# Proposta de Projeto - Computação Inspirada pela Natureza

2025.PP.CIN-DF

# Sistema Imunológico Artificial Aplicado à Detecção de Defeitos de Software

São Paulo, SP

Versão 1.0

Maio de 2025

# Identificação

*Título:* Proposta de Projeto - Computação Inspirada pela Natureza: Sistema Imunológico Artificial Aplicado à Detecção de Defeitos de Software
2025.PP.CIN-DF

*Projeto:* Sistema Imunológico Artificial Aplicado à Detecção de Defeitos de Software

*Data:* Maio de 2025

*Local:* São Paulo, SP

*Versão:* 1.0

# Revisões

| **Data** | **Alterações / Comentários** | **Autor(es)** |
|---|---|---|
| 2025.04.13 | Criação do documento inicial. | Gabriel e Vinícius |
| 2025.04.16 | Redação do primeiro capítulo (Introdução). | Vinícius |
| 2025.04.18 | Redação do capítulo de Fundamentação Teórica. | Gabriel e Vinícius |
| 2025.04.20 | Desenvolvimento da Metodologia (Materiais e Métodos). | Gabriel e Vinícius |
| 2025.04.22 | Apresentação da Proposta para a Co-Orientadora. | Gabriel, Vinícius e Veronica |

**Faculdade de Ciências - Câmpus de Bauru**

**Diretor Geral**

PROFA. ASSOCIADA VERA LUCIA MESSIAS FIALHO CAPELLINI

**Coordenação do Programa de Pós-Graduação em Ciência da Computação – PPGC**

**Coordenador do Programa**

LUIZ CARLOS FERREIRA GARCEZ, M. SC.

**Pesquisador(es)/Orientador(es)**

DR.FABRÍCIO APARECIDO BREVE

**Coorientador(es)**

DR(A).VERÔNICA OLIVEIRA DE CARVALHO

**Orientando(s) (Em Ordem alfabética)**

GABRIEL DE SOUZA LIMA - BACHARELADO EM CIÊNCIAS ATUARIAS

VINÍCIUS DE SOUZA SANTOS - BACHARELADO EM ENG. DE COMPUTAÇÃO

© *copyright* 2025 PPGCC – Todos os direitos reservados

Sistema Imunológico Artificial Aplicado à Detecção de Defeitos de Software / Coordenação do Programa de Pós-Graduação em Ciência da Computação. – : Faculdade de Ciências - Câmpus de Bauru, Maio de 2025-
12 p. : il. (algumas color.) ; 29,7 cm.

Proposta de Projeto - Computação Inspirada pela Natureza – Coordenação do Programa de Pós-Graduação em Ciência da Computação, Maio de 2025.
Versão final.

ISSN:

1. Arquitetura da Informação2. Tecnologia da InformaçãoI. Título

CDD 99.999

## RESUMO

Sistemas Imunológicos Artificiais (AIS) constituem uma subárea promissora da Computação Inspirada pela Natureza (CIN), cujos fundamentos biológicos simulam a capacidade do sistema imunológico humano de identificar e eliminar ameaças. Neste projeto, propõe-se a aplicação de um AIS para a detecção de defeitos de software utilizando dados reais do repositório PROMISE da NASA. A abordagem simula o processo de clonagem, mutação e seleção de anticorpos, adaptando-os para classificar corretamente módulos de código como defeituosos ou não. Os resultados esperados incluem a melhoria na precisão da classificação e a exploração de uma abordagem explicável e biologicamente inspirada para a análise de qualidade de software.

**Palavras-chave**: sistema imunológico artificial; defeitos de software; aprendizado de máquina; computação inspirada pela natureza; NASA PROMISE.

## ABSTRACT

Artificial Immune Systems (AIS) represent a promising subarea of Nature-Inspired Computing (CIN), simulating the human immune system's biological mechanisms to identify and eliminate threats. This project proposes the application of an AIS to detect software defects using real data from NASA's PROMISE repository. The model mimics the process of cloning, mutation, and antibody selection, adapting it to correctly classify software modules as defective or not. The expected results include improved classification accuracy and the exploration of a biologically inspired, explainable approach to software quality analysis.

**Keywords**: Artificial immune system; software defects; machine learning; PROMISE; nature-inspired computing.

# SUMÁRIO

# LISTA DE FIGURAS

# LISTA DE TABELAS

# 1 INTRODUÇÃO

A confiabilidade de sistemas de software constitui um requisito fundamental para aplicações críticas em setores como transporte, saúde, finanças e defesa. A ocorrência de falhas nesses sistemas compromete não apenas a funcionalidade, mas também a segurança e a continuidade operacional. De acordo com (CASTRO, 2002), a analogia entre sistemas computacionais e sistemas biológicos permite tratar falhas de software como disfunções celulares, sendo apropriada a adoção de mecanismos artificiais capazes de detectar e responder a tais anomalias de forma adaptativa.

Nesse contexto, os Sistemas Imunológicos Artificiais (AIS), baseados nos princípios da imunologia natural, representam uma abordagem bioinspirada eficaz para a resolução de problemas relacionados à classificação, detecção de padrões e resposta a anomalias. Tais sistemas simulam processos imunológicos como o reconhecimento de antígenos, a clonagem de anticorpos, a mutação genética e a maturação por afinidade (DASGUPTA, 1999). Estudos recentes demonstram a aplicabilidade do AIS em domínios diversos, incluindo segurança cibernética (BAI; LIU; HUANG, 2023), redes de sensores (VIJAYAKUMAR; RANI; PRASAD, 2021), e sistemas autônomos sensíveis a falhas (ZHANG; CHEN; LIN, 2021).

Embora a literatura evidencie a eficácia dos AIS em tarefas de detecção de falhas, sua aplicação no campo da engenharia de software, particularmente na predição de defeitos em código-fonte, permanece limitada. Modelos tradicionais de aprendizado de máquina, como Random Forest (BREIMAN, 2001), Máquinas de Vetores de Suporte (SVM) (CORTES; VAPNIK, 1995) e técnicas de balanceamento como SMOTE (CHAWLA et al., 2002), têm sido amplamente utilizados para esta finalidade. No entanto, tais modelos apresentam limitações no que se refere à adaptabilidade contínua e à interpretabilidade simbólica dos mecanismos de decisão.

Com base nesse cenário, este trabalho propõe a utilização de um Sistema Imunológico Artificial como alternativa para a detecção de defeitos de software, simulando mecanismos imunológicos adaptativos para a identificação de padrões defeituosos em instâncias de código. A abordagem será aplicada ao conjunto de dados NASA-JM1, disponibilizado pelo repositório PROMISE, e validada por meio de métricas de desempenho como F1-score,

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

acurácia e revocação.

A proposta visa contribuir para o avanço de modelos bioinspirados aplicáveis à engenharia de software, oferecendo uma abordagem interpretável, resiliente e adaptável ao diagnóstico automatizado de falhas.

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

## 2 Fundamentação Teórica

### 2.0.1 Computação Inspirada pela Natureza (CIN)

A Computação Inspirada pela Natureza (CIN) é um campo da ciência da computação que desenvolve algoritmos a partir da analogia com fenômenos naturais, como evolução biológica, sistemas imunológicos, comportamento de colônias e processos bioquímicos (GONZÁLEZ-LAREDO et al., 2023). A CIN busca explorar princípios como auto-organização, adaptação, paralelismo e robustez para solucionar problemas de alta complexidade.

As vertentes mais consolidadas da CIN incluem:

- **Computação Evolutiva:** inspirada na teoria da seleção natural, envolvendo algoritmos genéticos, evolução diferencial e programação evolutiva, aplicados amplamente em problemas de busca e otimização (CASTRO, 2002).
- **Computação Bioquímica:** simula mecanismos celulares como reações moleculares, replicação genética e imunidade. Nesta vertente se inserem os Sistemas Imunológicos Artificiais (AIS), além de técnicas como computação de DNA e sistemas de membrana (DASGUPTA, 1999).
- **Computação por Comportamento Coletivo:** representa sistemas baseados em agentes, como enxames de partículas (PSO), colônias de formigas e abelhas, onde a solução emerge da interação local entre os indivíduos (BECCENERI et al., 2010).

Esses modelos compartilham a capacidade de adaptação contínua ao ambiente, oferecendo soluções eficientes para problemas que exigem resiliência e aprendizado autônomo.

### 2.0.2 Sistemas Imunológicos Artificiais (AIS)

Os Sistemas Imunológicos Artificiais (AIS) são algoritmos baseados nos mecanismos de defesa do sistema imunológico humano, como reconhecimento de antígenos, seleção clonal, maturação de afinidade e memória imunológica (CASTRO, 2002; DASGUPTA, 1999).

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

Em sua forma computacional, AIS utilizam essas ideias para tarefas como classificação, detecção de anomalias e otimização.

Entre os mecanismos fundamentais destacam-se:

- **Seleção Clonal e Maturação por Afinidade:** os melhores detectores (anticorpos) são selecionados, clonados e mutados, permitindo a evolução de soluções mais eficazes (CASTRO, 2002).
- **Seleção Negativa:** detectores que reconhecem padrões legítimos (self) são eliminados. Os restantes são usados para identificar padrões anômalos (não-self), como falhas ou intrusões (ZHANG; CHEN; LIN, 2021).
- **Memória Imunológica:** anticorpos de alta afinidade são armazenados para resposta rápida a ameaças já reconhecidas, promovendo aprendizado contínuo (BAI; LIU; HUANG, 2023).

A Figura 1 ilustra o funcionamento de um AIS aplicado à detecção de falhas em software.

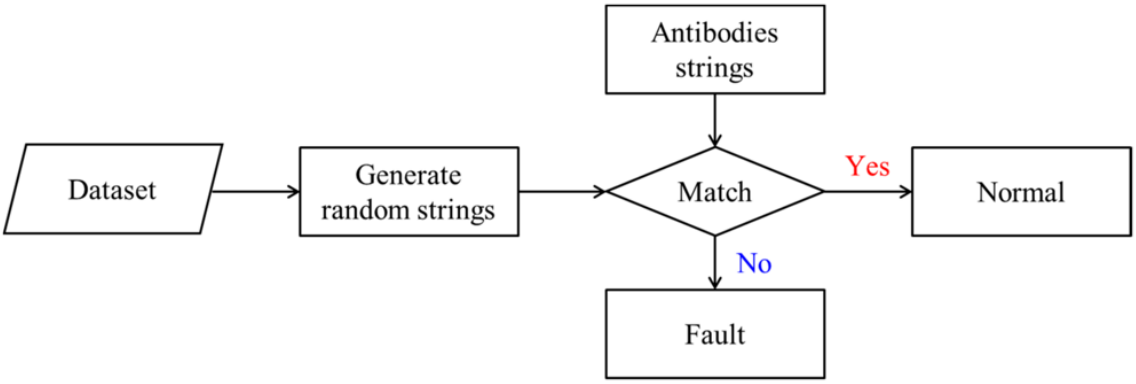


Figura 1 – Fluxo de detecção de falhas usando um algoritmo imunológico artificial.
**Fonte:** Elaborado pelos autores, 2025

### 2.0.3 Defeitos de Software: Conceituação e Relevância na Engenharia

Defeitos de software referem-se a anomalias ou imperfeições no código que comprometem o comportamento esperado do sistema. Segundo (PRESSMAN; MAXIM, 2016), um defeito ocorre quando uma implementação viola a especificação funcional, causando falhas em tempo de execução ou dificultando a manutenção e evolução do software.

© copyright 2025 Vinícius de Souza Santos – Todos os direitos reservados

Os defeitos podem ser categorizados em:

- **Defeitos sintáticos:** erros de compilação, má formatação ou ausência de símbolos.
- **Defeitos lógicos:** implementações incorretas que produzem saídas inválidas.
- **Defeitos semânticos:** desvios sutis do comportamento esperado, muitas vezes difíceis de identificar com testes convencionais (GOSEVA-POPSTOJANOVA, 2018).

No contexto de sistemas grandes e críticos, a predição de defeitos tornou-se uma área estratégica da engenharia de software. Técnicas como aprendizado de máquina vêm sendo aplicadas a dados históricos de métricas de código para identificar módulos com maior propensão a falhas (GOPAL; KUMAR, 2019).

Contudo, tais modelos apresentam limitações quando lidam com:

- Bases de dados desbalanceadas (maioria dos módulos sem defeito).
- Ausência de explicabilidade nos classificadores (e.g., redes neurais profundas).
- Incapacidade de adaptação contínua a novos tipos de falhas.

Diante dessas limitações, os Sistemas Imunológicos Artificiais oferecem uma abordagem promissora, interpretando defeitos como "antígenos"e construindo repertórios de detectores adaptáveis capazes de reconhecer padrões anômalos, conforme descrito a seguir.

Nesse cenário, os Sistemas Imunológicos Artificiais despontam como uma solução promissora para a tarefa de detecção autônoma de defeitos, conforme discutido na próxima subseção.

### 2.0.4 Aplicações de AIS na Detecção de Anomalias

AIS têm se mostrado eficazes em diversos domínios onde a detecção de padrões desconhecidos é essencial. Dentre as aplicações mais recentes estão:

- **Segurança Cibernética:** algoritmos de seleção negativa são amplamente utilizados em sistemas de detecção de intrusão (IDS), capazes de identificar ataques zero-day (ZHANG; CHEN; LIN, 2021).

© copyright 2025 Vinícius de Souza Santos – Todos os direitos reservados

- **Redes e Sistemas Distribuídos:** AIS são utilizados para detecção de falhas em redes de sensores, congestionamentos, e comportamentos atípicos em sistemas IoT (VIJAYAKUMAR; RANI; PRASAD, 2021).
- **Engenharia de Software:** pesquisas recentes demonstram a aplicação de AIS para predição de defeitos de software, seleção de métricas relevantes e identificação de módulos críticos em código-fonte (MUMTAZ et al., 2021).

Essas aplicações demonstram a flexibilidade e adaptabilidade dos AIS em ambientes dinâmicos.

### 2.0.5 Vantagens dos AIS Frente aos Modelos Convencionais

Comparados a modelos tradicionais como Random Forest (BREIMAN, 2001) e SVM (CORTES; VAPNIK, 1995), os AIS oferecem vantagens significativas:

- **Adaptatividade:** aprendizado contínuo com atualização dinâmica dos detectores.
- **Simbologia:** representação explícita de padrões (anticorpos e antígenos).
- **Explicabilidade:** maior transparência e justificativa das decisões.

Tais características tornam os AIS especialmente adequados para aplicações críticas que exigem interpretabilidade e adaptação contínua.

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

## 3 Trabalhos Relacionados

Diversos estudos têm explorado o potencial dos Sistemas Imunológicos Artificiais (AIS) na tarefa de predição de defeitos de software e na melhoria da qualidade de sistemas computacionais. Esta seção apresenta quatro trabalhos relevantes que fundamentam e contextualizam a presente proposta.

Soleimani e Asdaghi (SOLEIMANI; ASDAGHI, 2014) propuseram um método de seleção de atributos baseado em AIS para melhorar a acurácia de algoritmos de predição de falhas em software. Utilizando o conjunto de dados KC1 do repositório PROMISE, os autores demonstraram que o subconjunto de atributos selecionado por algoritmos imuno-inspirados aumentou a acurácia do classificador de 82,44% para 83,72%, superando métodos convencionais de seleção por filtro e wrapper.

No trabalho de Yang et al. (YANG et al., 2011), foi aplicado um algoritmo de seleção negativa com valores reais (Real-Valued Negative Selection Algorithm) para detectar envelhecimento de servidores web. O algoritmo, inspirado no sistema imune, utilizou apenas amostras normais (estado self) para detectar degradações de desempenho anômalas (estado não-self). O enfoque em detecção de anomalias demonstra a flexibilidade dos AIS na identificação de falhas latentes em sistemas de software.

Khan et al. (KHAN et al., 2020) propuseram uma arquitetura baseada em redes imunes artificiais otimizadas (Opt-aiNet) para otimização de hiperparâmetros em classificadores aplicados à predição de defeitos. O estudo utilizou sete algoritmos de aprendizado de máquina, demonstrando que a combinação com AIS elevou o desempenho preditivo em comparação às versões não otimizadas, reforçando a capacidade dos AIS de contribuir com modelos híbridos de alto desempenho.

Por fim, Gong et al. (GONG; XI; CAI, 2005) apresentaram um modelo imunológico para simulação de robôs móveis expostos a falhas provocadas por vírus computacionais. Embora não diretamente aplicado à engenharia de software, o modelo demonstra como princípios imunológicos — como adaptabilidade, memória e robustez — podem ser empregados para detecção e recuperação de falhas em sistemas complexos, incluindo bugs de software e anomalias estruturais.

Em conjunto, esses estudos reforçam o potencial dos AIS na predição de defeitos, detec-

© copyright 2025 Vinícius de Souza Santos – Todos os direitos reservados

ção de anomalias e adaptação contínua em ambientes computacionais, consolidando o embasamento científico para a aplicação proposta neste projeto.

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

# 4 Materiais e Métodos

© copyright 2025 Vinícius de Souza Santos – Todos os direitos reservados

## 5 RESULTADOS ESPERADOS

São Paulo, SP, Maio de 2025.

Vinícius de Souza Santos

Pesquisador(es)/Responsável(eis)

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

## REFERÊNCIAS

BAI, Y.; LIU, Z.; HUANG, Y. Threat detection system based on artificial immune recognition. *Information Sciences*, Elsevier, v. 619, p. 1187–1201, 2023. Citado 2 vezes nas páginas 1 e 4.

BECCENERI, J. C. et al. Otimizaçao por colônia de formigas (ant colony optimization). *Disponivel em mtc-m19. sid. inpe. br/col/sid. inpe. br/mtc-m19*, v. 80, n. 2010, p. 01–20, 2010. Citado na página 3.

BREIMAN, L. Random forests. *Machine learning*, Springer, v. 45, n. 1, p. 5–32, 2001. Citado 2 vezes nas páginas 1 e 6.

CASTRO, L. N. de. *Immune and neural models: theory and applications*. [S.l.]: Springer, 2002. Citado 3 vezes nas páginas 1, 3 e 4.

CHAWLA, N. V. et al. Smote: synthetic minority over-sampling technique. *Journal of artificial intelligence research*, v. 16, p. 321–357, 2002. Citado na página 1.

CORTES, C.; VAPNIK, V. Support-vector networks. *Machine Learning*, v. 20, n. 3, p. 273–297, 1995. Citado 2 vezes nas páginas 1 e 6.

DASGUPTA, D. *Artificial immune systems and their applications*. [S.l.]: Springer, 1999. Citado 2 vezes nas páginas 1 e 3.

GONG, T.; XI, S.; CAI, Z. An immune model and its application to a mobile robot simulator. In: *2005 IEEE International Conference on Robotics and Biomimetics*. [S.l.: s.n.], 2005. p. 30–34. Citado na página 7.

GONZÁLEZ-LAREDO, R. F. et al. Natural deep eutectic solvents (nades) as an emerging technology for the valorisation of natural products and agro-food residues: a review. *International Journal of Food Science and Technology*, Oxford University Press, v. 58, n. 12, p. 6660–6673, 2023. Citado na página 3.

GOPAL, M.; KUMAR, N. Machine learning approaches for software defect prediction: a review. *Computer Science Review*, v. 33, p. 1–22, 2019. Citado na página 5.

GOSEVA-POPSTOJANOVA, K. Defect prediction in software systems using hybrid ai techniques. *Journal of Systems and Software*, v. 143, p. 56–75, 2018. Citado na página 5.

KHAN, F. et al. Hyper-parameter optimization of classifiers, using an artificial immune network and its application to software bug prediction. *IEEE Access*, v. 8, p. 20954–20964, 2020. Citado na página 7.

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados

MUMTAZ, B. et al. Feature selection using artificial immune network: An approach for software defect prediction. *Intelligent Automation & Soft Computing*, v. 29, n. 3, 2021. Citado na página 6.

PRESSMAN, R. S.; MAXIM, B. R. *Engenharia de Software*. 8. ed. [S.l.]: McGraw-Hill Brasil, 2016. Citado na página 4.

SOLEIMANI, A.; ASDAGHI, F. An ais based feature selection method for software fault prediction. In: *2014 Iranian Conference on Intelligent Systems (ICIS)*. [S.l.: s.n.], 2014. p. 1–5. Citado na página 7.

VIJAYAKUMAR, V.; RANI, N.; PRASAD, M. Fault detection in wireless sensor networks using artificial immune system. *Sensors*, MDPI, v. 21, n. 4, p. 1120, 2021. Citado 2 vezes nas páginas 1 e 6.

YANG, H. et al. Detecting software aging of web servers with real-valued negative selection algorithm. In: *2011 IEEE 3rd International Conference on Communication Software and Networks*. [S.l.: s.n.], 2011. p. 298–302. Citado na página 7.

ZHANG, T.; CHEN, R.; LIN, X. Artificial immune system optimized with svm for threat detection in autonomous spacecraft. *IEEE Access*, v. 9, p. 15003–15015, 2021. Citado 3 vezes nas páginas 1, 4 e 5.

© *copyright* 2025 Vinícius de Souza Santos – Todos os direitos reservados