

Corso di Dottorato in INGEGNERIA ELETTRONICA ED INFORMATICA

articolato nei seguenti indirizzi:
- INGEGNERIA INFORMATICA E AUTOMATICA
- ELETTRONICA E TELECOMUNICAZIONI

AREE SCIENTIFICO - DISCIPLINARI	09 - INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE
COORDINATORE	PROF.SSA BARBARA CANNAS
SEDE	DIPARTIMENTO DI INGEGNERIA ELETTRICA ED ELETTRONICA
DURATA	3 ANNI
OBIETTIVI FORMATIVI E TEMAICHE DI RICERCA	Il Dottorato in Ingegneria Elettronica e Informatica prepara gli studenti a svolgere e gestire attività di ricerca nel settore delle tecnologie dell'informazione e della comunicazione, sia in ambito accademico che industriale. La formazione è di livello internazionale e comprende i seguenti curricula: - Elettronica e Telecomunicazioni - Ingegneria Informatica e Automatica Il corso di dottorato, che ha durata triennale, è la prosecuzione ideale degli studi universitari di secondo livello (laurea magistrale) nel settore dell'Ingegneria dell'Informazione, ma è aperto anche a chi provenga da altri corsi di laurea magistrale di ingegneria o di scienze. Al corso di dottorato possono partecipare studenti italiani e stranieri. Esso è l'unico corso di dottorato in Sardegna che ricopre l'area dell'Ingegneria dell'Informazione. Per favorire la collocazione delle figure formate sul mercato internazionale il dottorato promuove l'internazionalizzazione delle attività dei docenti e dei dottorandi. Punto centrale della formazione è lo sviluppo di un progetto di ricerca originale, da seguire a stretto contatto con il tutor accademico assegnato al dottorando, orientato all'avanzamento delle conoscenze nel relativo settore. Tale progetto, gestito in prima persona dal dottorando, dovrà avere significativa rilevanza scientifica di natura fondamentale o applicativa. Il dottorato prevede anche che il dottorando completi la sua formazione frequentando corsi e seminari, partecipando a congressi, pubblicando lavori scientifici e svolgendo periodi di studio all'estero. I temi di ricerca del Curriculum in Elettronica e Telecomunicazioni interessano i seguenti settori: Bioingegneria (IBIO-01/A) Sensoristica e biosensoristica basata su materiali innovativi. Analisi ed elaborazione di segnali biomedici. Intelligenza artificiale in ingegneria biomedica. Sistemi e dispositivi medici, anche indossabili, per diagnostica, monitoraggio di parametri fisiologici, telemedicina, e riabilitazione. Campi elettromagnetici (IINF-02/A) Il gruppo di Elettromagnetismo Applicato del DIEE si occupa di: antenne in tecnologia planare e stampata, in particolare per tag RFID e antenne indossabili; realizzazione di antenne mediante tecniche di stampa 3D (antenna additive manufacturing); propagazione radio in ambienti urbani; analisi e progetto di sistemi di esposizione a microonde per applicazioni terapeutiche, bio-tecnologiche e bio-agricole; caratterizzazione di materiali dielettrici; modellazione dei fenomeni bioelettromagnetici in particolare per il trattamento dell'ipertermia; studio della produzione e della sintesi di biomateriali magnetici per applicazioni nel campo dell'ingegneria dei tessuti; utilizzo delle microonde per applicazioni agri-food, biotecnologiche e ambientali. Convertitori, macchine e azionamenti elettrici (IIND-08/A) Sistemi di accumulo dell'energia. L'attività di ricerca in questo ambito riguarda la

	modellistica e la caratterizzazione di dispositivi di accumulo dell'energia, nuove configurazioni di sistemi di accumulo ibridi, lo sviluppo e l'implementazione di strategie e algoritmi di gestione e controllo per applicazioni stazionarie e veicolari. Mobilità Elettrica. L'attività di ricerca in questo ambito consiste nello sviluppo di strategie e algoritmi di pianificazione delle infrastrutture di ricarica per veicoli elettrici, strategie di gestione e controllo per la ricarica dei veicoli elettrici (grid-to-vehicle e vehicle-to-grid), dimensionamento, gestione e controllo di sistemi di accumulo dell'energia stazionari per stazioni di ricarica dei veicoli elettrici. Elettrotecnica (IJET-01/A) Algoritmi per la diagnosi e il controllo nei dispositivi per la fusione termonucleare controllata mediante apprendimento automatico, elaborazione dei segnali e data mining. Supporto alla diagnosi e prognosi mediante apprendimento automatico, con applicazioni all'epilessia, alla sclerosi multipla e al SARS-COVID-19. Monitoraggio, previsione, gestione e conversione dell'energia. Progettazione ottima. Analisi termomeccanica agli elementi finiti (FEM) di sensori magnetici per dispositivi per la fusione termonucleare controllata. Elettronica (IINF-01/A) Metodologie diagnostiche per la analisi dei guasti e le stime di affidabilità della Microelettronica. Elettronica impiantabile ed indossabile; sensori e biosensori; circuiti integrati di elaborazione e trasduzione dei segnali. Elettronica a semiconduttore organico; dispositivi bioelettronici a tecnologia CMOS e organica. Sistemi di processing e tecniche di ottimizzazione per sistemi embedded e cyber-fisici riconfigurabili e low-power. Misure elettriche ed elettroniche (IMIS-01/B) Il gruppo di ricerca di Misure Elettriche ed Elettroniche del DIEE si occupa di definire, progettare, implementare e caratterizzare dispositivi e sistemi di misura avanzati, basati sull'acquisizione dei dati e sull'elaborazione digitale del segnale. I campi di applicazione principali sono quelli delle misure distribuite e sincronizzate per le reti elettriche intelligenti, delle misure per esperimenti di ricerca per osservazione diretta della materia oscura e delle misure di qualità dell'aria. Telecomunicazioni (IINF-03/A) Le tematiche di ricerca ricadono nell'ampio settore del trattamento e della trasmissione dell'informazione. Nello specifico gli studenti di dottorato affrontano problematiche legate a: valutazione della qualità dell'esperienza per applicazioni multimediali; sistemi per le comunicazioni immersive; architetture, servizi ed applicazioni per l'Internet degli Oggetti; sicurezza nelle reti; sistemi di localizzazione; soluzioni per la gestione delle reti mobile 5G/6G; infrastrutture e servizi IoT a supporto della gestione dell'energia negli edifici; aspetti legali e tecnici del trattamento dei dati (privacy) e dell'impiego di tecnologie emergenti; architetture Digital Twin; profilazione, riconoscimento e predizione delle attività tramite l'analisi delle informazioni di contesto. I temi di ricerca del Curriculum in Ingegneria Informatica e Automatica interessano i seguenti settori: Automatica (IINF-04/A) Sistemi ad eventi discreti e ibridi: controllo supervisivo; diagnosi e opacità di sistemi parzialmente osservabili; sicurezza di sistemi ciber-fisici. Sistemi Multi-agente; Ottimizzazione, stima e controllo distribuito; problemi di consenso. Applicazioni: automazione; sistemi flessibili di produzione; smart cities; Sistemi multi-robot, reti di sensori, coordinamento di risorse energetiche distribuite. Sistemi di elaborazione delle informazioni (IINF-05/A) Studio e sviluppo di metodi ed algoritmi di machine learning e progettazione di sistemi di intelligenza artificiale sicuri e affidabili, per la sicurezza informatica, la biometria, l'analisi di contenuti multimediali, l'analisi dei segnali cerebrali. Sicurezza di sistemi e reti informatiche, spam, attacchi di tipo 'phishing', cyber intelligence volta anche alla protezione di sistemi critici. Analisi a basso livello e tecniche di machine learning per la rilevazione di applicazioni malevole su X86/64
--	--

	e su Android. Analisi e rilevazione di attacchi contro applicazioni web ed infrastrutture di rete (network security), anche mediante machine learning. Analisi d'immagini e video per applicazioni di videosorveglianza. Sbocchi occupazionali e professionali previsti Sono previsti sbocchi occupazionali e professionali in Italia e all'estero presso: - strutture accademiche - centri di ricerca scientifica e applicate - aziende ad alta tecnologia, in particolare nel settore dell'ICT - pubbliche amministrazioni - nella creazione di intraprese economiche ad alto contenuto scientifico e tecnologico. - nelle libere professioni ad alto contenuto di innovazione. Le aspettative occupazionali e professionali previste sono confermate dal continuo monitoraggio della situazione occupazionale dei dottori di ricerca che hanno acquisito il titolo negli ultimi anni. Il DRIE ha sottoposto dei questionari agli alumni che hanno conseguito il dottorato fra il 2018 e il 2024. Gli alumni confermano un alto livello di soddisfazione e riconoscono il valore del dottorato per la crescita culturale e professionale. Più del 60 % ha trovato occupazione in accademia e quasi il 20 % in centri di ricerca industriale. Poco più del 10 % risulta occupato presso aziende, mentre il restante 10 % lavora come freelance o consulente.
TITOLI DI STUDIO RICHIESTI PER L'AMMISSIONE (ART. 2 BANDO) ED EVENTUALI ALTRI REQUISITI	TUTTE LE LAUREE MAGISTRALI/SPECIALISTICHE/V.O. E TITOLI STRANIERI EQUIVALENTI RICONOSCIUTI IDONEI
PROVE DI AMMISSIONE PER CANDIDATI/E CHE CONCORRONO PER I POSTI ORDINARI	VALUTAZIONE DEI TITOLI E DEL CURRICULUM VITAE E COLLOQUIO IN PRESENZA Il colloquio sarà teso ad accertare la capacità del/della candidato/a di orientarsi sui principali ambiti di studio inerenti al dottorato e a verificare le sue capacità di analisi, elaborazione e comunicazione. Durante il colloquio sarà, tra l'altro, discusso un progetto di ricerca triennale proposto dal/dalla candidato/a, che dovrà essere presentato obbligatoriamente, in aggiunta ai documenti previsti dall'art. 3 del bando di concorso, mediante upload sul sistema entro la data di scadenza del bando (nome del file: progetto_di_ricerca_cognome_nome). Ai/Alle candidati/e impossibilitati/e, per giustificati motivi, a sostenere il colloquio presso la sede stabilita, può essere accordata la possibilità di svolgerlo in videoconferenza, nella medesima data e ora stabilita per i colloqui in presenza, secondo le modalità indicate nel bando di concorso.
PROVE DI AMMISSIONE PER CANDIDATI/E STRANIERI/E CHE CONCORRONO PER IL POSTO RISERVATO CON BORSA	VALUTAZIONE DEI TITOLI, CURRICULUM VITAE E COLLOQUIO A DISTANZA Nel corso del colloquio sarà, tra l'altro, discusso un progetto di ricerca triennale proposto dal/dalla candidato/a, che dovrà essere presentato obbligatoriamente, in aggiunta ai documenti previsti dall'art. 3 del bando di concorso mediante upload sul sistema, entro la data di scadenza del bando (nome del file: progetto_di_ricerca_cognome_nome). Le lettere di referenza, in numero massimo di 3, devono essere predisposte, utilizzando obbligatoriamente il modulo disponibile alla pagina https://web.unica.it/unica/it/studenti_s01_ss05.page (Istruzioni per l'iscrizione al concorso e modulistica - Reference letter Template), in lingua inglese, da un/una docente universitario/a o da un/una esperto/a degli ambiti di riferimento del dottorato, su carta intestata dell'ente di appartenenza, datate e sottoscritte. Le lettere dovranno essere inviate dai/dalle valutatori/trici all'email phdcall_referenceletter@unica.it, indicando nell'oggetto il cognome e nome del/della candidato/a valutato/a e la denominazione del dottorato per il quale lo/la stesso/a presenta domanda di partecipazione.

POSTI	21, di cui 2 senza borsa e 5 riservati: -1, con borsa, riservato a candidati/e stranieri/e in possesso di titolo conseguito all'estero; - 2 a borsisti/e di Stati Esteri; - 2 a borsisti/e di mobilità internazionale
BORSE DI STUDIO	15: - 1 borsa Università di Cagliari - 4 borse finanziate dal Dipartimento di Ingegneria elettrica ed elettronica, con risorse dei progetti di ricerca (1 ANTA-RES - Responsabile Prof. Alfonso Damiano, 1 RICDIP_SIXGEN_2021_MURRONI. RICUE_WP_CTC_2024_HEAT_MURRONI (HEAT), 1 RICDIP_2023_COSD_NITTI, 1 RICALTRO_WP_CTC_2025_EOPAC) -1 borsa nel settore della cybersicurezza finanziata dall'Agenzia per la Cybersicurezza Nazionale (CUP F82B26000530005). Titolo del progetto: <i>TrustID: Safe Sensing e AI Robusta per la Verifica dell'Identità Digitale nell'Era del GPAI</i> (ID progetto: XLII_124705_211_UniCA). Responsabile scientifico: Prof. Gian Luca Marcialis. Il/La dottorando/a destinatario/a della borsa finanziata dall'Agenzia dovrà svolgere il progetto di ricerca in linea con quanto indicato nella Scheda sottostante. - 9 borse PR Sardegna FSE+ 2021-2027 STEP -Settore di intervento 145a - CUP F82B26000510008 - Tecnologie digitali e innovazione delle tecnologie deep tech - Settore della tecnologia digitale o deep tech: Area I - Tecnologie di intelligenza artificiale e alla Connettività avanzata, navigazione e tecnologie digitali Area II - Tecnologie di intelligenza artificiale, Tecnologie di rilevamento avanzato e Connettività avanzata, navigazione e tecnologie digitali Area III - Tecnologie di semiconduttori avanzati, la Connettività avanzata, navigazione e tecnologie digitali e le Tecnologie di rilevamento avanzato Tecnologia/e critica corrispondente: Area I - Algoritmi di IA, Tecnologie di analisi dei dati, Visione artificiale, Trattamento del linguaggio, Tecnologie di cybersicurezza, compresi la sorveglianza informatica, i sistemi di sicurezza e intrusione, la scienza forense digitale Area II - Algoritmi di IA, Tecnologie di analisi dei dati, Cloud computing ed edge computing, Rilevamento distribuito Area III - Microelettronica, compresi i processori, Tecnologie di comunicazione 5G e 6G, Internet delle cose (IoT) Cloud computing ed edge computing, Rilevamento distribuito Titolo del Progetto di Ricerca: Area I - Tecnologie per la Cybersecurity e l'IA Affidabile Area II - Tecnologie Digitali per Infrastrutture Critiche ed Energia Area III - Microelettronica, Connettività e Sensoristica Intelligente
REFERENTE	PROF.SSA BARBARA CANNAS EMAIL: barbara.cannas@unica.it - TEL. +39 0706755858
SITO WEB	https://web.unica.it/unica/it/phd_200_1111.page

Scheda borsa finanziata dall'Agenzia per la Cybersicurezza Nazionale		
Argomenti di Ricerca e Innovazione sulla Cybersicurezza	Argomento 1	4.1.3 - Modelli per il rilevamento sicuro dei dati
	Argomento 2	5.1.3 - Metodologie per la prevenzione degli attacchi di ingegneria sociale e riduzione dei rischi legati all'uomo
	Argomento 3	2.1.3 - Messa in sicurezza di algoritmi e modelli per il machine learning
	Argomento 4	2.2.2 - Metodologie per monitorare la

		disinformazione
OBIETTIVI DEL PROGETTO E CAPACITÀ DI REALIZZAZIONE		
Obiettivi del progetto		La proposta mira a sviluppare metodi, modelli e protocolli per proteggere la fase oggi più vulnerabile dei servizi di identità digitale: l'acquisizione del dato biometrico e la sua successiva interpretazione automatica da parte di sistemi basati su apprendimento automatico. L'ipotesi di partenza è che gli attacchi abilitati da sistemi GPAI, quali deepfake video, clonazione vocale, morphing, replay attack, presentation attack, identità sintetiche e manipolazioni multimodali, stiano progressivamente spostando il rischio dal solo matching biometrico all'intera catena sensore-dispositivo-modello-decisione. In questo scenario, il dispositivo di acquisizione, tipicamente uno smartphone o un sistema embedded edge, costituisce un nodo sensore critico la cui affidabilità non può più essere assunta a priori, ma deve essere stimata, verificata e quantificata in modo continuo. Il primo obiettivo è costruire un threat model cyber realistico per i moderni processi di verifica dell'identità, distinguendo tra attacchi fisici al momento della cattura (presentation attack, artefatti stampati o display), attacchi digitali sui contenuti acquisiti (deepfake injection, replay via canale digitale) e attacchi avversari contro i modelli di analisi (adversarial perturbation, model evasion). Sul piano hardware, l'analisi coprirà le vulnerabilità specifiche dei sensori edge e le relative implicazioni per l'integrità, la provenienza e l'affidabilità dei dati trasmessi, colmando un gap tuttora aperto tra sicurezza biometrica e sicurezza del nodo sensore. Il secondo obiettivo è progettare modelli di safe sensing capaci di stimare l'affidabilità del dato già alla sorgente, ossia a livello del dispositivo di cattura, combinando artefatti di acquisizione rilevabili direttamente dall'hardware, tracce di provenienza, metadati di dispositivo, segnali di liveness e indicatori di coerenza intra- e inter-modale. Tali modelli opereranno come un livello di verifica del dato anteriore alla fase di matching, producendo un punteggio calibrato di fiducia che accompagni il dato lungo l'intera pipeline decisionale. Il terzo obiettivo è sviluppare algoritmi robusti per rilevare impersonazione e manipolazioni sintetiche, con particolare attenzione alla generalizzazione cross-device, cross-attack e open-set: condizione indispensabile per l'impiego in scenari reali, nei quali i sistemi devono mantenere affidabilità anche

	in presenza di vettori di attacco non osservati durante l'addestramento. I modelli saranno progettati con tecniche di adversarial hardening, stima dell'incertezza e analisi della confidenza, in modo da evitare soluzioni efficaci soltanto in condizioni chiuse di laboratorio. Il quarto obiettivo è integrare le componenti sviluppate in una pipeline di decisione affidabile, in grado di restituire non soltanto una classe, ma anche un punteggio calibrato di fiducia utile alla gestione del rischio operativo. La pipeline incorporerà inoltre meccanismi di trasparenza, auditabilità e tracciabilità coerenti con i requisiti previsti dall'AI Act europeo per i sistemi ad alto rischio, categoria nella quale ricadono esplicitamente i sistemi di identificazione biometrica remota. Sul piano scientifico, la proposta intende contribuire in tre direzioni. La prima riguarda l'avanzamento di modelli per il rilevamento sicuro del dato nei nodi sensori edge in scenari di identità digitale ad alto rischio. La seconda riguarda la robustezza dei modelli di machine learning rispetto a manipolazioni intenzionali, dataset shift e attacchi non visti. La terza riguarda la costruzione di benchmark e protocolli di valutazione che riflettano l'evoluzione reale delle minacce GPAI-enabled, superando la tradizionale separazione tra spoofing fisico, deepfake detection e sicurezza del modello che ancora caratterizza la letteratura. L'esito atteso è un insieme di metodi, dataset, protocolli e linee guida trasferibili a servizi di identificazione e autenticazione in ambiti quali e-government, controllo accessi, onboarding remoto e tutela documentale. Il fine ultimo del progetto è rafforzare la fiducia nei processi di identità digitale attraverso una visione integrata di sensing sicuro, AI robusta e valutazione del rischio.
Pertinenza del progetto agli argomenti dell'Agenda	La proposta è coerente in modo diretto con quattro argomenti dell'Agenda di Ricerca e Innovazione per la Cybersicurezza, secondo un'architettura tematica che copre l'asse principale prioritario, l'asse applicativo, l'asse metodologico e l'asse di contesto. L'asse principale è l'Argomento 4.1.3 (Modelli per il rilevamento sicuro dei dati), rispetto al quale il progetto fornisce il proprio contributo più originale. La proposta sviluppa infatti modelli per assicurare la generazione affidabile del dato da parte di nodi sensori edge – in questo caso dispositivi mobili di cattura biometrica – e per verificarne l'integrità lungo la catena di acquisizione, trasmissione ed elaborazione. Lo smartphone o il terminale

	embedded che acquisisce il dato biometrico è a tutti gli effetti il nodo sensore del sistema di identità digitale: stimarne l'affidabilità a livello hardware-software costituisce la declinazione applicativa diretta di questo argomento prioritario. L'asse applicativo è l'Argomento 5.1.3 (Metodologie per la prevenzione degli attacchi di ingegneria sociale e riduzione dei rischi legati all'uomo), poiché il progetto si concentra sugli attacchi di impersonazione abilitati da GPAI e sulle minacce all'identità digitale, ambiti per i quali l'Agenda richiama esplicitamente deepfake, identità sintetiche, verifica sicura dell'identità e prevenzione delle frodi. In questo senso, il progetto affronta la superficie di attacco umana e socio-tecnica dei servizi digitali, nei quali l'inganno dell'operatore o del sistema avviene sempre più spesso attraverso contenuti sintetici credibili. L'asse metodologico è l'Argomento 2.1.3 (Messa in sicurezza di algoritmi e modelli per il machine learning), dato che il progetto studia la robustezza dei modelli rispetto a manipolazioni avversarie, attacchi di evasione, contaminazione del dato e dataset shift, sviluppando tecniche di adversarial hardening, uncertainty estimation e calibrazione della fiducia. Il progetto si colloca dunque anche nel cuore della AI security, contribuendo alla definizione di modelli affidabili in scenari ostili. L'asse di contesto è infine l'Argomento 2.2.2 (Metodologie per monitorare la disinformazione), in quanto i contenuti sintetici audio-video-fotografici che alimentano la disinformazione costituiscono anche il vettore tecnologico centrale dei moderni attacchi all'identità digitale e ai processi di trust online. Il progetto intercetta quindi tale ambito non sul piano mediatico, ma su quello della sicurezza delle infrastrutture digitali di fiducia.
Modalità di realizzazione del progetto, anche in termini di fattori abilitanti a disposizione	Il progetto sarà organizzato in tre Work Package (WP), con output tangibili e verificabili al termine di ciascuna fase. WP1 - Threat modeling e raccolta dati (mesi 1-6) WP1 coprirà la caratterizzazione sistematica degli scenari di attacco: cattura su dispositivi edge e mobili, attacchi fisici e digitali, contenuti sintetici generati da GPAI, metadati di dispositivo, tracce di provenienza e segnali utili alla stima di affidabilità alla sorgente. Output attesi: (i) una tassonomia formale delle minacce GPAI-enabled per l'identità digitale, con mappatura sulle categorie dell'Agenda; (ii) un dataset sperimentale di riferimento per scenari cross-device, cross-attack e open-set, costruito ad hoc e reso disponibile alla comunità scientifica. WP2 - Progettazione e

	sviluppo dei modelli (mesi 7–30) WP2 si concentrerà sulla progettazione delle componenti algoritmiche: modelli di safe sensing per la stima dell'affidabilità alla sorgente, rilevatori robusti di deepfake e spoofing con adversarial hardening, stima calibrata dell'incertezza, analisi della confidenza e fusione multimodale. Output attesi: (i) una libreria open-source di modelli per safe sensing e impersonation detection; (ii) almeno due pubblicazioni su riviste Q1 o conferenze di riferimento del settore (es. TIFS, CVIU, ESWA, FG, ICCV). WP3 - Validazione, benchmark e trasferimento (mesi 31–36) WP3 riguarderà la validazione estensiva in scenari open-set, benchmark cross-device e cross-dataset, analisi di robustezza e definizione di linee guida per l'integrazione in servizi reali. Output attesi: (i) un benchmark pubblico e riproducibile per la valutazione di sistemi di identità digitale in presenza di attacchi GPAI-enabled; (ii) linee guida operative per fornitori di servizi di onboarding remoto, e-government e controllo accessi, allineate ai requisiti dell'AI Act per sistemi ad alto rischio. La capacità di realizzazione è sostenuta da fattori abilitanti già presenti nel contesto proponente. Il laboratorio sAlfer Lab dell'Università di Cagliari dispone di infrastrutture di calcolo dedicate (GPU cluster), dataset sperimentali su biometria e media forensics costruiti in anni di ricerca, e consolidata esperienza in campagne di benchmark internazionali (es. LivDet). A ciò si aggiunge l'esperienza maturata in iniziative interdisciplinari e ad alta rilevanza applicativa, quali il Centro Interuniversitario BullyBuster, che ha contribuito a consolidare competenze nella progettazione, valutazione e trasferibilità di sistemi AI in contesti sensibili e complessi. Il progetto potrà inoltre beneficiare del contributo scientifico complementare di Battista Biggio sui temi della sicurezza dei modelli di apprendimento automatico, dell'adversarial machine learning e della robustezza algoritmica, rafforzando in modo diretto la componente cyber della proposta. Il gruppo apporta pertanto competenze integrate su biometria, fingerprint PAD, deepfake detection, AI security e valutazione sperimentale in scenari realistici, con ulteriore potenziale di confronto applicativo attraverso stakeholder industriali quali DEDEM S.p.A. e Detesia.
ELEMENTI DEL PROGETTO RELATIVI ALLE TEMATICHE PRIORITARIE	

Contributo distintivo del progetto in relazione agli argomenti prioritari	Argomenti prioritari <i>4.1.3 – Modelli per il rilevamento sicuro dei dati (Subarea 4.1 – Hardware, Area 4 – Sicurezza delle Infrastrutture Digitali).</i>
	Il contributo distintivo del progetto consiste nel declinare l’Argomento 4.1.3 nello scenario, oggi particolarmente critico, dell’identità digitale sotto attacco GPAI. Il dispositivo mobile o embedded che acquisisce il dato biometrico dell’utente (sensore di impronte, fotocamera frontale, microfono) è a tutti gli effetti un nodo sensore edge del sistema di identità digitale. L’Agenda definisce l’Argomento 4.1.3 come ricerca su nuovi modelli per assicurare la generazione sicura dei dati da parte di nodi sensori e la loro integrità durante la trasmissione: la proposta traduce questa priorità in una catena concreta sensore-dispositivo-servizio, nella quale il dato acquisito non viene assunto attendibile a priori, ma viene verificato in termini di provenienza, coerenza di cattura, liveness e resistenza a manipolazioni sintetiche o fisiche. L’originalità del progetto non risiede soltanto nel rilevare deepfake o presentation attack, ma nel costruire modelli che stimino quantitativamente la fiducia nel dato prima e durante la decisione automatica. Il progetto integrerà indizi di acquisizione rilevabili a livello hardware-software del dispositivo (pattern di compressione, metadati EXIF, anomalie del sensore), tracce di replay e segnali biometrici in una misura unificata, calibrata e interpretabile di affidabilità. In questo modo il contributo alla tematica prioritaria non sarà marginale o indirettamente evocato, ma costituirà il cuore metodologico della proposta. Un ulteriore elemento di originalità rispetto allo stato dell’arte è la copertura simultanea di tre livelli di attacco (fisico alla cattura, digitale sul contenuto e avversario sul modello) che nella letteratura attuale vengono ancora trattati prevalentemente come problemi separati. Il framework unificato proposto consentirà di valutare e confrontare la robustezza di sistemi di identità digitale in scenari di attacco composti, fornendo alla comunità scientifica e ai fornitori di servizi uno strumento di valutazione e benchmark oggi sostanzialmente assente nello stato dell’arte.
COLLABORAZIONI CON ALTRI SOGGETTI PUBBLICI E PRIVATI	
Motivazione ed evidenze del coinvolgimento nel progetto di ricerca di imprese, enti e laboratori di ricerca pubblici o privati riconducibili a realtà italiane e/o europee, organismi internazionali	Il progetto si inserisce in una rete consolidata di collaborazioni scientifiche nazionali ed europee nel campo della biometria, della media forensics e della sicurezza dei sistemi di AI. In particolare, il gruppo di ricerca dell’Università degli Studi di Cagliari ha partecipato a iniziative e benchmark internazionali nel dominio della biometric presentation attack detection (es. LivDet), sviluppando nel tempo collaborazioni con centri di ricerca attivi su fingerprint PAD, face recognition, morphing e deepfake detection. Tale rete si inserisce in un contesto più ampio di ricerca interdisciplinare e trasferimento, al quale contribuisce anche l’esperienza maturata attraverso il Centro Interuniversitario BullyBuster, che ha rafforzato la

	capacità del gruppo di operare su sistemi intelligenti affidabili in scenari sensibili e ad alta rilevanza sociale e operativa. Il progetto beneficerà inoltre del confronto con ricercatori e istituzioni europee attive nei temi della AI security, della robustezza dei modelli e della trustworthy AI, con particolare riferimento a ecosistemi scientifici di eccellenza quali ELSA (European Lighthouse on Secure and Safe AI) ed ELLIS (European Laboratory for Learning and Intelligent Systems), che rappresentano oggi due riferimenti strategici per la ricerca europea sull'intelligenza artificiale sicura, affidabile e robusta. In tale contesto, la collaborazione scientifica con Battista Biggio, figura di riferimento internazionale nell'ambito dell'adversarial machine learning e della sicurezza dell'AI, costituisce un elemento qualificante del progetto, poiché rafforza direttamente la componente metodologica legata alla robustezza dei modelli e alla valutazione in scenari ostili. Un ruolo particolarmente rilevante potrà essere svolto anche da stakeholder industriali attivi nei servizi di identità digitale, onboarding remoto, tutela documentale e sicurezza dei sistemi biometrici. In tale prospettiva, il coinvolgimento di DEDEM S.p.A., azienda italiana attiva nel settore della documentazione fotografica e dei processi di acquisizione per servizi identitari, e di Detesia, realtà europea specializzata nella rilevazione spiegabile di contenuti sintetici e deepfake, rappresenta un fattore concreto di trasferimento tecnologico e di confronto con casi d'uso reali. Questo contesto collaborativo assicura la rilevanza applicativa del progetto e la validazione dei metodi proposti in scenari operativi coerenti con le priorità dell'Agenda nazionale di cybersicurezza.
Svolgimento di un periodo di studio all'estero nei Paesi dell'Unione Europea contestualizzato al progetto di ricerca	È previsto un periodo di ricerca all'estero presso un'istituzione europea di eccellenza, da svolgersi indicativamente tra il secondo e il terzo anno, con l'obiettivo di rafforzare le competenze del dottorando su AI robusta, biometria, media forensics e rilevamento di contenuti sintetici. Il soggiorno sarà finalizzato allo sviluppo congiunto di modelli per la rilevazione di attacchi di impersonazione GPAI-enabled, alla validazione in scenari cross-dataset e cross-device e al confronto con protocolli sperimentali avanzati non sempre disponibili localmente. La scelta della sede ospitante sarà effettuata privilegiando istituzioni europee di riconosciuta eccellenza con cui il gruppo proponente intrattiene relazioni scientifiche attive o potenzialmente

	attivabili. Tra le sedi particolarmente coerenti con gli obiettivi del progetto si segnalano il gruppo del Prof. Julian Fierrez presso la Universidad Autónoma de Madrid, con consolidata esperienza su biometria, morphing, document forensics e deepfake detection; il gruppo del Prof. Vitomir Struc presso la University of Ljubljana, rilevante per biometria, face analysis e anti-spoofing; e il gruppo del Prof. Mario Fritz presso CISPA Helmholtz Center for Information Security, di particolare interesse per trustworthy AI, sicurezza dei modelli e robustezza dei sistemi intelligenti. Il periodo all'estero consentirà al dottorando di accedere a dataset avanzati, infrastrutture sperimentali e competenze complementari, contribuendo alla definizione di benchmark condivisi, alla validazione esterna dei modelli sviluppati e alla produzione di risultati scientifici di elevato impatto. Inoltre, favorirà l'integrazione del progetto nel contesto europeo della ricerca sulla cybersicurezza e sull'AI affidabile, rafforzandone la visibilità e la trasferibilità.
Durata del periodo all'estero	6 mesi