MECADE: Modelo de Engenharia do Caos para Avaliação da Garantia de Dependabilidade em Sistemas Financeiros

Richardson Edson de Lima, Johnny Marques

Instituto Tecnológico de Aeronáutica (ITA).
Praça Marechal Eduardo Gomes, 50 - Vila das Acacias, São José dos Campos – SP – Brazil, 12228-900
{richardson,johnny}@ita.br

Abstract. The objective of this paper is to create and present a model to guarantee the reliability of critical financial market systems, to assess the resilience of these systems and identify recommendations for necessary modifications. This work is a master's research in progress in the postgraduate program in Electronics and Computer Engineering, informatics area of the Instituto Tecnológico de Aeronáutica. The model will be evaluated through the execution of isolated experiments based on chaos engineering, considering the banking scenario. In Brazil it is an incipient topic, however, the characteristics of the market represent a relevant opportunity to expand studies on the subject.

Resumo. Este artigo tem como objetivo geral criar e apresentar um modelo de avaliação da garantia de dependabilidade de sistemas críticos do mercado financeiro, visando avaliar a resiliência desses sistemas e identificar recomendações de modificações necessárias. Este trabalho é uma pesquisa de mestrado em andamento no programa de pós-graduação em Engenharia Eletrônica e Computação, área informática do Instituto Tecnológico de Aeronáutica. A avaliação do modelo se dará por meio da execução de experimentos isolados com base na engenharia de caos, tendo em vista o cenário bancário. No Brasil é um tema incipiente, contudo as características do mercado representarem oportunidade relevante de ampliação de estudos a respeito.

1. Introdução

Durante o processo de planejamento da arquitetura de um ecossistema de *cloud-native applications* [P. D. Francesco, I. Malavolta and P. Lago 2017], não é incomum encontrar certos desvios relacionados a qualidade de implementação e testes de software [Kassab, Mohamad, Joanna F DeFranco, and Phillip A Laplante 2017], que podem resultar em mau funcionamento de alguns componentes da aplicação. Descobrir esses desvios e trabalhar de maneira contínua, com foco em melhorar as reações sistêmicas e chegar a ter respostas a possíveis falhas é de fato um esforço nobre e valioso.

Atualmente em escala global, instituições financeiras mantêm inúmeros ecossistemas computacionais, sendo esses sistemas, distribuídos e atualmente muitos deles nascem nativos na nuvem (*cloud-native*). Os sistemas baseados em microsserviços com aplicações na nuvem [Kratzke, Nane, and Peter-Christian Quint 2017] tem como

premissa serem escaláveis, ágeis e resilientes [S. Newman 2015]. Neste cenário é fundamental avaliar as questões de dependabilidade [Bukowski, L 2016], principalmente em sistemas de natureza do mercado financeiro. A dependabilidade de um sistema de computação é a capacidade de fornecer um serviço que pode ser justificadamente confiável [Avizienis A, Laprie J-C, Randell B]. Dada a complexidade dos sistemas atuais, o objetivo da pesquisa em andamento no programa de pós-graduação em Engenharia Eletrônica e Computação, área informática do Instituto Tecnológico de Aeronáutica, envolve uma proposta de criação e apresentação de um modelo para avaliação da garantia da dependabilidade, onde o foco seja usar os princípios de engenharia de caos aplicados de forma controlada e injetar falhas de forma intencional em sistemas de software [Orzell, Gregory S. & Yury Izrailevsky 2019], ajudando validar aspectos como disponibilidade, confiabilidade, confidencialidade, segurança, integridade, e superar aos incertezas dos sistemas distribuídos atuais. Espera-se com este trabalho que sejam intencionalmente feitas ações contemplando conjuntos de falhas, proporcionando reflexões e auxiliando projetos na construção de sistemas mais tolerantes a falhas.

Todos os sistemas estão sujeitos a falhas. Solucionar essas falhas antes que elas causem danos maiores para o negócio é o cenário ideal. Para isso, precisamos entender como um sistema se comporta e reage a determinados estímulos negativos. É com esse propósito que a Engenharia do Caos (ou *Chaos Engineering*, em inglês) se popularizou como método entre as empresas mais inovadoras do mundo. Apesar da promessa de "quebrar sistemas", a Engenharia do Caos é um campo de estudos que exige controle e observação. Ela requer a elaboração de uma hipótese, experimentação e análise dos resultados. Seu nome faz referência à Teoria do Caos, segundo a qual pequenas alterações nas condições iniciais de sistemas dinâmicos podem causar resultados imprevisíveis a longo prazo.

Além dessa seção 1, o trabalho contém mais 5 seções. A seção 2 apresenta a metodologia de pesquisa. A seção 3 apresenta a definição do problema de pesquisa. A seção 4 apresenta a principal contribuição do trabalho de pesquisa, que é o modelo. A seção 5 apresenta os próximos passos dessa pesquisa e finalmente a seção 6 apresenta as considerações finais.

2. Metodologia de Pesquisa

A metodologia de pesquisa aplicada neste projeto de mestrado contém 4 etapas. Na etapa 1 são identificadas as questões de pesquisa. Com as questões de pesquisa, a etapa 2 prevê a condução de uma revisão da literatura. Já na etapa 3, o modelo de avaliação da garantia de dependabilidade em sistemas financeiros. Finalmente, na etapa 4 serão conduzidas atividades de avaliação da validade desse modelo. A Figura 1 apresenta uma representação da metodologia de pesquisa.

Figura 1. Metodologia de pesquisa

3. Apresentação do Problema de Pesquisa

O termo dependabilidade vem substituindo gradualmente no meio acadêmico outro termo chamado tolerância a falhas. A tolerância a falhas, introduzida por Avizienis em 1967 [A. Avizienis 1967], tem sido amplamente utilizada na comunidade acadêmica para determinar toda área de pesquisa focada no comportamento de sistemas computacionais sujeitos a ocorrência de falhas.

Atualmente o setor de serviços financeiros trabalha com *buffer* de capital [Abbas, Faisal, Imran Yousaf, Shoaib Ali, and Wing-Keung Wong 2021] para evitar que choques de mercado tragam colapsos econômicos para instituições. Além dos controles financeiros, muitas instituições financeiras e plataformas de negociação constroem resiliência a partir de tecnologias da informação, tendo em vista esse ponto, podemos considerar a implementação ciclos envolvendo planejamento, objetivos, indicadores e agentes de caos seguindo o modelo que será proposto nesse trabalho.

O problema abordado nesta pesquisa relaciona-se com o fato de que, atualmente, não existe um modelo de avaliação da garantia de dependabilidade disponível, além disso, customizado para sistemas da área financeira, o problema endereçado nesta pesquisa consiste em "Como avaliar a garantia de dependabilidade em sistemas de aplicações financeiras?".

O modelo em questão se torna importante porque apesar das precauções e controles atuais, ainda estamos vendo interrupções nos tempos atuais, impedindo que os clientes depositem e retirem seu dinheiro, concluam transações e executem negociações. Além disso, as instituições financeiras precisam fazer o trabalho de inovar e modernizar para melhorar a experiência do cliente e controlar os custos de plataforma cada vez maiores. No entanto, garantir confiabilidade e inovação nos projetos de sistemas é desafiador em um mundo de regulamentação pesada e crescente, bem como sistemas que dependem de sistemas legados que não podem ser modernizados. Órgãos reguladores também podem reprimir instituições financeiras, exigindo a divulgação de dados de interrupção e a apresentação de relatórios sobre como as instituições estão construindo sistemas mais resilientes. Sistemas legados baseados em mainframe tornam-se uma bagagem extra ao tentar implementar mudanças para melhorar a experiência do usuário, contudo, instituições financeiras devem encontrar uma maneira de aumentar sua vantagem competitiva sem abandonar a resiliência de seus sistemas.

3. Modelo MECADE

A Tabela 1 apresenta o MECADE: Modelo de Engenharia do Caos para Avaliação da Garantia de Dependabilidade em Sistemas Financeiros, sendo uma maneira apoiar garantia da confiabilidade aliada a modernização em sistemas financeiros. A Engenharia do Caos [Orzell, Gregory S. & Yury Izrailevsky 2019] é a prática de realizar experimentos precisos em um sistema injetando quantidades medidas de dano para observar como o sistema responde com o objetivo de descobrir como melhorar a dependabilidade do sistema. Essas são situações que os serviços inevitavelmente enfrentarão, mas no mundo crítico das finanças, devemos testar proativamente sistemas

quanto a fraquezas para garantir operações perfeitas. O modelo proposto contém 7 camadas distribuídas em distintas categorias hierárquicas.

A Figura 1 apresenta as camadas do modelo, até a terceira camada temos atividades e ações que apresentam conceitos iniciais voltados para o planejamento, objetivos internos, indicadores internos importantes para tomada de decisão. A partir da quarta camada temos atividades relacionadas a ciclos de implementações puramente técnicas, incluindo interações com o ambiente alvo.

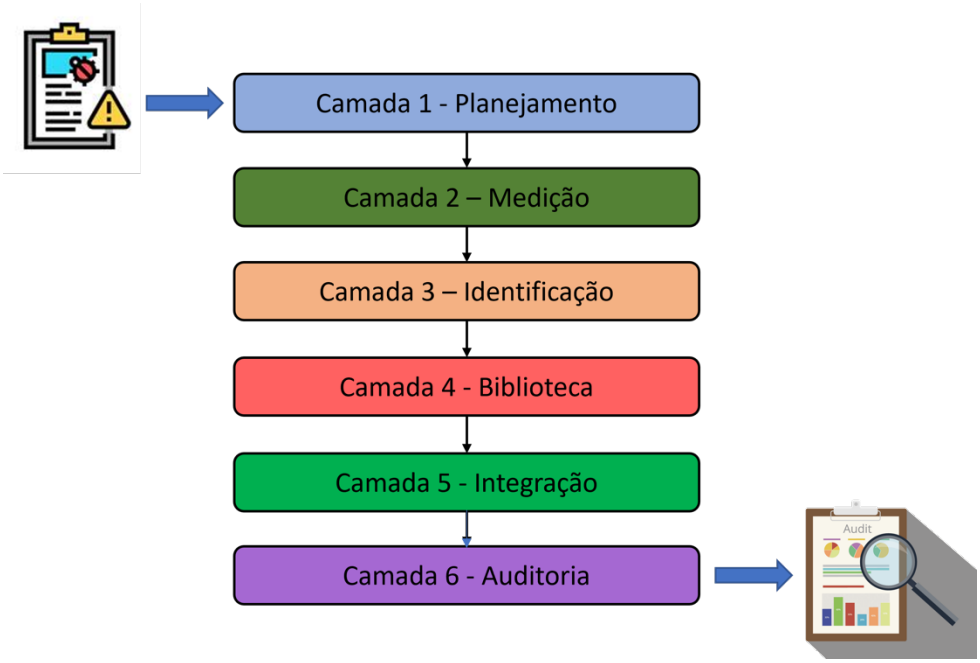

Figura 2. Classificação das camadas do modelo

A camada 1 define o planejamento do que fazer quando ocorrer uma inatividade em sistemas de tecnologia responsáveis por operações financeiras, seja transacionais entre bancos para a liquidação de pagamentos de pessoas físicas e/ou jurídicas, compensações de cheques, compras com cartões de crédito, câmbio, investimentos. O avanço da tecnologia no cenário financeiro, permitiu que a inovação ocorresse de forma muito acelerada. As *fintechs*, na modalidade de bancos digitais, baseiam seus produtos inteiramente por meio de aplicativos, no internet banking ou mobile banking, aumentando bastante o contexto e complexidade do planejamento das ações caso ocorra algum incidente gerador de inatividade. Além disso, existem muitos outros modelos de negócios no cenário financeiros como bancos de investimento, bancos múltiplos, bancos de câmbio, bancos de desenvolvimento e bancos comerciais, oferecendo inúmeros serviços. Quanto melhor for o plano, mais rápida e eficaz vai ser a resposta das equipes ao incidente.

A camada 2 define os objetivos de medição com a formulação de indicadores, como disponibilidade e tempo de resposta. Será usado para definir a expectativas a serem atingidas pela equipe de engenharia de tecnologia, além disto, indicará quais metas precisam ser atingidas e consideradas como referência. Esta mesma camada

também envolve a execução das medições e construção dos resultados usando os indicadores.

A camada 3 envolve a detecção automatizada de todos os serviços em um ambiente, oferecendo visibilidade dos sistemas, isolando as ações, tais como, direcionamento de ataques a serviços distribuídos e desestabilização de componentes com perturbações, não importando onde eles estejam sendo executados, o processo irá ajudar a descobrir quaisquer anomalias desconhecidas.

A camada 4 envolve sugestão de adoção de algumas bibliotecas de ataque abrangentes para criar resiliência a condições de falha comuns, como carga nos núcleos de processamento em condições estressantes causadas por alta demanda ou tráfego intenso, vazamentos de memória ou aplicativos com uso intensivo de recursos, armazenamento de dados com alta latência e baixo rendimento, volumes de armazenamento esgotados, falhas por desligamento de ponto de conexão ou terminal de rede, alteração de relógio entre sistemas, expiração de certificados *Secure Sockets Layer/Transport Layer Security* (SSL/TLS), eventos sensíveis ao tempo, encerramento de processo de sistema operacional específico ou conjunto de processos, falhas de aplicativos por falta de memória, interrupção completa da rede, resposta de sistemas em condições de rede lentas, envio e recebimento dados com sucesso, apesar das más condições de rede e interrupções de *Domain Name System* (DNS).

A camada 5 envolve a sugestão de adoção de algumas interfaces de programação de aplicações, com conjunto de definições e protocolos para criar e integrar softwares de aplicações de experimentos de engenharia de caos com sistemas de monitoramento, gerenciamento de incidentes e práticas combinadas de integração contínua e entrega contínua.

A camada 6 envolve a execução de auditoria, aonde cada ação na plataforma é rastreada para conformidade exigida por áreas internas do negócio, devido ao fato de as instituições financeiras terem a obrigação de reportarem sempre as áreas de auditoria internas e aos órgãos regulatórios responsáveis por fiscalizar e adotar normas para garantir que as outras entidades financeiras prestem seus serviços de forma satisfatória, estabelecendo medidas que garantam o maior controle e eficiência do sistema financeiro, tendo em vista os riscos em suas operações, principalmente por utilizarem o dinheiro de terceiros em suas atividades.

4. Considerações Finais e Situação Atual da Pesquisa

Este artigo descreveu os primeiros resultados de uma pesquisa de mestrado em andamento no Programa de Pós-graduação em Engenharia Eletrônica e Computação, área Informática do Instituto Tecnológico de Aeronáutica (ITA).

As etapas 1 e 2 da metodologia apresentada na Figura 1 já foram executadas e finalizadas. A revisão sistemática da literatura propiciou a visualização sobre o estado da arte no uso da Engenharia do Caos e sobre dependabilidade. Embora a pesquisa de mestrado em andamento foque em sistemas financeiros, foi possível perceber a baixa disponibilidade de trabalhos sobre o uso de Engenharia do Caos.

Atualmente, o foco está nas etapas 3 e 4. O modelo apresentado na Figura 2 ainda precisa ser detalhado visando definir as métricas da Camada 2, as bibliotecas da Camada 5 e os procedimentos de auditoria para a Camada 6.

Já na etapa 4, encontra-se em planejamento a execução de um experimento que prevê o uso do modelo MECADE em um sistema financeiro visando o exercício do modelo. Também é planejado realizar um grupo focal com especialistas de tecnologia em sistemas financeiros para avaliação independente do modelo MECADE.

Referências

Avieniezis, A. (1998) Infraestructure-based design of fault-tolerant systems. In: Proceedings of the IFIP International Workshop on Dependable Computing and its Applications. DCIA 98, Johannesburg, South Africa, January 12-14, 1998. p. 51-69.

Avizienis, A. (1967) “Design of Fault-Tolerant Computers,” Proc. 1967 Fall Joint Computer Conf., AFIPS Conf. Proc., vol. 31, p. 733-743.

Avizienis A, Laprie J-C, Randell B (2001) Fundamental Concepts of Dependability. Department of Computing Science, University of Newcastle upon Tyne. p. 2-3.

Bukowski, L. (2016) "System of Systems Dependability – Theoretical Models and Applications Examples." Reliability Engineering & System Safety 151 (2016): 76-92.

Faisal, A., Yousaf, I., Ali S., and Wong, W. (2021) "Bank Capital Buffer and Economic Growth: New Insights from the US Banking Sector." Journal of Risk and Financial Management 14, no. 4: 142.

Francesco, P. D., Malavolta, I. and Lago, P. (2017) "Research on Architecting Microservices: Trends Focus and Potential for Industrial Adoption", 2017 IEEE International Conference on Software Architecture (ICSA), p. 21-30.

Kratzke, N., and Quint, P. (2017) "Understanding Cloud-native Applications after 10 Years of Cloud Computing - A Systematic Mapping Study." The Journal of Systems and Software 126: 1-16.

Mohamad, K. DeFranco, J. F. and Laplante, P. A. (2017) "Software Testing: The State of the Practice." IEEE Software 34.5 (2017): p. 46-52.

Newman, S. (2021) Building Microservices: Designing Fine-grained Systems, O'Reilly Media; 2nd edition.

Toffetti, G., Brunner, S., Blöchlinger, M., Spillner, J. and Bohnert, T. M. (2017) "Self-managing Cloud-native Applications: Design, Implementation, and Experience." Future Generation Computer Systems 72: 165-79.

US20120072571 A1, Orzell, Gregory S. and Yury I., (2019) "Validating the resiliency of networked applications" Acesso em: 02 de abril. de 2021."Cloud-Native Chaos Engineering – Enhancing Kubernetes Application Resiliency". CNCF. 2019-11-06.