UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

TESI DI LAUREA

Modelli di classificazione e regressione per la predizione di attacchi terroristici: un confronto empirico

RELATORE

Prof. **Fabio Palomba**

Università degli studi di Salerno

CANDIDATO

Leonardo Monaco

Matricola: 0512107459

Anno Accademico 2021-2022

"Le masse non si ribellano mai in maniera spontanea, e non si ribellano perché sono oppresse. In realtà, fino a quando non si consente loro di poter fare confronti, non acquisiscono neanche coscienza di essere oppresse."

-George Orwell

Sommario

Oggigiorno è difficile stabilire con sicurezza la prevenzione delle città, le quali sono sempre sotto la costante minaccia dei terroristi.
Lo sviluppo tecnologico ha portato a delle innovazioni sul tema della previsione degli attacchi terroristici, ma ciò purtroppo non basta infatti, vi è un esigenza dello sviluppo di uno strumento di questo tipo, siccome al momento non esistono delle tecniche di prevenzione che abbiano un'elevata efficacia e facilità d'uso contro eventuali attacchi terroristici.
L'utilizzo di eventuali tecniche di previsione di attacchi terroristici,ha sempre dato un buon risconto, un esempio può essere la PRA(Probabilistic Risk Analysis) essa è sempre stata considerata affidabile da molti governi per più di 30 anni per gestire decisioni di risk managment, altre tecniche come l'Agent Based Simulation che si è focalizzata sullo studio degli hotspot e su come vengono considerati poi in base alla propria reputazione, tecniche come la Geografical Information System che ha come scopo di prevenire attacchi terroristici solo nella regione Indocinese, la tecnica ALTER basata su un dataset videoludico come GTA V, una tecnica molto interessante, che non riesce a rispecchiare però nei minimi dettagli la rappresentazione del mondo reale.
Come detto già in precedenza in letteratura al momento non vi sono delle tecniche che risultano affidabili, ma chissà un giorno, con lo sviluppo tecnologico l'esito potrebbe variare.

Indice

Elenco delle figure

Elenco delle tabelle

CAPITOLO 1

Introduzione

1.1 Contesto applicativo

Le ragioni alla base del terrorismo moderno sono apparentemente complesse e intangibili. Fra i vari progressi che si sono raggiunti nell'ambito dell'intelligenza artificiale sicuramente vanno evidenziati i progressi tecnologici che hanno portato a questo sviluppo.
L'11 Settembre 2001 ha segnato la storia degli attacchi terroristici, un attacco simile, infatti ha devastato una nazione intera.
Dietro questo attacco vi sono molteplici cospirazioni, ma per certo sappiamo che da quel giorno la concenzione di attacco terroristico è cambiata, l'America da quel giorno è cambiata.

1.2 Obiettivo della tesi

L'obiettivo del lavoro di tesi consiste nell'analisi del terrorismo e delle tecniche di intelligenza artificiale applicate nello studio del fenomeno. In particolare si focalizza sull'esigenza di prevenire il fenomeno in futuro, mediante uno sviluppo tecnologico mirato.

1.3 Struttura della tesi

All'interno di questa sezione verrà esposta la struttura della tesi la quale è organizzata in 5 capitoli ognuno dei quali a sua volta è costituito dalle rispettive sotto sezioni.

- Il capitolo 2 descrive in maniera approfondita i diversi tipi di attacchi terroristici, agenti intelligenti e alcune tecniche esistenti di Intelligenza artificiale utilizzate per gli attacchi terroristici.
- Il capitolo 3 descrive le diverse fasi di costruzione del modello di predizione nello specifico Data Preparation, Data Evaluation e si focalizza sui modelli di regressione e classificazione.
- Il capitolo 4 analizza i risultati ottenuti nel capitolo precendente.
- Il capitolo 5 contiene le conclusioni sul lavoro svolto.

CAPITOLO 2

Backgroud e Stato dell'arte

2.1 Introduzione agli attacchi Terroristici

Da cosa deriva il termine terrorismo? Il termine terrorista cosi come il termine terrorismo si presentano per la prima volta durante la rivoluzione francese, inizialmente il termine era un termine positivo ma con il passare degli anni cambiò radicalmente, infatti successivamente al termine terrorista vennero associate associazioni criminali e da quel momento il terrorismo è diventato ciò che conosciamo oggi, una forma immaginabile di violenza.[1]

Come funzionano le organizzazioni terroristiche?

Ideologicamente i praticanti hanno come scopo quello di rivoluzionare un sistema politico o religioso cercando con le loro azioni di cambiare il sistema, le caratteristiche includono uno o più leader che mobilitano la gente per le attività terroristiche, l'uso delle armi, la segretezza dei piani operativi e il sostegno popolare.

Esistono numerevoli tattiche come ad esempio operazioni militari ed operazioni contro i militari, dove vengono prese di mira le persone in singolo oppure in gruppo causando vere e proprie stragi.

Solitamente si pianificano degli attacchi in alcuni "hotspot", ovvero nei luoghi più affollati e nei luoghi meno coperti da impianti di videosorveglianza.

Quando si parla di terrorismo il più delle volte associamo questa parola ad un evento, l'11 Settembre 2001, non è una data qualsiasi ma ricorre ad uno dei più "famosi" attacchi terroristici della storia: l'attacco alle torri gemelle, quest'ultimo è considerato in questo lavoro di

tesi un evento che è riuscito a dividere due ere ben diverse, la brutalità dell'evento lo porta ad essere considerato come una delle stragi più irruente e più crudeli.
Dietro a questo attacco ci sono tante cospirazioni e molteplici dubbi, che in questo lavoro di tesi non staremo a trattare ma sappiamo per certi che gli attacchi terroristici da quel giorno sono cambiati, possiamo distinguere infatti due ere diverse contestualizzando il pre 11 Settembre e il post 11 Settembre.
Questo giorno del 2001 infatti va a dividere anche due millenni o secoli completamente diversi, in cui vi sono state innumerevoli innovazioni e progressi in tutti gli ambiti e in tutti i settori.
Ma cosa è successo il giorno dell'11 Settembre?

Figura 2.1: Attentato dell'11 Settembre

La mattina dell'11 Settembre[2], nell'arco di poche ore quattro voli commerciali diretti in California dall'Est del paese vengono sequestrati e dirottati verso gli edifici di Wolrd Trade Center, le due torri gemelle di New York, il pentagono e Capitol Hill la sede del congresso USA a Washington, l'ultimo bersaglio sarà l'unico che verrà mancato, il tutto sotto la regia dell'organizzazione terroristica di Al Qaida. Non sono ancora le 9 di mattina in una mattina di estate in quel di New York l'11 Settembre, liddove un areo di linea che vola ad una quota bassisima attira e provoca stupore tra i passanti, lo stupore nel giro di pochi minuti si trasforma in orrore perchè il velivolo si schianterà sulla torre nord delle Twin Tower e successivamente dopo nemmeno 20 minuti arriverà un altro velivolo a schiantarsi verso la torre sud, successivamente alle 9:37 un ulteriore schianto un Boeing 757 precipita sulla facciata

ovest del Pentagono, l'ultimo aereo che doveva schiantarsi sul Campidoglio fù dirottato dai civili presi in ostaggio.

Il dipartimento di Stato americano, includendo nell'elenco anche le vittime del quarto aereo dirottato e precipitato in una zona disabitata, ha informato che i caduti, in quella che viene considerata "un'operazione bellica", provenivano da 90 Paesi.

Dalle cifre ufficiali risultano nei crolli delle Torri a New York 2.823 vittime, inclusi i passeggeri dei due aerei; 125 nell'incendio del pentagono; nei 4 aerei dirottati, e precipitati, c'erano 264 passeggeri[3].

Figura 2.2: Twin Tower 25 Settembre 2019

È necessario alcune domande:

- **Quanto può essere facile o difficile pianificare ed eseguire attacchi terroristici?**
- **Quali sono le cause?**
- **Come potremmo immaginare uno scenario simile?**

Le cause di un attacco terroristico, possono essere molteplici, politiche, religiose ecc.
Per rispondere a queste domande occore immergerci notevolmente nell'argomento infatti è necessario scoprire quante più informazioni possibile, in questo lavoro di tesi partiremo dall'etimologia della parola.
Gli innumerevoli sviluppi tecnlogici ci hanno permesso di utillizzare in questo lavoro di tesi degli agenti intelligenti che ci permetteranno di eseguire un lavoro di predizione sugli attacchi terroristici.

2.2 Agenti Intelligenti

Un Agente intelligente percepisce l'ambiente circostante mediante dei sensori e riesce ad eseguire delle azioni attraverso degli attuatori. Un prototipo di agente intelligente è sicuramente l'essere umano, esso infatti percepisce l'ambiente mediante occhi, naso e orecchie, effettua azioni attraverso piedi e mani.
Nel nostro contesto applicativo tratteremo di apparecchiature specifiche, contestualizzando la realizzazione dell'agente, infatti non sarà importante l'oggetto in se ma ci concentreremo sul come viene esso realizzato.
Sarà importante che per definizione l'agente realizzi la cosa giusta al momento giusto, verrà posta molta attenzione nei dettagli quando l'agente verrà applicato.
Il modello verrà addestrato e verrà effettuato un confronto sui risultati ottenuti, potremmo con un esempio valutare i risultati ottenuti prendendo in considerazione due agenti intelligenti entrambi impegnati nella risoluzione dello stesso puzzle, verificheremo il lavoro svolto e la sua qualità svolgendo degli esami in un lasso di tempo. Gli agenti potrebbero essere stati concepiti con qualche differenza o con strumenti informatici diversi, effettuando una misurazione temporale le migliori performance saranno date dagli agenti più veloci, nel caso effettuassimo un test dopo un ora potrebbe cambiare il risultato, l'agente partito lentamente potrebbe avere messo insieme più pezzi.

Da cosa è dato questo cambiamento?

Troveremo una risposta nella definizione di agente intelligente, gli agenti riescono ad ottimizzare le proprie performance in base alle percezioni, cercando sempre di massimizzarle, questo avviene a prescindere dallo scopo dell'agente, in ogni caso la procedura da seguire è sempre la stessa.

Descrizione dell'Agente, specifica PEAS

La specifica PEAS è l'acronimo di:

- **P**: **performance** è la misura adottata per valutare l'operato di un agente.
- **E**: **enviroment** elementi che formano l'ambiente.
- **A**: **actuators** disponibili all'agente per intraprendere le azioni.
- **S**: **sensors** attraverso i quali riceve gli input percettivi [4].

Parleremo successivamente di un dispositivo in cui viene utilizzata l'intelligenza artificiale, introdurremmo infatti gli UAV, in questo lavoro di tesi cercheranno di dare una risposta alla domanda che ci siamo posti in precedenza sulla difficoltà di esecuzione di un attacco terroristico.

2.2.1 Che cos'è un UAV

Un UAV [5] è un disposito areo senza pilota dotato di un IA che gli permette di ispezionare e rilevare obiettivi, la sua applicazione è dedicata al controllo e al salvataggio infatti vengono utilizzati in situazioni delicate dove il controllo umano è poco pratico.

Nella sociètà odierna il ruolo degli UAV è di notevole importanza infatti le attività che oggi svolgono gli UAV grazie all'utilizzo dell'intelligenza artificiale in passato erano impossibili da svolgere, anche utilizzando delle apparecchiature simili il controllo a distanza in determinate situazioni rendevano poco pratico l'utilizzo, dato che in alcune situazioni occorre prendere delle decisioni in pochi frazioni di secondi, adesso invece utilizzando dispositivi intelligenti alcune attività possono essere automatizzate.

Ma da cosa è composto un UAV?

Vengono utilizzati dei sensori ottici per sorvolare e per riconoscere gli obiettivi, in entrambe le azioni svolge un ruolo chiave l'IA, un IA che può essere basata su algoritmi o su reti neurali. In questo lavoro di tesi ritengo molto importanti i dispositivi UAV perchè tutto ciò che riguarda minacce terroristiche e cyberwar sono effettuabili da UAV infatti sono in grado di dare la caccia ad obiettivi specifici, riconoscere obiettivi specifici e intraprendere azioni per

la quale sono stati programmati.
Tuttavia il riconoscimento delle immagini viene eseguito con le reti neurali e questo non è ancora stato perfezionato del tutto, tuttavia i gruppi terroristici potrebbero non preoccuparsi di colpire un obbiettivo errato.
A questo punto occorre chiederci quanto è difficile da parte di alcuni gruppi terroristici costruire un UAV?
Tutti i componenti hardware per costruire un UAV si trovano sulla rete ad un prezzo irrisorio, a questa domanda non c'è una risposta certa in quanto occorrono comunque delle competenze, che sono disponibili in rete infatti diverse organizzazioni rilasciano gratuitamente dei software e il materiale didattico per riuscire a realizzare un UAV.

2.3 Tecniche esistenti di Intelligenza Artificiale per attacchi terroristici

In questa sezione introdurremo le tecniche esistenti di Intelligenza artificiale volte a prevenire e simulare attacchi terroristici.
Nell'analisi svolta[6] si è riscontrato che in letteratura non vi sono tecniche particolarmente efficaci bensì vi sono diverse tecniche che vengono utilizzate in diversi casi a seconda di diversi fattori, queste tecniche però data la scarsa efficacia nella prevenzione e nella simulazione non vengono utilizzate come strumenti principali delle agenzie governative.
Lo scopo infatti sarà quello di evidenziare i vantaggi e gli svantaggi di ciascuna tecnica.

2.3.1 PRA- Probabilistic Risk Analysis

La prima tecnica che prenderemo in considerazione è la Probabilist Risk Analisys conosciuta anche come PRA.
Questa tecnica come si evince già dal nome è una tecnica a rischio probabilistico,la PRA per più di 30 è stata utilizzata da molti governi come strumento principale, infatti è stata molto importante per gestire le decisioni di risk management.
Sono stati proposti alcuni tipi di approcci di carattere probabilistico ognuno delle quale utilizzano strumenti diversi:

- Albero degli eventi(event tree)
- Albero dei gausti (fault tree)
- Albero di decisione (decision tree)

Al momento non ci sono degli approcci in grado di effettuare correttamente un' analisi di un intero scenario terroristico che individui decisioni corrette. Un importante aspetto essenziale da tenere in considerazione, è quello relativo alla modellazione degli avversari ovvero i terroristi che a differenza di un sistema ingegneristico, sono degli avversari intelligenti che riescono ad adattarsi alle nuove misure difensive, infatti si assume che ad ogni decisione presa nella definizione dell'attacco l' avversario effettui una scelta che gli permetta di massimizzare i suoi obiettivi.
La difficoltà di questo approccio è dato dalla difficoltà nel convertire le informazioni ottenute dall'Information Community in dati consistenti che possano essere input nella Risk Analysis.
Il comitato NRC, il cui scopo è quello di difendere gli Stati Uniti da dei possibili attacchi bioterroristici, ha proposto di modellare l'interazione fra i difensori e attaccanti con l'uso di un decision tree, dove ogni attaccante tenta di massimmizzare la propria funzione obiettivo, mentre le risposte dei difensori sono descritte come degli eventi incerti che vengono influenzati dalle scelte degli attaccanti.
Oltre a questa soluzione ci sono altre tre soluzioni adottabili utilizzando gli alberi di decisione o alberi degli eventi.

1. Un albero di decisione in cui la propria interazione tra attacante e difensore viene descritta come un difensore che tenta di massimizzare la propria funzione di utilità mentre gli attaccanti vengono descritti come eventi incerti, che vengono influenzati dalle risposte dei difensori.

2. Un albero di decisione in cui sia gli attaccanti che i difensori tendono a massimmizzare la propria funzione obiettivo.

3. Un albero degli eventi in cui sia le scelte degli attaccanti e sia le risposte dei difensori vengono descritte come eventi incerti.

Tra i vari modelli che sono stati individuati Ezell et al. [7] sceglie quello proposto dal comitato della NRC.
Ma come viene modellato dal punto di vista probabilistico il Rischio?
Secondo l'opione dei più influenti ricercatori del terrorism risk lo si può descrivere come il prodotto fra minaccia, la vulnerabilità e le conseguenze.
Gli elementi che costituiscono il rischio sono i seguenti:

- Una minaccia, che viene definita come la probabilità di un attacco;

- La vulnerabilità, definita come la probabilità che abbia successo un attacco effettuato;
- Le conseguenze, definite come le perdite (morti, feriti, impatti economici diretti e indiretti) che si hanno nel caso in cui l'attacco abbia successo.

In termini matematici si ha:

$$Risk = P(A) \times P(S|A) \times C \tag{2.3.1}$$

In questa applicazione la probabilità di un attacco terroristico P(A) è un valore difficile da stimare in quanto, per avere un valore stimato attendibile bisogna avere un approfondita conoscenza dei dati, delle motivazioni, degli intenti e delle capacità dei terroristi.
Solitamente quando gli analisti dell'intelligence effettuano una stima del valore di P(A) calcolano la credenza di ciò che un terrorista può fare sulla base delle informazioni disponibili che sono state fornite dall'Intelligence Community, da esperienze personali e giudizi.
Dalle analisi svolte si tende ad evidenziare come detto anche in precedenza che i valori di questi dati non sono statici bensì sono in continua evoluzione, l'avversario è intelligente ed osserva sempre le azioni intraprese dal difensore, questo aspetto rende difficile la modellazione del problema.
Un ulteriore problematica riscontrata nella PRA è legata al fatto che le probabilità associate ad eventi complessi sono spesso difficili da calcolare, questo ci porta a scomporre questi eventi in più componenti, infatti ci aiuta successivamente ad andare a determinare la probabilità di ciascuna componente, andando poi a riassemblare in unici eventi in seguito.
Per la decomposizione in componenti vengono utilizzati vari strumenti come alberi logici, modelli di sistemi dinamici, reti Bayesiane e influence diagram.
Possiamo suddividere gli alberi logici in due categorie:

- Alberi di probabilità, eventi e decisione
- Alberi di guasti, attacco e successo

Nonostante Ezell abbia proposto una serie di strumenti, gli strumenti maggiormenti utilizzati saranno gli strumenti che utilizzano la prima categoria degli alberi logici e la modellazione attraverso le reti Bayesiane [8] .

2.3.2 Agent - Based Simulation

La seconda tecnica analizzata è la tecnica di Agent Based Simulator proposta da Bosse et al.[9]. uno studio basato sul crimine a larga scala il cui scopo è quello di indagare le dinamiche

spazio temporali.
In dettaglio questa tecnica analizza come prevedere il comportamento degli autori dei reati e dei bersagli e si focalizza su come evidenziare la dislocazione e la simulazione degli hotspot criminali utilizzando un modello agent-based.
Utilizzando il modello sono state eseguiti diversi esperimenti di simulazioni e i risultati analizzati con tecniche formali riproducono in modo adeguato i modelli di spostamento.
Per la simulazione sono stati proposti diverse teorie, in particolare ci concentremo delle seguenti teorie:

1. Teoria delle attività routinarie
2. Teoria della Prevenzione della criminalità situazionale

Nel modello di simulazione sulla dislocazione dei crimini ci sono tre tipi di agenti :

- Criminali
- Guardiani
- Passanti

1. La teoria delle attività routinarie è una teoria informale ed è considerata come la più influente: si concentra sugli autori del reato ovvero i criminali, i guardiani e i passanti affermando che un crimine si presenta quando un criminale motivato a commettere un crimine incontra un bersaglio adatto e non sono presenti i guardiani.
2. La teoria della Prevenzione della criminalità situazionale afferma che alcuni crimini possono essere prevenuti posizionando dei guardiani nei luoghi appropriati ovvero nei luoghi che possono essere maggiormente colpiti da crimini, i guardiani all'interno di questa teoria possono variare in:
    - Forze di polizia
    - Sistemi di allarme
    - Telecamere di sorveglianza

Entrambe le teorie risultano attendibili per le loro dinamiche spazio- temporali, l'analisi suscita attenzione per l'interazione tra il comportamento degli autori di reato, dei passanti e dei guardiani e pone una domanda rilevante sui fattori che influenzano l'emergere dei cosidetti hotspot.
Sulla base dell'idea di hotspot si possono porre alcune domande correlate, tra cui:

- la posizione degli hotspot cambia nel tempo?
- come si può prevedere l'affermazione di hotspot?
- come si può prevenire l'insoregere di hotspot?
- qual'è la relazione tra l'emergere di hotspot e la geografia di una città?
- qual'è la relazione tra l'emrgere di hotspot e la demografia della popolazione?

Alcuni esempi di hotspot sono le stazione ferroviarie oppure i centro commerciali.
Tra le numerose caratteristiche in comune, fra queste vi sono la presenza di molti passanti e la mancanza di sistemi di videosorveglianza.
Inoltre, con il trascorrere del tempo le situazioni spesso cambiano poiché le attività criminali si spostano in altri luoghi.
Tale fenomeno probabilmente è causato dal miglioramento dei sistemi di videosorveglianza in quel luogo oppure da un incremento del numero degli ufficiali di polizia.
Un altro aspetto da tenere in considerazione è la "reputazione": un luogo dopo aver ricevuto un certo numero di assalti inizia a sviluppare una cattiva reputazione quindi i passanti iniziano a spostarsi da quel luogo.
Per descrivere i pattern nel dislocamento dei crimini è necessario conoscere il numero degli agenti per ogni tipologia (criminali, guardiani e passanti).
Successivamente occorre individuare la densità di criminali, guardiani e passanti ed infine è necessario avere informazioni relative alla reputazione di un luogo.
I concetti appena esposti vengono formalizzati attraverso la seguente tabella che mostra tutte le variabili presenti all'interno del modello di simulazione.

Name	Explanation
c	Total number of criminals
g	Total number of guardians
p	Total number of passers by
c(L, t)	Density of criminals at location L at time t.
g(L, t)	Density of guardians at location L at time t.
p(L, t)	Density of passers-by at location L at time t.
β(L, a, t)	Attractiveness of location L at time t for type a agents: c (criminals), p (passers-by), or g (guardians)
ba(L, a, t)	Basic attractiveness of location L at time t for type a agents: c (criminals), p (passers-by), or g (guardians)
assault_rate(L, t)	Number of assaults taking place at location *L* per time unit.

Figura 2.3: Variabili nel modello di simulazione

Come viene effettuato il calcolo del numero degli agenti?
Il calcolo del numero di agenti nei vari luoghi viene effettuato determinando il movimento di essi in funzione della reputazione del luogo.

$$c(L, t + \Delta t) = c(L, t) + \eta * (\beta(L, c, t) * c - c(L, t))\Delta t \tag{2.3.2}$$

A densità $c(L, t + \Delta t)$ dei criminali nel luogo L all'istante $t + \Delta t$ è pari alla densità dei criminali al medesimo luogo all'istante t più una costante η la quale esprime la velocità con la quale i criminali si spostano per ogni unità di tempo.
Nel caso in cui, invece, si volesse calcolare la densità relativa ai passanti, sulla base della la formula precedente, ottenendo:

$$p(L, t + \Delta t) = p(L, t) + \eta * (\beta(L, p, t) * p - p(L, t))\Delta t \tag{2.3.3}$$

Diversa sarà la formula per ottenere la densità dei guardiani in quanto essa è dinamica.
Per individuare la reputazione di un luogo è necessario ricorrere all'utilizzo di due combinazioni lineari di densità:

$$\beta(L, c, t) = \beta_{c1} * (1 - g(L, t)/g) + \beta_{c2} * p(L, t)/p + \beta_{c3} * ba(L, c, t) \tag{2.3.4}$$

$$\beta(L, p, t) = \beta_{p1} * (1 - c(L, t)/c) + \beta_{p2} * g(L, t)/g + \beta_{p3} * ba(L, p, t) \tag{2.3.5}$$

Negli ultimi decenni l'interesse per l'area della simulazione sociale basata su agenti, questo è un approccio combinato basato su agenti, simulazione informatica e scienze sociali, in cui i ricercatori sfruttano la simulazione basata su agenti per ottenere una migliore comprensione dei fenomeni sociali.
I vantaggi di questo approccio sono dovuti alla combinazione del paradigma ad agenti con quelli della simulazione sociale, infatti questo approccio permette di fornire esperimenti sociali su larga scala, quindi sicuramente uno dei vantaggi riconducibili è la scalabilità.

Per sviluppare un modello di prevenzione corretto bisogna studiare una serie di strategie:

1. Strategie reattive
2. Strategie di anticipo

Tutte le strategie che vengono prese si basano sulle azioni intraprese dai guardiani.
In totale, sono state sviluppate otto differenti strategie:

- La prima strategia è Baseline strategy. In questa strategia i guardiani non effettuano spostamenti e la loro densità nei differenti luoghi è la stessa in tutti gli istanti di tempo;
- La seconda strategia è una strategia di tipo reattivo e prende il nome di Reactive 1. In questa strategia la quantità di guardiani che si muove verso un nuovo luogo è proporzionale alla densità dei criminali presenti in questo nuovo luogo;
- La terza strategia, è la strategia Reactive 2, in questa strategia il numero di guardiani che si spostano verso un nuovo luogo è proporzionale alla percentuale di attacchi che vi sono stati recentemente;
- La quarta strategia è la strategia Reactive 3, è una strategia molto simile alla Reactive 2 con l'unica differenza che, invece di calcolare la percentuale di attacchi nell'ultimo periodo, si fa riferimento a tutti gli attacchi che vi sono stati in precedenza;
- La quinta strategia è la strategia Reactive 4 è l'utilma strategia reattiva e anziché far riferimento alla densità di guardiani è proporzionale alla densità dei passanti, questo comporta che il numero di guardiani che si dirige verso un nuovo luogo cresce all'aumentare della densità dei passanti che si trovano in quel punto;
- La sesta strategia viene definita è una strategia di anticipo,la strategia Anticipate 1, dove la quantità di guardiani che si sposta verso una nuova posizione è proporzionale alla densità di criminali che in futuro ci si aspetta di trovare in quel determinato luogo;
- La settima strategia è la strategia Anticipate 2, rispetto alla prioma strategia di anticipo non fa più riferimento alla densità dei criminali, ma fa riferimento a quella dei passanti che ci si aspetta di trovare presso quella posizione in futuro;
- L'ottava strategia è la strategia Anticipate 3, questa è l'ultima strategia di anticipo e anche l'ultima strategia in totale. In questo strategia il numero di guardiani è direttamente proporzionale al numero di assalti che si potrebbero verificare in una specifica posizione nel futuro. Questo valore viene calcolato tramite una media delle densità attese dei criminali e dei passanti, quindi non è altro che una combinazione lineare di esse, questo numero si ottiene dalla combinazione della strategia Anticipate 2 e della strategia Anticipate 3.

2.3.3 Temporal Trace Language- TTL

Per modellare i diversi aspetti dello spostamento criminale dal punto di vista degli agenti è necessario un linguaggio di modellazione espressivo in cui modellare gli aspetti qualitativi e gli aspetti quantitativi. Modellando gli aspetti qualitativi andremmo a modellare le osservazioni, le convinzioni e le decisioni da compiere quando avviene un'aggressione o un arresto tutto questo sempre valutando anche gli aspetti dell'ambiente che ci circondano. Andando a modellare gli aspetti quantitavi invece si vanno ad affrontare delle dinamiche legate come la reputazione del luogo.
Un ulteriore requisito del linguaggio di modellazione è la sua idoneità nello esprimere sia i meccanismi base dello spostamento dei criminali nel contesto delle simulazione e sia invece le proprietà globali sullo spostatemento dei criminali:

- Nel primo caso coinvolgono funzioni decisionali per i singoli agenti.
- Invece un esempio di proprietà globali sullo spostamento dei criminali tratta la posizione dei criminali nei punti caldi che variano nel tempo.

Il Temporal Trace language TTL soddisfa tutti i requisiti trattati in precedenza, integrando per l'appunto sia aspetti qualitativi e sia aspetti quantitativi.
Integrando entrambi gli aspetti il TTL consente al modellatore di sfruttare sia i metodi logici e sia i metodi numerici, questi metodi lo rendono in grado di esprimere diverse proprietà dinamiche a diversi livelli di aggregazione rendendolo adatto nelle fasi di analisi e nellla simulazione.
Il TTL si basa sul presupposto che la dinamicità che può essere descritta come un evoluzione del tempo. Vi sono una serie di proprietà che vengono chiamate proprietà di stato esse vengono chiamate in questo modo proprio per distinguerle dalle proprietà dinamiche che mettono in relazione stati diversi nel tempo.
Vi sono una serie di proprietà che mantengono lo stato e una serie di proprietà che non si mantengono nello stato. Alcuni esempi di proprietà di stato sono "ci sono alcuni agenti criminali nella posizone A" oppure "l'agente 1 esegue un' aggresione criminale contro l'agente 2", nel primo caso andiamo ad assegnare dei valori reali alle variabili, anche questo tipo di assegnazioni vengono considerate come delle descrizioni possibili di una proprietà di stato.
Per poter formalizzare delle proprietà di stato occorre innanzi tutto sapere cos'è un ontologia.
Che cos'è un ontologia? Un ontologia è un insieme finito di ordinamenti, in cui le relazioni e le funzioni su questi ordinamenti sono delle costanti.

Come viene utilizzata un ontologia, a cosa serve?
Un ontologia ci permette di poter formalizzare delle proprietà di stato, infatti occorre avere delle ontologie che per formalizzare le proprietà devono essere specificate in un formato logico del primo ordine.

2.3.4 LEADSTO

LEADSTO[10] viene considerato un sottolinguaggio di TTL, in quanto per poter eseguire pseudo esperimenti non occorre utilizzare tutta l'espressività di TTL,infatti LEADSTO nasce con uno scopo quello di sviluppare modelli di simulazione in modo dichiarativo.
Le dipendenze temporali in LEADSTO, sono modellate da proprietà dinamiche eseguibili.
Il formato LEADSTO è definito come segue:

- Se la proprietà dello stato è valida per un certo intervallo di tempo di durata g, allora dopo un certo ritardo tra e e f la proprietà dello stato si manterrà per un certo intervallo di tempo con durata h.

Come funziona il modello di simulazione LEADSTO?
Gli aspetti geografici dell'ambiente sono modellati da un grafo che consiste in una serie di località alcune di esse sono collegate da bordi.
All'interno di questo ambiente, diversi agenti si muovono e si incontrano nelle diverse località.
Anche in questo caso i tipo di agente sono tre:

- Criminali
- Passanti
- Guardiani

Si presume che i passanti siano i bersagli adatti, perchè ad esempio sembrano ricchi e deboli, il loro livello di protezione è dato dallo spostamento dei guardiani.
Il crimine verrà commesso dal criminale nel momento in cui si troverà in luogo in cui vi è un passante e non vi è nessun guardiano.

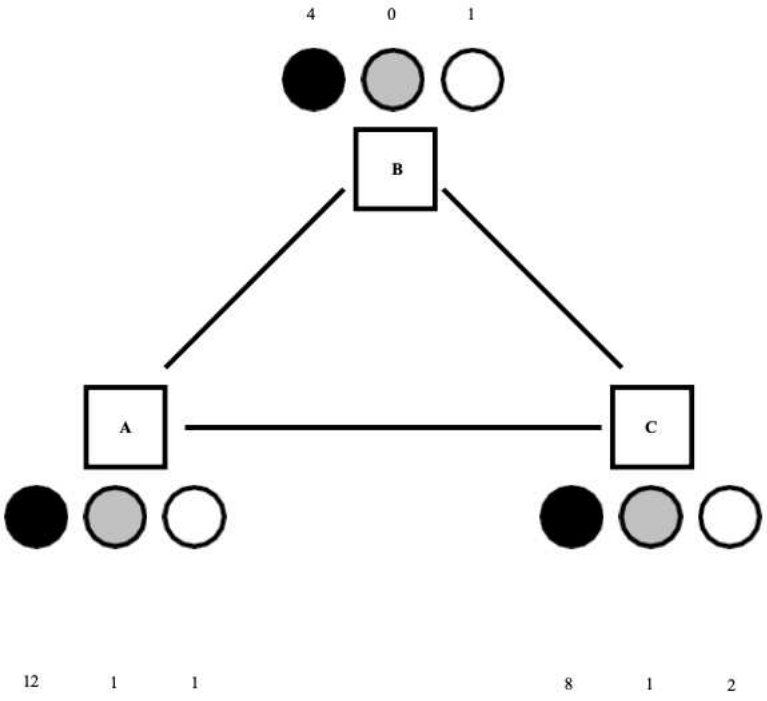

Figura 2.4: La seguente immagine rappresenta una città con soli tre luoghi importanti A,B,C ed è popolata da 30 agenti.

Nella figura sono presenti tre tipi di cerchi, ognuno indica un target:

- I cerchi neri individuano i passanti
- I cerchi grigi individuano i guardiani
- I cerchi bianchi individuano i criminali

Nella figura presentata i crimini possono essere commessi soltanto nel punto B, in quanto in quel punto non vi è la copertura di guardiani, poichè vi sono 1 criminale, 4 passanti e 0 guardiani.
L'interazione tra l'agente e l'ambiente è modellata dalle informazioni sull'ambiente(es. luogo in cui si trova, dove sono i bersagli adatti) e dall' esecuzione di azioni(andare in luogo diverso o commettere un reato).

Per prendere decisioni sul luogo in cui andare gli agenti aggiornano in continuazione l'attrattiva che assegnano a ciascun luogo, viene rappresentata da un numero reale nel dominio di valori [0;1].

Come viene calcolata l'attrattiva? L'attrattiva viene calcolata come somma ponderata di tre valori:

1. Attrattiva di base individuale che l'agente assegna a quel luogo.
2. Reputazioni delle aggressioni del luogo.
3. Reputazione degli arresti della località.

Successivamente vengono attribuiti dei fattori di peso, precisamente tre w1,w2,w3 per ogni agente.

Come funzionano i fattori di peso?

I fattori di peso possono essere positivi e negativi a seconda delle azioni che compiono gli agenti.

Ad esempio i criminali avranno dei fattori di peso positivo nel momento in cui effettueranno delle aggressioni e un fattore di peso negativo per la reputazione di arresto.

Vicecersa invece varrà per i passanti: avranno un fattore di peso molto negativo per la reputazione di aggressione e un fattore di peso negativo per l'arresto.

Gli agenti si sposteranno in base all'attrattiva dei luoghi, preferirendo il luogo con maggiore attrattiva.

Il criminale dopo aver compiuto un crimine diventerà noto ai guardiani per diverse fasi temporali(4 sono le fasi temporali), questo per far in modo che guardiani siano in grado di riconoscere ed arrestare i criminali.

2.3.5 GIS e Random Forest - Geografical Information System

La tecnica che analizzeremo è la tecnica di Hao et al.[11] la particolarità di questa tecnica è data dall'intento con cui è nata ovvero quello di prevenire attacchi terroristici solamente nella penisola dell'Indocina.

Hao nel suo approccio ricorre all'utilizzo del sistema informativo geografico GIS (Geographic Information System) in combo con la tecnica della Random Forest.

Gis permette di effettuare una serie di operazioni come analisi,registrazione,acquisizione, e molto altro su "geo-riferiti". Vengono chiamati "geo-riferiti" le informazioni che derivano da dati grafici: infatti utilizzando ArcGIS un software che permette di creare e utilizzare mappe sulla base delle informazioni che il sistema rileva.

Il secondo strumento Random Forest è un metodo di machine learning che permette di predirre il rischio di attacchi terroristici nella penisola dell'Indocina. Il metodo della Random

Forest ha mostrato delle buone performance con valori AUC di 0.839. L'AUC lo si può interpretare come la probabilità che il modello di machine learning classifichi un esempio positivo casuale più alto di un esempio negativo casuale. L'AUC ha un valore compreso tra 0 e 1. Infatti se le previsioni fornite da un modello sono errate al 100% allora l'AUC avrà valore di 0.0; l'inverso invece se le previsioni sono corrette al 100% il modello avrà un AUC di 1.0. In altri termini l'AUC corrisponde all'area sotto la curva ROC, la quale mostra graficamente le prestazioni di un modello di classificazione e permette di tracciare:

- Tasso di veri positivi;
- Tasso di falsi positivi.

La combo GIS Random Forest porta con sé un grande potenziale nella simulazione degli attacchi terroristici.
Lo scopo dello studio era quello di capire l'evoluzione spazio-temporale degli attacchi terroristici e predire le zone che si trovano a rischio. Lo studio condotto da Hao et al.[11] lo si può schematizzare attraverso una serie di steps:

1. Estrarre scenari terroristici che si sono verificati nella penisola dell'Indocina dal database del terrorismo globale, definito come GTD (Global Terrorism Dataset), e usare il software ArcGIS per localizzare gli attacchi terroristici e per vedere le aree localizzate sulla mappa;
2. Utilizzare la funzione "Kernel Density" su ArcGIS e OriginLab (software per la rappresentazione grafica dei dati) e analizzare l'evoluzione degli attacchi a seconda delle variabili spazio/tempo;
3. Avviare una procedura di data preparation con i dati geografici e individuare i corrispondenti raster data dell'attacco terroristico. Per raster data intendiamo "raster data" una matrice di pixel organizzata in righe e in colonne dove ogni cella contiene un valore che rappresenta un'informazione, come ad esempio la temperatura. Solitamente si utilizza questa struttura dati nel caso in cui le informazioni da elaborare constano di fotografie aeree, immagini prese dai satelliti oppure mappe;
4. Costruire l'algoritmo della Random Forest per predire attacchi terroristici su una scala geografica spaziale nella penisola dell'Indocina.

Viene mostrata l'architettura del sistema per la predizione di attacchi terroristici.

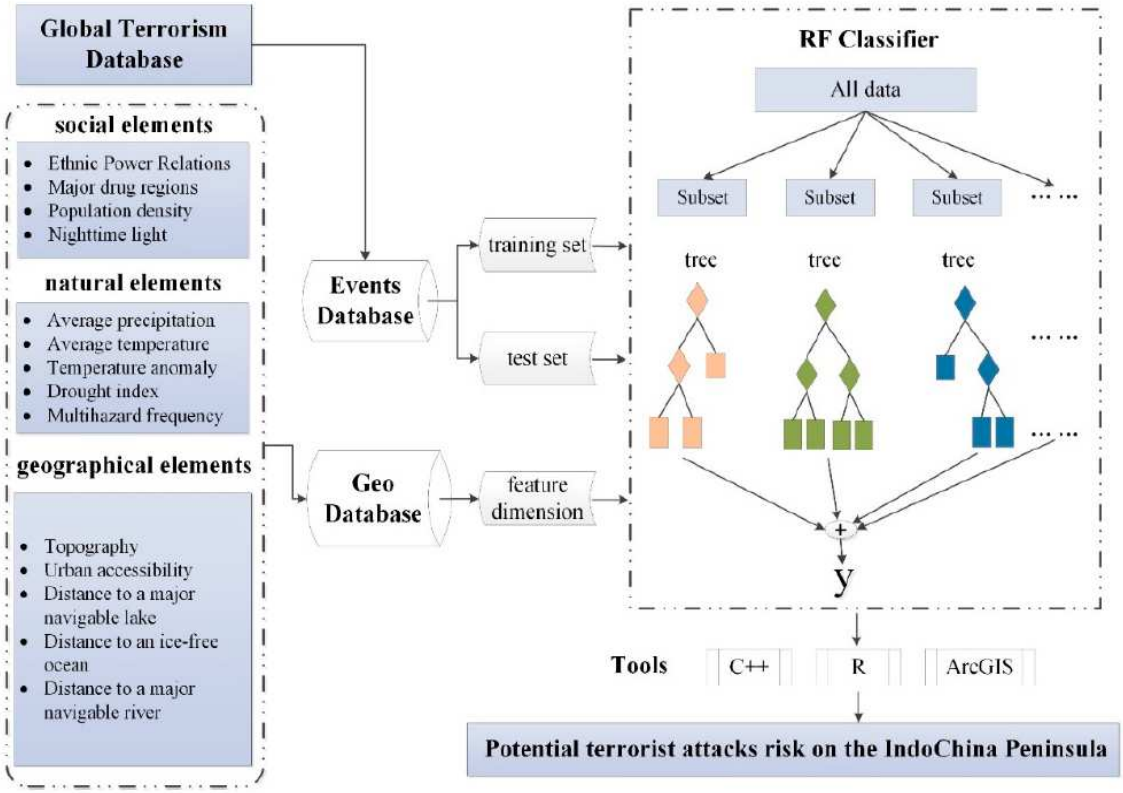

Figura 2.5: La figura mostra come utilizzare il modello della Random Forest per la simulazione. Vengono introdotte differenti caratteristiche utilizzate dal classificatore durante la predizione.

L'immagine appena mostrata si concentra su tre categorie di elementi:

- Elementi sociali;
- Elementi naturali;
- Elementi geografici.

Creazione del dataset

I dati utilizzati nella ricerca sono presenti nel Global Terrorist Database, il quale è un database open-source disponibile in rete e contiene informazioni su attentati terroristici che si sono verificati nel mondo fra il 1970 e il 2016. Si può accedere a questo dataset al seguente indirizzo: Global Terrorist Dataset.

Il database in questione si basa su una copia della banca dati creata dalla Pinkerton Global Intelligence Service (PGIS). Ogni elemento del GTD contiene informazioni relative alla data dell'attentato e altre caratteristiche, come le armi utilizzate, gli ostaggi presi dai terroristi, il luogo e i responsabili, qualora tali informazioni fossero disponibili.

Per maggiore consistenza nonchè per maggiore coerenza tra i dati, le informazioni del dataset sono state convertite in un raster data in cui la risoluzione spaziale dei dati geografici è la stessa.Vi sono delle aree con alto rischio, in queste aree vi sono verificati degli attacchi terroristici e vengono rappresentante con un pixel corrispondente al raster di valore 1: con il valore 1 viene rappresentanta un area ad alto rischio, con il valore 0 invece si rappresentano invece le restanti aree.

Stima kernel di densità

Si utilizza la stima kernel di densità per il riconoscimento dei pattern e per la classificazione attraverso una stima di densità negli spazi metrici, questo metodo permette di convertire un insieme di punti in un raster. Questo metodo permette di calcolare per ogni x all'interno dello spazio metrico la probabilità di appartenere ad una classe X, considerando la densità di X in un intorno h del punto x.
La funzione proposta da Hao et al.[11] è la seguente:

$$\hat{f}_h(x) = \frac{1}{nh} \sum_{i=1}^{n} K(\frac{x - X_i}{h}) \tag{2.3.6}$$

dove h rappresenta l'ampiezza dell'intorno; $f_h(X)$ è la stima del kernel nel punto X con ampiezza dell'intorno h; $x - X_i$ è la distanza fra il punto x e il punto X_i; in conclusione, K è la funzione Kernel.
L'ampiezza dell'intorno è pari a 50km. Utilizzando il software ArcGIS è possibile calcolare la funzione con lo strumento "Densità Kernel", inoltre, sempre grazie al software, è possibile distribuire geograficamente i punti degli attacchi terroristici.

Algoritmo della Random Forest

La Random Forest è stata implementata grazie all'utilizzo dell'ambiente di sviluppo R. Questo approccio non è altro che una tecnica di ensemble learning sviluppata sulla base di un grande insieme di alberi di decisione. Ogni albero è addestrato selezionando solo un numero casuale di variabili e di campioni dal dataset di training. Per utilizzare questa tecnica è necessario scegliere il valore di tre parametri:

- il numero di campioni di bootstrap;
- il numero di variabili campionate ad ogni divisione;

- la dimensione minima dei nodi terminali, valore al di sotto del quale le foglie non vengono più suddivise.

Inoltre per evitare che il modello sviluppato mostri un fenomeno di overfitting sul dataset si può applicare il metodo di 10-fold cross-validation che consiste nel suddividere la banca dati in campioni da training e campioni da validazione.

Dopo aver eseguito tutti gli step elencati precedentemente, si passa allo step successivo ovvero a sviluppare mediante il software ArcGIS le distribuzioni spaziali con zone ad alto rischio di attentati terroristici. Di seguito viene riportato il risultato ottenuto.

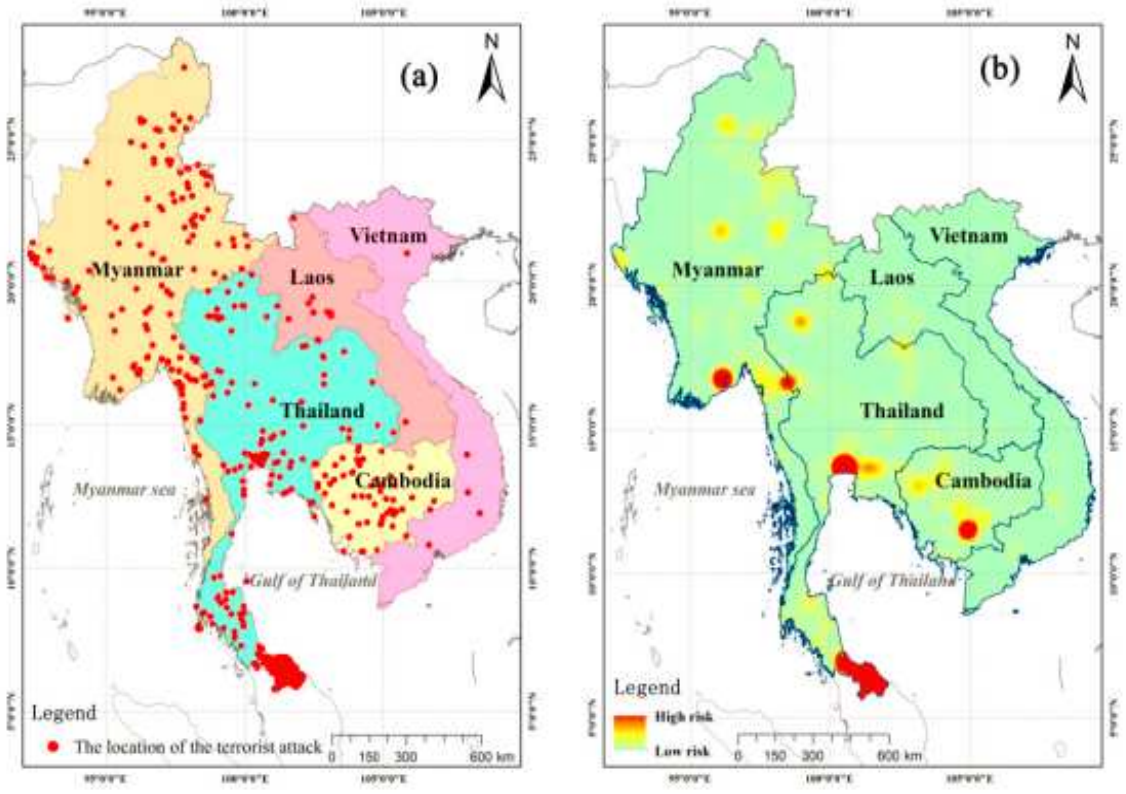

Figura 2.6: Nella figura a sinistra vengono mostrati in rosso tutti i luoghi dove si sono verificati numerosi attacchi, mentre nella figura a destra sono mostrate le zone ad alto rischio di attacchi.

Sono stati individuati in totale cinque hot spot distribuiti negli Stati di Cambodia, Myanmar e Tailandia, questo dimostra come la maggior parte degli hotspot si trovino sulle frontiere. Basandosi sui cinque Stati presenti nella penisola dell'Indocina e dalla rappresentazione grafica delle frequenze di attacchi terroristici in ciascun paese, emerge che negli ultimi anni

la Tailandia, v lo si può evincere molto facilmente dal grafico disegnato grazie al software OriginLab.

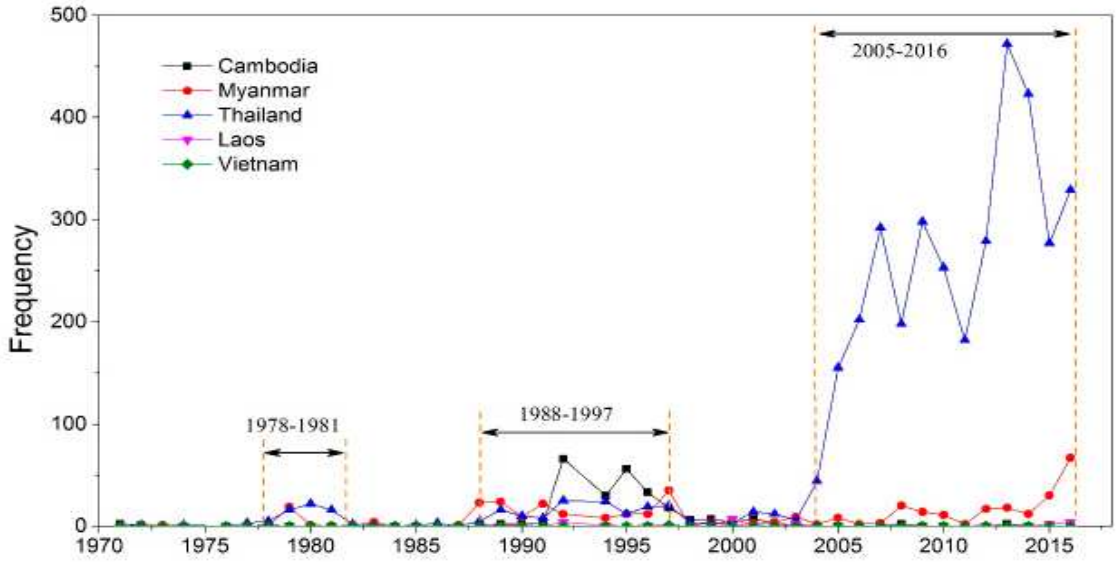

Figura 2.7: Nella figura viene rappresentata la frequenza con la quale si sono verificati attacchi terroristici in ogni Stato dal 1970 al 2016.

In conclusione si può affermare che i risultati ottenuti con questo studio si sono rivelati particolarmente efficienti e ciò è dovuto alla combinazione di tecniche di machine learning, come la Random Forest, con sistemi di geo-informazione per la simulazione della distribuzione del rischio di attacchi terroristici.
Si vuole evidenziare come questo approccio non è context-dependent e quindi non è legato solamente all'ambito del terrorismo, ma può essere utilizzato senza alcun problema laddove la variabile geo-spaziale assuma un ruolo di principale importanza.

Algoritmo Random Forest

L'algoritmo Random Forest è stato implementato in R.
Questo algorimto utilizza una tecnica di ensemble learning sviluppata sulla base di un grande insieme di alberi di decisione.Ogni albero viene addestrato selezionando un numero casuale di variabili e di campioni dal dataset di training. Per utilizzare questa tecnica è necessario scegliere il valore di tre parametri:

- il numero di campioni di bootstrap;

- il numero di variabili campionate ad ogni divisione;
- la dimensione minima dei nodi terminali, valore al di sotto del quale le foglie non vengono più suddivise.

Per evitare che il modello sviluppato mostri un fenomeno di overfitting sul dataset si può applicare il metodo di 10-fold cross-validation suddividendo in campioni di training e campioni di validazione.

Dopo aver eseguito tutti gli step software ArcGIS le distribuzioni spaziali con le relative zone ad alto rischio di attentati terroristici. Di seguito viene riportato il risultato ottenuto.

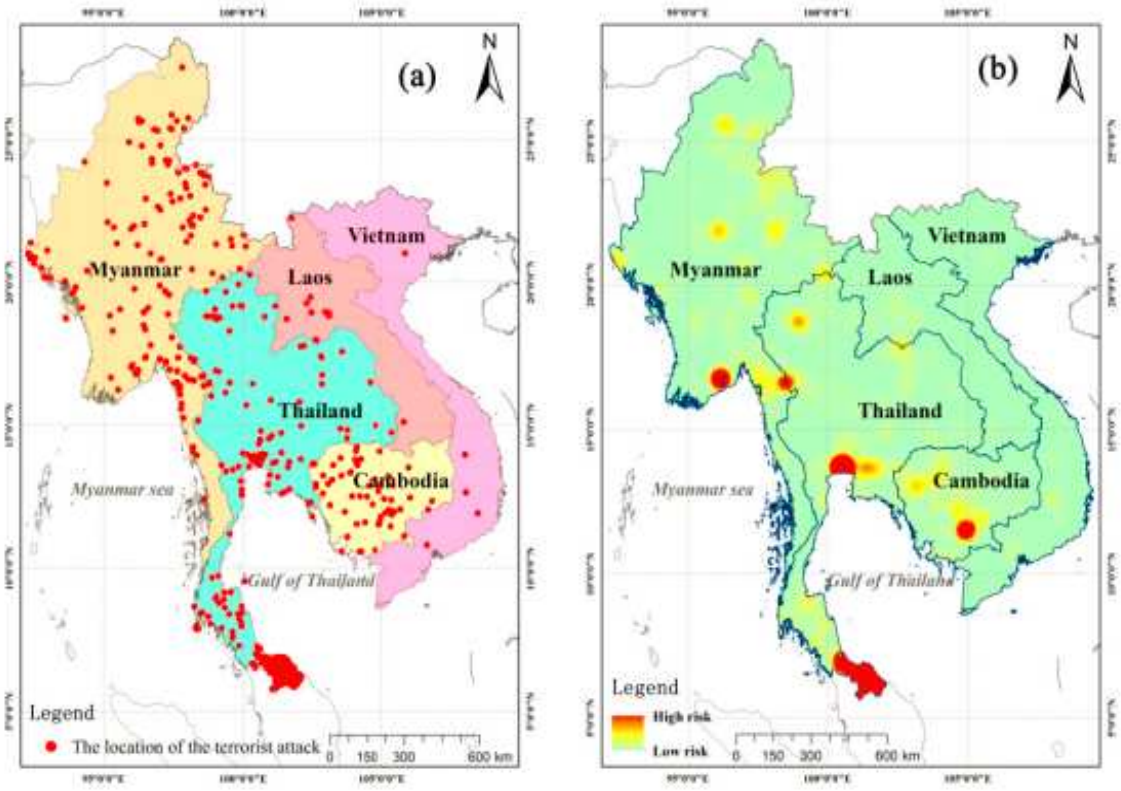

Figura 2.8: Nella figura sulla sinistra vengono mostrati in rosso tutti i luoghi dove si sono verificati numerosi attacchi, mentre nella figura a destra sono mostrate le zone ad alto rischio di attacchi.

Sono stati individuati in totale cinque hot spot distribuiti negli Stati di Cambodia, Myanmar e Tailandia, in particolare in questo caso si è notatata una particolarità, la maggior parte degli hotspot si trovano sulle frontiere.

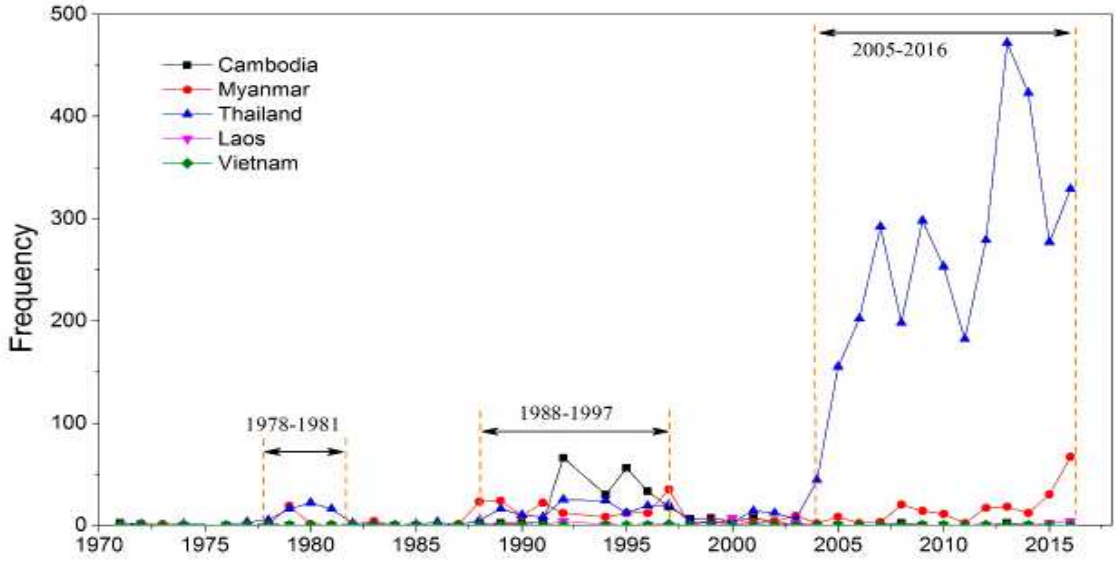

Figura 2.9: Nella figura viene rappresentata la frequenza con la quale si sono verificati attacchi terroristici in ogni Stato dal 1970 al 2016.

In conclusione i risultati ottenuti da questa ricerca si sono rivelati particolarmente efficienti, sopratutto grazie alla combinazione di tecniche di machine learning, come la Random Forest, con sistemi di geo-informazione per la simulazione della distribuzione del rischio di attacchi terroristici.
E' doveroso sottolineare che questo tipo di approccio non è legato soltanto al terrorismo, ma può essere utilizzato senza alcun problema laddove la variabile geo-spaziale assume un ruolo di principale importanza.

2.3.6 ALTER - Adversial Learning for counTerrorism

L'approccio analizzato prevede la simulazione di scenari terroristici mediante tecniche di computer vision e deep learning.
Lo studio è stato condotto da Palomba, Fabio et al.[12] e lo scopo di questo studio è quello di permettere alle forze dell'ordine di prevedere le conseguenze che si potrebbero verificare con il verificarsi di questi attacchi, individuando anticipatamente quali zone rafforzare e come rispondere in caso di attentato.
Il problema viene modellato mediante tecniche di computer vision nelle quali viene addestrata una Generative Adversial Network su immagini di attacchi terroristici. **Da cosa è costituiata una GAN?** La GAN (rete generativa avversaria) è composta da due reti neurali, le quali vengono addestrate in maniera competitiva seguendo le caratteristiche del gioco

minimax.

Nella prima rete neurale vi è una rete generativa il cui compito è quello di creare un'imitazione basandosi sulle foto iniziali. Questa rete crea, quindi, un'immagine completamente nuova che non è un duplicato di uno dei dati di partenza.

La seconda rete è il discriminatore, riceve in input sia i dati di base che le informazioni generate dalla rete generativa. Il discriminatore in questa fase ha come scopo quello di verificare l'autenticità dei dati ricevuti,occorre ricordare che questi dati possono essere autentici oppure falsi.

Un'immagine viene classificata come falsa in due contesti, sia quando si discosta in modo particolare dai dati di base e anche quando è troppo perfetta,nel secondo caso evita che si accettino immagini che non hanno un effetto naturale.

Questo approccio ci permette di considerare numerosi problemi poiché il trasferimento degli scenari non si limita ad "inserire" semplicemente delle persone da un'immagine ad un'altra ma occorre garantire sopratutto una consistenza dell'immagine, difatti l'evento deve essere un evento che si può verificare nella realtà. La rete in questo contesto non dovrebbe dare origine ad immagini di questo tipo.

Questo sviluppo ha avuto una crescita esponenziale negli ultimi anni e, fra le varie architetture esistenti, è stata selezionata la StyleGAN.

Questa rete neurale è stata sviluppata da NVIDIA e Karras, Tero et al.[13] ne descrive accuratamente ogni aspetto.

Per l'addestramento della StyleGAN è necessario un dataset di training e per generare questi dati occorre un ambiente di simulazione, in cui la maggior parte delle informazioni riguardanti gli attacchi terroristici sono sensibili e non sono quindi disponibili. Per ovviare a questo problema è stato creato un dataset.

Grazie al videogioco Grand Theft Auto V sono stati generati scenari in cui si simulava un attacco terroristico attraverso la registrazione del gameplay.

Nella figura successiva vengono mostrati alcune scenari catturati dal videogioco, nei quali vengono intraprese azioni criminali.

Figura 2.10: Esempi di scenari terroristici nel videogioco Grand Theft Auto V.

Il motivo per il quale è stato scelto GTA V è dato dal fatto che è un gioco open world con una grande accuratezza nei minimi dettagli e la rappresentazione del mondo virtuale è molto vicina a quella del mondo reale.
Ad esempio sono presenti sia componenti statiche come edifici, alberi e strade, sia componenti dinamiche come persone e macchine in movimento. Bisogna ammettere però che il numero di passanti e il numero di macchine in circolazione nelle strade è molto basso, mentre nel mondo reale è molto più elevato.
Come detto anche in precedenza non è possibile trovare all'interno del videogioco strade affollate con migliaia di persone, cosa che nel mondo reale, nelle città densamente abitate, si verifica. Questo aspetto è uno dei più importanti da considerare poiché uno dei fattori maggiormente considerati dai terroristi è il numero di persone che potrebbero essere coinvolte nell'attentato. Di seguito viene mostrato un confronto mediante un'immagine.

Figura 2.11: Sulla sinistra viene mostrato uno screenshot catturato dal videogioco GTA V; sulla destra è presente uno scenario di vita quotidiana nella città di New York.

Dopo aver effettuato il training della rete, il passo successivo è quello di eseguirne il reverse e mappare le caratteristiche dell'immagine nelle loro variabili all'interno dello spazio

latente. Attraverso un encoder ci assicuriamo che a partire dalle immagini create vi è una mappatura nella loro rappresentazione all'interno dello spazio.
In altri termini la StyleGAN possiede tre componenti principali:

- l'input delle rete;
- i parametri;
- l'output della rete.

Per ottimizzare la rete neurale si fissano i vari input e i vari output e si scelgono i valori dei parametri mediante la backpropagation dall'input all'output. Vi sono delle proposte di alcuni studiosi,in cui si propone di mantenere fissi gli output e i parametri e di mappare le immagini ottenute in output all'interno dello spazio latente.
Per fare ciò non basta altro che generare un vettore casuale in un certo intervallo, ad esempio N(0, 1), e inviarlo in input al generatore. In seguito si calcola la loss function e si cerca di minimizzarne il valore facendo un confronto fra l'immagine generata e l'immagine target. Grazie a questa comparazione si può sfruttare la backpropagation all'interno della rete per modificare il valore delle variabili latenti. Si segue questo passaggio fin quando non si minimizza la funzione di perdita.

Architettura della StyleGAN

Sono stati raggiunti importanti traguardi nell'ambito del neural style transfer negli ultimi anni poiché sono state sviluppate nuove tecniche e nuove architetture. Fra le architetture sviluppate va evidenziata l'adaptive instance normalization (AdaIN), un metodo di normalizzazione, che allinea la media e la varianza delle funzionalità del contenuto con quelle delle funzionalità di stile.
L'azienda Statunitense NVIDIA partendo dall'AdaIn e combinando le caratteristiche della precedente con le caratteristiche delle GANs ha dato origine ad una nuova architettura chiamata StyleGAN
Questo perchè si è mostrato che le tecniche utilizzate nello style transfer possono essere applicate non solo nel dominio in cui sono nate, cioè nella creazione di dipinti, ma anche in altri domini.
Da ciò Karras et al.[13] sono riusciti a creare volti finti indistinguibili dai volti reali semplice-

mente prendendo alcune caratteristiche, come occhi, naso e bocca da un insieme di immagini reali.

Figura 2.12: Volti di persone generati grazie alla Stylegan.

Il progresso dell'AdaIN è il motivo principale alla base dello sviluppo della rete neurale che si sta analizzando. Questa crescita progressiva ha permesso di migliorare la qualità della rete neurale. L'operazione di normalizzazione AdaIN ha permesso di controllare le funzionalità della rete neurale attraverso il codice nascosto nei differenti livelli della StyleGAN.
Questo è stato possibile in quanto l'architettura della rete presenta tre spazi latenti anziché uno solo.
I tre spazi latenti sono i seguenti: oltre al normale spazio latente Z è presente anche un nuovo spazio latente libero che viene definito spazio intermedio W; inoltre è presente anche lo spazio esteso W+, il quale si ottiene dalla media di tutti i differenti livelli di W.
In una GAN normale il vettore nascosto Z è dato in pasto solo all'input layer, mentre nella StyleGAN il vettore inziale Z è prima mappato in un vettore intermedio W grazie a una rete neurale feed-forward di otto livelli. Questo vettore W è in seguito fornito come input ad ogni livello convoluzionale nella StyleGAN.
Per comprendere meglio questo concetto da un punto di vista grafico viene mostrata una figura rappresentante le differenze fra l'architettura di una normale GAN e la StyleGAN.

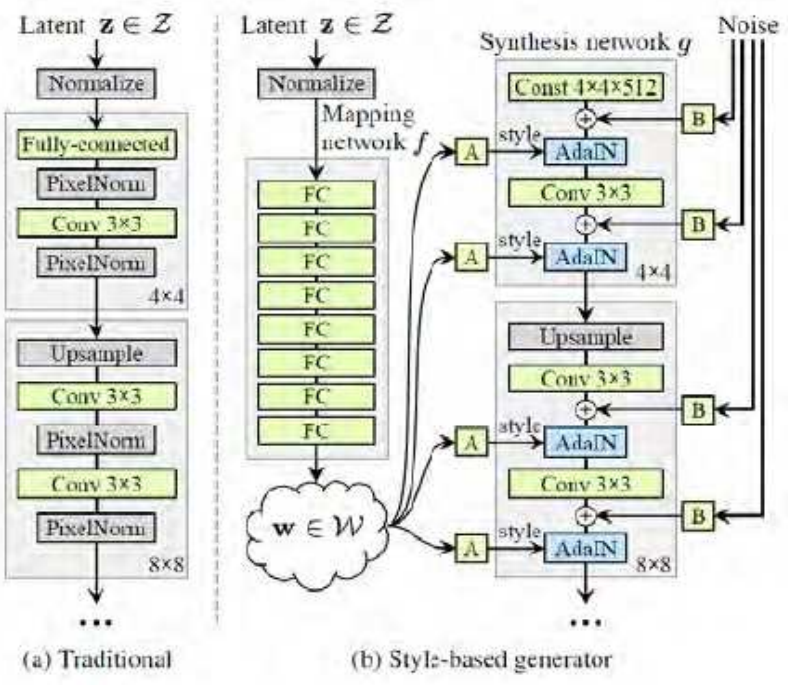

Figura 2.13: Differenze fra l'architettura di una normale GAN e la Stylegan.

L'operazione di normalizzazione è una delle caratteristiche fondamentali di questa architettura e a tal proposito Karras et al.[13] procedono definendo l'AdaIN come:

$$AdaIN(x_i, y) = y_{s,i}\frac{x_i - \mu(x_i)}{\sigma(x_i)} + y_{b,i} \tag{2.3.7}$$

Dove $y = (y_s, y_b)$ controlla i parametri della normalizzazione, la x_i rappresenta la mappa delle funzionalità che è normalizzata separatamente e la y rappresenta le variabili scalari.

Durante la definizione dell'architettura della rete neurale e durante l'operazione di normalizzazione, si può definire il processo di inversione, che consiste in un problema di minimizzazione rappresentato come:

$$z^* = min_z - E_x log[G(z)] \tag{2.3.8}$$

Dove z appartiene a Z e corrisponde allo spazio latente, x appartiene allo spazio R^{mxm}, ovvero l'immagine target e G(z) è il grafo computazionale della GAN.

Funzione obiettivo

Bisogna individuare un ulteriore parametro per procedere con la simulazione di scenari terroristici,la funzione obiettivo. **Qual'è lo scopo dello funzione obiettivo?** Lo scopo è quello

di minimizzare tale valore e rappresenta la qualità dell'immagine generata. L'idea adottata nello studio condotto da Palomba, Fabio et al.[12] è quella di utilizzare una combinazione lineare di più loss function.
Si possono distinguere due categorie di funzioni:

- Differenza assoluta;
- Differenza percettiva.

La prima si basa sul confronto dei pixel delle due immagini che si analizzano, invece, la seconda si basa sulla differenza percettiva delle immagini. Per la differenza assoluta si considera la Pixel-wise loss, la quale si calcola tramite il logaritmo del coseno iperbolico della predizione dell'errore. Si preferisce questa funzione alla funzione dell'errore quadratico medio perché meno sensibile ad eventuali outlier.
Per la differenza percettiva si considerano le seguenti funzioni: VGG loss, LPSIS loss e MS-SIM loss. Senza entrare nel dettaglio di ciascuna di esse, si riporta solamente la combinazione delle quattro funzioni obiettivo:

$$\begin{aligned} w^* = min_w \lambda_{Pixel-wise} * \frac{1}{N} * log(cosh(G(w) - I) \\ + \lambda_{VGG} * L_{VGG}(G(w), I) \\ + \lambda_{LPSIS} * L_{LPSIS}(G(w), I) \\ + \lambda_{MS-SIM} * L_{MS-SIM}(G(w), I) \end{aligned} \tag{2.3.9}$$

Affinché la Stylegan utilizzata nella ricerca possa convergere, la funzione obiettivo del generatore deve assumere un valore prossimo a -0.5, mentre la funzione obiettivo del discriminatore deve valere circa 0.5. Nella fase di training del modello si è notato che la rete neurale ha avuto difficoltà nel convergere ai valori sopracitati.
In generale, l'addestramento della rete con immagini ad una risoluzione più bassa (128px) ha mostrato una progressione migliore rispetto alle immagini con una risoluzione più elevata. Entrambi i casi sembravano avvicinarsi ai valori indicati, ma ad un certo punto la curva subiva un'inversione e se ne allontanava nuovamente, generando così scarsi risultati.
Riconfigurando molte volte i parametri della rete ci si è resi conto che le prestazioni continuavano a non essere delle migliori e grazie ad un'attenta analisi si è notato che le immagini riprese dall'alto degradavano le performance della rete e per questo motivo sono state rimosse dal dataset.

Nella figura sotto vengono mostrate alcune delle immagini che hanno provocato particolari problemi nell'efficacia del modello di simulazione.

Figura 2.14: Esempi di immagini scattate dall'alto.

A seguito delle modifiche descritte in precedenze in cui i risultati non hanno subito miglioramento e per questo motivo è stata modificata la banca dati utilizzando le immagini prese dal dataset Unreal, il quale trascura una notevole quantità di dettagli. Da questa modifica ci si aspetta che le performance miglioreranno, ma non si sarà in grado di codificare immagini prese dal mondo reale, ad esempio nella seguente immagine si può notare un campione estratto dallo studio. Qui è evidente come le immagini siano molto più elementari e completamente differenti da quelle del dataset di partenza costruito artificialmente mediante il videogioco GTA V.

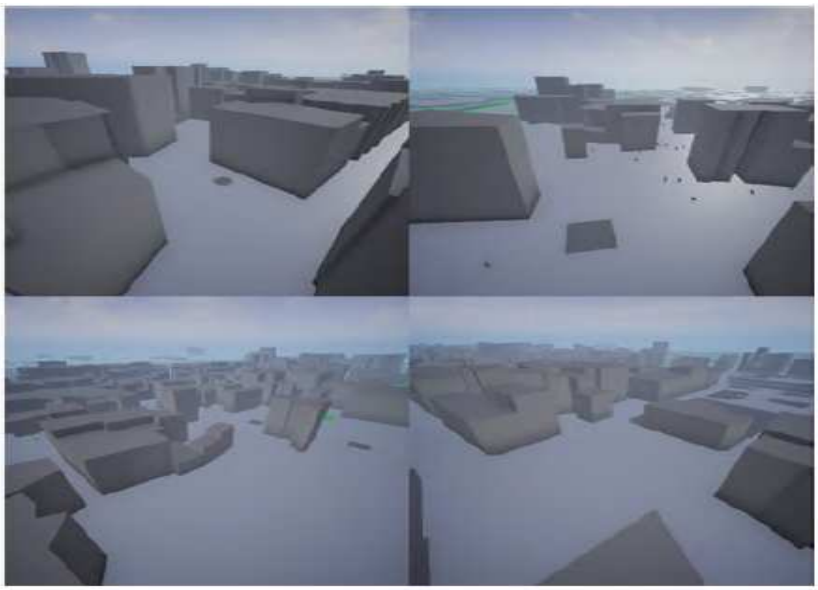

Figura 2.15: Esempi di immagini contenenti solo la struttura degli edifici.

In conclusione, la combinazione lineare delle loss function non ha portato ad un vantaggio, bensì ad uno svantaggio.
Solo una funzione converge ed è la Pixel-wise, appartenente alla categoria differenza assoluta. Ciò si è verificato poiché la rete non è in grado di codificare correttamente tutte le caratteristiche che costituiscono l'immagine.

L'idea alla base di questa tecnica risulta essere particolarmente rivoluzionaria, è davvero molto utile ai fini della sicurezza dei cittadini del mondo. In futuro con l'avvento di nuove tecnologie tale tecnica potrà essere più facilmente applicata.

2.3.7 Temporal Meta-Graph

Quest'ultima tecnica analizzata è quella proposta da Campedelli et al.[14] in questa tecnica si propone l'uso dei meta-grafi temporali e del deep learning per prevenire i futuri target su attacchi terrorististici.
Il terrorismo in se porta ad avere elevati livelli di incertezza e imprevedibilità, la ricerca nell'ambito dell'intelligenza artificiale può aiutare a fornire soluzioni utili per contrastare questo fenomeno. In questa tecnica si sfruttano così i seguenti elementi: il potere dei dati, i quali oggigiorno sono sempre più preziosi, i potenti modelli computazionali e le teorie relative al comportamento dei terroristi.
Questo studio si concentra sull'unione fra l'intelligenza artificiale e la prevenzione di attacchi terroristici proponendo un nuovo framework basato sui meta-grafi, sulle serie storiche e sugli algoritmi di previsione utilizzati nel campo del machine learning e nel campo del deep learning.
I dati sui quali è stato condotto lo studio sono stati prelevati dal Global Terrorism Database, già utilizzato nello studio condotto da Kao et al.[11], ma in questo caso ci si è focalizzati sugli attacchi avvenuti in Afghanistan e Iraq tra il 2001 e il 2018.
L'evento terroristico presenta tre dimensioni:

- armi utilizzate;
- tattiche schierate;
- target individuati.

Una volta che i meta-grafi sono creati, si derivano le serie storiche mappando la centrality di ogni nodo nella dimensione corrispondente. In seguito le serie vengono utilizzate per individuare pattern ricorrenti per prevenire i prossimi target che potrebbero essere presi di mira.

Vengono proposte le seguenti teorie per descrivere e spiegare le azioni dei terroristi. Queste ultime è possibile dividerle in tre macrocategorie:

- psicologiche;
- organizzative;
- strategiche.

Le teorie psicologiche trovano le singole cause che hanno portato i criminali a prendere parte nelle attività terroristiche. Le teorie organizzative si focalizzano sull'organizzazione interna e sul simbolismo formale di ciascun gruppo e ne cerca di comprenderne il comportamento. Infine, le teorie strategiche si focalizzano sul processo decisionale dei terroristi e sulla base di ciò originano lo studio dei conflitti.

La letteratura mostra come gli attacchi terroristici non avvengono in maniera casuale, ma vi sono dei cluster temporali dai quali si possono inferire informazioni sui prossimi attacchi, analizzando i pattern ricorrenti. Per catturare le connessioni fra gli eventi e le loro caratteristiche non è sufficiente suddividere il problema in serie storiche. Per questo motivo si è introdotto un nuovo framework che sfrutta i vantaggi delle serie storiche derivanti dai grafi.
Per prima cosa, per ogni unità di tempo vengono generati i grafi pesati, i quali rappresentano le connessioni esistenti nelle tre dimensioni di dati considerate (tattiche, armi e obiettivi). Una volta che il seguente step è stato completato, si calcola, per ogni dimensione e per ogni unità di tempo, il grado normalizzato della centrality di ogni caratteristica.
L'attività di pre-processing dei dati avviene a partire dal dataset D_{Axz} che contiene |A| attacchi terroristici e |z| variabili associate ad ogni attacco, corrisponde esattamente al formato originale del Global Terrorism Database.
Arrivati a questo punto, si filtrano i dati prendendo in considerazione solamente gli attacchi che si sono verificati in Afghanistan e Iraq fra il 2001 e il 2018. Si ottengono così i due dataset separati: D_{txz}^{AFG} e D_{txz}^{IRA}.
I due nuovi dataset sono costituiti da |t| osservazioni e |z|caratteristiche. Il valore che

possono assumere tali caratteristiche non è altro che il numero di volte che quella caratteristica era presente negli attacchi eseguiti in quell'unità di tempo, come ad esempio il singolo giorno.

Come detto fin'ora, le dimensioni utilizzate in questo studio sono tre quindi è possibile individuare tre insiemi: l'insieme delle caratteristiche tattiche (X), l'insieme delle caratteristiche delle armi (W) e l'insieme delle caratteristiche degli obiettivi (Y). Se si indica con C il paese di riferimento, anziché utilizzare AFG oppure IRA, il dataset lo si può scrivere come $D^C = \{D_X, D_W, D_Y\}$.

Per ogni $\{D_X, D_W, D_Y\}$ si crea una finestra temporale U tale che $u = 2t$. In altre parole, per ogni dimensione, si collassano i dati in unità di tempo di due giorni e ciascun dato è pari alla somma del numero di ogni caratteristica nei due giorni.

Il motivo dietro alla creazione di unità di tempo basate su due giorni è duplice. In primis, fare affidamento su serie storiche di un singolo giorno aumenta il rischio di avere serie troppo scarse, con grafi molto piccoli che non produrrebbero alcuna informazione.

D'altro canto, nella realtà le risorse richiedono tempo per elaborarle e avere un sistema di previsione che opera di giorno in giorno produrrebbe informazioni che sarebbe difficile trasformare in decisioni concrete e piene di significato. Per questo motivo un'architettura con unità di tempo due giorni risulta essere un buon compromesso.

Nella seguente figura viene schematizzato graficamente la struttura che si ottiene a seguito dell'operazione di processing dei dati.

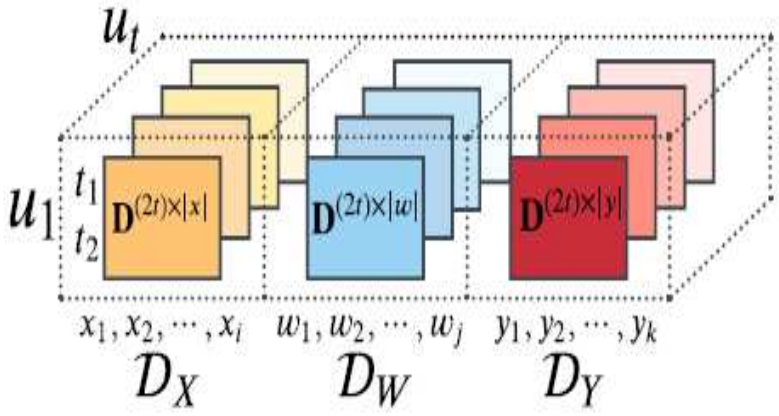

Figura 2.16: Rappresentazione grafica del risultato ottenuto dall'operazione di processing dei dati.

N Nel seguente grafico si mostra un esempio, sempre grafico, dei meta-grafi temporali che vengono creati. I vari u_i rappresentano le differenti unità di tempo e poi in giallo sono presentati i grafi relativi alla prima dimensione, le tattiche; in blu sono rappresentati i grafi

relativi alla seconda dimensione, le armi; infine, in rosso sono rappresentati i grafi dell'ultima dimensione, gli obiettivi.

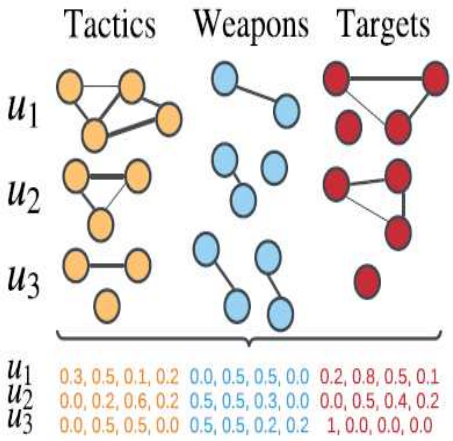

Figura 2.17: Esempio grafico della trasformazione dei meta-grafi temporali.

Per mostrare come evolve il modello per ogni unità di tempo, si riportano di seguito le immagini relative all'evoluzione della centralità della terza dimensione.

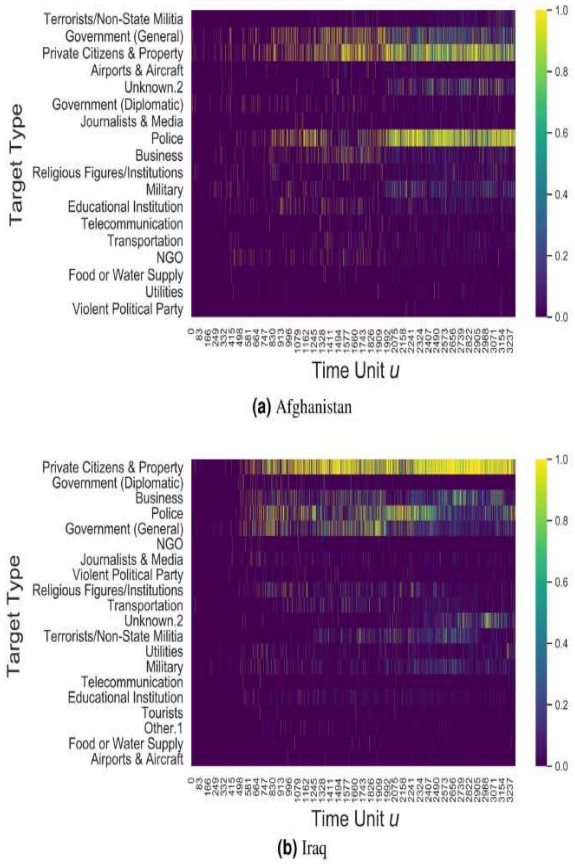

Figura 2.18: Evoluzione temporale della centralità della dimensione relativa agli obiettivi per i casi dell'Afghanistan e per quelli dell'Iraq.

2.4 Confronto fra le tecniche analizzate

In questa sezione [6] vengono confrontate le tecniche analizzate in precedenza in modo di riuscire ad individuare eventuali vantaggi e svantaggi.
Gli approcci considerati sono:

- Probabilistic Risk Analysis;
- Agent-Based Simulation;
- GIS e Random Forest;
- Computer Vision e Deep Learning;
- Temporal Meta-Graph.

Ognuno degli approcci considerati presenta caratteristiche differenti, ad esempio l'approccio proposto da Kao et al.[11] e quello proposto da Campedelli et al.[14] sono legati strettamente ad alcune aree geografiche.
La tecnica che utilizza la Random Forest è stata modellata su una specifica zona, ovvero la penisola dell'Indocina, così come nello studio che sfrutta i meta-grafi temporali i luoghi analizzati sono l'Afghanistan e l'Iraq.
Il problema relativo alla prevenzione di attacchi terroristici dovrebbe slegarsi dal context-based; in altri termini, l'approccio adottato non deve essere limitato ad un solo contesto, ma dovrebbe essere estendibile a più contesti.
Tra le tecniche analizzate risalta in modo particolare quella relativa alla StyleGAN in quanto, nel caso in cui si riescano a superare le difficoltà riscontrate, risulterebbe essere particolarmente efficace. Basti pensare che nel momento in cui si sviluppa tale framework, le forze dell'ordine e le agenzie governative non devono fare altro che mostrare un immagine, che può essere data da innumerevoli fonti. Una volta che l'immagine viene elaborata si ha in output una foto che mostra eventuali pericoli e punti deboli poiché aggiunge elementi allo scenario di partenza, come criminali, agenti di polizia e passanti.
A questo punto è evidente come uno strumento di questo tipo può risultare utile, visto che può essere utilizzato in qualsiasi Stato e in qualsiasi città, sia in una grande metropoli che in una piccola cittadina. Si può sostenere che, insieme al progresso dell'intelligenza artificiale vi possa essere un progresso con le Generative Adversial Network, andando ad implementare un software che permetta un'analisi accurata di questo tipo.

Considerando la prima tecnica analizzata bisogna evidenziare che è stata utilizzata da alcuni governi per alcuni decenni, ma è completamente diversa da quella proposta da Palomba, Fabio et al.[12] in quanto lo studio sviluppato da Ezell et al.[7] si focalizza solamente su un'analisi del rischio di tipo probabilistico.
Una volta sviluppati gli alberi di decisione si calcolano le probabilità che si verifichi uno scenario piuttosto che un altro. Nonostante questo approccio possa inizialmente apparire banale da implementare, vi sono delle difficoltà nel codificare le informazioni ottenute dall'Intelligence Community in probabilità. Nel caso in cui si calcola erroneamente questo valore i risultati che ne conseguono non risultano attendibili.
La tecnica che fa riferimento al sistema informativo geografico combinata con algoritmi di machine learning come la Random Forest si è rivelata particolarmente utile per individuare i cosiddetti hotspot, luoghi nei quali vi è un elevato rischio di attacco terroristico. La caratteristica peculiare di questo studio è stato il sistema Geo-Informativo, il quale si è adattato perfettamente nella simulazione di attentati.
Nonostante non siano state individuate nello specifico le vulnerabilità degli hot spot, le agenzie governative sono riuscite comunque a comprendere che la zona più pericolosa è Bangkok e quindi è necessario migliorare la sicurezza in questo luogo.
Un'altra tecnica innovativa è quella proposta da Bosse et al.[15].La tecnica si focalizza sull'obiettivo dei guardiani, i quali scelgono una strategia fra alcune a loro disposizione per mantenere il tasso di criminalità il più basso possibile. I risultati migliori di questa tecnica si ottengono con la strategia secondo cui i guardiani si spostano verso nuovi luoghi focalizzandosi sul numero di passanti che ci si aspetta di trovare nel periodo futuro. Bisogna ammettere che anche le altre strategie elaborate da Bosse hanno prodotto buoni risultati.
Nonostante quest'analisi sia particolarmente positiva, bisogna ricordare che i risultati non vanno generalizzati ne banalizzati poiché sono stati raggiunti in un ambiente di simulazione nel quale sono stati semplificati molti vincoli, il livello di complessità di questi scenari infatti risulta essere minore rispetto alla complessità degli scenari del mondo reale.
Da un punto di vista pratico non è facile calcolare l'esatto valore dell'attractiveness di un luogo oppure il numero di assalti che si possono verificare. Tuttavia i risultati di queste simulazioni sono stati utili per le forze dell'ordine, in quanto essendoci molteplici strategie si può scegliere quella più congeniale alla situazione in cui ci si trova.
In conclusione, le tecniche che abbiamo preso in esame finora sono tutte molto efficaci, tuttavia quella che riteniamo più promettente è quella relativa alla StyleGAN.

Questa tecnica è stata sviluppata per sfruttare al meglio le qualità di una rete neurale generativa in una determinata immagine in modo da evidenziare eventuali scenari di attacco. Tale metodo ha un grande potenziale, poiché è in grado di generare immagini più accurate ed è più versatile rispetto agli altri sistemi esaminati.
Nella seguente tabella vengono mostrate tutte le tecniche e per ciascuna di esse vengono mostrate in modo schematico vantaggi e svantaggi.

Tabella 2.1: Tabella che indica pro e contro di ciascuna tecnica analizzata.

Tecnica analizzata	Pro	Contro
PRA - Probabilistic Risk Analysis	Semplicità d'uso	Difficoltà nel codificare le informazioni in probabilità
Agent-Based Simulation	Differenti strategie da adottare	Molti dettagli della realtà vengono trascurati
GIS e Random Forest	Grande efficacia nell'individuare gli hot spot	Tecnica context-based limitata solo alla penisola dell'Indocina
ALTER – Adversial Learning for counTERrorism	Forte efficacia e facilità d'uso per le forze dell'ordine	Elevata complessità computazionale richiesta
Temporal Meta-Graphs	Grande adattamento al modello dinamico che evolve nel tempo	Tecnica context-based limitata solo all'Afghanistan e all'Iraq

CAPITOLO 3

Metodologie

3.1 Data Understanding

I dataset utilizzati per addestrare il modello di machine learning, sono il **Global Terrorism Database** definito in seguito anche come GTD e il **Word Happines Report**, la manipolazione dei dataset è avvenuta mediante pandas una libreria di python. Questi due dataset successivamente sono stati uniti in unico dataset ma prima di ciò ho diviso il dataset del Global Terrorism Database in tre dataset, ogni dataset infatti contiene gli attacchi terroristici effettuati nel lasso di tempo che va dal 1 Gennaio al 31 Dicembre, è stata effettuata questa scelta per far si che ogni dataset in questione contenesse solo le informazioni di quel determinato anno, in modo da ottenere per gli anni 2015,2016 e 2017 tre dataset separati ottenendo quindi il GTD che conteneva solo le informazioni del 2015, il GTD che conteneva solo le informazioni del 2016 e il GTD che conteneva le informazioni del 2017. Mentre i tre dataset del World Happines Report venivano già divisi per anno il Global Terrorism Database conteneva attacchi svolti dal 1970 fino al 2017. Successivamente realizzando le seguenti operazioni è stato ottenuto il dataset finale: Il primo step si è concluso, dopo aver confrontato le colonne dei due dataset e dopo aver riscontrato di avere delle colonne in comune.
Gli elelmenti in comune trovati nei due dataset sono:

- La regione
- La nazione

Dopo aver trovato gli elementi in comune sono state eliminate dal dataset del Word Happiness Report le colonne "Region_y" e Standard Error. Viene eliminata la colonna "Region_y" in quanto questa informazione è irrilevante, infatti è già presente un ulteriore colonna chiamata "Region_x", la colonna Standard Error invece viene eliminata in quanto delineava una chiara incongruenza con i report del 2016 e con i report del 2017 che non possedevano tale informazione.
Viene eseguita la stessa procedura anche per il dataset del World Happiness Report del 2016, l'obiettivo è quello di creare un dataset omogeneo e con le stesse colonne del World Happiness Report dell'anno 2015, infatti, durante questa fase verrà eliminata nuovamente la colonna "Region_y, Lower Confidence Interval, Upper Confidence Interval dal dataset World Happiness.
Viene eseguita la stessa procedura per l'anno 2017, durante questa fase vegono eliminate le righe Wisker.high e Whisker.low dal dataset World Happiness Report dell'anno 2017. In questa fase non vengono effettuate delle operazioni sui tre dataset del Global Terrorism Database in quanto le colonne presenti in questi tre dataset sono conformi, viene effettuata solo una riduzione generale del dataset infatti vengono prese in considerazione solo le seguenti colonne, rispetto alle 135 colonne totali. Invece per i dataset del World Happiness Report più

Tabella 3.1: La tabella in figura mostra le caratteristiche del dataset

Year	Month	Country
city	longitude	AttackType
latitude	Wounded	Region
Target	Summary	Group
Target-type	Weapon_type	Killed

in particolare per il dataset del 2016 e il dataset del 2017 viene effettuata un operazione di rename delle colonne. Questa operazione viene effettuata con lo scopo di rendere le colonne dei tre dataset uniformi, in quanto i tre dataset seppur in nomi e anni diversi contengono la stessa informazione.
Infatti ad esempio la colonna Happiness Score del dataset World Happiness Report del 2017 è denominata "Happiness.Score" mentre nello stesso dataset dell'anno 2015 questa colonna è denominata "Happiness Score". L'operazione di rename ha permesso una standardizzazione sul nome delle colonne, racchiudendo così le informazioni sui tre anni negli stessi anni.

Tabella 3.2: La tabella in figura mostra le caratteristiche del dataset World Happiness Report

Region	Happiness Rank	Happiness Score
Standard Error	Economy (GDP per Capita)	Family
Health (Life Expectancy)	Freedom	Trust (Government Corruption)
Generosity	Dystopia Residual	

Successivamente è stata effettuata un operazione di merge in particolare è stata effettuata un inner join sui due dataset, questa operazione ha permesso la creazione del primo dataset, che conteneva sia informazioni sugli attacchi terroristici e sia i report mondiali della felicità nell'anno 2015, dopodichè la stessa operazione è stata effettuata sui dataset del 2016 e del 2017. Sono stati ottenuti dalla fase precedente tre dataset, ognuno dei quali conteneva le informazioni ottenute in quel determinato anno sia sugli attacchi terroristici e sia sui report mondiali della felicità(World Happiness Report).
Il dataset in questa fase è quasi pronto infatti, dalle fasi precedenti si sono ottenuti i tre dataset differenti che vengono sottoposti ad ulteriori confronti infatti, utillizzando il metodo setdiff1d contenuto in numpy si va a verificare che il dataset dell'anno 2015 non abbia differenze con il dataset del 2016 e successivamente che il dataset del 2015 non abbia differenze con il dataset dell'anno 2017.
Effettuando questa operazione per ogni anno inserendo le possibili configurazioni per i diversi anni, si otterrà un riscontro sulle differenze possibili dei vari dataset.

Year	Month	Country
city	latitude	longitude
AttackType	Summary	MotiveRegion
Killed	Wounded	Target
Group	Target-type	Weapon_type
Happiness Rank	Happiness	Score
Family	Health (Life Expectancy)	Freedom
Generosity	Dystopia Residual	Region
Trust (Government Corruption)	Economy (GDP per Capita)	happines

Tabella 3.3: La tabella in figura mostra le caratteristiche del dataset finale creato dall'unione del Global Terrorism Database e dal World Happiness Report

Il lavoro svolto è visualizzabile nella seguente **repository**.

3.2 Data cleaning

Nella prima fase di ingegnerizzazione dei dati ci siamo soffermati sul data cleaning, ovvero siamo andati ad analizzare i dati valutando se ci fossero valori nulli o non validi.
Da un analisi preliminare dei dati a nostra disposizione è risultato che:

```
merge.isnull().any()
```

```
Year                                False
Month                               False
Day                                 False
Country                             False
Region                              False
city                                False
latitude                             True
longitude                            True
AttackType                          False
Killed                               True
Wounded                              True
Target                              False
Summary                             False
Group                               False
Target_type                         False
Weapon_type                         False
Motive                               True
Happiness Rank                      False
Happiness Score                     False
Economy (GDP per Capita)            False
Family                              False
Health (Life Expectancy)            False
Freedom                             False
Trust (Government Corruption)       False
Generosity                          False
Dystopia Residual                   False
dtype: bool
```

Figura 3.1: Tabella che mostra con true i valori nulli o invalidi

L'immagine soprastante presenta dati nulli o invalidi tra quelli presenti, per cui sono necessarie tecniche di data cleaning. In particolare è stata eliminata la colonna Motive e rimosso le righr nulle e le righe N.A nei campi Killed, Wounded, latitude e longitude.

3.3 Feature scaling

Nella seconda fase ci siamo focalizzati sulla feature scaling ovvero l'insieme di tecniche che consentono di normalizzare o scalare l'insieme di valori di una caratteristica.
Abbiamo utilizzato un metodo della libreria "*sklearn*" che ci ha permesso di scalare i valori delle variabili presi in considerazione. Sono state analizzate le prestazioni dell'agente in seguito alla tecnica di normalizzazione usata. Sono state prese in considerazione, la Z-Score Normalization, la MinMax Normalization e la Robust Scaling.

- la Z-Score Normalization: $x' = \frac{(x-\mu)}{\sigma}$ normalizza i valori in modo da avere la somma delle medie pari a 0 e la deviazione standard a 1.
- la MinMax Normalization: normalizza i valori dei dati, in valori compresi fra a e b
- la Robust Scaling: normalizzazione che rimuove la mediana e scala i dati in base al range interquartile.

3.4 Feature selection

Nella terza fase ci siamo focalizzati sulla feature selection con l'obiettivo di definire delle caratteristiche, anche chiamate feature, metriche, o variabili indipendenti che possano caratterizzare gli aspetti principali del nostro problema in esame e, quindi, avere una buona potenza predittiva.

Abbiamo utilizzato un metodo della libreria "*matplotlib*", che ci ha permesso di visualizzare le dipendenze tra le diverse variabili.

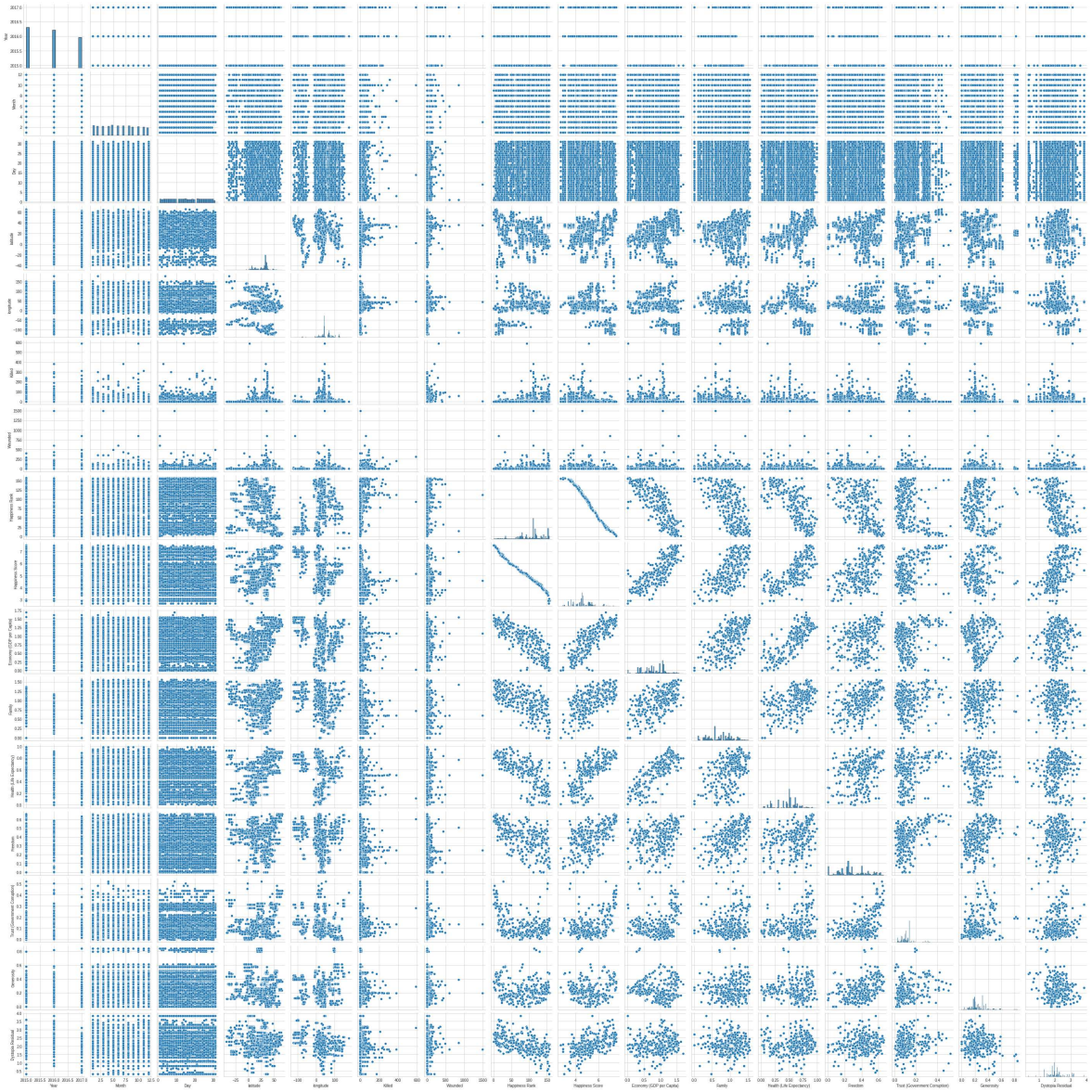

Figura 3.2: Plot dei dati

3.5 Data balancing

Nella quarta fase ci siamo focalizzati sul Data balancing, ovvero un insieme di tecniche per convertire un dataset sbilanciato in un dataset bilanciato.
Nel nostro caso,non abbiamo avuto la necessità di verificare il bilanciamento delle classi.

3.6 Model evaluation

In seguito alla definizione delle tecniche di ingegnerizzazione dei dati dell'agente intelligente, è necessario stabilire le metriche e le tecniche di validazione delle prestazioni dello stesso. Occorre suddividere l'insieme dei dati fin'ora analizzato in due insiemi: il *training set*, composto dalle istanze di dati che saranno utilizzate per l'addestramento, e il *test set*, composto dalle istanze di dati per cui l'agente dovrà predire il valore della variabile dipendente. Abbiamo preso in considerazione diverse tecniche per effettuare questa suddivisione: K-Fold validation, Stratified K-fold validation, Repeated K-fold validation e Repeated Stratified K-fold validation. In particolare, le tecniche Stratified K-fold e Repeated Stratified sono state scartate in quanto non risultano adatte ad essere applicate su dati continui e a dataset con più variabili indipendenti. Per tutte è stato necessario definire il valore di K, ovvero il numero di insiemi, mentre per le tecniche di tipo "Repeated" è stato stabilito anche il numero di ripetizioni da effettuare. Le metriche che sono state impiegate per valutare la bontà delle previsioni effettuate sono state:

- MAE (Mean Absolute Error) = $\frac{\sum_{i=1}^{n} |y_i - x_i|}{n}$
- MSE (Mean Squared Error) = $\frac{\sum_{i=1}^{n} (y_i - x_i)^2}{n}$
- RMSE (Root Mean Squared Error) = $\sqrt{\frac{\sum_{i=1}^{n} (y_i - x_i)^2}{n}}$

3.7 Regressione

3.7.1 Regressione lineare

Una volta definito il processo di feature engineering e scelte le tecniche di valutazione, è stato possibile definire un modello di regressione lineare tramite la libreria "*sklearn.linear_model*", in particolare si è utilizzato il metodo "fit" per addestrare il modello sull'insieme dei dati di training e in seguito "predict" sull'insieme dei dati di test per predirne il valore della variabile dipendente basandoci sulle feature dell'insieme di dati di training. In particolare, sono stati creati diversi modelli di regressione: uno basato sul dataset normalizzato tramite Z-Score normalization, uno tramite MinMax normalization e un terzo basato su Robust scaling.
I risultati in termini di MAE, MSE e RMSE sono stati salvati in un oggetto da noi creato (Metrics1), al fine di confrontare le prestazioni delle diverse configurazioni dei modelli.
I modelli così creati sono stati valutati tramite l'utilizzo della tecnica del K-fold validation e del Repeated K-fold validation. Per la scelta del k migliore abbiamo utilizzato la formula: k= (len(df)/(len(df)*0.3)), dove len(df) indica il numero di campioni del nostro dataset. Il K così ottenuto è uguale a 3.3333, ma per eccesso è stato approssimato 4.
La predizione è avvenuta sulla variabile dipendete Happiness Score.
I risultati generati dai dati normalizzati con Z-score e con MinMax sono stati così confrontati:

Tabella 3.4: Risultati ottenuti applicando Regressione Lineare

Test	Regressor	Alg	Scaler	MAE	MSE	RMSE
1	Linear	KF	ZScore	0.08205148396585915	0.01323574779148373	0.11503408759723158
2	Linear	RKF	ZScore	0.08205237283510569	0.013235081182110203	0.11503572386089692
3	Linear	KF	MinMax	0.08205148396585915	0.013235747791483739	0.11503408759723162
4	Linear	RKF	MinMax	0.08205237283510566	0.013235081182110208	0.11503572386089692
5	Linear	KF	Robust	0.08205148396585919	0.013235747791483737	0.1150340875972316
6	Linear	RKF	Robust	0.08205237283510569	0.013235081182110203	0.11503572386089692

Decision Tree Regression

In seguito alla realizzazione del modello utilizzante un semplice algoritmo di Regressione Lineare, le sue prestazioni sono state confrontate con altri modelli che fanno utilizzo di diversi algoritmi di regressione.
Il primo algoritmo con cui è stato confrontato è stato il Decision Tree, che non si limita a predire dati con vincoli di linearità, ma permette anche di predire valori che si presentano sotto forma di curve.
Riportiamo di seguito i risultati ottenuti:

Tabella 3.5: Risultati ottenuti applicando Decision Tree Regression

Test	Regressor	Alg	Scaler	MAE	MSE	RMSE
7	DecisionTree	KF	ZScore	0.00012780653343933123	1.261403734581765e-05	0.0035037249696091444
8	DecisionTree	RKF	ZScore	0.00013610549045983824	1.5253530334100399e-05	0.0037745726461181433
9	DecisionTree	KF	MinMax	0.00012999095626104085	1.2910376370464573e-05	0.003565238553600899
10	DecisionTree	RKF	MinMax	0.00013606754053187 61	1.4966228408388132e-05	0.0037665921963568605
11	DecisionTree	KF	Robust	0.00013598491626644 91	1.4649733038954635e-05	0.0037935322973819
12	DecisionTree	RKF	Robust	0.00013569671065012 92	1.4639378762179356e-05	0.003707989900299612

Random Forest Regression

Il confronto del modello è continuato andando a testare le prestazioni utilizzando l'algoritmo Random Forest Regression. Questo è un algoritmo di tipo "*ensemble*", cioè esegue n volte (nel nostro caso, $n = 100$) l'algoritmo Decision Tree Regression, ogni albero decisionale è creato in modo autonomo ed effettua le sue personali predizioni.
In seguito, le predizioni finali sono poi ottenute tramite una media di quelle effettuate dai singoli alberi.
Di seguito riportiamo i risultati:

Tabella 3.6: Risultati ottenuti applicando Random Forest

Test	Regressor	Alg	Scaler	MAE	MSE	RMSE
13	RandomForest	KF	ZScore	0.0001903103851035871	1.2009825842104264e-05	0.0034285012606982577
14	RandomForest	RKF	ZScore	0.0034285012606982577	1.542488274627364e-05	0.003834617404572745
15	RandomForest	KF	MinMax	0.00018637163836357742	1.1869675299273282e-05	0.0034127850713290956
16	RandomForest	RKF	MinMax	0.00022078473462670739	1.5221333828475278e-05	0.0038127083485660685
17	RandomForest	KF	Robust	0.00018471134031327067	1.1950795830677379e-05	0.00342888779023369
18	RandomForest	RKF	Robust	0.00022434792552847012	1.578957308446205e-05	0.0038796708843994955

Support Vector Regression

A scopo di analisi, il modello è stato testato anche utilizzando un algoritmo diverso rispetto ai precedenti, ovvero il Support Vector Regression (SVR). Questo si basa sul più noto algoritmo di classificazione SVM, il quale costruisce un *iperpiano* che utilizza per la predizione di risultati. Come per l'algoritmo Random Forest, anche per questo abbiamo dovuto modificare i parametri della Repeated K-Fold validation.
I risultati ottenuti sono i seguenti:

Tabella 3.7: Risultati ottenuti applicando SVR

Test	Regressor	Alg	Scaler	MAE	MSE	RMSE
19	SVR	KF	ZScore	0.06275080541906397	0.005159960821417611	0.07181018398846659
20	SVR	RKF	ZScore	0.06293474721295676	0.005211201326079287	0.07216244029391325
21	SVR	KF	MinMax	0.06536044515724661	0.00555432863934081	0.07452674066141879
22	SVR	RKF	MinMax	0.06647026121256205	0.005704117159038258	0.0755167001626653
23	SVR	KF	Robust	0.06460363104758571	0.005298088024527838	0.07274991898165015
24	SVR	RKF	Robust	0.06431199122737533	0.005297182142850114	0.07274211799074429

Lasso Regression

In seguito abbiamo analizzato l'algoritmo Lasso Regression, dove Lasso sta per "Least Absolute Selection Shrinkage Operator". Questo algoritmo infatti opera trovando e applicando un vincolo agli attributi del modello che porta i coefficienti di regressioni per alcune variabile a diminuire verso lo zero. Le variabili con coefficiente di regressione pari a zero sono poi escluse dal modello. Questo algoritmo aiuta quindi a determinare quali dei predittori sono i più importanti. Per utilizzare questa tecnica è necessario definire un parametro "*alpha*", con valore numerico compreso tra 0 e ∞, dove per $alpha = 0$ la Lasso Regression si comporta come Linear Regression. La scelta di questo parametro è stata affidata alla funzione di Python "linear_model.Lasso()". Si può notare come i risultati ottenuti utilizzando questa configurazione non siano soddisfacenti:

Tabella 3.8: Risultati ottenuti applicando Lasso Regression

Test	Regressor	Alg	Scaler	MAE	MSE	RMSE
25	Lasso	KF	ZScore	0.6350066267218144	0.7312313627385884	0.8551082391820571
26	Lasso	RKF	ZScore	0.6350359988486943	0.7312752173360947	0.8551258882427469
27	Lasso	KF	MinMax	0.6350066267218144	0.7312313627385884	0.8551082391820571
28	Lasso	RKF	MinMax	0.6350359988486943	0.7312752173360947	0.8551258882427469
29	Lasso	KF	Robust	0.6350066267218144	0.7312313627385884	0.8551082391820571
30	Lasso	RKF	Robust	0.6350359988486943	0.7312752173360947	0.8551258882427469

Ridge Regression

In fine è stato analizzato l'algoritmo di Ridge Regression anche conosciuto come Tikhonov regularization. E' una versione regolarizzata della Regressione Lineare, aggiungendo un termine di regolarizzazione "alpha" alla *cost function*, l'algoritmo di apprendimento viene forzato a tenere i weight quanto più bassi possibili. I modelli di regressione lineare semplici hanno principalmente 2 limitazioni, che li rendono difficilmente utilizzati nel concreto:

1. Difficile esprimere relazioni non lineari
2. Tendono all'overfitting quando il numero di feature aumenta

La Ridge Regression è in grado di determinare l'importanza di una feature tramite un **fattore di penalità**, in particolare L2 (squared size) penalizza il quadrato del valore dei coefficienti del modello. In pratica questo produce coefficienti piccoli, ma nessuno di loro è mai annullato. Quindi i coefficienti non sono mai 0. Il fenomeno è denominato **feature shrinkage.**

Tabella 3.9: Risulati ottenuti applicando Ridge Regression

Test	Regressor	Alg	Scaler	MAE	MSE	RMSE
31	Ridge	KF	ZScore	0.08204096848267174	0.013235753441504631	0.11503410987832646
32	Ridge	RKF	ZScore	0.08204274341834476	0.013236544170143368	0.11504322895755373
33	Ridge	KF	MinMax	0.08183164907724155	0.013236618318107123	0.11503782236352864
34	Ridge	RKF	MinMax	0.08180776720427758	0.01323756127538574	0.11504760144211959
35	Ridge	KF	Robust	0.08203635302473297	0.01323575691981652	0.11503412372828645
36	Ridge	RKF	Robust	0.08203749876766202	0.013236545552046099	0.1150432337168575

3.8 Classificazione

Dopo aver trattato il problema in analisi tramite l'utilizzo di modelli di regressione, è stato tentato un approccio diverso, basato sulla classificazione. Il dataset è rimasto invariato,è stata effettuato una sola modifica ed è sulla variabile dipendente, infatti la predizione avverrà su Happiness Rank. Le operazioni di feature engineering (data cleaning, feature scaling e selection) effettuate sui dati sono state le medesime eseguite nel caso del modello di regressione. L'unica modifica è stata ovviamente apportata alle metriche di validazione. Non potendo utilizzare metriche come MAE, MSE e RMSE, i risultati dei nostri modelli sono stati valutati tramite metriche derivate della matrice di confusione:

- Precision = $\frac{TP}{(TP+FP)}$
- Recall = $\frac{TP}{(TP+FN)}$
- Accuracy = $\frac{TP+TN}{(TP+TN+FP+FN)}$
- MCC = $\frac{TP*TN+FP*FN}{\sqrt{(TP+FP)*(TP+FN)*(TN+FP)*(TN+FN)}}$

Inoltre, in seguito al plot delle categorie così create,sono state così applicate due tecniche di Data Balancing: Undersampling e Oversampling. Non si è notato un notevole sbilanciamento dei dati.

3.8.1 Naive Bayes

Il primo algoritmo di classificazione ad essere stato testato è il Naive Bayes, in particolare in Gaussian Naive Bayes. Come ben noto, questo tipo di algoritmo assume che le caratteristiche non siano correlate l'una all'altra. E' stato quindi necessario verificare che questa condizione fosse verificata anche nel nostro dataset: Applicando questo algoritmo di classificazione, è stato possibile ottenere i seguenti risultati:

Tabella 3.10: Risultati ottenuti con Gaussian Naive Bayes

Test	Classifier	Alg	Scaler	Precision	Recall	Accuracy	Mcc
61	Gaussian	KF-U	ZScore	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
62	Gaussian	RKF-U	ZScore	0.9580244544328373	0.9580244544328373	0.9993435524560408	0.9559066848907453
63	Gaussian	KF-U	MinMax	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
64	Gaussian	RKF-U	MinMax	0.9580244544328373	0.9580244544328373	0.9993435524560408	0.9559066848907453
65	Gaussian	KF-U	Robust	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
66	Gaussian	RKF-U	Robust	0.9580244544328373	0.9580244544328373	0.9993435524560408	0.9559066848907453
67	Gaussian	KF-O	ZScore	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
68	Gaussian	RKF-O	ZScore	0.9580244544328373	0.9580244544328373	0.9993435524560408	0.9559066848907453
69	Gaussian	KF-O	MinMax	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
70	Gaussian	RKF-O	MinMax	0.9580244544328373	0.9580244544328373	0.9993435524560408	0.9559066848907453
71	Gaussian	KF-O	Robust	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
72	Gaussian	RKF-O	Robust	0.9580244544328373	0.9580244544328373	0.9993435524560408	0.9559066848907453

Oltre ad aver testato il Gaussian Naive Bayes, è stato analizzato anche il Bernoulli Naive Bayes, da cui i seguenti risultati:

Tabella 3.11: Risultati ottenuti con Bernulli Naive Bayes

Test	Classifier	Alg	Scaler	Precision	Recall	Accuracy	Mcc
73	Bernoulli	KF-U	ZScore	0.3431174711704245	0.3431174711704245	0.9896722172766508	0.3066437563187886
74	Bernoulli	RKF-U	ZScore	0.34331313065549407	0.34331313065549407	0.9896322641653225	0.30640608607715475
75	Bernoulli	KF-U	MinMax	0.23394386326684596	0.23394386326684596	0.9879567044372779	0.16966512687233584
76	Bernoulli	RKF-U	MinMax	0.23337125626356037	0.23337125626356037	0.9878840938942389	0.16872020914743602
77	Bernoulli	KF-U	Robust	0.42705696332111465	0.42705696332111465	0.9909921846699856	0.400642728497029
78	Bernoulli	RKF-U	Robust	0.4167964424096405	0.4167964424096405	0.9907827817006611	0.39210655550397167
79	Bernoulli	KF-O	ZScore	0.3431174711704245	0.3431174711704245	0.9896722172766508	0.3066437563187886
80	Bernoulli	RKF-O	ZScore	0.34331313065549407	0.34331313065549407	0.9896322641653225	0.30640608607715475
81	Bernoulli	KF-O	MinMax	0.23394386326684596	0.23394386326684596	0.9879567044372779	0.16966512687233584
82	Bernoulli	RKF-O	MinMax	0.23337125626356037	0.23337125626356037	0.9878840938942389	0.16872020914743602
83	Bernoulli	KF-O	Robust	0.42705696332111465	0.42705696332111465	0.9909921846699856	0.400642728497029
84	Bernoulli	RKF-O	Robust	0.4167964424096405	0.4167964424096405	0.9907827817006611	0.39210655550397167

3.8.2 Decision Tree

Come altro algoritmo di classificazione, è stato individuato l'algoritmo Decision Tree, prima già utilizzato per la regressione. Questo mira a creare un albero i cui nodi rappresentano un sotto-insieme di feature e i cui archi rappresentano delle condizioni decisionali. Per ogni nodo, la scelta della feature da porre in ogni nodo avviene tramite il calcolo dell' *information gain*. Questo algoritmo ha portato alle seguenti prestazioni del modello:

Tabella 3.12: Risultati ottenuti con Decision Tree

Test	Classifier	Alg	Scaler	Precision	Recall	Accuracy	Mcc
85	DecisionTree	KF-U	Zscore	0.9980139811566334	0.9980139811566334	0.9999693512376366	0.9979031739015352
86	DecisionTree	RKF-U	Zscore	0.9980051966121906	0.9980051966121906	0.9999687745148694	0.9978940044741365
87	DecisionTree	KF-U	MinMax	0.9979263575096662	0.9979263575096662	0.9999679498835699	0.9978106937382459
88	DecisionTree	RKF-U	MinMax	0.9980051962709636	0.9980051962709636	0.9999688284518644	0.9978939989359381
89	DecisionTree	KF-U	Robust	0.9980139811566335	0.9980139811566335	0.9999691650517996	0.9979031664150086
90	DecisionTree	RKF-U	Robust	0.9980110380749128	0.9980110380749128	0.999968937974731	0.9979001659169325
91	DecisionTree	KF-O	Zscore	0.9980431901763789	0.9980431901763789	0.9999697751645057	0.9979340206370472
92	DecisionTree	RK-O	Zscore	0.9980110370512321	0.9980110370512321	0.9999688946946605	0.997900181834984
93	DecisionTree	KF-O	MinMax	0.9979555665294115	0.9979555665294115	0.9999683017748404	0.9978415305744126
94	DecisionTree	RKF-O	MinMax	0.9980139572707529	0.9980139572707529	0.9999689210150532	0.9979032609582227
95	DecisionTree	KF-O	Robust	0.9980139845689022	0.9980139845689022	0.9999691906611288	0.9979032091416242
96	DecisionTree	RKF-O	Robust	0.9979905914198641	0.9979905914198641	0.999968538808195	0.9978785959020072

3.8.3 Voting Classifier

Come ultimo algoritmo di classificazione è stato scelto il Voting classifier. Questo si differenzia dai precedenti in quanto è un algoritmo di tipo "*ensemble*", ovvero utilizza diversi algoritmi di classificazione, e restituisce la classe che ha ottenuto più "voti" dai vari algoritmi. I 3 classificatori utilizzati sono: Decision Tree, K neighbors classifier e SVC (Support Vector Classification).I risultati ottenuti vengono riportati di seguito:

Tabella 3.13: Risultati ottenuti con Voting

Test	Classifier	Alg	Scaler	Precision	Recall	Accuracy	Mcc
96	Voting	KF-U	ZScore	0.986944738582003	0.986944738582003	0.9997958416304232	0.9862257886477982
97	Voting	RKF-U	ZScore	0.9868512284303673	0.9868512284303673	0.9997934571652014	0.9861252479532283
98	Voting	KF-U	MinMax	0.9850755455808119	0.9850755455808119	0.9997666863648462	0.984253110012249
99	Voting	RKF-U	MinMax	0.9851514303411285	0.9851514303411285	0.9997667113604585	0.98433155405503
100	Voting	KF-U	Robust	0.9867695288230239	0.9867695288230239	0.9997936812817247	0.9860419955667743
101	Voting	RKF-U	Robust	0.9866029763308667	0.9866029763308667	0.9997898380078369	0.9858641475513805
102	Voting	KF-O	ZScore	0.986944738582003	0.986944738582003	0.9997958416304232	0.9862257886477982
103	Voting	RKF-O	ZScore	0.9868512284303673	0.9868512284303673	0.9997934571652014	0.9861252479532283
104	Voting	KF-O	MinMax	0.9850755455808119	0.9850755455808119	0.9997666863648462	0.984253110012249
105	Voting	RKF-O	MinMax	0.9851514303411285	0.9851514303411285	0.9997667113604585	0.98433155405503
106	Voting	KF-O	Robust	0.9867695288230239	0.9867695288230239	0.9997936812817247	0.9860419955667743
107	Voting	RKF-O	Robust	0.9866029763308667	0.9866029763308667	0.9997898380078369	0.9858641475513805

Il lavoro svolto è disponibile alla seguente **repository** .

CAPITOLO 4

Analisi dei Risultati

In questo capitolo verranno analizzati i risultati e verranno selezionati i risultati migliori. Per l'elaborazione di tutte le possibili configurazioni è stato utilizzato lo strumento Google Colab.

4.0.1 Regressione

Facendo riferimento ai risultati ottenuti nel capitolo 3: possiamo affermare che all'interno del modello di regressione lineare, analizzando i risultati ottenuti utilizzando l'algoritmo KF e lo scaler ZScore, dalle diverse metriche è scarurito essere migliore l'algoritmo Random Forest, infatti esso risulta avere dei valori minori rispetto agli altri.

Tabella 4.1: Confronto risultati in regressione ottenuti utilizzando KF e ZScore

1	Linear	KF	ZScore	0.08205148396585915	0.01323574779148373	0.11503408759723158
7	DecisionTree	KF	ZScore	0.00012780653343933123	1.261403734581765e-05	0.0035037249696091444
13	RandomForest	KF	ZScore	0.0001903103851035871	1.2009825842104264e-05	0.0034285012606982577
19	SVR	KF	ZScore	0.06275080541906397	0.005159960821417611	0.07181018398846659
25	Lasso	KF	ZScore	0.6350066267218144	0.7312313627385884	0.8551082391820571
31	Ridge	KF	ZScore	0.08204096848267174	0.013235753441504631	0.11503410987832646

4.0.2 Classificazione

Facendo riferimento ai risultati ottenuti nel capitolo 3: possiamo affermare che all'interno del modello di classificazione, analizzando i risultati ottenuti utilizzando l'algoritmo KF e lo scaler ZScore, dalle diverse metriche è scarurito essere migliore l'algoritmo Decision Tree, infatti esso risulta avere dei valori più alti rispetto agli altri dimonstrando di avere una precision e un accuracy molto vicina all'1.

Tabella 4.2: Confronto risultati in classificazioe ottenuti utilizzando KF e ZScore

Test	Classifier	Alg	Scaler	Precision	Recall	Accuracy	Mcc
61	Gaussian	KF-U	ZScore	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
73	Bernoulli	KF-U	ZScore	0.3431174711704245	0.3431174711704245	0.9896722172766508	0.3066437563187886
85	DecisionTree	KF-U	Zscore	0.9980139811566334	0.9980139811566334	0.9999693512376366	0.9979031739015352
96	Voting	KF-U	ZScore	0.986944738582003	0.986944738582003	0.9997958416304232	0.9862257886477982
67	Gaussian	KF-O	ZScore	0.9574462356125104	0.9574462356125104	0.999337168347974	0.9552927462304279
79	Bernoulli	KF-O	ZScore	0.3431174711704245	0.3431174711704245	0.9896722172766508	0.3066437563187886
91	DecisionTree	KF-O	Zscore	0.9980431901763789	0.9980431901763789	0.9999697751645057	0.9979340206370472
102	Voting	KF-O	ZScore	0.986944738582003	0.986944738582003	0.9997958416304232	0.9862257886477982

CAPITOLO 5

Conclusioni e sviluppi futuri

L'obiettivo della tesi era quello di analizzare le tecniche esistenti per predire attacchi terroristici infatti:

- nella prima fase il focus è stato incentrato sulle possibili nuove tecnologie e sullo studio delle attuali tecnologie.

- nella seconda fase invece il focus è stato incentrato sulla costruzione di un modello di machine learning capace di predire dei possibili attacchi terroristici in base alla salute di una nazione.

Gli sviluppi futuri del lavoro di tesi saranno possibili in un futuro maggiormente sviluppato tecnologicamente, il focus potrà essere incentrato, su uno studio inverso, quello di analizzare le nazioni che non hanno subito attacchi terroristici negli ultimi anni e analizzare i diversi fattori sia politici sia religiosi e sia tecnologici che hanno portato a questa stabilità, rispetto alle altre nazioni.
Concludo allegando il lavoro svolto nella seguente **repository github**

Bibliografia

[1] "tesi.luiss.it," (Citato a pagina 3)

[2] "www.ilsole24ore.com," (Citato a pagina 4)

[3] "https://www1.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala$_s tampa/notizie/ar$

[4] "www.intelligenzaartificiale.it," (Citato a pagina 7)

[5] "https://www.researchgate.net/publication/345172560$_c yberphysical - systems - and - artificial - intelligence$," (*Citatoapagina* 7)

[6] "Tecniche di prevenzione di attacchi terroristici: Un confronto empirico tra le tecniche esistenti,roberto esposito," (Citato alle pagine 8 e 37)

[7] B. C. Ezell, S. P. Bennett, D. Von Winterfeldt, J. Sokolowski, and A. J. Collins, "Probabilistic risk analysis and terrorism risk," *Risk Analysis: An International Journal*, vol. 30, no. 4, pp. 575–589, 2010. (Citato alle pagine 9 e 38)

[8] "onlinelibrary.wiley.com," (Citato a pagina 10)

[9] T. Bosse and C. Gerritsen, "Comparing crime prevention strategies by agent-based simulation," in *2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*, vol. 2, pp. 491–496, IEEE, 2009. (Citato a pagina 10)

[10] "https://www.jasss.org/13/2/5.html," (Citato a pagina 16)

[11] M. Hao, D. Jiang, F. Ding, J. Fu, and S. Chen, "Simulating spatio-temporal patterns of terrorism incidents on the indochina peninsula with gis and the random forest method,"

ISPRS International Journal of Geo-Information, vol. 8, no. 3, p. 133, 2019. (Citato alle pagine 18, 19, 21, 33 e 37)

[12] G. Cascavilla, J. Slabber, F. Palomba, D. Di Nucci, D. A. Tamburri, and W.-J. van den Heuvel, "Counterterrorism for cyber-physical spaces: A computer vision approach," in *Proceedings of the International Conference on Advanced Visual Interfaces*, pp. 1–5, 2020. (Citato alle pagine 25, 31 e 38)

[13] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," 2019. (Citato alle pagine 26, 28 e 30)

[14] G. M. Campedelli, M. Bartulovic, and K. M. Carley, "Learning future terrorist targets through temporal meta-graphs," *Scientific reports*, vol. 11, no. 1, pp. 1–15, 2021. (Citato alle pagine 33 e 37)

[15] T. Bosse, C. M. Jonker, L. van der Meij, and J. Treur, "Leadsto: A language and environment for analysis of dynamics by simulation," in *Innovations in Applied Artificial Intelligence* (M. Ali and F. Esposito, eds.), (Berlin, Heidelberg), pp. 363–366, Springer Berlin Heidelberg, 2005. (Citato a pagina 38)

Ringraziamenti