Laboratório de Projecto
Ano lectivo: 2023-24

DEPARTAMENTO
DE ENGENHARIAS E DE
CIÊNCIAS DA COMPUTAÇÃO

Ficha de Registo do Projecto

Nota: O projeto tem um conjunto de horas previsíveis, entre 500 a 1000 horas, a afetar pelos alunos que o desenvolverem (250 horas por aluno, equivalente a 10 ECTSs- European Credi Transfer and Accummulation System).

Identificação dos Alunos (* Chefe do Grupo)	**Nome(*): Miguel Fernandes**	N.º 30008210	Curso 3º Ano – IG PL
	e-mail: 30008210@students.ual.pt	Tel. +351 927092044	
	Nome: Edgar Casimiro	N.º 19970423	Curso 3º Ano – IG PL
	e-mail: 19970423@students.ual.pt	Tel.	
	Nome: Pedro Brito	N.º 30008361	Curso 3º Ano – IG PL
	e-mail: 30008361@students.ual.pt	Tel.	
	Nome: Tiago Mateus	N.º 30010863	Curso 3º Ano – EI PL
	e-mail: 30010863@students.ual.pt	Tel.	
Orientador	Nome: Héctor Dave Orrillo Ascama		
Designação do Projecto	Sistema de Autenticação digital anti *Deepfakes*		
Organização parceira (se existente)			
Se houver produto software criado / Licença do projeto	**( ) GPL ( ) BSD ( ) Outro** **Se "outro", justificar**		
Descrição sumária do Projeto (Além de preencher os items desta secção, pode juntar neste documento mais uma ou duas páginas descritivas)	Resumo: Para este projeto foi proposto que desenvolvêssemos um sistema de autenticação digital "*Anti-Deepfakes*" baseado em biometria de reconhecimento facial e biometria de voz. Temos como objetivo utilizar uma abordagem integrada, onde a aplicação se conectará a um servidor *Python*, responsável por processar dados biométricos e integrar diferentes componentes do sistema. Para implementação, faremos uso das seguintes ferramentas propostas pelos docentes. *(descrição sumária do projeto) Este sistema proporcionará uma camada adicional de segurança contra *deepfakes*, garantindo a autenticidade das identidades digitais dos utilizadores por meio de técnicas avançadas de reconhecimento facial e de voz. A integração de diversas ferramentas e		

tecnologias permitirá uma abordagem abrangente e eficaz na deteção, comprovação e prevenção de fraudes digitais.

Objectivos:

- Implementar bibliotecas de reconhecimento facial, baseados no modelo *FaceNet*, para identificação de indivíduos e deteção de alterações suspeitas nas características faciais, de forma a mitigar o uso de *deepfakes*.
- Implementar técnicas avançadas de processamento de voz, utilizando o *TFLite*, para autenticar usuários por meio de biometria de voz e detetar tentativas fraudulentas de manipulação de voz.
- Integrar os algoritmos de reconhecimento facial e de voz à aplicação móvel, estabelecendo uma conexão eficiente com o servidor em *Python* para processamento seguro e armazenamento dos dados biométricos.
- Testar e validar a robustez do sistema contra tentativas de fraude, incluindo a utilização de *deepfakes*, por meio de testes de segurança e simulações de ataques.
- Promover a compreensão, sobre os desafios e soluções relacionadas à autenticação biométrica facial e de voz.

Bibliografia do domínio:

Šandor, Oskar — "*Resilience of biometric authentication of voice assistants against deepfakes*". BRNO, 2023. Bachelor's Thesis, presented to BRNO UNIVERSITY OF TECHNOLOGY.
Available in:
https://theses.cz/id/nr5tm7/OS_BP_FINAL.pdf

REŠ, Jakob — "*Testing the robustness of a voice biometrics system against deepfakes*". BRNO, 2023. Master's Thesis, presented to BRNO UNIVERSITY OF TECHNOLOGY.
Available in:
https://theses.cz/id/wfbqy4/DP.pdf

Forrest, D., et al. (2024). "Challenges in voice biometrics: Vulnerabilities in the age of deepfakes."
https://bankingjournal.aba.com/2024/02/challenges-in-voice-biometrics-vulnerabilities-in-the-age-of-deepfakes/

Peixoto, M., et al. (2023). "A era dos Deepfakes: como a biometria de voz é uma ferramenta crucial na prevenção de fraudes.
https://tiinside.com.br/30/06/2023/a-era-dos-deepfakes-como-a-biometria-de-voz-e-uma-ferramenta-crucial-na-prevencao-de-fraudes/

Gonzalez, B., (2024). “Cybercriminals use malware to obtain face biometrics, break into banking apps.” https://www.biometricupdate.com/202402/cybercriminals-use-malware-to-obtain-face-biometrics-break-into-banking-apps

(se necessário utilizar a folha seguinte)

Assinaturas dos alunos:

Assinado por: **MIGUEL ÂNGELO DUARTE FERNANDES**
Num. de Identificação: BI14252917
Data: 2024.03.14 22.32.53 GMT Standard Time
CHAVE MÓVEL

Assinado por: **Edgar Miguel Amieiro Casimiro**
Num. de Identificação: 10532080
Data: 2024.03.14 22:37:09 +0000
CHAVE MÓVEL

Assinado por: **Tiago Filipe da Silva Mateus**
Num. de Identificação: 30326103
Data: 2024.03.15 14:38:48 +0000
CHAVE MÓVEL

Data do registo:

14/03/2024

Aprovação Orientador:

Data da aprovação:

Assinado por: **PEDRO JOSÉ DE SOUSA BRITO**
Num. de Identificação: 10500128
Data: 2024.03.15 18:22:21+00'00'
CARTÃO DE CIDADÃO

***Descrição sumária do Projeto (continuação se necessário):**

- *Python*: Será utilizado para escrever scripts e aplicações de “*backend*”, processar dados biométricos e integrar os diferentes componentes do sistema.
- *Google ML Kit*: Implementaremos funcionalidades de comprovação facial e processamento de imagem/video na aplicação móvel usando o *Google ML Kit*.
- *TFLite* (*TensorFlow Lite*): O *TFLite* será utilizado para implementar o modelo de reconhecimento de voz e outros modelos de aprendizagem automática (Machine Learning) na aplicação móvel, garantindo eficiência e desempenho.
- *FaceNet*: Utilizaremos o modelo *FaceNet* para detetar e reconhecer rostos em imagens capturadas pela aplicação, garantindo a precisão e a segurança do sistema.
- *Firebase*: Gestão do processo de autenticação do utilizador e armazenaremos dados biométricos de forma segura na nuvem (*Cloud*) utilizando o *Firebase*, garantindo a integridade e a confidencialidade dos dados do utilizador.
- *Flutter*: Desenvolveremos a “interface” de usuário da aplicação móvel utilizando o *Flutter*, permitindo uma experiência fluída e consistente em diferentes dispositivos e serviços mencionados acima.