Título do Projeto: "Aplicação de Modelos de Machine Learning para Testes de Segurança em Smart Contracts do Tesouro Direto do Brasil, com Enfoque na Interoperabilidade dos sistemas. "

Nome da Equipe: GUIZO

Data: 04/12/2023

Resumo Executivo:

Este projeto propõe a aplicação de modelos de machine learning para realizar testes de segurança em smart contracts do Tesouro Direto do Brasil, com ênfase na interoperabilidade entre soluções da Web2 e Web3. Inspirado no artigo "Deep learning-based solution for smart contract vulnerabilities detection (Xueyan Tang *, Yuying Du , Alan Lai , Ze Zhang & Lingzhi Shi)" nosso objetivo é identificar vulnerabilidades específicas e desenvolver modelos personalizados. As contribuições esperadas incluem diretrizes para reforço da segurança, identificação de padrões de fraude e simulações realistas para treinamento. A implementação de inteligência artificial visa fortalecer a resiliência do sistema financeiro, garantindo a integridade e segurança dos ativos no contexto do Tesouro Direto.

Introdução:

O avanço da tecnologia blockchain, notadamente no contexto de contratos inteligentes, tem desempenhado um papel crucial na transformação de setores financeiros tradicionais, como evidenciado pelo Tesouro Direto do Brasil. Este estudo propõe a utilização de modelos de machine learning para testes de segurança em smart contracts, com ênfase na interoperabilidade, quando esses contratos inteligentes interagem com soluções da Web2.

Embasa-se no Artigo:

Para embasar esta tese, destacamos o artigo "Deep learning-based solution

for smart contract vulnerabilities detection" (autor Xueyan Tang *, Yuying Du , Alan Lai , Ze Zhang & Lingzhi Shi), que aborda a aplicação bem-sucedida de técnicas de aprendizado profundo na detecção de vulnerabilidades em contratos inteligentes. A proposta apresentada no artigo, denominada Lightning Cat, utiliza

modelos como Optimized-CodeBERT, Optimized-LSTM e Optimized-CNN para identificar e corrigir vulnerabilidades, demonstrando a eficácia dessas abordagens.

Contextualização:

Considerando a crescente adoção de soluções da Web2 pelo Tesouro Direto do Brasil, a segurança dos smart contracts torna-se uma preocupação essencial. A interoperabilidade entre contratos inteligentes e sistemas legados exige uma abordagem abrangente para garantir a integridade, confidencialidade e disponibilidade dos ativos financeiros envolvidos.

Objetivo:

O objetivo principal desta tese é investigar a aplicação de modelos de machine learning, inspirados na abordagem do Lightning Cat, para avaliar a segurança dos smart contracts utilizados pelo Tesouro Direto do Brasil. Em particular, o foco será na identificação de vulnerabilidades relacionadas à interoperabilidade.

Metodologia:

A metodologia adotada envolverá a seleção e adaptação de modelos de machine learning, incluindo técnicas de aprendizado profundo, para analisar o código-fonte e a execução dos smart contracts do Tesouro Direto. O uso de dados históricos e cenários simulados será crucial para treinar os modelos, garantindo uma cobertura abrangente de possíveis vulnerabilidades.

Contribuições Esperadas:

1. Identificação de Vulnerabilidades Específicas: Espera-se a identificação de vulnerabilidades específicas relacionadas à interoperabilidade entre smart contracts e sistemas da Web2.

A identificação de vulnerabilidades específicas relacionadas à interoperabilidade entre smart contracts e sistemas da Web2 é de extrema importância para garantir a integridade e segurança dos ativos financeiros no contexto do Tesouro Direto do Brasil. Para alcançar esse objetivo, a abordagem adotada envolverá uma análise minuciosa dos protocolos de comunicação, integrações e interações entre os smart contracts e as soluções da Web2.

Será realizada uma avaliação abrangente das possíveis vulnerabilidades, como:

- Exposição de Dados Sensíveis: Identificação de pontos em que dados sensíveis podem ser expostos durante a interoperabilidade, mitigando o risco de vazamento de informações confidenciais.
- Manipulação Não Autorizada: Análise das interfaces de comunicação para evitar manipulações não autorizadas dos contratos inteligentes, protegendo contra a execução indevida de transações.
- Falhas na Autenticação e Autorização: Verificação minuciosa da autenticação e autorização entre os smart contracts e as soluções da Web2, evitando acessos não autorizados e atividades maliciosas.
- Integridade dos Dados: Garantia da integridade dos dados durante o processo de interoperabilidade, prevenindo a inserção de dados falsos ou comprometidos.

Essa fase do estudo buscará mapear as potenciais vulnerabilidades específicas, proporcionando uma compreensão aprofundada dos riscos associados à interoperabilidade.

2. Desenvolvimento de Modelos Personalizados: O desenvolvimento de modelos de machine learning personalizados, adaptados às nuances dos contratos inteligentes do Tesouro Direto, será uma contribuição significativa.

O desenvolvimento de modelos de machine learning personalizados é uma etapa fundamental para adaptar as técnicas de detecção de vulnerabilidades às particularidades dos contratos inteligentes do Tesouro Direto. Isso envolverá a criação de modelos treinados com conjuntos de dados específicos, contemplando as características únicas dos contratos inteligentes e as nuances das soluções da Web2.

Treinamento com Dados do Tesouro Direto: A coleta e seleção cuidadosa de dados provenientes dos smart contracts do Tesouro Direto servirão como base para treinamento dos modelos. Esses dados incluirão informações sobre transações passadas, padrões de interação e eventos relevantes.

Consideração das Características Específicas: Os modelos serão projetados para considerar as particularidades dos contratos inteligentes, levando em conta as regras de negócios específicas do Tesouro Direto, estrutura do código-fonte e os requisitos de interoperabilidade.

Validação Iterativa: O processo de desenvolvimento será iterativo, com validação constante utilizando conjuntos de dados de teste que representem cenários realistas de interoperabilidade.

A criação de modelos personalizados garantirá uma abordagem adaptada à complexidade e singularidade dos smart contracts do Tesouro Direto, proporcionando maior precisão na detecção de vulnerabilidades específicas.

3. Diretrizes para Reforço da Segurança: Com base nos resultados obtidos, serão propostas diretrizes para reforçar a segurança dos smart contracts, proporcionando um ambiente mais robusto e resistente a ataques.

Implementação de Mecanismos de Autenticação Forte: Recomendações para a implementação de mecanismos robustos de autenticação, visando prevenir acesso não autorizado aos contratos inteligentes.

Monitoramento Contínuo: Estabelecimento de práticas de monitoramento contínuo das transações e interações entre os smart contracts e sistemas da Web2, permitindo a detecção precoce de atividades suspeitas.

Atualizações de Segurança Regulares: Orientações para a realização de atualizações regulares nos smart contracts, incorporando patches de segurança e adaptando-se às evoluções das soluções da Web2.

Treinamento e Conscientização: Desenvolvimento de programas de treinamento e conscientização para as partes envolvidas, promovendo uma cultura de segurança desde o desenvolvimento até a implementação e manutenção contínua dos smart contracts.

Essas diretrizes servirão como um guia prático para reforçar a segurança dos smart contracts do Tesouro Direto, mitigando os riscos identificados durante a

análise de vulnerabilidades e fortalecendo a resiliência do sistema financeiro contra potenciais ataques.

Entrando especificamente no tema de IA, abaixo estão algumas maneiras como ela pode ser aplicada no contexto do Tesouro Direto:

Análise Estática de Código:

Utilização de Modelos de Linguagem Pré-Treinados: Assim como o CodeBERT mencionado no artigo, modelos de linguagem pré-treinados podem ser aplicados para realizar uma análise semântica do código-fonte dos smart contracts. Esses modelos podem identificar padrões suspeitos, possíveis vulnerabilidades e anomalias sem depender apenas de regras estáticas predefinidas.

Identificação de Padrões de Segurança Conhecidos: A IA pode aprender a reconhecer padrões associados a vulnerabilidades conhecidas, como reentrancy, dependência de timestamp incorreta, entre outros. Isso permite uma detecção mais precisa e abrangente, reduzindo a probabilidade de falsos positivos e falsos negativos.

Análise Dinâmica de Execução:

Simulação de Transações: A IA pode simular transações e interações entre smart contracts e sistemas da Web2 para avaliar dinamicamente como o código se comporta em diferentes cenários. Isso inclui a análise de fluxos de dados, execução de contratos em ambientes controlados e observação de possíveis pontos de falha durante a interoperabilidade.

Detecção de Comportamento Anormal: Algoritmos de aprendizado de máquina podem ser treinados para identificar comportamentos anormais durante a execução de smart contracts, alertando para possíveis atividades maliciosas ou transações suspeitas.

Aprendizado Contínuo:

Adaptação a Mudanças no Ambiente: A IA pode ser treinada para se adaptar a mudanças nas soluções da Web2, atualizando seus modelos à medida que novas versões de contratos inteligentes e tecnologias são introduzidas. Isso permite uma abordagem dinâmica à evolução do ambiente de segurança.

Feedback Iterativo: O sistema de IA pode aprender com feedback iterativo, ajustando seus modelos com base em eventos de segurança reais e refinando sua capacidade de detectar ameaças específicas à medida que ocorrem.

Integração com Sistemas de Monitoramento e Resposta a Incidentes:

Monitoramento em Tempo Real: A IA pode ser integrada a sistemas de monitoramento em tempo real para detectar e responder automaticamente a possíveis ameaças ou atividades suspeitas. Isso reduz o tempo de resposta a incidentes de segurança.

Tomada de Decisões Automatizada: Em casos de detecção de ameaças graves, a IA pode tomar decisões automatizadas, como a interrupção temporária de transações ou a aplicação de medidas de segurança preventivas.

Interpretação de Contratos e Normas:

Análise de Conformidade: Algoritmos de IA podem ser treinados para interpretar contratos e normas de segurança específicos do Tesouro Direto, garantindo que os smart contracts estejam em conformidade com regulamentações e melhores práticas.

Recomendações para Atualizações de Segurança: Com base em análises contínuas, a IA pode fornecer recomendações proativas para atualizações de segurança, sugerindo melhorias no código ou na lógica do contrato.

A aplicação dessas técnicas de IA pode tornar o processo de validação de segurança mais eficiente, preciso e adaptável às complexidades dos smart contracts do Tesouro Direto.

Simulações Realistas para Treinamento:

Ao abordar simulações realistas para treinamento, a ideia é criar conjuntos de dados sintéticos que representem fielmente os cenários operacionais do Tesouro Direto. Essas simulações podem ser fundamentais para o treinamento eficiente dos modelos de machine learning, especialmente em situações onde dados históricos podem ser limitados ou não abrangem uma variedade suficiente de casos.

Geração de Dados Sintéticos:

- Desenvolver algoritmos e técnicas para gerar dados sintéticos que imitem padrões de transações e interações nos smart contracts do Tesouro Direto. Considerar a inclusão de diferentes tipos de transações, usuários e condições de mercado.

- Utilizar técnicas avançadas, como Redes Generativas Adversárias (GANs), para criar dados sintéticos que se assemelhem de perto às características dos dados reais.

Aprimoramento da Diversidade:

- Certificar-se de que as simulações abranjam uma ampla gama de cenários possíveis, incluindo variações nos volumes de transações, condições de mercado voláteis e eventos inesperados que possam afetar o desempenho dos smart contracts.

Validação e Ajuste Iterativo:

- Implementar um processo de validação iterativo, onde os dados sintéticos gerados são comparados com os dados reais para garantir a precisão e a relevância. Ajuste os algoritmos de geração conforme necessário com base nos resultados da validação.

- Considerar o feedback contínuo de especialistas do Tesouro Direto para garantir que as simulações capturem nuances específicas do ambiente financeiro.

- Incorporação de Anomalias Conhecidas:

- Introduzir intencionalmente anomalias conhecidas nos dados sintéticos para treinar os modelos a identificarem e lidarem com situações adversas. Isso pode incluir padrões de fraude, transações atípicas e variações nos comportamentos dos usuários.

- Garantir que as anomalias introduzidas se alinhem com os riscos reais enfrentados pelos smart contracts.

Benefícios Esperados:

A abordagem de simulações realistas visa enriquecer o treinamento dos modelos, proporcionando-lhes uma base mais sólida para a detecção de vulnerabilidades. Ao replicar de forma precisa os ambientes operacionais do Tesouro Direto, os modelos estarão mais bem preparados para enfrentar desafios do mundo real, resultando em uma avaliação de segurança mais robusta e confiável.

IA para Detecção de Padrões de Fraude:

A detecção de padrões de fraude é uma aplicação crítica da IA, especialmente em ambientes financeiros como o Tesouro Direto. Neste contexto, é essencial que os modelos de machine learning sejam capazes de identificar comportamentos suspeitos e transações fraudulentas para proteger os ativos financeiros e a integridade do sistema.

Feature Engineering Específico para Fraude:

- Desenvolver características específicas para detecção de fraude, levando em consideração padrões típicos associados a atividades fraudulentas. Isso pode incluir análise de padrões temporais, comportamentais e transacionais que podem indicar atividade maliciosa.

- Utilizar técnicas avançadas, como análise de redes complexas, para identificar relacionamentos suspeitos entre diferentes entidades envolvidas em transações.

Aprendizado Supervisionado e Não Supervisionado:

- Explorar abordagens de aprendizado supervisionado para treinar modelos com dados rotulados de transações conhecidas como fraudulentas ou não fraudulentas. Além disso, empregue técnicas não supervisionadas para detectar padrões anômalos sem depender de rótulos explícitos.

- Considerar a aplicação de algoritmos de clusterização para agrupar comportamentos semelhantes, identificando assim anomalias que podem indicar atividades fraudulentas.

Atualização Contínua do Modelo:

- Implementar um sistema que permita a atualização contínua do modelo de detecção de fraude com base em novos dados e padrões emergentes. Isso pode envolver o uso de técnicas de aprendizado online para incorporar informações em tempo real.

- Integrar feedback humano e histórico de decisões de especialistas para melhorar a precisão do modelo ao longo do tempo.

Integração com Sistemas de Prevenção:

- Projetar o sistema de detecção de fraude para operar em conjunto com outros sistemas de prevenção de fraudes, possibilitando a resposta proativa a atividades suspeitas.

- Considerar a implementação de bloqueios automáticos ou alertas para transações identificadas como potencialmente fraudulentas, permitindo uma resposta rápida a possíveis ameaças.

A aplicação de IA na detecção de padrões de fraude visa fortalecer a segurança do Tesouro Direto, protegendo contra atividades maliciosas. Ao adotar uma abordagem multifacetada que combina técnicas supervisionadas e não supervisionadas, o sistema de detecção de fraude pode evoluir continuamente, adaptando-se a novos métodos de fraude e proporcionando uma camada adicional de proteção contra ameaças financeiras.

Conclusão:

O avanço tecnológico no setor financeiro, impulsionado pela tecnologia blockchain e contratos inteligentes, apresenta oportunidades substanciais para o Tesouro Direto do Brasil. No entanto, a interoperabilidade entre sistemas traz consigo desafios significativos, especialmente em relação à segurança dos smart contracts. Esta tese propôs uma abordagem inovadora, utilizando modelos de machine learning inspirados no Lightning Cat, para realizar testes de segurança com foco na interoperabilidade.

Os resultados esperados, destacados nas contribuições previstas, visam fortalecer a resiliência do sistema financeiro, proporcionando um ambiente mais seguro e confiável para as transações do Tesouro Direto. A identificação de vulnerabilidades específicas, o desenvolvimento de modelos personalizados e a proposição de diretrizes de segurança constituem passos essenciais para enfrentar os desafios associados à complexidade da interoperabilidade.

A análise estática e dinâmica de código, juntamente com o aprendizado contínuo, integração com sistemas de monitoramento e resposta a incidentes, e interpretação de contratos e normas, representam uma abordagem abrangente para a aplicação de inteligência artificial nesse contexto. A sinergia dessas

técnicas pode oferecer uma cobertura ampla, identificando ameaças potenciais, adaptando-se a mudanças no ambiente e promovendo uma cultura de segurança desde o desenvolvimento até a manutenção contínua dos smart contracts.

Além disso, a proposta de aplicação de IA no contexto do Tesouro Direto destaca a importância de modelos personalizados, ajustados às particularidades dos contratos inteligentes em questão. Isso não apenas aumenta a precisão na detecção de vulnerabilidades, mas também demonstra a adaptabilidade da IA às nuances específicas do Tesouro Direto.

Em última análise, a contribuição desta tese estende-se para além da academia, fornecendo orientações práticas e soluções inovadoras para fortalecer a segurança no contexto financeiro emergente. A aplicação de modelos de machine learning, aliada a uma abordagem cuidadosa e adaptada, representa um avanço significativo na garantia da integridade e confiança nos smart contracts do Tesouro Direto do Brasil, preparando o caminho para um futuro financeiro mais seguro e resiliente.