Universidade Federal de Uberlândia
Faculdade de Computação

IX FACOM TECHWEEK E XVI WORKSHOP DE TESES E DISSERTAÇÕES EM CIÊNCIA DA COMPUTAÇÃO

Anais

07 a 11 de novembro de 2022

ISSN: 2447-0406

FACOM TECHWEEK

WTDCC
XVI Workshop de Teses e Dissertações em Ciência da Computação

Uberlândia
2022

Aplicação da Arquitetura LSTM para a Geração de Senhas

Marlon B Ramos (Universidade Federal de Uberlândia)*; Thiago Pirola Ribeiro (Universidade Federal de Uberlândia)

marlonbrendoramos@ufu.br*; tpribeiro@ufu.br

Resumo: Hoje em dia, com a crescente dependência da internet e dos sistemas computacionais, a segurança de informações é uma pauta cada vez mais recorrente dentro desse universo. Visando esse fato, as senhas são meios frequentemente utilizados para garantir a autenticação do usuário ao sistema. Dessa forma, mecanismos para obtenção e a possível quebra de senhas são cada vez mais aperfeiçoados para a realização de pentests ou invasões, como por exemplo os ataques de força bruta baseado em dicionários, na qual o atacante busca exaustivamente por tentativa e erro, a descoberta da senha por meio de um dicionário previamente conhecido. Concatenado a esses fatos, devido a importância das informações, a privacidade dos usuários e a quantidade informações a serem analisadas, os métodos de Inteligência Artificial (IA) propõe-se em automatizar algumas atividades que por sua vez, geram enormes quantidades de dados, permitindo além disso, que sejam obtidos resultados inerentes à base de dados. Desse modo, o presente trabalho visa conduzir e verificar aplicabilidade do Aprendizado de Máquina, em especial as Redes Neurais Recorrentes sob a arquitetura Long Short Term Memory (LSTM), que se baseiam em séries temporais de um conjunto de informações ordenados no tempo, permitindo o reconhecimento de padrões em sequências de dados, como texto, genomas, caligrafia, músicas. Este estudo propõe a utilização dessa arquitetura para capturar possíveis relações semânticas existentes entre os dados, como, por exemplo, a formação de padrões em escritas de senhas. E desse modo, o objetivo principal deste trabalho é prever e gerar novas senhas que viabilizariam a sua utilização em um ataque de dicionário. Além de delinear um bom modelo aplicando os melhores hiperparâmetros obtidos nas etapas de desenvolvimento, este trabalho investigou o equilíbrio entre a capacidade de gerar senhas por meio do Aprendizado de Máquina e a qualidade dos resultados obtidos. Devido à natureza dos dados, o uso da arquitetura LSTM gerou bons resultados no quesito de previsão e geração de senhas para os dicionários abordados na comparação. Além disso, os resultados obtidos são próximos aos propostos em trabalhos que utilizam as Redes Adversárias Generativas (GAN), para aprender autonomamente a distribuição de senhas e prever as senhas com base no dicionário RockYou. Da mesma forma, foram obtidos resultados extremamente satisfatórios para alguns dicionários quando aplicada diferentes combinações de parâmetros que controlam a aleatoriedade das previsões e quantidades de caracteres gerados. Pretendem-se expandir e validar o método proposto para outras bases e comparar com outras técnicas já estabelecidas da literatura.

Trilha: Trabalho de Graduação