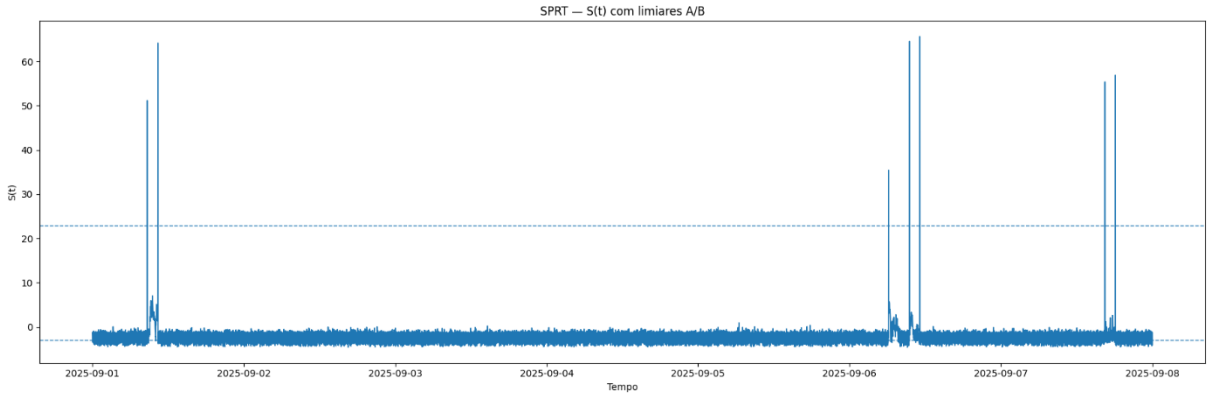
Figura 8 – Pressão de Negadas



Fonte: elaboração própria

A Figura 9 apresenta o resultado do *SPRT* aplicado sobre os dados de latência com picos simulados. Observa-se que, durante os períodos em que foram inseridas anomalias, o valor da estatística S(t) ultrapassou o limiar superior (A), caracterizando a detecção de eventos anômalos pelo modelo. Fora desses intervalos, os valores permaneceram abaixo dos limiares, indicando estabilidade e comportamento normal do sistema.

Figura 9 – *SPRT*: Identificação de Anomalias com Limiares A/B

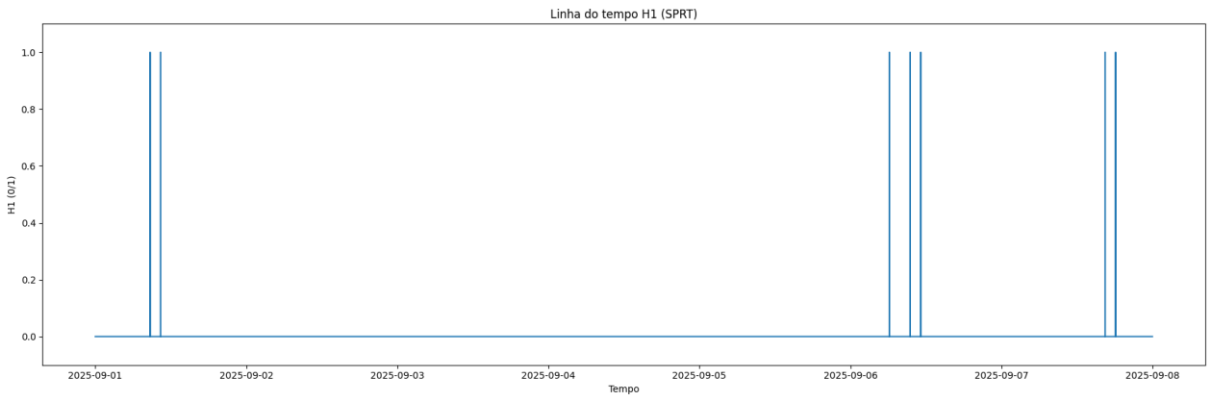


Fonte: elaboração própria

O comportamento observado confirma que o algoritmo é capaz de identificar de forma precisa e imediata picos de latência, mantendo baixo índice de falsos positivos e respondendo coerentemente às variações introduzidas.

A Figura 10 representa o gráfico de linha do tempo H_1 representa o momento exato em que o teste sequencial *SPRT* identificou a presença de anomalias nos dados de latência. Cada marcação em valor "1" no eixo vertical indica um instante em que a hipótese alternativa (H_1) foi aceita, ou seja, quando o algoritmo detectou uma mudança significativa no comportamento do sistema em relação ao padrão normal.

Figura 10 – Linha do Tempo H_1 (SPRT)



Fonte: elaboração própria

Observa-se que as ativações de H_1 coincidem com os mesmos períodos de picos de latência visualizados nos gráficos de *SPE* e *SPRT* com limiares A/B, confirmando a consistência e precisão da detecção. Fora desses intervalos, o valor permanece em zero, demonstrando que o modelo manteve a hipótese nula (H_0) e não identificou desvios anômalos.

Esse resultado reforça a eficácia do modelo *MSET-SPRT* em identificar pontualmente anomalias reais, evitando falsos alarmes e garantindo a confiabilidade necessária para aplicações em sistemas de monitoramento bancário em tempo real.

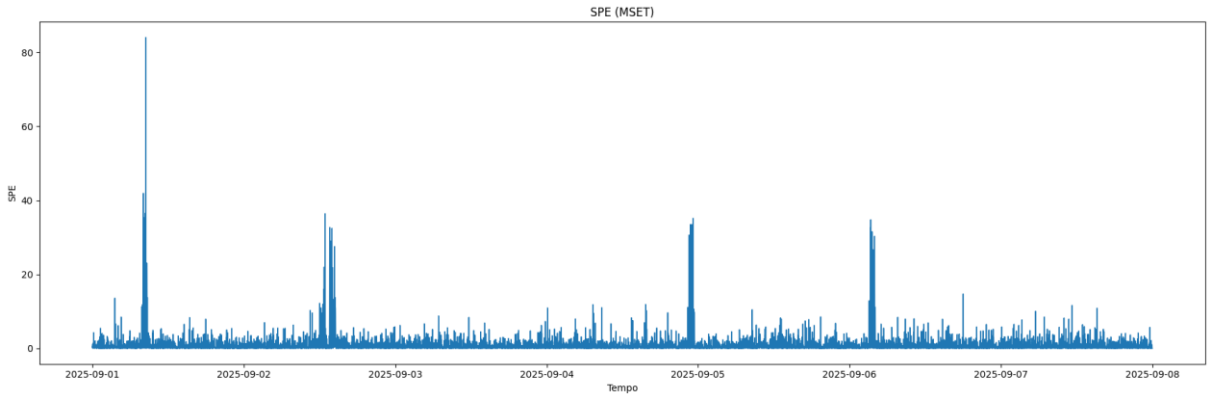
4.7.2 Simulação de picos de transações negadas

Nesta simulação, foram inseridos picos artificiais na quantidade de transações negadas, com o objetivo de reproduzir situações momentâneas de instabilidade nos sistemas bancários. Os dados originais, extraídos do Zabbix, foram modificados de forma controlada, aumentando o número de negações em curtos intervalos de tempo.

Esses picos simulam falhas temporárias em serviços internos e externos, lentidão de processamento ou bloqueios de regras de segurança, permitindo avaliar a eficiência do modelo *MSET-SPRT* na identificação de anomalias pontuais em séries de eventos transacionais.

A Figura 11 mostra o comportamento do *SPE* após a inserção de picos curtos de transações negadas. É possível observar elevações bem definidas do *SPE* nos intervalos em que os picos foram aplicados, indicando que o modelo detectou corretamente as anomalias simuladas. Fora desses períodos, o erro manteve-se em níveis baixos e estáveis.

Figura 11 – Erro quadrático de predição *(SPE)* com picos de transações negadas

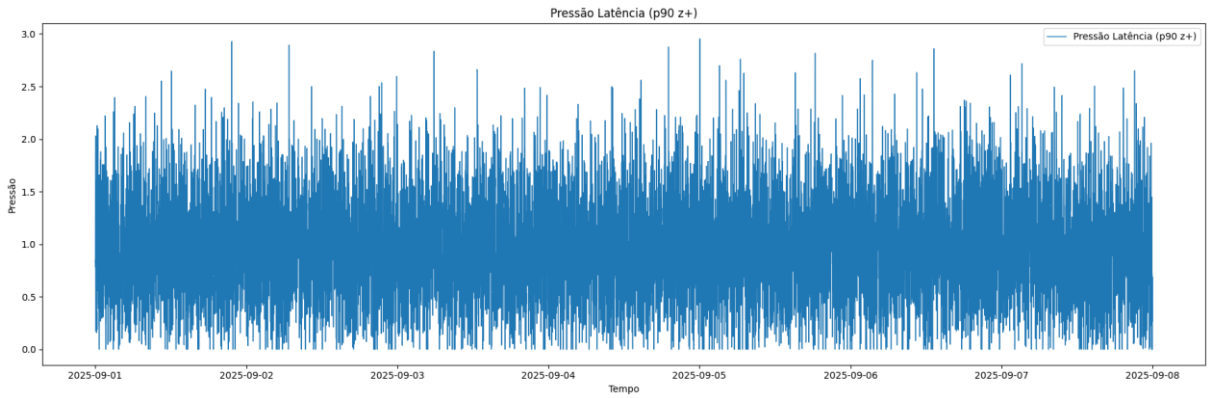


Fonte: elaboração própria

Assim como na simulação de picos de latência, em que o gráfico de pressão de transações negadas não evidenciou alterações, agora o gráfico de pressão de latência apresenta o comportamento original dos dados extraídos do OpenSearch, sem qualquer modificação ou inserção de anomalias. Novamente, a manutenção dessa série sem alterações, conforme mostra

a Figura 12, teve como objetivo servir como linha de base de comparação com os demais experimentos.

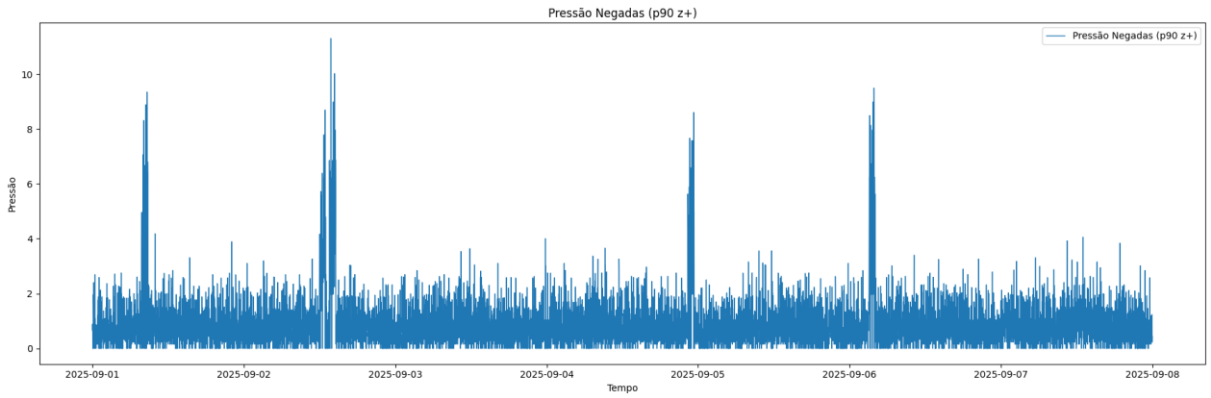
Figura 12 – Pressão de Latência



Fonte: elaboração própria

O gráfico de pressão de transações negadas, conforme a Figura 13, evidencia a ocorrência de picos curtos e bem definidos, resultantes da inserção artificial de aumentos na quantidade de transações negadas. Esses picos representam momentos de instabilidade temporária nos sistemas bancários.

Figura 13 – Pressão de Transações Negadas

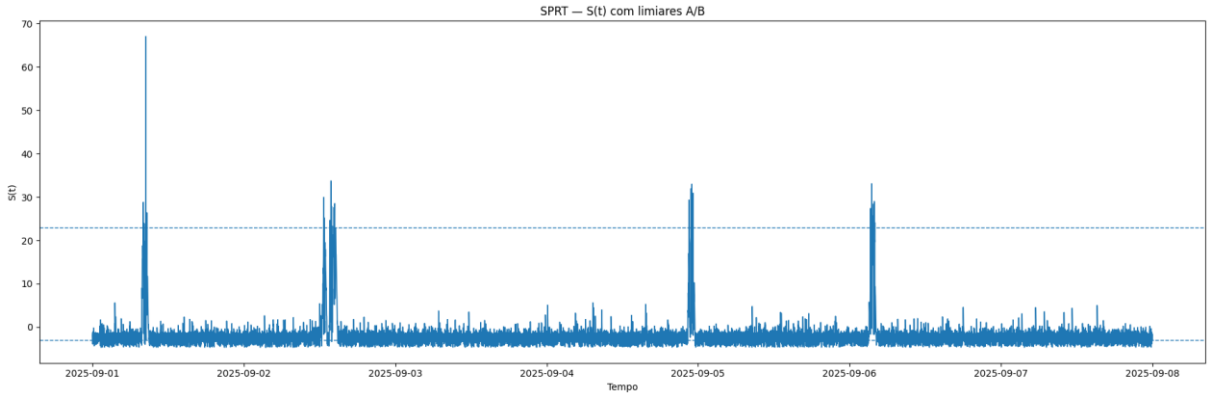


Fonte: elaboração própria

Observa-se que, fora desses períodos, os valores permanecem estáveis e próximos do comportamento normal, o que demonstra que as alterações foram pontuais e bem delimitadas. Esse padrão é coerente com a proposta da simulação, que buscou reproduzir eventos anômalos de curta duração para avaliação da sensibilidade do modelo *MSET-SPRT*.

A Figura 14 apresenta o resultado do *SPRT* aplicado sobre a série com picos de transações negadas. Observa-se que o valor de $S(t)$ ultrapassa o limiar superior (A) em momentos que coincidem com os picos identificados no gráfico de pressão de negadas, caracterizando a detecção de anomalias pelo algoritmo.

Figura 14 – *SPRT* com Identificação das Anomalias

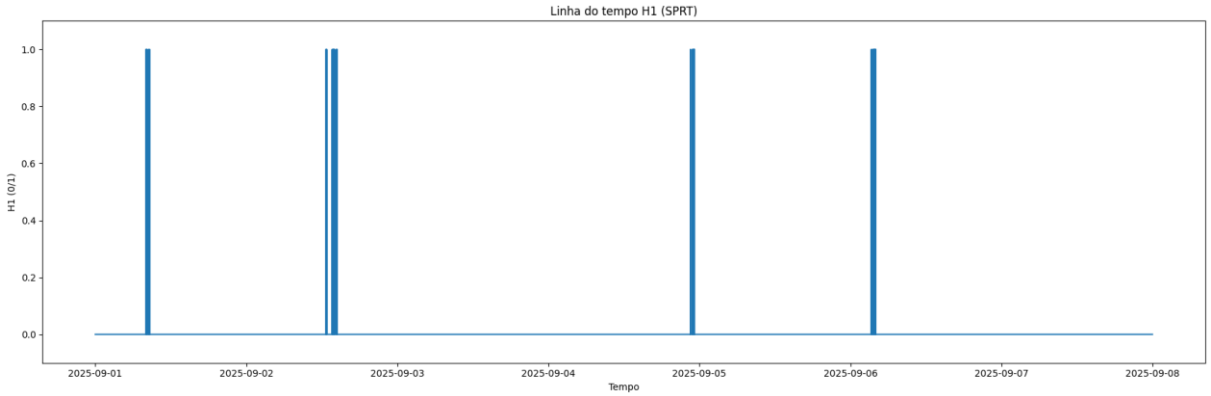


Fonte: elaboração própria

Esses pontos de superação do limiar indicam que o *SPRT* reconheceu corretamente as mudanças abruptas no comportamento da variável, confirmando sua capacidade de distinguir situações normais de eventos anômalos. Fora desses intervalos, o valor de $S(t)$ manteve-se dentro da faixa entre os limites A e B, demonstrando estabilidade e precisão na decisão estatística.

A linha do tempo do H_1 representa os momentos em que o teste sequencial (*SPRT*) identificou evidências suficientes para rejeitar a hipótese nula H_0 e aceitar a hipótese alternativa H_1, indicando a ocorrência de anomalias, conforme a Figura 15.

Figura 15 – Linha do Tempo H_1 (*SPRT*)



Fonte: elaboração própria

4.7.3 Simulação conjunta de picos de latência e de transações negadas

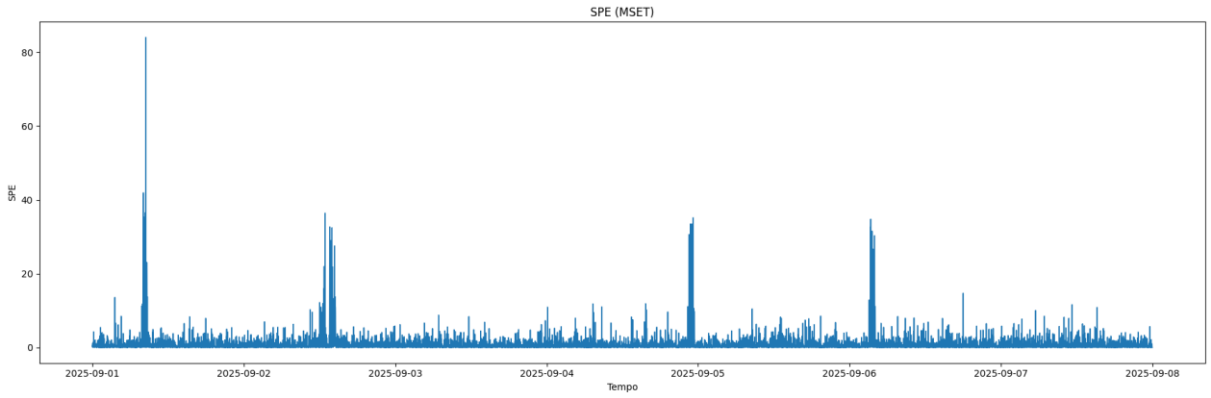
Nesta etapa foi realizada uma simulação em que picos de latência e picos de transações negadas ocorreram tanto de forma simultânea quanto em momentos distintos, representando cenários reais de sobrecarga e instabilidade em sistemas bancários.

Os dados originais foram modificados por meio de multiplicadores aplicados sobre as janelas temporais, reproduzindo variações abruptas semelhantes às que podem ocorrer em situações de alto volume de requisições ou falhas temporárias.

Essa simulação teve como objetivo avaliar a capacidade do modelo *MSET-SPRT* em detectar anomalias correlacionadas, verificando se o método mantém sua sensibilidade mesmo quando múltiplos indicadores sofrem degradação simultânea, além de validar sua precisão na identificação de eventos isolados em cada métrica.

Na Figura 16, observa-se que, durante a maior parte do período, os valores de *SPE* permanecem baixos e estáveis, indicando comportamento normal e previsível do sistema. Entretanto, surgem picos bem definidos em momentos específicos, que correspondem às janelas simuladas de picos de latência e transações negadas, tanto nas ocorrências simultâneas quanto nas alternadas.

Figura 16 – Erro quadrático de predição (*SPE*) após a inserção de picos de latência e de transações negadas

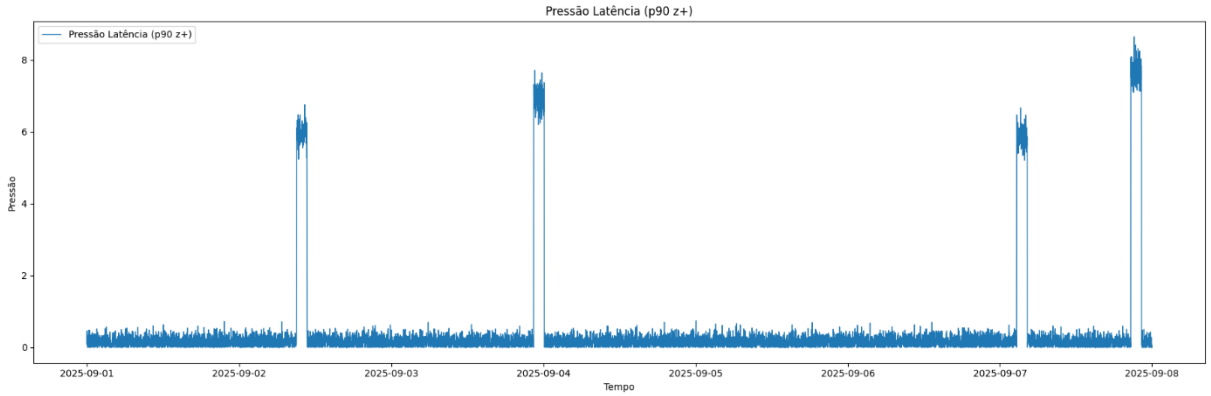


Fonte: elaboração própria

Esses aumentos abruptos do erro de predição evidenciam a sensibilidade do modelo *MSET* na detecção de anomalias conjuntas, demonstrando que o método responde de forma eficaz a desvios significativos do padrão normal de operação, mesmo quando as variações ocorrem em diferentes indicadores de desempenho.

No gráfico de pressão de latência, Figura 17, observam-se picos bem definidos em momentos específicos, que representam os períodos simulados de aumento abrupto na latência.

Figura 17 – Pressão de latência com inserção de picos simulados

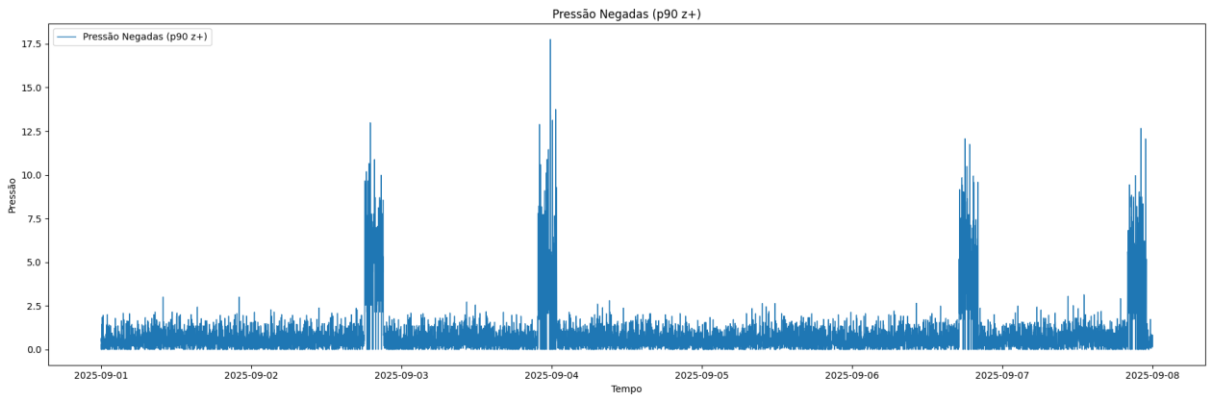


Fonte: elaboração própria

Essas elevações pontuais reforçam o comportamento esperado em situações de alta demanda ou degradação temporária do sistema, demonstrando que o método de simulação foi eficaz em reproduzir condições adversas de desempenho.

Já no gráfico de pressão de transações negadas, Figura 18, é possível observar picos bem definidos em momentos específicos, que representam as janelas de simulação, ocorrendo tanto de forma alternada quanto simultânea em relação aos picos de latência. Esses aumentos indicam períodos em que houve maior incidência de falhas ou rejeições nas transações processadas.

Figura 18 – Pressão de transações negadas

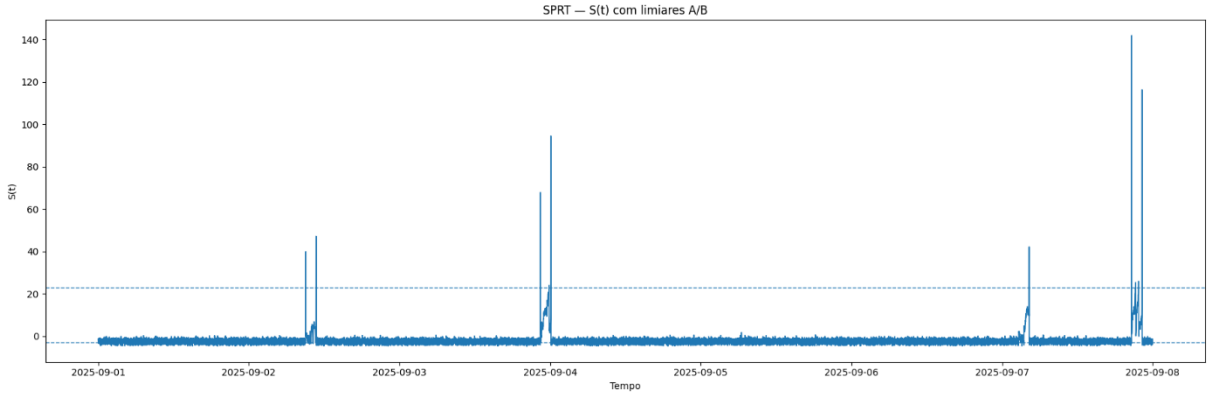


Fonte: elaboração própria

No gráfico *SPRT*, Figura 19, percebe-se que, durante a maior parte do período, o valor de S(t) permanece dentro da faixa delimitada pelos limiares, indicando condições normais de operação. Entretanto, em determinados instantes, assim como nas outras simulações, S(t) ultrapassa o limiar superior (A), caracterizando ocorrências de anomalias. Esses pontos

coincidem com os períodos de picos de latência e transações negadas, simulados tanto de forma conjunta quanto alternada.

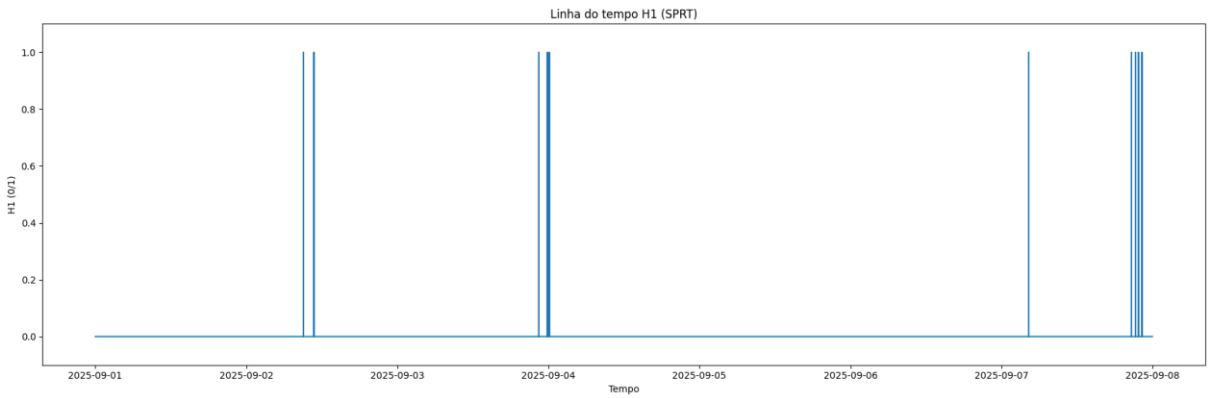
Figura 19 – *SPRT*: Identificação de anomalias com limiares A/B



Fonte: elaboração própria

No gráfico da linha do tempo H_1, Figura 20, nota-se que as detecções ocorrem de maneira concentrada e não contínua, refletindo a precisão e seletividade do método *SPRT*. Isso indica que o modelo é capaz de reagir rapidamente a eventos anômalos, mas sem sinalizar falsos alarmes em períodos estáveis, um aspecto fundamental em aplicações de monitoramento bancário em tempo real, onde a sensibilidade excessiva pode gerar ruído operacional.

Figura 20 – Linha do tempo H_1 (*SPRT*)



Fonte: elaboração própria

4.8 Discussão dos resultados práticos

A análise conjunta dos indicadores *SPE* e *SPRT* revelou uma forte correlação entre os dois mecanismos. O *SPE* atua como indicador contínuo de desvio, enquanto o *SPRT* funciona

como um filtro de decisão, confirmando apenas as anomalias com significância estatística. Essa relação proporciona robustez ao sistema, reduzindo falsos positivos e evitando alarmes baseados em flutuações transitórias.

Nos diversos experimentos simulados, verificou-se que o aumento do *SPE* antecede o cruzamento do limiar do *SPRT*, permitindo prever a ocorrência de anomalias com antecedência. Essa característica é particularmente valiosa em sistemas bancários, onde ações preventivas podem ser tomadas antes da interrupção dos serviços.

Os resultados obtidos indicam que a integração entre *MSET* e *SPRT* é uma abordagem eficaz para detecção precoce de anomalias em ambientes de produção. A principal vantagem observada é a capacidade do modelo em lidar com múltiplas variáveis simultaneamente, correlacionando latência e transações negadas de forma conjunta, o que amplia a precisão da detecção. Outra vantagem é que podem ser utilizadas outras variáveis que não foram utilizadas no experimento deste trabalho como transações com códigos de erros *HTTP*.

Outro ponto relevante é a natureza sequencial do *SPRT*, que possibilita decisões rápidas sem exigir grandes volumes de dados acumulados. Essa característica reduz o tempo médio de detecção, permitindo que o sistema atue quase em tempo real.

4.9 Benefícios e Limitações da Metodologia

Entre os benefícios mais relevantes da metodologia destacam-se:

- Robustez estatística do *MSET*;
- Capacidade do *SPRT* em fornecer decisões rápidas;
- Fácil integração com ferramentas de monitoramento já existentes, como Zabbix e OpenSearch.

Além dessas ferramentas, pode-se utilizar o Grafana para a visualização de gráficos e estados identificados pelos métodos.

A abordagem também apresenta boa interpretabilidade, facilitando a análise por equipes técnicas e de negócios.

Como limitação, observa-se a necessidade de ajuste fino dos parâmetros *ALPHA* e *BETA* do *SPRT*, que controlam os limiares de decisão. Parâmetros muito sensíveis podem aumentar falsos positivos, enquanto parâmetros muito restritivos podem atrasar a detecção de eventos críticos. Além disso, o desempenho do *MSET* pode ser afetado por grandes volumes de dados ou mudanças abruptas na estrutura das métricas monitoradas.

4.10 Perspectivas futuras

Como evolução natural deste trabalho, sugere-se o uso de técnicas de aprendizado de máquina supervisionado e não supervisionado para complementar o processo de detecção de anomalias. Modelos híbridos que combinem *MSET-SPRT* com redes neurais ou algoritmos de clustering podem aprimorar a sensibilidade e a capacidade de adaptação a novos padrões de comportamento.

Outra linha de evolução possível é a implementação de um módulo de automação que execute ações corretivas de forma autônoma, integrando a detecção estatística a políticas de resposta automatizada em incidentes. Esse avanço pode representar um passo importante em direção a um modelo completo de *AIOps (Artificial Intelligence for IT Operations)*.

Além disso, propõe-se a evolução do sistema para operação em tempo real nos ambientes de monitoramento bancário, integrando-se a plataformas como Zabbix, OpenSearch e Grafana. Essa integração permitiria o consumo contínuo de métricas de desempenho e transações diretamente das fontes de monitoramento do banco, aplicando o *MSET-SPRT* de forma dinâmica para identificar anomalias à medida que os dados são gerados.

Com isso, seria possível não apenas detectar desvios instantaneamente, mas também alimentar dashboards interativos e acionar alertas automáticos, contribuindo para a redução do tempo de resposta a incidentes e o fortalecimento da resiliência operacional dos sistemas financeiros.

5 CONCLUSÃO

A integração entre os modelos *MSET* e *SPRT* revelou-se uma estratégia eficaz para a detecção estatística de anomalias em sistemas complexos, notadamente em ambientes de operações bancárias críticas, que exigem alto grau de disponibilidade e confiabilidade. O modelo *MSET* demonstrou notável capacidade de representar o comportamento multivariado normal das métricas monitoradas, explorando as correlações entre variáveis para estimar o estado esperado do sistema. Essa modelagem permitiu identificar desvios sutis, porém significativos, a partir de discrepâncias residuais, proporcionando uma visão mais detalhada e precisa sobre o comportamento dinâmico das aplicações.

Por sua vez, o *SPRT* complementou o processo ao introduzir um mecanismo de decisão sequencial e probabilístico, capaz de avaliar continuamente as observações em relação aos limiares de confiança previamente definidos. Essa característica possibilitou a detecção em tempo real de eventos anômalos, com baixo custo computacional e reduzida quantidade de amostras necessárias para a tomada de decisão. Tal propriedade é essencial em cenários que demandam respostas imediatas e decisões precisas, como os ambientes de tecnologia bancária.

Com base nos experimentos realizados, constatou-se que o modelo híbrido *MSET-SPRT* é capaz de distinguir de maneira clara os períodos de estabilidade e os momentos de perturbação, identificando tanto picos de latência quanto aumentos abruptos nas transações negadas, ocorrendo de forma simultânea ou independente. Os resultados obtidos evidenciam que o modelo é sensível às variações combinadas e alternadas dessas métricas, refletindo com precisão a correlação temporal entre diferentes tipos de falhas no ambiente monitorado. Dessa forma, o método demonstrou potencial como ferramenta de apoio ao monitoramento.

Conclui-se, portanto, que o *MSET-SPRT* constitui uma abordagem estatisticamente consistente e operacionalmente viável para a detecção de anomalias em sistemas de alta criticidade. Sua adoção representa um avanço significativo em direção às práticas de *AIOps (Artificial Intelligence for IT Operations)*, nas quais a análise contínua de métricas, a correlação multicanal e a automação de respostas formam a base de uma infraestrutura autônoma, resiliente e orientada à experiência do usuário.

REFERÊNCIAS

AUGUSTO, Flávia. **Monitoramento da infraestrutura de TI: o que diz sobre o seu ambiente.** 2025. Disponível em: https://www.manageengine.com/br/blog/general/monitoramento-da-infraestrutura-de-ti-o-que-diz-sobre-o-seu-ambiente.html. Acesso em 22/10/2025.

BONINI, M. S.; JUNIOR, W. G. P. **A Importância do Monitoramento de TI**. 2022. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/24877/1/informaticanegocios_2022_1_mateusdossantosbonini_aimportanciadomonitoramentodeti.pdf. Acesso em: 22/03/2025.

BRAEI, M.; WAGNER, S. ***Anomaly Detection in univariate time-series****: a survey on the state-of-the-art*. 2020.

CHANDOLA, V.; BANERJEE, A.; KUMAR, V. ***Anomaly detection****: A survey*. 2009.

CHENG, S.; PECHT, M. ***Multivariate State Estimation Technique for Remaining Useful Life Prediction of Electronic Products***. Disponível em: https://cdn.aaai.org/Symposia/Fall/2007/FS-07-02/FS07-02-004.pdf. Acesso em 23/03/2025.

DELGAD, Zeynep. ***How digitalization impacts financial services companies and their audits.*** 2020. Disponível em: https://www.ey.com/en_gl/insights/assurance/how-digital-transformation-impacts-financial-services-companies-and-their-audits. Acesso em 22/10/2025.

GERDES, Jonas et al. ***A comparative study of Oracle's anomaly detection solution and modern alternatives in time series prognostics***. Proceedings of the 11th International Workshop on Mining and Learning from Time Series (MiLeTS 2025), 2025. Disponível em: https://kdd-milets.github.io/milets2025/papers/MILETS_2025_paper_9.pdf. Acesso em: 26/10/ 2025.

JOBS, Steve. **Discurso de formatura na Universidade de Stanford**. 2005. Disponível em: https://news.stanford.edu/2005/06/14/jobs-061505. Acesso em: 19/10/2025.

KHAIRI, M. et al. ***A review of anomaly detection techniques and distributed denial of service (DDoS) on software defined network (SDN)***. 2018.

MEHROTRA, K. G.; MOHAN, C. K.; HUANG, H. ***Anomaly Detection Principles and Algorithms***. 2017. Doi: https://doi.org/10.1007/978-3-319-67526-8.

ORACLE CORPORATION. ***Oracle MSET-SPRT algorithm***. *Oracle Machine Learning for SQL 23c Documentation*. Redwood Shores, CA: Oracle, 2023. Disponível em: https://docs.oracle.com/en/database/oracle/machine-learning/oml4sql/23/dmcon/mset-sprt.html. Acesso em: 26/10/2025.

PENG, Xing et al. ***Anomaly monitoring method for key components of satellite***. Mathematical Problems in Engineering, 2014. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC3920809. Acesso em: 26/10/2025.

SABHARWAL, N.; BHARDWAJ, G. ***Hands-on AIOps:*** *Best Practices Guide to Implementing AIOps*. 2022. Doi: https://doi.org/10.1007/978-1-4842-8267-0.

THEISSLER, A. et al. ***Predictive maintenance enabled by machine learning****: Use cases and challenges in the automotive industry, Reliability Engineering and System Safety*. 2021. Doi: https://doi.org/10.1016/j.ress.2021.107864.

YAN, Jie et al. ***Anomaly Detection of Aviation Bus Based on MSET-MOEA/D***. SSRN Electronic Journal, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203536. Acesso em: 08/10/2025.

ZAVALJEVSKI, N.; GROSS, K. ***Uncertainty Analysis for Multivariate State Estimation in Safety-Critical and Mission-Critical Maintenance Applications***. Argonne National Laboratory, 2000. Disponível em: https://digital.library.unt.edu/ark:/67531/metadc708750/. Acesso em: 08/10/2025.