IF848 - Detecção de Intrusão - 2023.2

Prof. Paulo Freitas

Especificação do Seminário e do Projeto da Disciplina

Escolha de artigo

- Cada equipe deverá escolher um artigo relacionado ao uso de inteligência artificial para segurança ou à segurança para sistemas baseados em inteligência artificial.
  - Lista com artigos sugeridos: Planilha com artigos sugeridos
  - Alternativamente, cada equipe também poderá sugerir algum artigo que não esteja na lista, o qual, neste caso, deverá ser aprovado pelo professor.
- O artigo escolhido será utilizado para o seminário e para o projeto da disciplina, portanto, escolham bem!
- Um mesmo artigo não poderá ser utilizado por mais de uma equipe, portanto, escolham rápido!

Seminário

- Cada equipe deverá estudar com profundidade o artigo escolhido para preparar e apresentar um seminário sobre ele.
- O seminário deverá cobrir, minimamente, os pontos descritos na seção **Detalhamento de requisitos - Seminário** deste documento.
- Duração:
  - Apresentação: 10 minutos;
  - Perguntas e respostas: 5 minutos.
- Entregáveis e prazos
  - Slides da apresentação pelo classroom: **05/02/2024**
  - Apresentação: **06/02/2024 e 08/02/2024**

Projeto

- Cada equipe deverá:
  - Reproduzir o artigo escolhido, implementando e executando o seu código, e obtendo resultados próximos o suficiente dos resultados exibidos no artigo.
  - Obter resultados do sistema proposto no artigo reproduzido em outro conjunto de dados (dataset). A escolha do novo conjunto de dados deve ser devidamente justificada no relatório.
  - Propor, implementar e obter resultados de melhorias no sistema proposto no artigo de referência. Enquanto todos os demais itens são obrigatórios, este item representará pontuação extra.
  - Escrever um relatório contendo os pontos descritos na seção **Detalhamento de requisitos - Projeto** deste documento.
- Requisitos adicionais podem ser exigidos especificamente para cada artigo escolhido.
- Entregáveis e prazos:
  - Relatório e link do Github com todos os códigos comentados: **12/03/2024**

- Slides de apresentação e apresentação de 15 minutos para as equipes que conseguirem realizar melhorias: **14/03/2024** (pontuação extra)

Requisitos adicionais:

- Cada equipe deverá ser composta por **3 pessoas** e indicar os seus integrantes em atividade do classroom até o dia **19/12/2023**.
- O artigo de referência deverá ser escolhido e indicado em atividade do classroom até o dia **19/12/2023**.
- Apresentações devem utilizar o formato de apresentação institucional do Centro de Informática, disponível em: modelos de apresentação CIn - UFPE.
- Relatórios devem ser entregues em PDF e usar o template do overleaf disponível em: template relatório. Vocês deverão fazer uma cópia do template e editar na sua própria cópia.

Detalhamento de requisitos - Seminário

O seminário deverá cobrir, minimamente, os pontos a seguir sobre artigo de referência:

- Introdução: motivação, justificativa e principais contribuições do trabalho;
- Trabalhos relacionados: os seus principais trabalhos relacionados, suas contribuições e limitações;
- Solução proposta: arquitetura e funcionamento do sistema proposto;
- Experimentos: dados utilizados e experimentos realizados;
- Resultados: expor e analisar os resultados obtidos pela solução proposta pelo artigo de referência;
- Conclusão: conclusões, **principais limitações e problemas do sistema proposto pelo artigo de referência e sugestões detalhadas de melhorias que poderiam ser feitas.**

O seminário deve conter apenas **tópicos, *bullet points* e imagens** para guiar o que será discutido. **Textos longos devem ser evitados**.

Detalhamento de requisitos - Projeto

O relatório do projeto deverá ser no formato de artigo, conter as seções a seguir e responder de maneira clara, precisa e em formato de texto as perguntas abaixo:

Abstract/Resumo
Resumo do contexto do trabalho, problema a ser abordado, soluções existentes, método proposto e resultados obtidos.

1. Introdução
   Deverá abordar a motivação, justificativa e principais contribuições do trabalho em questão. Alguns pontos que devem ser abordados de forma **breve**, são:
   - Qual o problema que está sendo investigado?

- Por que ele é interessante?
- Por que foi necessário que o artigo de referência propusesse tal solução?
- Quais as soluções existentes e suas desvantagens?
- O que está sendo proposto para resolver o problema em questão?
- As principais contribuições do trabalho em formato de lista.

2. Trabalhos relacionados
   Apresentar alguns dos artigos existentes na literatura sobre o tema que está sendo trabalhado, suas **principais contribuições e limitações**.

3. Modelo de ameaça (caso se aplique)
   Apresentar os ataques considerados para o trabalho. Utilizar figuras e/ou algoritmos e/ou equações para descrever os comportamentos dos ataques considerados. Também especificar as premissas consideradas para que a execução dos ataques seja possível.

4. Sistema proposto pelo artigo de referência
   Apresentar a arquitetura e funcionamento do sistema proposto pelo artigo de referência. Utilizar figuras e/ou algoritmos e/ou equações para descrever o sistema proposto.
   - Quais os componentes da solução? Quais as suas entradas e saídas? O que eles fazem? Como eles o fazem?
   - Quais métodos ou algoritmos estão sendo propostos ou empregados e por que?

5. Solução proposta pela equipe para melhorar a solução do artigo de referência (caso feita)
   Apresentar a arquitetura e funcionamento do sistema proposto pelo artigo de referência. Utilizar figuras e/ou algoritmos e/ou equações para descrever o sistema proposto.
   - O que espera-se melhorar em relação à solução proposta pelo artigo de referência?
   - Quais os componentes da solução? Quais as suas entradas e saídas? O que eles fazem? Como eles o fazem?
   - Quais métodos ou algoritmos estão sendo propostos ou empregados e por que?

6. Metodologia
   Descrever os dados e métricas utilizados para validar as soluções propostas e quais os experimentos realizados. Sobre os dados, descrever:
   - Dados usados pelo artigo de referência
     i. Quais foram os dados usados para avaliar o sistema proposto? Por que eles foram escolhidos? O que eles representam? Como os conjuntos de treino, validação e teste foram formados? Há quantos dados em cada classe nos conjuntos de treino, validação e teste?

- Outro conjunto de dados escolhido
    i. Quais foram os dados usados para avaliar o sistema proposto? Por que eles foram escolhidos? O que eles representam? Como os conjuntos de treino, validação e teste foram formados? Há quantos dados em cada classe nos conjuntos de treino, validação e teste?

7. Resultados e discussões
   Apresentar e analisar os resultados obtidos comparando-os com os resultados de outros trabalhos. Utilizar gráficos e tabelas. Atentar para não apenas descrever os resultados apresentados, mas também para explicá-los e discuti-los.
    - Pela solução do artigo de referência
        i. Nos dados usados pelo artigo de referência
        ii. No outro conjunto de dados escolhido
    - Pela proposta da equipe para melhorar o artigo de referência (caso feita)
        i. Nos dados usados pelo artigo de referência
        ii. No outro conjunto de dados escolhido

8. Conclusão e trabalhos futuros
   Conclusão, principais limitações e problemas do sistema proposto pelo artigo de referência e pela proposta de melhoria (caso feita), e trabalhos futuros.

9. Referências
   Utilizar o formato do IEEE.