Uso de esquemas de Edge computing para validação de transações em instituições financeiras

Rafael Z. Silva[1], Abner Q. Santos[1], Vitor A. Hasegawa[1], Ismar Frango[1]

[1]Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie (Mackenzie)
Brasil, SP, São Paulo, Rua da Consolação, 930 - Prédio 31, 1º andar

{rafaelzamith.silva, abner.queiroz, vitor.hasegawa}@mackenzista.com.br, ismarfrango@gmail.com

Abstract. *Since they were created, financial institutions are the target of fraud because they are institutions that manage millions of people's money as vitals operations for their business idea. With the evolution of transaction and payment methods to more agile and efficient models, fraud methods also evolve. Our goal is to use edge computing to identify fraud attempts in real time on these financial institutions.*

Resumo. *Desde que foram criadas, as instituições financeiras são alvo de fraudes, por se tratarem de Organizações que lidam com dinheiro de milhões de pessoas, com operações vitais para sua ideia de negócio. Com a evolução de métodos de transação e pagamento para modelos mais ágeis e eficientes, evoluem-se também os métodos de fraude; com isso, nosso objetivo é estudar o uso de edge computing para identificar e prevenir em tempo real as tentativas de fraude nessas instituições financeiras.*

1. Introdução

As atividades bancárias, altamente dependentes de relação interpessoal, eram mais facilmente manipuladas com técnicas simples, podendo envolver vários tipos de fraudes, como: documentos fraudulentos, dinheiro falsificado. Uma relação de proximidade com os bancários, possibilita facilitações para obtenção de empréstimos absurdos, abrir contas em nome de terceiros e realizar movimentações inadequadas; mesmo a evolução da checagem de informações, não foi suficiente para impedir essas práticas.

Com a robotização de muitas atividades, as táticas para fraude tiveram que se aprimorar, com clonagem de cartões, uso de câmeras para roubar senha e dados dos usuários, táticas de phishing, falsidade ideológica - simular uma identidade alternativa, fingindo ser funcionário do banco, para induzir o usuário ao erro. Então, a utilização de dados corretos e verdadeiros não barram atividades financeiras ilícitas. Por causa desta abertura para possíveis fraudes bancárias, novos métodos de detecção deverão ser desenvolvidos.

Um dos vários problemas enfrentados para o combate à fraude é a quantidade de informação disponibilizada ao sistema para analisar as transações, por ser cobrado um baixo tempo de latência ao realizar uma transação. Um celular ou um terminal de pagamento não pode mandar os dados brutos de tudo que acontece, quando recolhe os dados; usar um servidor intermediário de borda possibilita a captura de dados brutos pelos terminais, podendo capturar imagens, outros dados biométricos como segundo

fator de autenticação, em questão de instantes - relativo ao tempo tomado ao apertar uma única tecla.

Agora, com uso de um servidor de borda, a filtragem de dados pode ser muito mais avançada. Com o uso deste instrumento, a análise das informações pode ocorrer de forma refinada, com a aplicação de filtros, ou de maneira simples. Inicialmente, os dados podem ser tratados de forma mais bruta, com um refinamento posterior, se necessário, o dado poderia ser enviado ao servidor em cloud, ou até usar o servidor em cloud para um treinamento dos algoritmos usados nos servidores de borda, dispensando uma etapa.

Outro problema seria o balanceamento dos dados, já que existem significativamente mais transações lícitas do que ilícitas. Com mais informações é possível ter mais granularidade ao tratar esses dados, abrindo portas para estudos mais específicos, utilizando novos métodos de detecção que visam a maior quantidade de dados com menos latência.

Este trabalho tem o objetivo de analisar e quantificar as vantagens ou desvantagens do uso de edge computing para detecção de fraude, observando se é viável e benéfico para empresas financeiras, em quais casos esse modelo não deveria ser aplicado, considerando o desempenho do processamento das transações.

2. Referencial teórico

2.1 Edge Computing

Computação em borda (Edge computing) se difere do conceito da computação em nuvem tradicional, ao colocar o node de computação na borda da rede o mais próximo possível da fonte de dados [CAO, 2020].

Algumas vantagens do edge são: a análise e processamento rápido dos dados, já que não existe a limitação de banda em relação a nuvem tradicional [CAO, 2020] e o alívio de banda para a nuvem tradicional, uma vez que dados já processados e filtrados que seriam enviados a nuvem [SATYANARAYANAN, 2017].

Por último, cita-se a maior privacidade envolvida no método estudado. A utilização do edge permite que os dados sejam anonimizados na borda, na qual não existe armazenamento à longo prazo. Além disso, os dados percorreriam um caminho menos expositivo, somente até a borda, onde existe uma maior segurança. [KHAN ET AL., 2019].

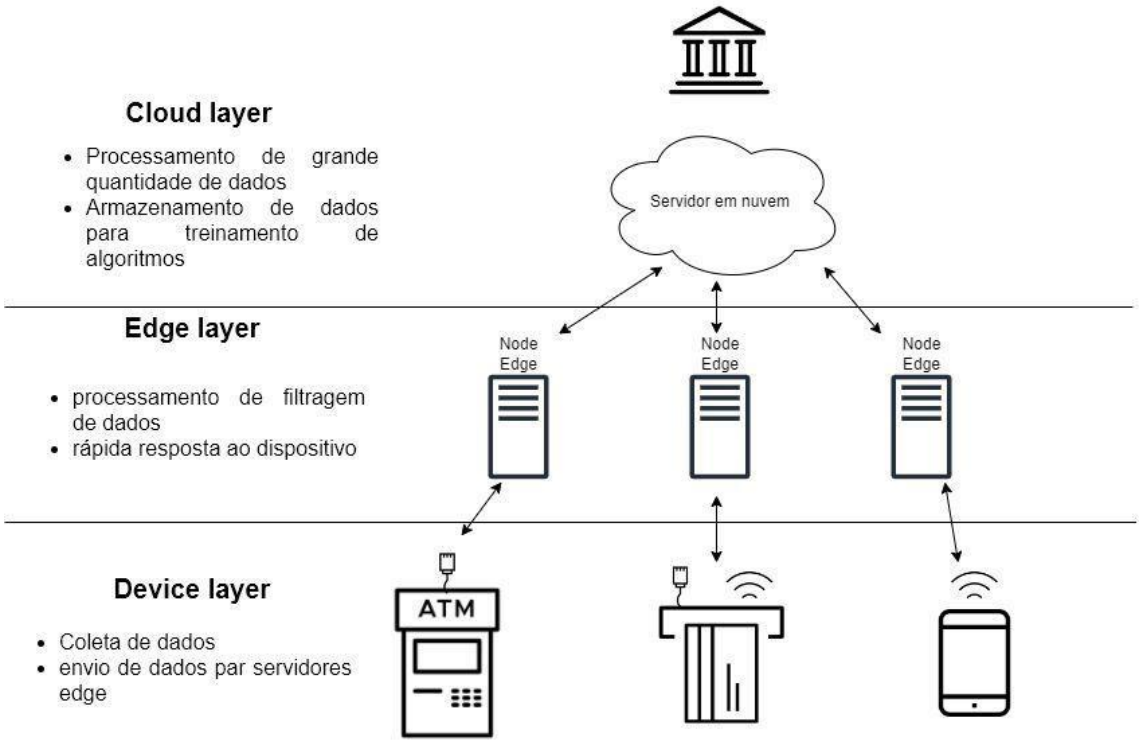

Figura 1. Modelo sugerido ao uso de edge.

Alguns desafios podem existir ao migrar para o modelo com edge, como o de transferência de dados e a de workload. O processo de transferência pode ser realizado por meio de duas técnicas principais de abordagem. O primeiro meio seria criar todo cenário de edge antes de utilizá-lo, existindo cópia de todas as informações; tal opção é mais segura, porém mais custosa. A outra técnica seria a transferência de tarefas e dados, ao mesmo tempo que se implementa o modelo edge [WANG, 2018]. Esses dois métodos deverem ser apurados ao calcular os custos do novo modelo sugerido.

Existem alguns meios de ataque nos quais o edge é mais vulnerável, como man in the midle ou DDOS. Isto acontece porque, ao estar na borda, existem menos camadas de defesa para os nodes - os nodes que receberão pacotes de aplicativos e site idealmente deverão ser diferenciados de servidores que trabalham com meios mais protegidos e sensíveis como os meios de pagamento e caixas. Um ataque localizado pode afetar uma região pequena, mas, se for focado em uma área de alto tráfego, pode causar mais dano que a mesma tentativa de ataque a um node de cloud, no qual existem melhores defesas [XIAO, 2019].

2.1.1 Localização de nodes

Ao pensar em uma localização, precisamos considerar a densidade demográfica relativa à área analisada. Em uma cidade como São Paulo, um node até conseguiria atender um bairro, mas com um custo altíssimo para o conjunto total de nodes. Tal custo está associado à liberdade de configuração de cada node para atender a necessidade local, que também inclui toda uma infraestrutura para sustentá-lo.

Entretanto, a questão da infraestrutura é menos relevante em São Paulo, pois existe a possibilidade de ação conjunta às operadoras de telefonia, já que muitos dispositivos utilizam de rede de celular de operadoras para comunicar com os bancos que irão permitir ou negar a transação.

2.2 Fraudes

Fraude é um artifício empregado com a finalidade de enganar uma pessoa e causar-lhe prejuízo patrimonial ou extrapatrimonial, pode abranger uma gama ilimitada de formas de atuação. À título exemplificativo, observam-se alguns tipos de fraude de cartões ou dados, descritos por Sam Maes et al. (2002):Copiar o cartão e conseguir sua senha por meio de algum artificio ou vendedores cobrando indevidamente mais que o acordado

2.2.1 Detecção de fraude

Para detecção de fraudes em cartões, normalmente, são usados modelos não supervisionados; o procedimento não utiliza dados de transações não fraudulentas ou fraudulentas, mas observa as mudanças de comportamento sobre um modelo, criado com o uso de redes neurais. [KOU, 2004].

Um problema para a detecção de fraude, seria o desbalanceamento dos datasets porque a maioria dos algoritmos não foram desenvolvidos pensando na grande diferença entre os dois conjuntos possíveis, onde esses algoritmos dependem de amostragem representativa e, dependendo dos parâmetros, pode ser que nem cheguem a pegar um caso de uma transação fraudulenta [POZZOLO, 2014].

Já existem análises no mercado que associam menores quantidades de fraudes realizadas em sites de compras às táticas de detecção de fraudes mais avançadas. Em 2013, a pesquisa de Leandro Alves et al. pontua: “Apesar da elevação na quantidade de transações fraudulentas no ano de 2010, chegando ao ápice em Set/12 (1,2%), a diminuição observada no período entre 2010 e 2012 deu-se principalmente devido à revisão e sistematização do processo de prevenção de fraude.”, ao analisar o seguinte gráfico sobre sua pesquisa:

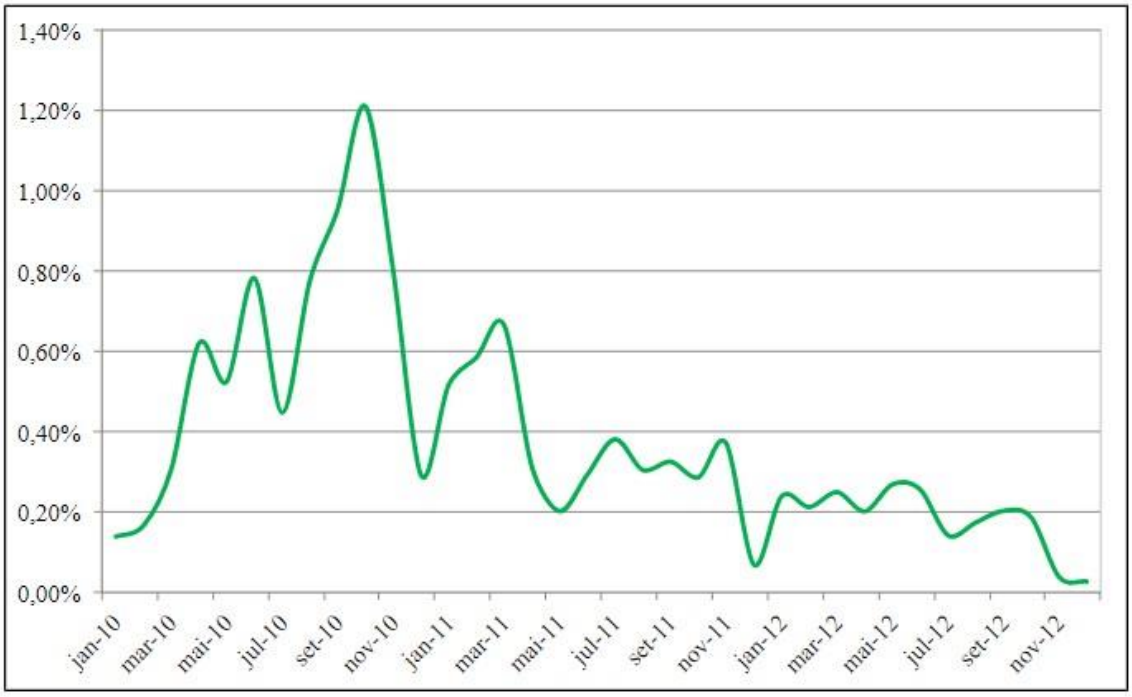

Figura 2. Resultado da pesquisa de Leandro Alves et al. (Alves et al., 2013).

2.3 Métodos de transferência de dinheiro

2.3.1 PIX

Introduzido em novembro de 2020, com o objetivo de atender a demanda de transferência rápida de dinheiro, o PIX eliminou custos transacionais e diminuiu erros, deficiências e barreiras práticas de outros meios de pagamento, como a obrigatoriedade de saber vários dados a quem transferir o dinheiro, ou a pagar uma conta (por TED ou DOC).

As vantagens deste meio de transação estão explicitadas em citações presentes no site do banco central, por exemplo: “[...] com PIX, as transações podem ser iniciadas por meio do telefone celular, sem a necessidade de qualquer outro instrumento” e “O PIX tende a ter um custo de aceitação menor por sua estrutura ter menos intermediários.” [BCB, 2021].

Ao entrar na parte mais técnica do PIX, encontra-se, em sua documentação, que várias medidas de segurança são tomadas seguindo boas práticas. Desta forma, um vetor de ataque seria mais viável a nível de usuário, por meio de phishing ou engenharia social, do que transações ilícitas no próprio sistema. Apesar da aparente confiabilidade, não é possível descartar essas transações e garantir que todas são legitimas; é possível aplicar medidas de segurança um nível acima do protocolo em si [BCB, 2021].

2.3.2 PIX, suas fraudes e seus meios de prevenção

Ao pesquisar notícias locais sobre fraudes do PIX, é possível obter os seguintes resultados: “Fraudes no PIX passam de R$ 300 milhões por mês e bancos ficam sob pressão” [Casado, et al. 2022]. Neste contexto de fraudes, o Diretor de organização do sistema financeiro e resolução do banco central, em entrevista ao Jornal Estadão, disse: "Poucas instituições utilizaram ferramentas para identificar fraudes, agora nós estamos obrigando [as instituições]" [Mello, 2021], o diretor acrescenta que o reforço da

segurança do PIX pode diminuir fraudes em outras áreas, como golpes com leitores de cartão.

Entretanto, apesar da segurança no meio da transação do PIX e da transparência, cabe às instituições financeiras controlarem a autenticidade e veracidade das transações. Tal análise deve ser realizada pelas instituições financeiras remetentes e receptoras do pagamento, cabendo a ambas o bloqueio da transação, resultando em uma maior efetividade no controle de fraudes.

2.4 Custos da fraude

Por conta da baixa quantidade de dados recentes publicados sobre o assunto, utiliza-se como base o cálculo que o diretor do BCB apresentou sobre a porcentagem de fraudes, no qual a cada 100mil transações, 0.5 são suspeitas de fraudes.

Conforme disposto no Site do BCB, seguem as métricas da quantidade de transações realizadas com o PIX e o respectivo valor:

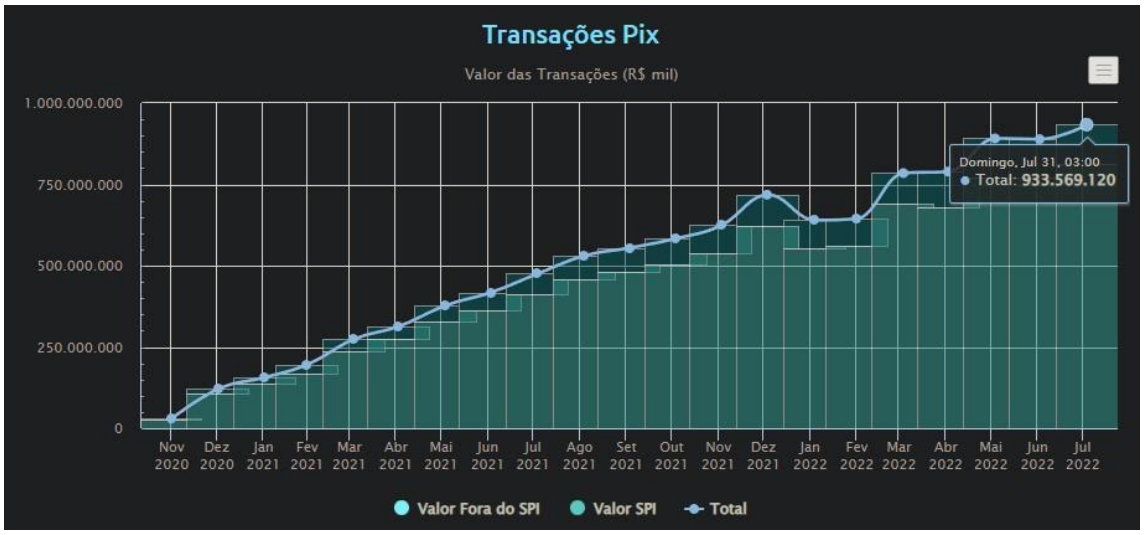

Figura 3. Transações do PIX por valor total (BCB, 2022).

Figura 4. Transações do PIX por quantidade (BCB, 2022).

De acordo com estes dados, são realizadas mensalmente 2.068.358.897 transações, com valor total de R$ 933.565.120,00 (em torno de 0,5 reais por transação); assim, conclui-se que as perdas, por conta de fraudes no PIX, alcançam 10.341,00 reais por mês, sem contar o equivalente necessário para cobrir os danos pela fraude.

2.5 Custos de operações

O estudo "Post-Quantum Cryptography methods applied to the Brazilian instant payment system (Pix): A feasibility study [NETO, et al, 2022]" comenta, brevemente, sobre tempo de transação médio necessário para o funcionamento ininterrupto da plataforma, que seria de 50ms, contendo 2000 TPs (transações por minuto) por node.

O PIX tem 777 participantes únicos cadastrados em seu sistema [BCB, et al, 2022], portanto seriam 2.661.980 transações mensalmente por participante e, em média, 62 transações por minuto de cada participante.

Com estas parâmetros temporais, é possível estimar um custo em cloud e em nodes edge, considerando que mais nodes edge seriam agregados a um cloud; enfatiza-se que a autenticação do usuário deve ocorrer antes da transação ser finalizada, o que acontece em um pouco menos de 1 segundo.

Comparando com métodos atuais, a autenticação é faseada: uma senha para acessar a plataforma bancária, uso de token digital para validação do aparelho e uma senha final para autorizar a transação, diferente da inicial para entrar na plataforma. Por consequência, ao simular uma transferência, o usuário perde em média 3,7s esperando a autenticação ocorrer, mais 1,2s digitando as senhas.

2.6 Escalabilidade

Para o contexto de escalabilidade, descreve-se a seguir a relação de localidade sobre alguns casos de uso práticos para Edge e Cloud. A arquitetura de Cloud, na qual, normalmente, a localização e posição dos agentes são questões primordiais, em contextos urbanos, especificamente metrópoles, a localização não se mostra um fator tão definitivo, visto que a densidade populacional e proximidade a datacenters é superior, em comparação ao contexto de cidades interiores, onde não há proximidade a datacenters, favorecendo o uso de Edge juntamente com Cloud, pois o processamento, em sua maior parte, ocorreria no próprio dispositivo.

2.7 Simulação

O simulador EdgeCloudSim é feito em Java e tem, com a base do framework para soluções em nuvem, o CloudSim. O simulador conta com aspectos configuráveis para obtenção de cenários de comparação de Edge e Cloud; tais aspectos são, por exemplo, o número de servidores edge e seus parâmetros de processamento de dados, como MIPs (Million Instructions Per Second), núcleos de processamento, quantidade de RAM, armazenamento, o número de aparelhos e as aplicações dentro desses aparelhos que cumprirão "tasks". Essas "tasks" são distribuídas entre os "tiers", de acordo como peso de processamento dado para cada aplicação configurada para os dispositivos, e geram dados para o fluxo

Através desses dados, o simulador elabora três cenários de fluxo de dados, chamados de "tier". O primeiro tier seria os dados desses aplicativos passando apenas

pelos servidores Edge, o segundo, seria com os dispositivos conectados em uma rede e processando dados em cloud e o terceiro, seria com o Orquestrador Edge, que é um módulo desenvolvido para a distribuição efetiva das tasks dos aplicativos em cada dispositivo. A simulação leva em conta também a mobilidade dos dispositivos, reproduzindo o funcionamento de smartphones ou dispositivos integrados.

2.7.1 Cenário da Simulação

O contexto relacionado aos nossos cenários de simulação, similar ao contexto referenciado no artigo do autor, configura um ambiente virtual, onde estudantes, utilizando servidores edge localizados no campus, realizam processos de transação de dados. O processo que utilizamos é de uma transação bancária com autenticação facial. Nesse cenário, os dados da transação seriam enviados juntamente a imagem fornecida para validação.

Para atingir o propósito de nossas simulações, assumimos que, ao obtermos tempos de processamento inferiores aos de cloud, teremos sucesso. O risco de fraudes em transações pode ser relacionado diretamente ao tempo e eficácia do processamento de dados porque técnicas de processamento de dados podem ser aplicadas para o conjunto de dados que induzem fraude [Martins E., et al. 2022]. Ao aliar Edge com Cloud, obtermos um processamento de baixa latência e escalável, possibilitando a verificação de dados, como: informações de conta, balanço disponível e execução de detecção de fraudes próximas ao tempo real. O resultado da simulação foi um tempo de execução próximo ao instantâneo, diminui-se o risco de fraudes e, por consequência, o prejuízo causado por fraudes em instituições financeiras, inclusive com a adição dos custos de manutenção dos servidores Edge e Cloud.

3. Metodologia

A metodologia de pesquisa consistiu na leitura de bibliografia relevante e na simulação apresentada. Os papéis de cada etapa da metodologia foram os seguintes: a revisão bibliográfica dos artigos referenciados foi realizada a fim de definir a avaliação de riscos e custos e foi basilar para a definição dos parâmetros e do tipo da simulação, utilizada para obter dos dados finais expostos.

Por fim, avaliamos os resultados obtidos na simulação e, a partir disso, obtivemos a conclusão sobre a eficiência de Edge Computing em detecção de Fraudes, com enfoque em diminuição de latência e de riscos de execução de métodos fraudulentos, em relação ao tempo de processamento.

Assim, desenvolvendo a metodologia deste estudo na seguinte sequência:

1. Revisão bibliográfica.
2. Estudo da bibliografia referenciada.
3. Escolha da plataforma de simulação.
4. Definição de parâmetros para a simulação.
5. Análise dos resultados.
6. Elaboração da conclusão.
7. Redação final do artigo.

8. Submissão do artigo na plataforma OJS.

4. Desenvolvimento

Para o desenvolvimento dos resultados da simulação, configuramos parte dos atributos para a devida adequação ao cenário de transações feitas através de dispositivos e ao processamento utilizando uma linha de Edge coligado com Cloud, observando que nesta situação há o aumento do poder de processamento para dados, quando aumentam as quantidades de dispositivos e suas transações.

Em nossa simulação, com base no cenário destacado anteriormente do PIX, não seria lógico analisar um node edge com menos de 500 devices, pois não representaria a aplicação real de edge computing frente ao crescente uso de dispositivos móveis para o contexto PIX, com mais de 130.000.000 usuários que realizaram transações PIX, com tendência de crescimento elevado nos próximos meses. [BCB, 2022].

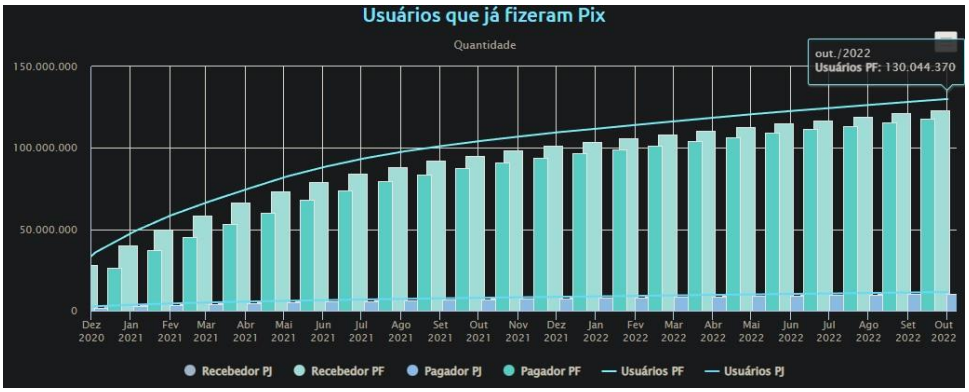

Figura 6. Gráfico do histórico de número de usuários que já fizeram Pix.

Ao observar o gráfico, percebe-se que estamos atingindo um limite possível de contas. Esta é uma etapa na qual a otimização dos custos operacionais se beneficiaria imensamente da plataforma, pois, após um investimento inicial mais elevado, os custos de expansão seriam extremamente baixos e os gastos à longo prazo seriam, majoritariamente, destinados à manutenção.

4.1 Configurações da Simulação

Após todas as pesquisas realizadas por nosso grupo, considerando o contexto atual de infraestrutura para computadores, servidores, datacenters e celulares, a disposição de usuários atuais do PIX e número de transações, escolhemos algumas configurações específicas para o desenvolvimento de nossas simulações.

Para nossa simulação, adotamos um node de cloud com 4 VMs, cada VM conta com 4 núcleos de processamento com potência de 10.000 MIPs (equivalente à um Intel Xeon E5-2609 v4), 32GB de RAM e disco de 1 TB; enquanto, o node Edge excuta suas tasks em duas VMs, com 2 núcleos cada e uma potência de 1000 MIPs (Intel Pentium N4200), 2 GB de RAM e 50GB de disco.

O parâmetro de tempo atribuído na simulação foi de 3 horas, com um node de cada tipo, e com transações trocadas com cada "tier" aumentando de 100 em 100 dispositivos, com o objetivo de proporcionar um teste de estresse sobre a simulação.

A seguir a configuração usada nos 4 cenários simultâneos (aplicativos) nos nodes:

- Primeiro seria um workload de 10% no edge e 2% na cloud, no qual seriam necessários 2000 ciclos para processar (consideramos 30% do processamento total para ele).
- Segundo com um workload de 5% no egde e 0.5% na cloud, no qual seriam necessários 400 ciclos para processar (consideramos 20% do processamento total para ele).
- Terceiro com um workload de 30% no egde e 3% na cloud, no qual seriam necessários 3000 ciclos para processar (consideramos 20% do processamento total para ele).
- Quarto seria um workload de 10% no edge e 1% na cloud, no qual seriam necessários 2000 ciclos para processar (consideramos 30% do processamento total para ele).

Ao atingir 2000 dispositivos simultâneos, a simulação passa para o próximo modelo. Seguem abaixo os modelos da simulação:

- "Single-Tier": resultados para os testes que consideram apenas servidores edge para processamento.
- "Two-Tier": neste modelo os dispositivos acessam o Cloud através de uma conexão com a internet.
- "Two-Tier_With_EO": são as duas camadas juntas com o Edge desembarcando tasks para cloud [SONMEZ, 2017].

Além disso, apreciamos uma falha na transação financeira, quando o tempo de processamento ultrapassa 20 segundos, já que é um intervalo considerável para processar um pacote pequeno de dados.

5. Resultados

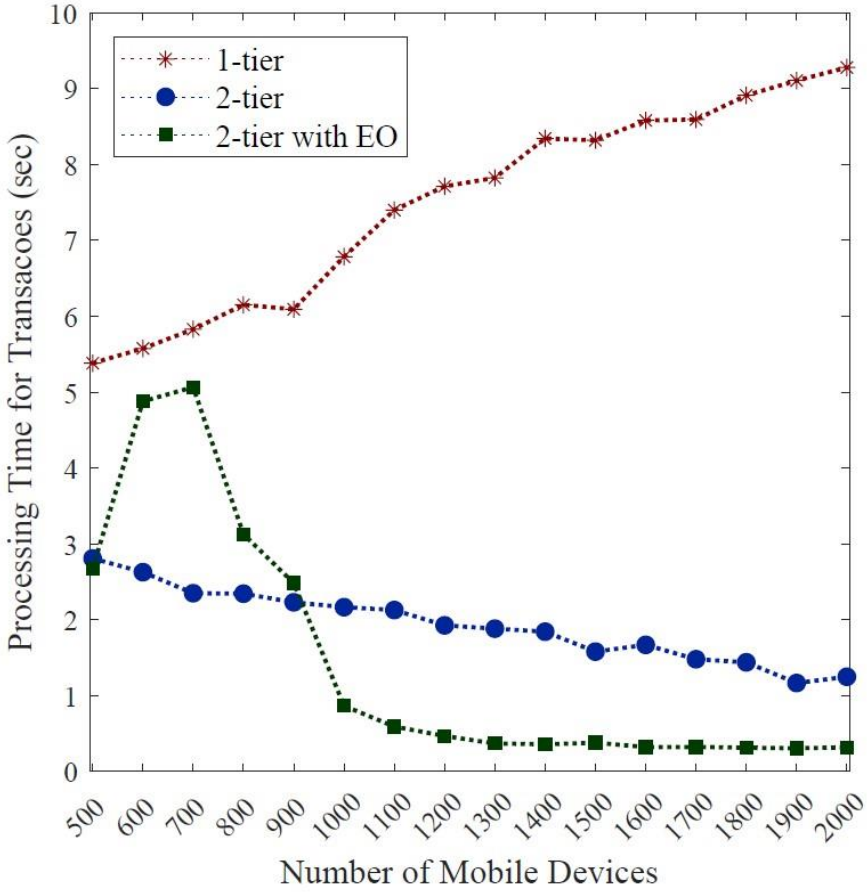

Figura 7. Tempo de Processamento para transações em segundos, por número de Dispositivos para o terceiro aplicativo.

Com a execução da a simulação nas métricas definidas acima, para as quais consideramos um load de 3% por transação na cloud e 30% no edge, averiguamos que o "Two-Tier_With_EO" possui uma vantagem considerável, por integrar o melhor dos dois mundos: com Cloud e o Edge, pois consegue processar as tasks enviadas pelas aplicações dos dispositivos. Entretanto, notamos que a arquitetura Two-Tier_With_EO acaba sendo ultrapassada, após 500 dispositivos, pelo processamento em Two-tier.

Desta forma, ao ampliarmos a escalabilidade, ou seja, em uma conjuntura com um maior número de dispositivos, visualiza-se a vantagem considerável da arquitetura TwoTier_With_EO, superando em 1 segundo.

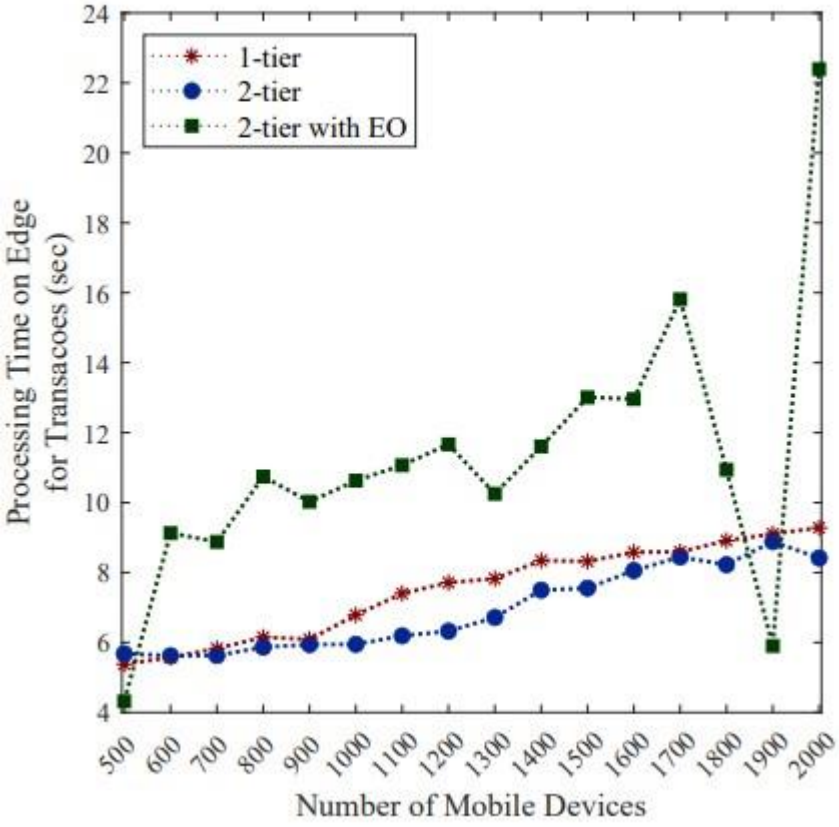

Figura 8. Tempo de Processamento para transações em segundos, por número de Dispositivos para o segundo aplicativo forçando processamento em edge.

Em relação aos demais aplicativos, a simulação resultou em uma certa paridade entre edge e cloud e, se forçamos uma preferência ao processamento à um node edge, o Two-Tier_With_EO acaba sendo desfavorecido, principalmente, por quantidade transações falhas, com quase 53% de transações falhas, indicando uma deficiência majoritária em um único node edge:

```
# of tasks (Edge/Cloud/Mobile): 1314318(1044999/269319/0)
# of failed tasks (Edge/Cloud/Mobile): 701689(700629/1060/0)
# of completed tasks (Edge/Cloud/Mobile): 612629(344370/268259/0)
# of uncompleted tasks (Edge/Cloud/Mobile): 304(282/5/17)
# of failed tasks due to vm capacity (Edge/Cloud/Mobile): 687847(687847/0/0)
# of failed tasks due to Mobility/WLAN Range/Network(WLAN/MAN/WAN/GSM): 13842/0/0(0/0/0/0)
percentage of failed tasks: 53.388069%
average service time: 4.964181 seconds. (on Edge: 8.041230, on Cloud: 1.014106, on Mobile: NaN)
average processing time: 4.576302 seconds. (on Edge: 7.996676, on Cloud: 0.185492, on Mobile: NaN)
```

Figura 9. Log da simulação para Two-Tier_With_EO com 1900 devices.

A performance no teste de estresse passa de um limite normal, no qual quase 1% de todas as transações seriam processadas, considerando que todos os usuários cadastrados fizessem uma transferência ao mesmo tempo. No entanto, obtivemos uma resposta viável de 344.370 transações processadas em menos de 20s para edge e 268.259 para 1900 dispositivos diferentes.

Em busca da melhor otimização, alcançamos um total de 573.872 transações com edge, processando 346.417 delas ainda no cenário de balanceamento entre nodes edge e cloud (Two-Tier_With_EO) e uma média de 1800 devices para cada node.

Com um olhar mais atento, delibera-se que existem mais vantagens no segundo cenário, ao comparar o número de tasks completas proporcionalmente ao valor de processamento total garantido (em amarelo, valor já corrigido), assim como pela quantidade de tasks recebidas vulgo sua eficiência (valor em azul):

cenário 1

# of tasks (Edge/Cloud): 841240(667259/173981)

# of failed tasks (Edge/Cloud): 410438(409807/631)

# of completed tasks (Edge/Cloud): 430802(257452/173350) - 1.436.006 - 50%

---

cenário 2

# of tasks (Edge/Cloud): 43029(34065/8964)

# of failed tasks (Edge/Cloud): 5860(5838/22)

# of completed tasks (Edge/Cloud): 37169(28227/8942) - 185.845 - 86%

---

cenário 3

# of tasks (Edge/Cloud): 33929(20336/13593)

# of failed tasks (Edge/Cloud): 20371(20321/50)

# of completed tasks (Edge/Cloud): 13558(15/13543) - 67.790 - 39,9%

---

cenário 4

# of tasks (Edge/Cloud): 200213(168504/31709)

# of failed tasks (Edge/Cloud): 107870(107781/89)

# of completed tasks (Edge/Cloud): 92343(60723/31620) - 307.810 - 46%

6. CONCLUSÕES

Com base nos estudos e simulações, para nossas conclusões, primeiramente, devemos esclarecer que os dados obtidos são dependentes de diversos fatores de configurações escolhidos para a simulação; logo, os dados podem variar de acordo com a demanda e com a especificação do local que será abordado. Todavia, analisando o cenário proposto para este estudo, as conclusões são que uma camada Edge para processamento de dados é efetiva.

Além disso, concluímos que o ganho de processamento usando camada de Edge computing e Cloud é extremamente significativo, à medida que aumentamos o número de dispositivos, tal aumento torna-se primordial quando enfocamos PIX e outras transações bancárias.

De qualquer forma, como foi observado na simulação, é necessária uma otimização por parte do código que roda nos servidores, já que, apesar da maior quantidade de dados processados pelo cenário 1, mais de 50% de suas tarefas foram perdidas por ultrapassar o tempo limite definido e, em termos de uma aplicação em produção, principalmente, com a importância das transações bancárias, este valor tem que estar o mais próximo possível de 0.

Portanto, Edge computing é um conceito muito relevante, não só na academia, mas em matéria de solução para processamento. Acreditamos que o conceito ainda está prematuro e pode evoluir, a partir de inovações na análise de custo, com avaliação em diversas áreas, por exemplo, em parcerias com operadoras de telefone e/ou grandes provedoras de computação em nuvem, que tiverem a intenção de expandir sua área geográfica.

Outro objeto de estudo interessante, inclusive pensando em benefícios para o mercado, seria a implementação de novos métodos de autenticação para o exercício de detecção de fraudes, principalmente voltado para as transações bancários. Dentre estes métodos de verificação de autenticidade, enfatiza-se o estudo da aplicação de Edge computing.

Nosso trabalho pode aumentar visibilidade do conceito e auxiliar na proliferação do uso de esquemas de Edge computing em conjunto a Cloud, direcionado para o processamento de pagamentos. Acreditamos que essa visibilidade, trazida pelos bons desempenhos de processamentos dos nodes edge em nossa pesquisa, pode incentivar pesquisas e investimentos de empresas, com o objetivo de diversificar tentativas de aplicações no mundo real, visto que o emprego deste conceito em situações concretas demonstrou-se eficiente, com redução de gastos, melhoria na experiência do usuário e, principalmente, como enfoque do nosso trabalho, aumento na segurança de transação.

Referências

ALMEIDA, Felipe Sousa Andrade de et al. A vulnerabilidade no ciberespaço: estudo sobre a prática de infração dos crimes cibernéticos. 2020.

ALVES, Leandro de Carvalho; GONÇALVES, Fabiolla Valeria; MOIZINHO, Luzelia Calegari Santos. O custo da fraude: uma análise de um eCommerce brasileiro. In: Anais do Congresso Brasileiro de Custos-ABC. 2013.

BCB. Manual de Segurança do Pix Versão 3.4, Banco Central do Brasil, 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados>. Acesso em: 10/11/2022.

BCB. Manual de Padrões para Iniciação do Pix 2.6.2. Banco Central do Brasil, 2021. Disponível em: <https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/II_ManualdePadro esparaIniciacaodoPix.pdf>. Acesso em: 10/11/2022.

BCB PIX Banco Central do Brasil, 2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix>. Acesso em: 10/11/2022.

BCB, Lista de Participantes do PIX, 2022. Banco Central do Brasil, 2021. Disponível em: <https://www.bcb.gov.br/content/estabilidadefinanceira/pix/ListadeparticipantesdoPi

x.pdf> Acesso em: 10/11/2022CAO, Keyan et al. An overview on edge computing research. IEEE access, v. 8, p. 85714- 85728, 2020.

CHAUDHARY, Khyati; YADAV, Jyoti; MALLICK, Bhawna. A review of fraud detection techniques: Credit card. International Journal of Computer Applications,v.45, n. 1, p. 39-44, 2012.

FERREIRA, Aurélio Buarque de Holanda. Novo dicionário Aurélio da língua portuguesa. 4. ed. Rio de Janeiro: Nova Fronteira, 2008.

JOHN, Samuel Ndueso et al. Realtime fraud detection in the banking sector using data mining techniques/algorithm. In: 2016 international conference on computational science and computational intelligence (CSCI). IEEE, 2016. p. 1186-1191.

KHAN, Wazir Zada et al. Edge computing: A survey. Future Generation Computer Systems, v. 97, p. 219-235, 2019.

KONG, Fanrong; LU, Hongxia. Risk Control Management of New Rural Cooperative Financial Organizations Based on Mobile Edge Computing. Mobile Information Systems, v. 2021, 2021.

KOU, Yufeng et al. Survey of fraud detection techniques. In: IEEE international conference on networking, sensing and control, 2004. IEEE, 2004. p. 749-754.

KOVACH, Stephan. Detecção de fraudes em transações financeiras via Internet em tempo real. 2012. Tese de Doutorado. Universidade de São Paulo.

KUMUTHINIDEVI, S. A study on effectiveness of the internal control system in the private banks of trincomalee. International journal of scientific and research publications, v. 6, n. 6, p. 600-612, 2016.

KURSHAN, Eren; SHEN, Hongda. Graph computing for financial crime and fraud detection: Trends, challenges and outlook. International Journal of Semantic Computing, v. 14, n. 04, p. 565-589, 2020.

MAES, Sam et al. Credit card fraud detection using Bayesian and neural networks. In: Proceedings of the 1st international naiso congress on neuro fuzzy technologies. 2002.

Martins, Emerson; Verardi Glegale, Napoleão. Detecção de fraudes no segmento de crédito financeiro utilizando aprendizado de máquina: uma revisão da literatura. e-TECH, Florianópolis, v. 15 n. 3 (2022)

NETO, Aristides Andrade Cavalcante, 2022. Post-Quantum Cryptography methods applied to the Brazilian instant payment system (Pix): A feasibility study.

NYAKARIMI, S. N., Kariuki, S. N., & Kariuki, P. (2020). Risk assessment and fraud prevention in banking sector.

OLOWOOKERE, Toluwase Ayobami; ADEWALE, Olumide Sunday. A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach. Scientific African, v. 8, p. e00464, 2020.

POZZOLO, Andrea Dal et al. Learned lessons in credit card fraud detection from a practitioner perspective. Expert systems with applications, v. 41, n. 10, p. 4915-4928, 2014.

RODRIGUES e Froufe, joão Manoel Pinho de Mello, Poucos bancos usaram ferramentas contra fraudes em Pix, TED e outros, diz BC. [Entrevista concedida a] Eduardo Rodrigues e Célia Froufe. Poucos bancos usaram ferramentas contra fraudes emPix, TED e outros, diz BC, UOL, agosto, 2021.

SABELLA, Dario et al. Developing software for multi-access edge computing. ETSI white paper, v. 20, p. 1-38, 2019.

SAMANEHSOROURNEJAD, Zahra Zojaji; ATANI, Reza Ebrahimi; MONADJEMI, Amir Hassan. A survey of credit card fraud detection techniques: Data and technique oriented perspective. 2016.

SANTOS, Rodrigo Usignolo dos. Análise do impacto do relacionamento dos portadores de cartões de crédito com os bancos no Brasil, na utilização do produto após casos de fraude. 2013.

SATYANARAYANAN, Mahadev. The emergence of edge computing. Computer, v. 50, n. 1, p. 30-39, 2017.

SINGH, Charan et al. Frauds in the Indian banking industry. IIM Bangalore Research Paper, n. 505, 2016.

SONMEZ, C., Ozgovde, A., and Ersoy, C. (2017). Edgecloudsim: An environment for performance evaluation of edge computing systems. IEEE.

WANG, Shangguang et al. A survey on service migration in mobile edge computing. IEEE Access, v. 6, p. 23511-23528, 2018.

XIAO, Yinhao et al. Edge computing security: State of the art and challenges. Proceedings of the IEEE, v. 107, n. 8, p. 1608-1631, 2019.

ZAREAPOOR, Masoumeh; SEEJA, K. R.; ALAM, M. Afshar. Analysis on credit card fraud detection techniques: based on certain design criteria. International journal of computer applications, v. 52, n. 3, 2012.