

Moving Target Defense em Nuvem: Segurança Dinâmica e seus Efeitos no Envelhecimento de Software

Emerson Felipe da Silva¹, Ivson Galdino Borges², Gustavo Callou¹

¹Departamento de Computação
Universidade Federal Rural de Pernambuco (UFRPE)
Recife – PE – Brazil

²Centro de Informática
Universidade Federal de Pernambuco (UFPE)
Recife – PE – Brazil

{emerson.felipesilva, gustavo.callou}@ufrpe.br, igb@cin.ufpe.br

Abstract. *Moving Target Defense (MTD) is a proactive information security strategy aimed at increasing the resilience of computational systems by introducing dynamism and unpredictability into the attack surface. In cloud computing environments, a common implementation approach consists of the dynamic migration of virtual machines across physical hosts, contributing to reduced exposure to threats and improved service availability. However, the continuous application of such mechanisms may impact system operational behavior, potentially triggering the phenomenon known as software aging. In this context, this paper investigates the interaction between MTD strategies and software aging in a private cloud environment based on the Apache CloudStack platform. The adopted methodology involves a controlled experiment with continuous virtual machine migration over a 24-hour period, combined with monitoring of CPU, memory, and disk usage metrics, followed by statistical validation using the Mann-Kendall test and Sen's slope estimator. The results reveal statistically significant increasing trends in resource consumption, indicating progressive system degradation and characterizing software aging. Furthermore, the findings demonstrate that, although MTD enhances security, its continuous application introduces operational overhead, impacting system reliability and availability. As a contribution, this work highlights the trade-off between security and operational stability, emphasizing the need to integrate proactive defense mechanisms with mitigation strategies, such as software rejuvenation.*

Resumo. *O Moving Target Defense (MTD) é uma estratégia proativa de segurança da informação que visa aumentar a resiliência de sistemas computacionais por meio da introdução de dinamismo e imprevisibilidade na superfície de ataque. Em ambientes de computação em nuvem, uma abordagem comum para sua implementação consiste na migração dinâmica de máquinas virtuais entre hospedeiros físicos, contribuindo para a redução da exposição a ameaças e para o aumento da disponibilidade dos serviços. Entretanto, a aplicação contínua desses mecanismos pode impactar o comportamento operacional do sistema, desencadeando o fenômeno de envelhecimento de software. Neste contexto, este artigo investiga a interação entre estratégias de MTD e o*

envelhecimento de software em um ambiente de nuvem privada baseado na plataforma Apache CloudStack. A metodologia adotada envolve a execução de um experimento controlado com migração contínua de máquinas virtuais durante 24 horas, aliado ao monitoramento de métricas de CPU, memória RAM e uso de disco, seguido de validação estatística por meio do teste de Mann-Kendall e do estimador de inclinação de Sen. Os resultados evidenciam tendências estatisticamente significativas de aumento no consumo de recursos, indicando degradação progressiva do sistema e caracterizando o envelhecimento de software. Além disso, os achados demonstram que, embora o MTD contribua para o fortalecimento da segurança, sua aplicação contínua introduz overhead operacional, impactando a confiabilidade e a disponibilidade dos serviços. Como contribuição, este trabalho evidencia o trade-off entre segurança e estabilidade operacional, destacando a necessidade de integração entre mecanismos de defesa proativa e estratégias de mitigação, como o rejuvenescimento de software.

1. Introdução

A Computação em Nuvem redefiniu a forma como serviços computacionais são provisionados e consumidos. Por meio da virtualização de recursos sob demanda, esse modelo viabiliza escalabilidade dinâmica, elasticidade e alta disponibilidade de serviços acessíveis via rede.

Entretanto, a crescente dependência de infraestruturas em nuvem introduz desafios significativos relacionados à confiabilidade, segurança e disponibilidade dos serviços [Callou and Vieira 2024]. Além desses aspectos tradicionalmente analisados, como desempenho e continuidade operacional, destaca-se um fator frequentemente negligenciado, porém crítico em sistemas de longa duração: O envelhecimento de software. Esse fenômeno refere-se à degradação progressiva do desempenho e ao aumento da taxa de falhas ao longo do tempo, decorrente do acúmulo de erros internos, vazamentos de memória e exaustão de recursos do sistema. Em ambientes de computação em nuvem, onde serviços operam continuamente e com alta demanda, a compreensão e mitigação do envelhecimento de software tornam-se fundamentais para garantir a estabilidade, a confiabilidade e a disponibilidade dos serviços. Tal fenômeno tem sido observado em diferentes arquiteturas, incluindo ambientes baseados em OpenStack [Melo et al. 2017], cujo estudo identifica empiricamente a degradação de componentes críticos da infraestrutura de nuvem, evidenciando o impacto do envelhecimento no consumo de recursos e na estabilidade do sistema. Resultados semelhantes também foram verificados em sistemas de bancos de dados [Couto et al. 2023] e em plataformas modernas de contêineres, como o Docker [Vinícius et al. 2022].

O envelhecimento de software manifesta-se por meio de sintomas como vazamentos de memória, esgotamento de recursos do sistema operacional, fragmentação de dados e acúmulo de erros internos, podendo resultar em degradação de desempenho, indisponibilidade de serviços e até corrupção de dados. Embora inicialmente associado a falhas de projeto, atualmente compreende-se que esse fenômeno é intrínseco a sistemas que operam continuamente. Em ambientes de computação em nuvem, onde a disponibilidade e a continuidade do serviço são requisitos fundamentais, torna-se essencial a adoção de estratégias eficazes de mitigação que também considerem aspectos de segurança operacional.

Nesse cenário, a técnica de MTD surge como uma abordagem promissora no campo da segurança da informação. O MTD baseia-se na modificação contínua e dinâmica de parâmetros do sistema, como endereços IP, portas de comunicação, instâncias de serviços e posicionamento de máquinas virtuais, com o objetivo de reduzir a previsibilidade do ambiente e, conseqüentemente, a superfície de ataque. Ao dificultar atividades de reconhecimento e exploração por parte de agentes maliciosos, o MTD contribui não apenas para o aumento da segurança, mas também para a preservação da disponibilidade e da confiabilidade dos serviços, aspectos críticos em infraestruturas de nuvem.

Além de seu papel na mitigação de ameaças cibernéticas, a aplicação do MTD pode influenciar diretamente o comportamento operacional do sistema, impactando métricas de desempenho e potencialmente interagindo com o fenômeno de envelhecimento de software. Dessa forma, torna-se relevante investigar não apenas os benefícios do MTD sob a perspectiva de segurança, mas também seus efeitos sobre a estabilidade e o consumo de recursos em ambientes de execução contínua.

Diante disso, este artigo apresenta um estudo investigativo sobre a aplicação da técnica de MTD [Matheus Torquato 2020] em um ambiente de computação em nuvem baseado na plataforma Apache CloudStack, com foco na análise integrada entre segurança e envelhecimento de software. Para tanto, foi adotada uma abordagem experimental, visando monitorar o comportamento do sistema ao longo do tempo e avaliar como a introdução de mecanismos dinâmicos de defesa impacta o consumo de recursos, a degradação de desempenho e a ocorrência de falhas em sistemas de longa duração.

Com base no exposto, este trabalho apresenta as seguintes contribuições principais:

- Propõe uma análise integrada entre segurança e envelhecimento de software em ambientes de computação em nuvem, explorando a aplicação da técnica de MTD sob a perspectiva de confiabilidade e disponibilidade;
- Desenvolve um ambiente experimental controlado baseado na plataforma Apache CloudStack, capaz de simular a aplicação contínua de estratégias de MTD por meio da migração dinâmica de máquinas virtuais;
- Avalia o impacto do MTD no consumo de recursos computacionais (CPU, memória RAM e uso de disco), identificando padrões associados ao envelhecimento de software;
- Aplica métodos estatísticos, como o teste de Mann-Kendall e o estimador de Sen, para validar quantitativamente as tendências de degradação observadas;
- Evidencia o trade-off entre segurança e estabilidade operacional, demonstrando que a aplicação contínua do MTD pode introduzir overhead e influenciar a confiabilidade e disponibilidade do sistema.

O artigo está estruturado da seguinte forma. A Seção 2 apresenta e discute os principais trabalhos da literatura sobre envelhecimento de software e estratégias de segurança em ambientes de computação em nuvem, destacando lacunas existentes. A Seção 3 descreve os conceitos fundamentais relacionados à análise de séries temporais e aos métodos de detecção de tendências, fornecendo a base teórica para a análise dos dados experimentais. A Seção 4 detalha o ambiente experimental, os recursos utilizados e os procedimentos adotados para a implementação da estratégia de MTD e coleta de métricas. A Seção

5 apresenta os estudos de caso realizados, bem como a análise dos resultados obtidos, incluindo a validação estatística das tendências observadas. Por fim, a Seção 6 sintetiza os principais achados do trabalho, discute suas implicações e aponta direções para pesquisas futuras.

2. Trabalhos Relacionados

A literatura tem investigado o envelhecimento de software como um fator crítico para a confiabilidade, disponibilidade e manutenibilidade de sistemas, especialmente em ambientes de execução contínua e infraestruturas críticas, como nuvem e servidores. Além de degradar o desempenho, esse fenômeno pode comprometer a segurança operacional, ao aumentar a suscetibilidade a falhas e vulnerabilidades. Nesse contexto, diferentes estudos analisam suas causas, métricas e estratégias de mitigação, com destaque para abordagens experimentais e sua relação com a resiliência dos sistemas.

De forma geral, as pesquisas se dividem em abordagens baseadas em medições, que monitoram recursos ao longo do tempo, e abordagens baseadas em modelos matemáticos, como Cadeias de Markov e Redes de Petri, para estimar métricas como o MTTF. Em ambientes de nuvem, o envelhecimento é influenciado por fatores como gestão de memória, fragmentação de recursos e variabilidade de carga. Com a crescente adoção de plataformas como o Apache CloudStack, surgem estratégias de mitigação, como o rejuvenescimento por reinicialização ou migração de máquinas virtuais. No entanto, essas soluções ainda são majoritariamente reativas e pouco exploram aspectos de segurança cibernética.

O estudo apresentado em [Andrade et al. 2021] investiga o envelhecimento de software em sistemas de classificação de imagens, comparando ambientes de nuvem e de borda. Os resultados evidenciam degradação de desempenho e esgotamento de memória, destacando que, sob cargas intensivas, ambientes de nuvem também estão sujeitos a degradações significativas.

Em uma linha distinta, [Oliveira et al. 2020] analisa o fenômeno em ecossistemas baseados em contêineres, evidenciando que a virtualização leve também está sujeita a efeitos cumulativos de degradação. Diferentemente dessas abordagens, o presente trabalho concentra-se em ambientes de virtualização completa, com foco na integração entre envelhecimento de software e mecanismos de segurança.

A metodologia SWARE, proposta em [Torquato et al. 2017], estabelece um arcabouço experimental robusto para caracterização do envelhecimento e validação de estratégias de mitigação. Estruturada em fases de estresse, observação e rejuvenescimento, essa abordagem tem sido amplamente adotada em estudos experimentais. No entanto, tais estratégias são tradicionalmente aplicadas de forma reativa. Neste trabalho, estende-se esse modelo ao incorporar o conceito de MTD, no qual a dinâmica de criação, migração e desativação de instâncias não apenas simula o uso prolongado, mas também atua como mecanismo de defesa proativa. Essa abordagem permite investigar se a dinamicidade introduzida pelo MTD contribui para o rejuvenescimento implícito do sistema ou se, por outro lado, introduz sobrecarga capaz de acelerar o envelhecimento.

Em [Vinícius et al. 2022], é apresentada uma análise do envelhecimento de software na plataforma Docker, com experimentos de longa duração e monitoramento

contínuo. Os resultados indicam crescimento monotônico no consumo de memória, evidenciando degradação sistemática. A relevância desse estudo reside na integração entre análise experimental e modelos preditivos. Em convergência com essa abordagem, o presente trabalho monitora métricas de CPU, memória e disco; contudo, diferencia-se ao inserir a análise no contexto de estratégias de segurança dinâmica, investigando como o MTD influencia padrões de consumo de recursos e estabilidade operacional.

O trabalho de [Couto et al. 2023] investiga o envelhecimento em sistemas de banco de dados PostgreSQL, utilizando testes estatísticos como o de Mann-Kendall para identificar tendências em séries temporais. Os resultados confirmam, com significância estatística, o aumento progressivo no consumo de recursos. De forma similar, [Couto et al. 2024] valida a presença do fenômeno em diferentes sistemas gerenciadores de banco de dados, reforçando a generalidade do envelhecimento de software. A adoção de métodos estatísticos robustos nesses estudos fundamenta a abordagem utilizada neste trabalho, que busca distinguir tendências reais de envelhecimento de flutuações operacionais, garantindo maior confiabilidade às análises.

No contexto de computação em nuvem, [Melo et al. 2017] analisa o envelhecimento na plataforma OpenStack, identificando degradação significativa em componentes críticos. Embora utilize padrões de carga semelhantes aos adotados neste trabalho, sua abordagem não considera mecanismos de defesa cibernética. Assim, o presente estudo avança ao investigar como estratégias de segurança, especificamente o MTD, influenciam a taxa de envelhecimento e a estabilidade do sistema, promovendo uma visão integrada entre segurança e confiabilidade.

Adicionalmente, [Avritzer et al. 2025] propõe modelos matemáticos para definição de políticas ótimas de rejuvenescimento em ambientes virtualizados, distinguindo entre envelhecimento intrínseco e ambiental. Embora forneça contribuições relevantes para otimização operacional, o estudo não aborda a influência de mecanismos de segurança dinâmica. Nesse sentido, o presente trabalho preenche essa lacuna ao introduzir o MTD como fator ativo no comportamento do sistema.

Os autores em [de Oliveira and Callou 2025] avaliam a eficácia do MTD em ambientes de computação em nuvem, com o objetivo de analisar seu impacto na performance e disponibilidade dos serviços ofertados. Para isso, implementa a técnica por meio da migração dinâmica de máquinas virtuais em um ambiente real com Apache CloudStack, comparando cenários com e sem MTD sob diferentes tipos de ataques. Os resultados mostram que, apesar de introduzir um overhead temporário, a abordagem melhora a resiliência e estabiliza o uso de recursos do sistema. No entanto, analisar indícios de envelhecimento de software não foi o foco dos autores.

Em síntese, embora a literatura tenha explorado extensivamente o envelhecimento de software sob a perspectiva de desempenho e confiabilidade, observa-se uma lacuna na integração com estratégias de segurança cibernética. A maioria dos estudos concentra-se em análises de desempenho [Melo et al. 2017, Couto et al. 2023, Vinícius et al. 2022, Andrade et al. 2021, Oliveira et al. 2020, Torquato et al. 2017], enquanto apenas uma parcela considera simultaneamente confiabilidade e estabilidade sistêmica [Couto et al. 2024, Avritzer et al. 2025]. Ademais, trabalhos puramente teóricos [Cho et al. 2020, Tajmilur Rahman 2022] carecem de validação experimental em

ambientes reais.

Diante desse cenário, este artigo distingue-se ao propor uma análise integrada do envelhecimento de software em uma infraestrutura baseada no Apache CloudStack, incorporando explicitamente o MTD como estratégia de segurança. A metodologia adotada reproduz o ciclos operacionais de serviços em nuvem por meio de processos dinâmicos de migração de máquinas virtuais, permitindo avaliar, a interseção entre segurança proativa e estabilidade de longo prazo. Assim, este trabalho contribui para o avanço do estado da arte ao investigar se mecanismos de defesa dinâmica podem simultaneamente fortalecer a segurança e influenciar o comportamento do envelhecimento de software, impactando diretamente a disponibilidade e a confiabilidade dos serviços.

A Tabela 1 apresenta um resumo comparativo de trabalhos relacionados encontrados na literatura sobre envelhecimento de software em diferentes ambientes computacionais. A partir desta tabela, é possível analisar as abordagens empregadas e as principais métricas avaliadas em cada estudo. Observa-se que a maioria dos trabalhos se concentra exclusivamente na análise de desempenho [Melo et al. 2017, Couto et al. 2023, Vinícius et al. 2022, Andrade et al. 2021, Oliveira et al. 2020, Torquato et al. 2017], enquanto apenas alguns investigam tanto o desempenho quanto a confiabilidade [Couto et al. 2024, Avritzer et al. 2025]. Por outro lado, alguns estudos são levantamentos puramente teóricos [Cho et al. 2020, Tajmilur Rahman 2022], sem experimentação prática.

Tabela 1. Comparação das características entre os trabalhos relacionados.

Trabalhos	Ambiente	Abordagem/Modelo	Métricas		
			Desempenho	Confiabilidade	Segurança (MTD)
[Melo et al. 2017]	Nuvem OpenStack	Ciclos de instanciação e finalização de VMs	X		
[Couto et al. 2023]	Banco de Dados PostgreSQL	Baseada em carga de trabalho + análise estatística	X		
[Vinícius et al. 2022]	Plataforma Docker	Metodologia SWARE	X		
[Cho et al. 2020]	Cibersegurança	Revisão sobre MTD			X
[Andrade et al. 2021]	Computação em Nuvem/Borda	Testes de estresse	X		
[Oliveira et al. 2020]	Virtualização de Contêineres	Ciclos de execução de instâncias	X		
[Torquato et al. 2017]	Nuvem Privada	Metodologia SWARE	X		
[Couto et al. 2024]	SQL Server/MySQL	Baseada em carga de trabalho + análise estatística	X	X	
[Tajmilur Rahman 2022]	Geral (Revisão)	Revisão da literatura			
[de Oliveira and Callou 2025]	Apache CloudStack	Medição do impacto do MTD	X	X	X
[Avritzer et al. 2025]	Clusters heterogêneos de VMs	Modelos matemáticos (MDP)	X	X	
Nosso trabalho	Apache CloudStack	Estratégia MTD aplicada à nuvem	X	X	X

3. Fundamentação Teórica

Esta seção apresenta os conceitos fundamentais sobre séries temporais e detecção de tendências, adotadas para detectar indícios de envelhecimento de software e MTD.

3.1. Séries Temporais

A análise de séries temporais é fundamental para compreender e mitigar o envelhecimento de software, especialmente em ambientes de computação em nuvem, nos quais o comportamento do sistema e o uso de recursos variam continuamente em função da dinamicidade das cargas de trabalho e da alocação de recursos. Nesse contexto, o monitoramento

sistemático de métricas de desempenho, como latência, utilização de CPU, consumo de memória, uso de disco e tráfego de rede, possibilita a construção de séries temporais que representam a evolução do estado operacional do sistema ao longo do tempo. Essas séries permitem identificar padrões recorrentes, tendências de crescimento ou degradação e possíveis anomalias, fornecendo subsídios para a análise do comportamento de sistemas de longa duração.

O envelhecimento de software, em particular, manifesta-se frequentemente por meio de tendências graduais e monotônicas, como o aumento progressivo no consumo de recursos ou a deterioração do desempenho, decorrentes de fatores como vazamentos de memória, fragmentação de dados e acúmulo de erros internos. Tais variações podem ser sutis e difíceis de detectar apenas por inspeção visual, o que torna necessária a aplicação de métodos estatísticos robustos para análise de tendências. Nesse sentido, testes não paramétricos, como o teste de Mann-Kendall, são amplamente utilizados para verificar a existência de tendências em séries temporais sem a necessidade de assumir distribuições específicas dos dados, enquanto o estimador de Sen permite quantificar a magnitude dessas tendências de forma robusta.

Além da detecção, técnicas baseadas em séries temporais também possibilitam a previsão do comportamento futuro do sistema, contribuindo para a antecipação de falhas e para a identificação de componentes mais suscetíveis ao envelhecimento. Em ambientes de computação em nuvem, essa capacidade é particularmente relevante, pois permite a adoção de estratégias proativas de mitigação, como o rejuvenescimento de software, a realocação dinâmica de recursos ou ajustes na carga de trabalho. Dessa forma, a análise de séries temporais não apenas auxilia na compreensão do fenômeno de envelhecimento de software, mas também desempenha um papel essencial na manutenção da disponibilidade, confiabilidade e eficiência operacional de sistemas computacionais em execução contínua.

3.1.1. Detecção de Tendência

Para identificar evidências de envelhecimento de software, foi utilizado o teste de Mann-Kendall [Mann 1945], um método estatístico não paramétrico amplamente empregado na detecção de tendências monotônicas em séries temporais. Esse teste avalia a hipótese nula de ausência de tendência contra a hipótese alternativa de existência de uma tendência crescente ou decrescente ao longo do tempo, sem a necessidade de pressupor uma distribuição específica para os dados. A significância estatística da tendência é determinada com base no valor de p , sendo considerada relevante quando $p < 0,05$. Além disso, a estatística S fornece a direção da tendência, indicando comportamento crescente $S > 0$ ou decrescente $S < 0$. No contexto deste estudo, o teste foi aplicado às séries temporais das métricas de utilização de CPU e consumo de memória RAM e uso do disco, com o objetivo de identificar padrões de degradação associados ao envelhecimento de software.

Para quantificar a magnitude das tendências detectadas, foi empregado o estimador de inclinação de Sen, que calcula a mediana das inclinações entre todos os pares possíveis de observações na série temporal. Essa abordagem confere maior robustez à análise, especialmente na presença de ruídos e valores atípicos (outliers), comuns em ambientes computacionais dinâmicos. Após a identificação de tendências estatisticamente significativas, o estimador de Sen foi utilizado com nível de confiança de 95% para de-

terminar a taxa de variação das métricas ao longo do tempo. Tal procedimento permite não apenas confirmar a existência do envelhecimento de software, mas também comparar quantitativamente o grau de degradação entre diferentes ambientes ou componentes analisados. A implementação dos testes estatísticos foi realizada na linguagem R, utilizando o pacote Kendall, amplamente reconhecido para análise de tendências em séries temporais.

4. Metodologia

Esta seção descreve a metodologia adotada para investigar o impacto de estratégias de segurança baseadas em MTD sobre o envelhecimento de software em ambientes de computação em nuvem. A abordagem proposta busca analisar, de forma integrada, como mecanismos de defesa dinâmica influenciam não apenas a segurança do sistema, mas também sua disponibilidade, confiabilidade e comportamento ao longo do tempo. A Figura 1 apresenta uma visão geral da metodologia, cujas etapas são detalhadas a seguir.



Figura 1. Metodologia

O estudo foi estruturado em etapas complementares. Inicialmente, foram definidos os objetivos experimentais e os critérios de avaliação, considerando métricas relevantes para caracterização do envelhecimento de software e seus impactos operacionais. Foram selecionados indicadores de consumo de recursos, como CPU, memória RAM e uso de disco, por sua relevância na identificação de degradação progressiva e potencial comprometimento da disponibilidade do serviço. Paralelamente, foi conduzida uma revisão da literatura com o objetivo de fundamentar a escolha das métricas, dos métodos experimentais e das estratégias de mitigação, com ênfase na interseção entre envelhecimento de software e segurança da informação.

A etapa seguinte consistiu na implantação do ambiente experimental, projetado para reproduzir um cenário realista de nuvem privada sob condições controladas. O ambiente foi composto por dois servidores físicos com configurações idênticas como mostra a Tabela 2, interconectados por meio de infraestrutura de rede dedicada, garantindo isolamento e reprodutibilidade dos experimentos. Em cada servidor, foi instalado o sistema operacional Rocky Linux versão 8, sobre o qual foi configurada a plataforma de computação em nuvem Apache CloudStack versão 4.20. Essa configuração permitiu a criação de uma infraestrutura de nuvem privada distribuída, adequada para experimentação controlada, como mostrado na Figura 2.

Com o ambiente estabelecido, foi implementado um cenário experimental que simula condições de operação contínua sob influência de mecanismos de defesa cibernética.

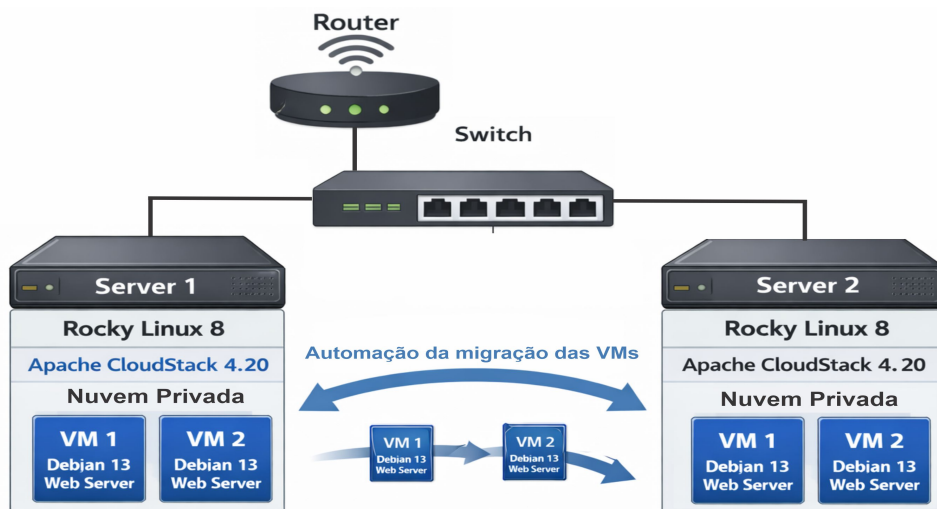


Figura 2. Ambiente de testes

Foram criadas duas máquinas virtuais (VMs), configuradas como servidores web e executando o sistema operacional Debian 13, foram inicialmente instanciadas em um dos hosts físicos. A estratégia de MTD foi então implementada por meio da migração periódica dessas VMs entre os hosts, simulando uma abordagem de defesa baseada em mudança contínua de configuração. Esse mecanismo foi automatizado utilizando scripts desenvolvidos em Python ¹, integrados à API da plataforma de nuvem, permitindo a execução contínua e controlada das migrações ao longo do experimento.

A adoção do MTD neste contexto tem como objetivo reduzir a previsibilidade do ambiente, dificultando potenciais ações de reconhecimento e exploração por agentes maliciosos. Ao mesmo tempo, a introdução dessa dinamicidade operacional permite investigar seus efeitos colaterais sobre o sistema, especialmente no que se refere ao consumo de recursos e à possível aceleração ou mitigação do envelhecimento de software. Assim, o experimento estabelece uma relação direta entre segurança proativa e comportamento de longo prazo da infraestrutura.

O experimento foi conduzido ao longo de um período contínuo de 24 horas, intervalo considerado suficiente para a observação de tendências iniciais de degradação, conforme evidenciado na literatura. Durante esse período, foram coletadas métricas de desempenho e utilização de recursos nos dois hosts físicos. A coleta foi realizada por meio de um segundo script em Python ², responsável por monitorar periodicamente o consumo de CPU, memória RAM e uso de disco. As medições foram realizadas em intervalos de 10 segundos, garantindo granularidade suficiente para análise de séries temporais.

Ao final da execução, os dados coletados foram consolidados e armazenados em formato CSV, possibilitando posterior análise estatística. Essa análise visa validar estatisticamente o comportamento dos dados e identificar tendências através de testes de Mann-Kendall e Sen's Slope de degradação associadas ao envelhecimento de software, bem como avaliar o impacto da estratégia de MTD sobre a estabilidade, confiabilidade

¹<https://github.com/emersonfelipe0813/cloudstack-experimentos/blob/main/migracao.py>

²<https://github.com/emersonfelipe0813/cloudstack-experimentos/blob/main/coletarmetricas.py>

e disponibilidade do sistema. Dessa forma, a metodologia proposta permite não apenas caracterizar o comportamento do sistema sob uso contínuo, mas também investigar, de maneira inédita, a interação entre mecanismos de defesa dinâmica e o envelhecimento de software em ambientes de computação em nuvem.

Tabela 2. Configuração dos Servidores

Component	Description
CPU	Intel® CORE I3®, 3.90 GHz
RAM	8 GB UDIMM RAM
Disk	250 GB SSD
Network Interface	Gigabit Ethernet
Operating System	Rocky Linux 8

5. Estudo de Caso

Esta seção apresenta dois estudos de caso que avaliam a aplicação da metodologia proposta na análise conjunta entre segurança e envelhecimento de software em ambientes de computação em nuvem. O foco é investigar como a técnica de MTD influencia o comportamento do sistema, considerando desempenho, confiabilidade e disponibilidade.

Esse trabalho estende [Felipe et al. 2025], considerando um cenário mais complexo e mais métricas para se detectar o envelhecimento de software. Dessa forma, o primeiro estudo analisa o consumo de recursos de CPU, memória RAM e disco para identificar padrões de degradação ao longo do tempo em um ambiente dinâmico. Já o segundo estudo realiza a validação estatística desses resultados, utilizando métodos de análise de séries temporais para confirmar tendências reais de envelhecimento. De forma integrada, os estudos permitem avaliar com maior robustez o impacto do MTD, evidenciando como estratégias de segurança proativa podem afetar simultaneamente o desempenho e a estabilidade operacional de sistemas em nuvem.

5.1. Estudo de Caso 1

Este estudo de caso investiga o envelhecimento de software em um ambiente de computação em nuvem sob a aplicação de MTD, utilizando a plataforma Apache CloudStack. O experimento foi conduzido em dois hosts físicos, com duas máquinas virtuais configuradas como servidores web, inicialmente alocadas em um único host.

As VMs foram submetidas a ciclos contínuos de migração entre os hosts durante 24 horas, por meio de um script automatizado, simulando uma estratégia de MTD baseada na mudança dinâmica da localização dos serviços. Essa abordagem visa aumentar a segurança ao reduzir a previsibilidade do ambiente.

Ao mesmo tempo, o experimento permite avaliar o impacto dessa dinamicidade no consumo de recursos, investigando se a aplicação contínua do MTD contribui para a degradação do sistema e para a manifestação do fenômeno de envelhecimento de software.

As Figuras 3 e 4 apresentam, respectivamente, a evolução temporal das métricas de utilização de CPU, memória RAM e uso de disco para os Hosts 1 e 2 durante o período experimental. A análise dos resultados evidencia uma tendência de aumento no consumo de recursos em ambos os hosts, indicando a presença de degradação progressiva ao longo do tempo. Esses resultados sugerem que, embora o MTD contribua para o fortalecimento da segurança ao introduzir imprevisibilidade no ambiente, sua aplicação contínua

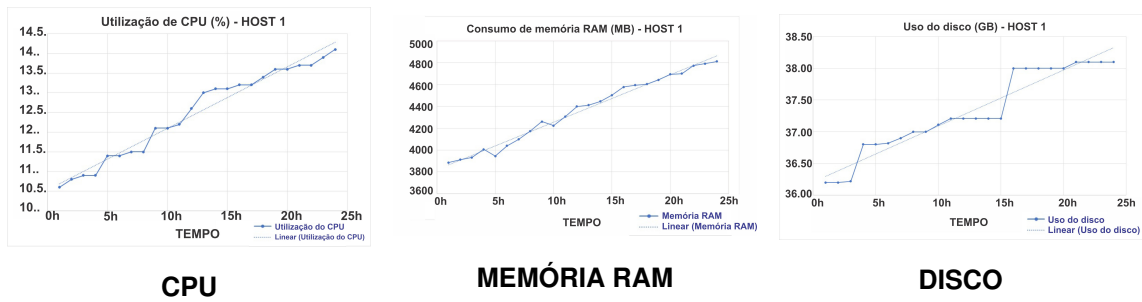


Figura 3. Consumo de recursos no HOST 1

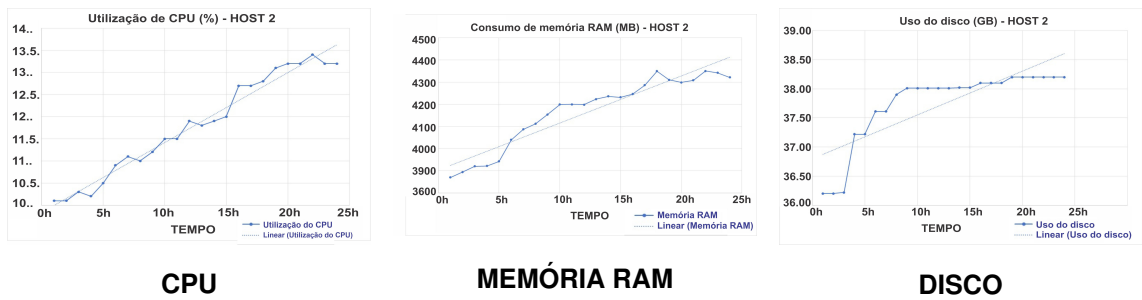


Figura 4. Consumo de recursos no HOST 2

pode gerar overhead operacional significativo, impactando diretamente o consumo de recursos e potencialmente acelerando o processo de envelhecimento de software. Dessa forma, o estudo evidencia a necessidade de avaliar, de maneira integrada, os benefícios de segurança proporcionados pelo MTD e seus efeitos colaterais sobre a confiabilidade e a estabilidade de sistemas em execução contínua.

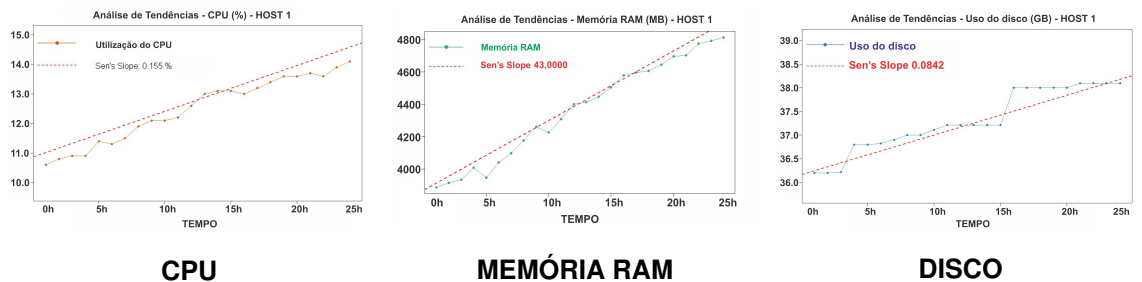


Figura 5. Análise de tendencia Mannkendall e Sen - HOST 1

5.2. Estudo de Caso 2

Com o objetivo de validar quantitativamente os resultados observados no Estudo de Caso 1, foi realizada uma análise de tendência das séries temporais por meio do teste estatístico não paramétrico de Mann-Kendall. Esse teste permite avaliar a hipótese nula de ausência de tendência frente à hipótese alternativa de existência de tendência monotônica ao longo do tempo, sendo amplamente utilizado na detecção de padrões de degradação em sistemas computacionais. Para quantificar a magnitude das tendências identificadas, foi empregado o estimador de Sen (Sen's Slope), que calcula a mediana das inclinações entre todos os pares de observações da série, fornecendo uma estimativa robusta da taxa de variação.

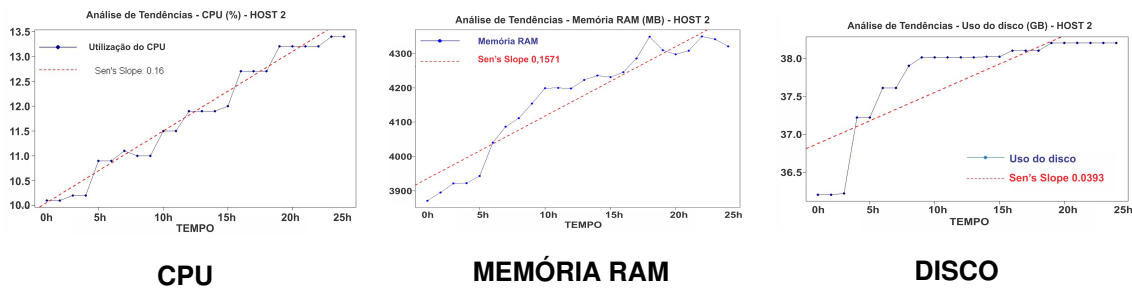


Figura 6. Análise de tendencia Mannkendall e Sen - HOST 2

As análises foram conduzidas no ambiente estatístico R, utilizando o pacote trend, com nível de significância de 5%. Os resultados obtidos para os Hosts 1 e 2, apresentados nas Tabelas 3 e 4, indicam tendências positivas e estatisticamente significativas ($p < 0,05$) para todas as métricas analisadas, evidenciando um comportamento consistente de degradação ao longo do tempo.

No Host 1, observa-se uma degradação mais acentuada no consumo de memória RAM, que apresentou a maior taxa de crescimento entre as métricas avaliadas, com inclinação de Sen igual a 43,0000 e $p = 1,79 \times 10^{-11}$. Esse comportamento sugere a ocorrência de vazamentos de memória ou acúmulo progressivo de estados não liberados, característicos do envelhecimento de software. Adicionalmente, as métricas de CPU e uso de disco também apresentaram tendências crescentes, com inclinações de 0,1548 e 0,0842, respectivamente, conforme ilustrado na Figura 5.

No Host 2, o comportamento mais crítico foi observado no consumo de CPU, que apresentou uma inclinação de 0,9520 com $p < 2,22 \times 10^{-16}$, indicando um aumento persistente da carga computacional ao longo do tempo. As métricas de memória RAM e uso de disco também mantiveram tendências crescentes, com inclinações de 0,1571 e 0,0393, respectivamente, conforme evidenciado na Figura 6 e na Tabela 4. Esses resultados indicam que a carga associada à migração contínua de máquinas virtuais impacta de forma diferenciada os recursos dos hosts, refletindo a distribuição dinâmica das operações induzidas pelo MTD.

As Figuras 5 e 6 apresentam as séries temporais acompanhadas das linhas de tendência estimadas pelo método de inclinação de Sen, evidenciando o crescimento consistente das variáveis ao longo do período analisado. A significância estatística dos resultados reforça que as variações observadas não se tratam de flutuações aleatórias, mas sim de um processo sistemático de degradação associado ao envelhecimento de software.

Sob a perspectiva integrada de segurança e operação, os resultados indicam que, embora a estratégia de MTD contribua para o aumento da resiliência e da proteção contra ameaças cibernéticas, sua aplicação contínua introduz overhead operacional capaz de impactar negativamente o consumo de recursos e acelerar o envelhecimento de software. Esse comportamento evidencia a necessidade de adoção de mecanismos complementares, como políticas de rejuvenescimento de software, de modo a equilibrar os ganhos de segurança com a manutenção da disponibilidade e da confiabilidade do sistema.

Por fim, destaca-se que a identificação de tendências estatisticamente significativas de degradação em um intervalo de 24 horas justifica a delimitação temporal do ex-

perimento. Esse período mostrou-se suficiente para evidenciar o fenômeno investigado, permitindo a obtenção de resultados representativos com menor custo computacional e maior reprodutibilidade em ambientes controlados.

Tabela 3. ANÁLISE DE TENDÊNCIAS DE USO DE RECURSOS - HOST 1

Recurso	Sen's Slope	p-valor	Tendência
Memória RAM	43,0000	$1,79 \times 10^{-11}$	Crescente
Uso de CPU	0,1548	$1,02 \times 10^{-10}$	Crescente
Uso de Disco	0,0842	$6,09 \times 10^{-10}$	Crescente

Tabela 4. ANÁLISE DE TENDÊNCIAS DE USO DE RECURSOS - HOST 2

Recurso	Sen's Slope	p-valor	Tendência
Memória RAM	0,1571	$2,64 \times 10^{-10}$	Crescente
Uso de CPU	0,9520	$2,22 \times 10^{-16}$	Crescente
Uso de Disco	0,0393	$8,92 \times 10^{-10}$	Crescente

6. Conclusão

Esta pesquisa investigou o envelhecimento de software em ambientes de computação em nuvem sob a aplicação da técnica de MTD, utilizando a plataforma Apache CloudStack. Os resultados experimentais evidenciaram degradação progressiva no consumo de recursos ao longo de 24 horas, caracterizando o fenômeno de envelhecimento. A validação estatística, por meio do teste de Mann-Kendall e do estimador de Sen, confirmou a significância dessas tendências.

Sob a perspectiva de segurança, verificou-se que, embora o MTD aumente a resiliência do sistema, sua aplicação contínua introduz overhead operacional, podendo acelerar o envelhecimento de software. Como contribuição, o estudo demonstra a existência de um trade-off entre segurança e estabilidade operacional, destacando a necessidade de integrar mecanismos de defesa com estratégias de mitigação, como o rejuvenescimento de software. Como trabalhos futuros, propõe-se a modelagem do sistema por meio de Redes de Petri Estocásticas e métodos de aprendizagem de máquina para análise preditiva e definição de políticas otimizadas.

Agradecimentos

Os autores agradecem à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo suporte financeiro para a realização desta pesquisa.

Referências

Andrade, E., Pietrantuono, R., Machida, F., and Cotroneo, D. (2021). A comparative analysis of software aging in image classifiers on cloud and edge. *IEEE Transactions on Dependable and Secure Computing*, PP:1–1.

- Avritzer, A., Janes, A., Marin, A., Trubiani, C., van Hoorn, A., Camilli, M., Menasché, D., and Bondi, A. (2025). Software aging detection and rejuvenation assessment in heterogeneous virtual networks. *IEEE Transactions on Emerging Topics in Computing*, PP:1–15.
- Callou, G. and Vieira, M. (2024). Availability and performance analysis of cloud services. In *Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing, LADC '24*, page 262–271, New York, NY, USA. Association for Computing Machinery.
- Cho, J.-H., Sharma, D. P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T. J., Kim, D. S., Lim, H., and Nelson, F. F. (2020). Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys & Tutorials*, 22(1):709–745.
- Couto, H., Andrade, E., Silva, F. A., and Callou, G. (2023). Analysis of software aging in a database environment. *IEEE Latin America Transactions*, 21:821–828.
- Couto, H., Machida, F., Callou, G., and Andrade, E. (2024). A comparative analysis of software aging in relational database system environments.
- de Oliveira, A. B. and Callou, G. (2025). Quantifying the impact of security strategies on the performance and availability of cloud services. In *2025 IEEE 36th International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pages 225–228.
- Felipe, E., Borges, I., and Callou, G. (2025). The impact of moving target defense on software aging in cloud computing. In *2025 IEEE 36th International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pages 01–08.
- Mann, H. B. (1945). Nonparametric tests against trend. *Econometrica: Journal of the econometric society*, pages 245–259.
- Matheus Torquato, M. V. (2020). Moving target defense in cloud computing: A systematic mapping study.
- Melo, C., Araujo, J., Alves, V., and Maciel, P. R. M. (2017). Investigation of software aging effects on the openstack cloud computing platform. *J. Softw.*, 12(2):125–137.
- Oliveira, F., Araujo, J., Matos, R., Lins, L., Rodrigues, A., and Maciel, P. (2020). Experimental evaluation of software aging effects in a container-based virtualization platform. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 414–419.
- Tajmilur Rahman, Joshua C. Nwokeji, T. V. M. (2022). Analysis of current trends in software aging: A literature survey.
- Torquato, M., Maciel, P., Araujo, J., and Umesh, I. M. (2017). An approach to investigate aging symptoms and rejuvenation effectiveness on software systems. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6.
- Vinícius, L., Rodrigues, L., Torquato, M., and Silva, F. A. (2022). Docker platform aging: a systematic performance evaluation and prediction of resource consumption. *The Journal of Supercomputing*, 78(10):12898–12928.