Avaliando o Impacto da Criptografia Homomórfica no Aprendizado Federado

Orientador: Prof. Rodrigo Cesar Pedrosa Silva

17 de novembro de 2023

1 Introdução

O avanço contínuo da inteligência artificial (IA) e a crescente importância da privacidade de dados apresentam desafios únicos e oportunidades no campo da tecnologia da informação. Este projeto, intitulado 'Avaliando o Impacto da Criptografia Homomórfica no Aprendizado Federado', se propõe a explorar a interseção de duas tecnologias emergentes: a criptografia homomórfica e o aprendizado federado.

Enquanto o aprendizado federado oferece um paradigma promissor para treinar modelos de IA de forma distribuída e colaborativa, a criptografia homomórfica promete um novo nível de segurança e privacidade, permitindo operações em dados criptografados sem revelar suas informações subjacentes.

Através de uma abordagem investigativa rigorosa, este projeto visa compreender profundamente como a integração dessas duas tecnologias pode transformar o cenário da IA, abordando as preocupações de privacidade e segurança em uma era cada vez mais digitalizada. Com o objetivo de contribuir tanto para o avanço acadêmico quanto para a aplicação prática, este estudo explora questões críticas em segurança cibernética e inteligência artificial, com potenciais aplicações em diversos setores.

2 Objetivos

2.1 Objetivo Geral

Investigar como a criptografia homomórfica influencia a eficiência, a segurança e a privacidade do aprendizado federado. Isso envolve avaliar as mudanças nos protocolos de aprendizado federado quando a criptografia homomórfica é aplicada, focando em aspectos como desempenho computacional, integridade dos dados e capacidade de manter a confidencialidade dos dados.

2.2 Objetivos Específicos

1. Compreender os Fundamentos: Estudar e analisar os princípios básicos da criptografia homomórfica e do aprendizado federado, focando em seus mecanismos, vantagens e limitações.

2. Avaliar a Compatibilidade e Integração: Examinar como a criptografia homomórfica pode ser integrada com os sistemas de aprendizado federado existentes, considerando aspectos técnicos e práticos.

3. Medir o Impacto no Desempenho: Realizar experimentos e simulações para medir o impacto da criptografia homomórfica no desempenho do aprendizado federado, incluindo tempo de processamento, uso de recursos computacionais e eficiência da comunicação de rede.

4. Analisar a Segurança e a Privacidade: Avaliar como a criptografia homomórfica melhora a segurança e a privacidade dos dados no aprendizado federado, considerando cenários como ataques de terceiros e vazamento de dados.

5. Estudo de Casos e Aplicações Práticas: Investigar aplicações práticas do uso combinado de criptografia homomórfica e aprendizado federado em diferentes domínios, como saúde, finanças e telecomunicações.

6. Desenvolver Recomendações e Melhores Práticas: Com base nas descobertas, elaborar recomendações e melhores práticas para implementar a criptografia homomórfica no aprendizado federado de maneira eficiente e segura.

7. Identificar Desafios e Propor Soluções: Identificar os principais desafios técnicos, legais e éticos associados e propor soluções ou direções para pesquisas futuras.

Este projeto pode contribuir significativamente para a compreensão de como a criptografia avançada pode ser utilizada para melhorar a segurança e a privacidade em modelos de aprendizado de máquina distribuídos, um tópico de grande relevância na era atual da computação.

3 Justificativa/Relevância

Em um mundo onde a geração de dados aumenta de forma exponencial, especialmente em setores sensíveis como saúde e finanças, a segurança e a privacidade dos dados tornaram-se de extrema importância. A criptografia homomórfica surge como uma solução inovadora, permitindo a realização de operações em dados criptografados, mantendo sua confidencialidade. Paralelamente, o aprendizado federado emerge como uma abordagem promissora para o treinamento de modelos de machine learning, descentralizando o processo e mantendo os dados em seus locais de origem para proteger a privacidade. No setor de saúde, por

exemplo, essa combinação pode permitir o treinamento de modelos de IA em dados sensíveis de forma segura, acelerando o desenvolvimento de diagnósticos e tratamentos personalizados sem comprometer a privacidade do paciente

A integração da criptografia homomórfica no aprendizado federado representa uma convergência tecnológica significativa, prometendo fortalecer ainda mais a segurança dos dados. No entanto, é crucial entender como essa integração afeta a eficiência computacional aprendizado de máquina. Essa compreensão é fundamental para a aplicabilidade prática dessas tecnologias em setores que manuseiam informações sensíveis. .

Este projeto visa, portanto, explorar essa interseção, avaliando o impacto prático da criptografia homomórfica no contexto do aprendizado federado. A pesquisa tem implicações diretas em diversos setores, podendo levar a avanços significativos em termos de segurança de dados e privacidade, beneficiando a sociedade em geral. Além disso, a pesquisa contribuirá para o campo de segurança de dados e machine learning, oferecendo insights valiosos para futuras inovações e desenvolvimento tecnológico.

Finalmente, este projeto responde diretamente às crescentes demandas regulatórias globais para a proteção de dados, como o GDPR na Europa, CCPA na Califórnia e a LGPD do Brasil. A aplicação prática de tecnologias que cumprem essas regulamentações é crucial. Além disso, enfrentar e superar os desafios técnicos associados à criptografia homomórfica, como sua complexidade computacional, pode impulsionar inovações significativas, beneficiando tanto a comunidade acadêmica quanto a indústria.

Assim, a justificativa do projeto está enraizada na necessidade urgente de endereçar as preocupações de privacidade e segurança de dados na era digital, buscando soluções que mantenham a eficiência e precisão no processamento desses dados. Este estudo não é apenas uma investigação técnica, mas também uma resposta a uma necessidade emergente com amplas implicações sociais e tecnológicas.

4 Resultados Esperados

1. Dados concretos sobre o impacto da criptografia homomórfica no tempo de processamento, uso de memória e outros recursos computacionais no aprendizado federado. Isso ajudaria a entender as implicações práticas da adoção dessa tecnologia em termos de eficiência computacional.

2. Uma análise aprofundada das melhorias na segurança e privacidade dos dados proporcionadas pela criptografia homomórfica, incluindo qualquer desafio ou limitação identificada.

3. Comparação entre os sistemas de aprendizado federado que utilizam criptografia homomórfica e aqueles que não a utilizam, destacando vantagens, desvantagens e cenários de uso ideais para cada abordagem.

4. Desenvolvimento de diretrizes e melhores práticas para a implementação

eficiente de criptografia homomórfica em ambientes de aprendizado federado. Isso ajudaria outras entidades e pesquisadores a adotar essas tecnologias de forma mais eficaz.

5. Produção de artigos científicos, relatórios técnicos que possam orientar futuras pesquisas e aplicações práticas nesta área.

6. Avaliação de como essa abordagem tecnológica se alinha com as regulamentações globais de privacidade de dados, fornecendo insights valiosos sobre como a conformidade regulatória pode ser alcançada de forma mais eficiente.