MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA LOTTA ALLA CONTRAFFAZIONE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

| | |
|---|---|
| **DOMANDA DI INVENZIONE NUMERO** | **102021000021104** |
| **Data Deposito** | **05/08/2021** |
| **Data Pubblicazione** | **03/11/2021** |

Classifiche IPC

| Sezione | Classe | Sottoclasse | Gruppo | Sottogruppo |
|---|---|---|---|---|
| G | 06 | F | 21 | 55 |

Titolo

Sistema e metodo per l?individuazione di anomalie di sicurezza nell?utilizzo di dati contenuti in database multi-accesso nell?ambito di servizi front-office e back-office

**DESCRIZIONE dell'invenzione avente per TITOLO**

**"Sistema e metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office"**

**a nome di CIA PUGLIA SERVIZI s.r.l., partita iva e codice fiscale 07965220721 con sede legale in Via Cacudi n. 40 – 70132 Bari (BA)**

DESCRIZIONE

Campo della tecnica a cui l'invenzione fa riferimento e modalità di utilizzo in ambito industriale

La presente invenzione si riferisce a un sistema e metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office.

Stato della tecnica preesistente

Le violazioni di dati provenienti da soggetti interni rappresentano una parte non più trascurabile dei rischi informatici che incombono sulle aziende. Lo stato attuale della ricerca fornisce prove inequivocabili che sottolineano la gravità e la prevalenza di questa minaccia nelle aziende [1-3]. Attraverso le analisi degli incidenti pregressi è possibile inquadrare al meglio l'entità della minaccia. Il Threat Landscape Report 2016 [4] dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) ha classificato i quattro principali incidenti/azioni insider come segue: utilizzo scorretto dei privilegi (60%), cattiva gestione dei dati (13%), uso di hardware non approvato (10%) e abuso di possesso di privilegi (10%).

Secondo il Threat Landscape Report 2018 [5] dell'ENISA, il 27% degli incidenti di violazione dei dati è stato causato da fattori umani o negligenza e, secondo uno studio, il phishing (67%) costituisce il problema principale in ambito di minacce non intenzionali da parte di soggetti interni all'azienda. Inoltre, il rapporto ENISA del 2020 attesta che la frequenza di questo tipo di incidenti è incrementata del 47%, con un relativo incremento del costo per le imprese del 31% fino a 11,45 milioni di dollari a livello globale [6].

I dipendenti interni (insider) possono abusare del loro accesso autorizzato ai sistemi al fine di sottrarre o modificare i dati per intenti malevoli o per guadagno personale [1]. Poiché i lavoratori dispongono del know how aziendale e hanno accesso diretto a risorse informative non facilmente disponibili agli esterni, i danni sono potenzialmente considerevoli. Inoltre, queste minacce stanno aumentando in scala, portata e sofisticazione, enfatizzando così la necessità per le organizzazioni di applicare tecnologie specifiche per sicurezza dei dati.

Secondo il Centre for the Protection of National Infrastructure (CPNI) [7], un insider è qualcuno che sfrutta o ha l'intenzione di sfruttare il suo accesso legittimo alle risorse di un'organizzazione per scopi non autorizzati. Questa minaccia è abbastanza sofisticata da compromettere i principi di sicurezza di riservatezza, integrità e disponibilità che devono essere garantiti per qualsiasi sistema di difesa sicuro [8]. Di particolare rilevanza risultano essere le attività in diretto contatto con i dati sensibili dei clienti, quali le attività di front office e back office [9].

Allo stato dell'arte sono noti metodi di individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso con utilizzo di tecniche informatiche standard.

Ad esempio il brevetto US 10.003.608 B2 descrive un metodo che prevede l'individuazione di attività anomale sulla base della comparazione di valori soglia impostati in riferimento profilo comportamentale di ogni utente, a cui seguono azioni di prevenzione sulla base di policy settate a livello di sistema. L'individuazione delle anomalie comporta in questo caso il settaggio singoli valori soglia per ogni utente (es. dimensione massima dei file nei trasferimenti tramite e-mail).

Il brevetto US 2020/0163605 A1 descrive un metodo per l'individuazione di insider threat basato sull'analisi automatizzata delle risposte degli utenti tramite specifiche survey finalizzate ad ottenere una risposta emotiva da parte dell'utente.

Il brevetto US 10.178.116 B2 descrive un metodo e sistema per l'analisi comportamentale degli utenti finalizzata ad individuare anomalie nella sicurezza, basato sull'osservazione degli eventi presso gli endpoint e l'estrazione di specifici indicatori comportamentali (opportunità, pressione, razionalizzazione) da cui viene ricavato automaticamente uno scoring di rischio per la sicurezza.

Nello stato dell'arte esistono inoltre metodi per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso con utilizzo di tecniche di machine learning.

Ad esempio il brevetto US 9.043.905 B1 descrive un metodo e sistema per l'individuazione di insider threat basato sull'utilizzo della tecnica Hierachical Random Graphs (HRG) per la creazione di cluster dei dati riferiti a pattern di attività degli utenti, e della tecnica Bayesian Probabilistic Tensor Decomposition (BPTD) per estrarre le azioni osservabili dai pattern di attività. Inoltre un modello probabilistico Bayesiano è utilizzato per combinare le azioni osservabili, ridurre il rumore e fornire indicazioni sul contesto. Infine un modulo confronta le potenziali anomalie riscontrate con le policy di sicurezza impostate per suggerire strategie di sicurezza dinamiche nel tempo.

Il brevetto US 8.793.790 B2 descrive un metodo e sistema per l'individuazione di insider threat attraverso l'utilizzo di tecniche di machine learning su alberi semantici per l'individuazione di anomalie nell'accesso a risorse fisiche e virtuali da parte degli utenti, sulla base di modelli teorici e probabilistici.

Il brevetto WO 2021/089196 A1 descrive un metodo per l'individuazione di intrusioni nel sistema e insider threat attraverso la determinazione di pattern comportamentali con l'utilizzo di reti neurali

ricorsive e l'identificazione di eventi riconducibili ad attività normali e anormali con l'utilizzo di una rete neurale feed forward.

Esposizione del problema tecnico e della soluzione proposta

Il monitoraggio dell'attività dei lavoratori e l'applicazione di ruoli specifici per l'accesso ai dati risultano strategie essenziali per la gestione del rischio. Con tali presupposti si permette l'applicazione di approcci di outlier analysis, finalizzati a individuare comportamenti anomali rispetto a gruppi di attività internamente omogenei [10]. I metodi presenti nello stato dell'arte che utilizzano tecniche di machine learning si dimostrano particolarmente utili in questo ambito applicativo perché permettono l'analisi di grandi volumi di dati, tuttavia questi approcci comportano molteplici criticità, dovute a:

- Irregolarità delle routine dei lavoratori sulla base di fattori quali tipologia di attività assegnate, stagionalità, carico di lavoro, collaborazione in team, scadenze particolari etc.
- Caratterizzazione individuale delle attività svolte da singoli lavoratori.
- Forte sbilanciamento delle classi nei dataset di riferimento
- Possibile presenza di insider malevoli precedente al periodo di osservazione, tale da introdurre bias significativi nei dati osservati
- Onerosità della rilevazione di falsi positivi, in termini di reputazione aziendale, influenza sul rapporto con le risorse umane, blocco di risorse informatiche e processi lavorativi.
- Variabilità degli strumenti informatici utilizzati per l'espletamento delle attività, sempre più spesso basati su portali esterni in cloud.
- Possibile complessità dell'articolazione delle attività svolte – con l'utilizzo di molteplici strumenti software – e difficoltà nel rilevare minacce basate sull'utilizzo improprio di set limitati di dati (es. sottrazione di singole anagrafiche di clienti per finalità di concorrenza sleale).

L'invenzione proposta permette un'individuazione efficace delle anomalie di sicurezza nell'utilizzo dei dati nello specifico caso operativo delle attività di front-office e back-office attraverso un metodo articolato in:

- prima classificazione della tipologia di operazione svolta tramite autodichiarazione da parte dell'operatore attraverso opportuna interfaccia grafica.
- tracciamento dell'attività dell'operatore di accesso e modifica dei dati del sistema informativo aziendale, nonché dell'accesso a siti esterni tramite browser.
- classificazione dei tentativi di inferenza da parte dell'operatore verso dati presenti nel sistema informativo aziendale normalmente non accessibili sulla base dei livelli di accesso stabiliti, effettuata tramite rete neurale convoluzionale.

- classificazione delle operazioni anomale svolte nel web con accesso a portali esterni, effettuata tramite rete neurali ricorsive (Long Short Term Memory) e convoluzionali concatenate in un unico modello.
- classificazione delle anomalie nei records registrati nel sistema informativo aziendale, effettuata tramite algoritmo Vertex Feature Classification [11].
- classificazione delle anomalie globali di sicurezza tramite motore inferenziale con utilizzo di logiche fuzzy al fine di combinare i risultati delle altre classificazioni di cui ai punti precedenti.

La combinazione degli algoritmi di classificazione permette al sistema di essere efficace nel caso operativo delle attività di front-office e back-office, in cui nell'ambito di singole operazioni si fa tipicamente ricorso a query in lettura e modifica nel sistema informativo aziendale associate a sessioni di navigazione nel web per l'accesso a portali esterni (es. pubblica amministrazione) per il reperimento di dati sensibili relativi al cliente. L'utilizzo della tecnica Vertex Feature Classification permette un'efficace classificazione delle anomalie nei records associati alle singole operazioni con tempi di addestramento estremamente ridotti nello specifico ambito applicativo trattato [11]. Inoltre il trovato combina vantaggiosamente una classificazione dei tentativi di inferenza da parte dell'operatore, effettuata tramite rete neurale convoluzionale, in modo tale da proteggere il sistema da questo tipo di attacchi, difficilmente rilevabili attraverso altre metodologie nello stato dell'arte.

Descrizione dell'invenzione e delle modalità di attuazione

Scopo della presente invenzione è quello di fornire un metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office, atto a risolvere il suddetto problema.

È oggetto della presente invenzione un metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office conformemente alle rivendicazioni 1-8.

È anche oggetto della presente invenzione un sistema di per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office atto a risolvere il suddetto problema, conformemente alla rivendicazione 9.

Vantaggiosamente, il presente trovato consente di ottenere:

- robustezza del metodo per l'individuazione di anomalie rispetto alla variabilità delle attività degli utenti in base a tipologia di attività assegnate.
- robustezza del metodo rispetto all'eventuale complessità dell'articolazione delle attività svolte tramite sistema informativo aziendale e accesso a portali web esterni (es. pubblica amministrazione)

- tempi ridotti per l'addestramento di modelli di individuazione anomalie nei records associati a singole operazioni tramite utilizzo della tecnica Vertex Feature Classification.

Nel seguito della descrizione si indica con operatore un utente possessore di credenziali di accesso al sistema informativo aziendale (es. ERP) e a portali web esterni utili all'espletamento della propria attività lavorativa (es. portali della pubblica amministrazione) che intende accedere a detti dati sia lettura che in scrittura per la fornitura di un servizio a un privato o a un'impresa (cliente).
Si indica con servizio una tipologia di operazione svolta da un operatore a vantaggio di un cliente tramite l'accesso al sistema informativo aziendale e a portali web esterni utili all'espletamento della stessa, con registrazione (manuale o automatica) nel sistema informativo aziendale del risultato della stessa operazione.
Le rivendicazioni dipendenti descrivono realizzazioni preferite dell'invenzione, formando parte integrante della presente descrizione.

Descrizione Sintetica delle figure

Ulteriori caratteristiche e vantaggi dell'invenzione risulteranno maggiormente evidenti alla luce della descrizione dettagliata di forme di realizzazione preferite, ma non esclusive, di un metodo e sistema per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office, illustrato a titolo esemplificativo e non limitativo, con l'ausilio delle unite tavole di disegno in cui:
la Fig.1 rappresenta schematicamente un esempio di sistema conforme col presente trovato.
La Fig.2 raffigura un diagramma di flusso dettagliato di una modalità di funzionamento del metodo applicato nel sistema di figura 1 relativo alla classificazione di query ambigue e controllo dell'inferenza (116).
La Fig. 3 rappresenta uno schema logico esemplificativo del metodo applicato per la classificazione di operazioni web ambigue (126) in figura 1.
La Fig.4 illustra schematicamente la procedura di addestramento e test del modello Vertex Feature Classification per la classificazione di records attribuibili ad operazioni anomale, riferibile all'elemento (132) in figura 1.

Gli stessi numeri e le stesse lettere di riferimento nelle figure identificano gli stessi elementi o componenti.

Descrizione in dettaglio di una forma di realizzazione preferita dell'invenzione

Secondo una variante preferita del trovato, un sistema preferito comprende:

- Un modulo di gestione degli accessi (110) comprendente:
  i. Un'interfaccia di accesso operazione (111) in cui l'operatore deve accedere attraverso un sistema di autenticazione sicuro (es. Multi Factor Authentication, One Time Password etc.).
  ii. Un filtro multilivello (112) atto ad attribuire un set di privilegi di accesso e scrittura ai dati in base all'operatore (ad esempio limitando l'accesso ai dati anagrafici dei clienti ai soli comuni collegati con la sede in cui l'operatore si connette).
  iii. Un'interfaccia per l'avvio e la conclusione di una nuova operazione su cliente (113) o nuova operazione interna (114), in cui l'operatore deve dichiarare un set di parametri, al minimo:
    1. tipologia di operazione;
    2. avvio dell'operazione (es. tramite opportuno pulsante di "avvio operazione");
    3. cliente di riferimento (nel caso di 113);
    4. conclusione dell'operazione (es. tramite opportuno pulsante di "conclusione operazione").
  iv. Un'interfaccia di accesso ai dati statistici delle operazioni effettuate (115) in cui l'operatore, a prescindere dai privilegi di accesso, può accedere in lettura a un set limitato di dati aggregati relativi alle statistiche delle operazioni effettuate (es. numero di operazioni effettuate in una determinata sede in un periodo di tempo definito). Gli accessi ai dati da parte dell'operatore vengono registrati nella forma di query.
  v. Un dizionario delle query e associazione tra i servizi (116) popolato dalle query effettuate tramite (115) con indicazione di un set di parametri descrittivi della stessa, al minimo:
    1. tipologia di query;
    2. data;
    3. operatore autore della query;
    4. numero totale delle tuple restituite dalla query.

    Il dizionario delle query può opzionalmente conservare traccia dei servizi tra loro dipendenti, in modo tale da fornire una base dati più efficace per l'individuazione dei tentativi di inferenza.
  vi. Un classificatore delle query ambigue e controllo dell'inferenza (117), realizzato attraverso una rete neurale convoluzionale (CNN) per la classificazione delle query ambigue riferibili a tentativi di inferenza da parte degli operatori per l'accesso a dati di cui non dispongono dei permessi di visualizzazione necessari.
- Un modulo di monitoraggio WEB (120) comprendente:
  i. Un metodo di Single Sign On (121) attivato dall'avvio di una nuova operazione su cliente (113) tramite cui l'operatore può accedere un'unica volta con una sola coppia di credenziali alle applicazioni web necessarie all'espletamento dell'operazione.

ii. Un metodo di monitoraggio della sessione web (122) tale da permettere la registrazione di log di navigazione (cronologia web) associati all'operazione (113).
iii. Un metodo di estrazione di feature dal contenuto in linguaggio naturale dei descrittori dei siti web visitati tramite tecniche di Natural Language Processing (123).
iv. Un metodo di associazione dei siti web visitati ad uno score di reputazione web (124) tramite l'utilizzo di Application Programming Interface verso servizi in cloud di monitoraggio della web reputation.
v. Un metodo di preprocessing delle sequenze di navigazione web (125) finalizzato all'estrazione di un set di feature utile a descrivere il comportamento dell'operatore durante l'esecuzione dell'operazione (come da modalità di attuazione esemplificativa descritta in seguito)
vi. Un metodo di classificazione delle operazioni anomale svolte nel web (126), effettuata tramite reti neurali ricorsive (Long Short Term Memory) e convoluzionali concatenate.

- Un modulo di monitoraggio operazioni su sistema informativo aziendale (es. ERP) (130) comprendente:
  i. Un metodo di preprocessing dei dati riferiti ai records delle operazioni presenti nel sistema informativo aziendale (131).
  ii. Un metodo di classificazione tramite Vertex Feature Classification per l'individuazione di operazioni anomale (132).
- Un modulo di motore inferenziale (140) per la classificazione di anomalie di sicurezza dei dati secondo logiche fuzzy, comprendente:
  i. Un metodo per il buffering dei dati (141) ottenuti dalle classificazioni dei moduli connessi (110,120,130);
  ii. Un metodo per la progettazione e configurazione di regole inferenziali secondo logiche fuzzy (142) (ad esempio implementabile con strumenti tecnici esistenti come software CLIPS o libreria python Experta). Dette regole inferenziali sono impostate sulla base di policy di sicurezza decise dall'amministratore di sistema;
  iii. Un metodo per il confronto (143) dei dati ottenuti (141) con le regole impostate (142).
  iv. Un metodo per l'esecuzione (144) delle regole applicabili nel caso osservato (singola operazione).

Dunque, l'invenzione proposta permette un'individuazione efficace delle anomalie di sicurezza nell'utilizzo dei dati nello specifico caso operativo delle attività di front-office e back-office attraverso un metodo articolato in:

1. prima classificazione della tipologia di operazione svolta tramite autodichiarazione da parte dell'operatore attraverso opportuna interfaccia grafica (113,114).

2. tracciamento dell'attività dell'operatore di accesso e modifica dei dati del sistema informativo aziendale (115,131), nonché dell'accesso a siti esterni tramite web browser (122).
3. classificazione dei tentativi di inferenza da parte dell'operatore verso dati presenti nel sistema informativo aziendale normalmente non accessibili sulla base dei livelli di accesso stabiliti, effettuata tramite rete neurale convoluzionale (117).
4. classificazione delle operazioni anomale svolte nel web con accesso a portali esterni, effettuata tramite rete neurali ricorsive (Long Short Term Memory) e convoluzionali concatenate in un unico modello (126).
5. classificazione delle anomalie nei records registrati nel sistema informativo aziendale, effettuata tramite algoritmo Vertex (132).
6. classificazione delle anomalie globali di sicurezza tramite motore inferenziale con utilizzo di logiche fuzzy al fine di combinare i risultati delle altre classificazioni di cui ai punti precedenti (140).

In accordo con il presente trovato, ogni accesso di detto operatore al sistema viene registrato in un file di log, insieme a dati quantitativi riferiti alle operazioni effettuate.

Detta interfaccia di accesso fornisce all'operatore la possibilità di avviare tutte le operazioni necessarie all'espletamento della propria attività lavorativa, permettendone un esatto monitoraggio (da effettuarsi attraverso tecniche esistenti di registrazione della cronologia web, web scraping, registrazione degli input da tastiera, registrazione del trasferimento dei file etc. sulla base delle specifiche necessità dell'attività lavorativa).

All'operatore si rende disponibile anche un'interfaccia di accesso ai dati statistici delle operazioni effettuate (115) in cui l'operatore, a prescindere dai privilegi di accesso, può accedere in lettura a un set limitato di dati aggregati relativi alle statistiche delle operazioni effettuate (es. numero di operazioni effettuate in una determinata sede in un periodo di tempo definito). Gli accessi ai dati da parte dell'operatore vengono registrati nella forma di query (es. query SQL del tipo: "SELECT * FROM operazione WHERE data BETWEEN Var_1 AND Var_2 AND cliente= Var_3").

L'interfaccia di generazione delle query è quindi connessa ad uno script di popolamento di un dizionario delle query (116) con indicazione di: 1) data; 2) operatore-autore della query; 3) il numero totale delle tuple restituite dalla query.

Detto dizionario delle query (116) permette una corretta classificazione delle query attraverso un algoritmo di estrazione di feature, con la creazione di un dataset con relativo label utilizzabile per l'addestramento di reti neurali per la classificazione di query riferibili a tentativi di inferenza (117).

Detto classificatore delle query (117) è realizzato attraverso una rete neurale convoluzionale (CNN) che riceve in input un set di feature del tipo:

1. cliente_id: feature categoriale associata al cliente (numero intero)
2. tipo_utente: query eseguita da un utente interno o esterno (booleano)
3. utente_id: feature categoriale associata all'utente che esegue la query (numero intero)
4. operatore_id: feature categoriale associata all'operatore oggetto della ricerca (numero intero)
5. sede_id: feature categoriale associata alla sede (numero intero)
6. durata_ricerca: feature categoriale associata all'operatore oggetto della ricerca (numero intero)
7. num_operazioni: numero di operazioni (tuple) restituite dalla query (numero intero)
8. numero_query_cliente: numero di query effettuate nello stesso giorno con chiave di ricerca per cliente (numero intero)
9. associazione_servizio: Associazione del servizio ad altre tipologie di servizi (booleano)
10. inferenza: feature label di inferenza o meno (booleano)

Detto modulo di monitoraggio web (120) comprende un classificatore delle operazioni web ambigue (126) attraverso l'applicazione di un modello di rete neurale ricorsiva del tipo Long Short Term Memory (LSTM - 304') concatenato a una rete neurale di tipo convoluzionale (CNN - 304'') secondo lo schema raffigurato in figura 3. Alla rete LSTM (304'), più efficace nell'individuare pattern di comportamento in serie temporali, viene fornito in input un set di feature del tipo:

1. Sequenza $\Delta T$ singoli URL: sequenza dei tempi di sosta sui singoli URL durante l'operazione, espresso in secondi (es. per un'operazione con 6 URL "80; 242; 320; 362; 125; 20")
2. Sequenza score reputazioni URL: sequenza dello score reputazione dei singoli URL visitati nel range 0-1(ottenuta tramite API da web service; es: "0,4; 0,2; 0,9;0,8")
3. Sequenza vettori parole descrizione URL: sequenza di valori derivata dalla vettorializzazione dei termini utilizzati nella descrizione dell'URL (ad esempio, in base alla sequenza di parole in cui la parola "mail" viene impiegata, viene assegnato una posizione in uno spazio n-dimensionale descritto da un array di vettori del tipo: "array([2.02280000e-01, -7.66180009e-02, 3.70319992e-01.... ], dtype=float32)")

Alla rete CNN (304''), viene fornito in input un set di feature riferite all'operazione nel suo complesso, ad esempio:

4. Tempo totale: tempo totale in secondi dell'operazione (es: "788")
5. Orario lavorativo (si/no): valore boleano che contrassegna se l'attività è stata svolta in orario lavorativo previsto per le attività specifiche (0) oppure in altre fasce orarie (1)
6. Numero di URL visitato: numero di link visitati durante una singola sessione per lo svolgimento di un'operazione (es: "26")
7. Tempo medio per URL: tempo medio in secondi speso su un singolo URL durante l'operazione (es: 788/26= "30.3")

8. Numero di visite al dominio principale: numero di visite al dominio visitato più frequentemente durante una singola operazione (es: "12")
9. Score reputazionale URL più frequente: score reputazione dell'URL visitato più frequentemente durante l'operazione, nel range 0-1(ottenuta tramite API da web service; es: "0,4")

Entrambi gli output delle reti (305' e 305'') vengono concatenati (306) ed ulteriormente elaborati in una rete neurale densamente connessa (307) ottenere uno score unico di affidabilità dell'operazione web (308).

Detto modulo di monitoraggio operazioni su sistema informativo aziendale (es. ERP) (130) comprende un metodo di preprocessing dei dati (131) tramite tecniche di scaling, ordinal encoder e fastICA, al fine di trovare una rappresentazione lineare di dati non gaussiani in modo che i componenti siano statisticamente indipendenti o il più indipendenti possibile. Tale rappresentazione è utilizzata per acquisire la struttura essenziale dei dati, finalizzata ad una più chiara estrazione delle caratteristiche e separazione dei segnali. Il metodo di classificazione per l'individuazione di operazioni anomale (132) ricorre alla tecnica denominata Vertex Feature Classification. L'algoritmo mappa dati di input in uno spazio costruito ad hoc, chiamato "spazio simplex" al fine di eseguire una classificazione geometrica, al minimo su un set di variabili in input riferiti all'anagrafica cliente o al risultato dell'operazione.

Più precisamente, ogni classe viene prima associata a un vertice specifico del politopo calcolato nello spazio delle caratteristiche. Successivamente, la classificazione viene eseguita in base alla disposizione geometrica in uno spazio di caratteristiche di dimensione superiore. L'algoritmo Vertex Feature Classification (VFC) sfrutta il potenziale del politopo e delle tecniche di multi-laterazione nella creazione di uno spazio di caratteristiche iper-dimensionali in cui sono disposte classi diverse in base alla struttura del politopo e la classificazione di un modello sconosciuto viene eseguita utilizzando la tecnica di multi-laterazione (trilaterazione con più di 3 lati). Più specificamente, il modello calcolato durante la fase di training è lo "spazio simplex": lo spazio che contiene le classi e il valore di riferimento di ogni classe e di ogni caratteristica. Una volta appreso lo spazio simplex, è possibile eliminare i dati di training. Il VFC è costituito dai seguenti passaggi:

• Fase di addestramento (410)

1. Calcolo Kernel Principal Component dei dati di training (411)
2. Generazione dello spazio simplex (412)
3. Ridimensionamento dei valori (413)
4. Calcolo dei centroidi (414)

• Fase di test (420)

1. Proiettare il campione di test nel modello Kernel Principal Component (421)

2. Ridimensionamento dei valori (422)
3. Stima delle coordinate e localizzazione delle stesse nello spazio del simplesso (423)
4. Calcolo del baricentro (424)
5. Classificazione operazioni anomale (425)

Nell'algoritmo VFC, una volta raggruppate le istanze in base al rispettivo identificatore di classe, ogni caratteristica viene analizzata in modo isolato. Per ogni funzione, viene calcolato il valore del centroide analizzando tutti i valori di quella funzione e per la classe di raggruppamento specificata in precedenza. Il valore di questo centroide è associato alle coordinate della classe precedentemente specificata all'interno dello spazio simplex. Dato un campione di test sconosciuto, per ogni caratteristica, vengono calcolate le distanze tra il valore per quella caratteristica del campione di test sconosciuto e i centroidi precedentemente calcolati (uno per ogni classe) sempre per quella caratteristica specifica.

Queste distanze, calcolate per ciascuna caratteristica del campione di test sconosciuto, sono inviate all'interno di un algoritmo multi-laterazione in cui il risultato sono le coordinate all'interno dello spazio simplex. Dopo aver calcolato le coordinate di ciascuna caratteristica del campione di test, è valutato il baricentro. Successivamente viene calcolato il baricentro tenendo conto delle coordinate di ciascuna caratteristica del campione di test all'interno dello spazio simplex. Il risultato di questo calcolo del baricentro sono le coordinate finali del campione di test. Ciò è stato ottenuto proiettandolo all'interno dello spazio simplex. Il campione di test è classificato come appartenente alla classe più vicina (appartenenza), rispetto alla metrica di distanza utilizzata, alle coordinate del baricentro nello spazio simplex costruito ad hoc. I risultati ottenuti dalle sperimentazioni, sia per quanto riguarda gli approcci non supervisionati che quello supervisionato sono di interesse, in particolare i risultati ottenuti con il sistema Vertex, che superano lo stato dell'arte, dove il sistema VFC con Kernel lineare ottiene il 95,69% di precisione. Inoltre, le qualità dell'algoritmo VFC non sono solo riscontrabili in precisione, ma bensì anche sul tempo di addestramento, che risulta essere spesso di appena pochi millisecondi, o nel caso di utilizzo della KPCA sono necessari alcuni secondi aggiuntivi. Pertanto, questa soluzione è assolutamente utilizzabile in contesto reale e modalità real time.

Gli elementi e le caratteristiche illustrate nelle diverse forme di realizzazione preferite possono essere combinate senza peraltro uscire dall'ambito di protezione della presente domanda.

Bibliografia:

[1] Omar, M. Insider Threats: Detecting and Controlling. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism; IGI Global: Hershey, PA, USA, 2015; p. 162.

[2] Barrios, R.M. A multi-leveled approach to intrusion detection and the insider threat. J. Inf. Secur. 2013, 4, 54–65.

[3] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.

[4] European Union Agency for Network and Information Security (ENISA). ENISA Threat Landscape Report. 15 Top Cyber-Threats and Trends, Heraklion. 2016. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/

[5] European Union Agency for Network and Information Security (ENISA). ENISA Threat Landscape Report. 15 Top Cyber-Threats and Trends, Heraklion. 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[6] European Union Agency for Network and Information Security (ENISA). ENISA Threat Landscape Report. Insider threat. 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat

[7] CPNI Insider Data Collection Study. Centre for the Protection of National Infrastructure: London, UK, 2013. https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-studyreport-of-main-findings.pdf

[8] Warkentin, M.; Willison, R. Behavioral and policy issues in information systems security: The insider threat. Eur. J. Inf. Syst. 2009, 18, 101–112.

[9] Yang, S.C.; Wang, Y.L. Insider threat analysis of case based system dynamics. Adv. Comput. Int. J. ACIJ 2011, 2, 1–17.

[10] Eldardiry, H., Bart, E., Liu, J., Hanley, J., Price, B., & Brdiczka, O. (2013, May). Multi-domain information fusion for insider threat detection. In 2013 IEEE Security and Privacy Workshops (pp. 45-51). IEEE.

[11] Dentamaro, V., Impedovo, D., Pirlo, G., & Massaro, A. (2020, May). Vertex Feature Classification (VFC). In 2020 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS) (pp. 1-8). IEEE.

RIVENDICAZIONI

1. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office, detto metodo è caratterizzato dal fatto di comprendere le seguenti fasi:
    a. registrare l'accesso dell'operatore al sistema informativo aziendale (111)
    b. classificare la tipologia di operazione svolta tramite richiesta di autodichiarazione da parte dell'operatore attraverso opportune interfacce grafiche (113,114).
    c. registrare l'attività dell'operatore di accesso e modifica dei dati del sistema informativo aziendale (115,131), nonché dell'accesso a siti esterni tramite web browser (122).
    d. classificare tentativi di inferenza da parte dell'operatore verso dati presenti nel sistema informativo aziendale normalmente non accessibili sulla base dei livelli di accesso stabiliti, da effettuarsi tramite rete neurale (117).
    e. classificare le operazioni anomale svolte con navigazione in web browser e accesso a portali esterni, effettuata tramite rete neurale (126).
    f. classificare le anomalie nei records registrati nel sistema informativo aziendale, effettuata tramite algoritmo Vertex Feature Classification (132).
    g. classificare le anomalie globali di sicurezza tramite motore inferenziale con utilizzo di logiche fuzzy al fine di combinare i risultati delle altre classificazioni di cui ai punti precedenti sulla base di policy di sicurezza decise dall'amministratore di sistema (140).
2. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la rivendicazione 1, in cui detto accesso da parte dell'operatore avviene attraverso un sistema di autenticazione sicuro multifattore.
3. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la rivendicazione 1, in cui detta classificazione dei tentativi di inferenza avviene tramite modello di rete neurale di tipo convoluzionale (CNN) addestrata al minimo sui seguenti input: codice identificativo cliente, codice identificativo dell'operatore che esegue la query, codice identificativo dell'operatore oggetto della ricerca, codice identificativo della sede oggetto della ricerca, numero di operazioni (tuple) restituite dalla query, numero di query effettuate nello stesso giorno con chiave di ricerca per cliente, associazione del servizio ad altre tipologie di servizi, valore booleano attestante il tentativo di inferenza.
4. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la

rivendicazione 1, in cui detta classificazione delle operazioni anomale avviene tramite modello di rete neurale con concatenazione di reti neurali ricorsive (del tipo Long Short Term Memory) e convoluzionali (CNN).

5. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la rivendicazione 4, in cui detta classificazione delle operazioni anomale svolte con navigazione in web browser avviene tramite modello di rete neurale con concatenazione di reti neurali ricorsive (del tipo Long Short Term Memory) e convoluzionali (CNN) secondo lo schema in figura 3.
6. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la rivendicazione 5, in cui detto modello di rete neurale viene addestrato al minimo con i seguenti dati in input per la rete LSTM (303'): sequenza dei tempi di sosta sui singoli URL durante l'operazione, sequenza dello score reputazionale dei singoli URL visitati (ottenuto tramite API da web service dedicato allo scopo), sequenza di valori derivata dalla vettorializzazione tramite tecniche di Natural Language Processing dei token utilizzati nella descrizione dell'URL.
7. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la rivendicazione 5, in cui detto modello di rete neurale viene addestrato al minimo con i seguenti dati in input per la rete CNN (303''): tempo totale dell'operazione, valore boleano che contrassegna se l'attività è stata svolta in orario lavorativo previsto per le attività specifiche (0) oppure in altre fasce orarie (1), numero di link visitati durante una singola sessione per lo svolgimento di un'operazione, tempo medio in secondi speso su un singolo URL durante l'operazione, numero di visite al dominio visitato più frequentemente durante una singola operazione, score reputazionale dell'URL visitato più frequentemente durante l'operazione (ottenuto tramite API da web service dedicato allo scopo).
8. Metodo per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office secondo la rivendicazione 1, in cui detto algoritmo Vertex Feature Classification di classificazione le anomalie nei records registrati nel sistema informativo aziendale viene addestrato al minimo su un set di variabili in input riferiti all'anagrafica cliente o al risultato dell'operazione.
9. Sistema per l'individuazione di anomalie di sicurezza nell'utilizzo di dati contenuti in database multi-accesso nell'ambito di servizi front-office e back-office in accordo con una

qualunque delle rivendicazioni da 1 a 8, detto metodo è caratterizzato dal fatto di comprendere:

a. Un modulo di gestione degli accessi (110) comprendente:
    i. Un'interfaccia di accesso operazione (111) in cui l'operatore deve accedere attraverso un sistema di autenticazione sicuro (es. Multi Factor Authentication).
    ii. Un filtro multilivello (112) atto ad attribuire un set di privilegi di accesso e scrittura ai dati in base all'operatore.
    iii. Un'interfaccia per l'avvio e la conclusione di una nuova operazione su cliente (113) o nuova operazione interna (114), in cui l'operatore deve dichiarare un set di parametri, al minimo: tipologia di operazione, avvio dell'operazione, cliente di riferimento (nel caso di 113), conclusione dell'operazione.
    iv. Un'interfaccia di accesso ai dati statistici delle operazioni effettuate (115) in cui l'operatore, a prescindere dai privilegi di accesso, può effettuare query in lettura su un set limitato di dati aggregati relativi alle statistiche delle operazioni effettuate.
    v. Un dizionario delle query e associazioni tra i servizi (116) popolato dalle query effettuate tramite (115) con indicazione di un set di parametri descrittivi della stessa, al minimo: tipologia di query, data, operatore autore della query, numero totale delle tuple restituite dalla query.
    vi. Un classificatore delle query ambigue e controllo dell'inferenza (117), realizzato attraverso una rete neurale convoluzionale (CNN) per la classificazione delle query ambigue riferibili a tentativi di inferenza da parte degli operatori per l'accesso a dati di cui non dispongono dei permessi di visualizzazione necessari.
b. Un modulo di monitoraggio WEB (120) comprendente:
    i. Un metodo di Single Sign On (121) attivato dall'avvio di una nuova operazione su cliente (113) tramite cui l'operatore può accedere un'unica volta con una sola coppia di credenziali alle applicazioni web necessarie all'espletamento dell'operazione.
    ii. Un metodo di monitoraggio della sessione web (122) tale da permettere la registrazione di log di navigazione (cronologia web) associati all'operazione (113).

iii. Un metodo di estrazione di feature dal contenuto in linguaggio naturale dei descrittori dei siti web visitati tramite tecniche di Natural Language Processing (123).

iv. Un metodo di associazione dei siti web visitati ad uno score di reputazione web (124) tramite l'utilizzo di Application Programming Interface verso servizi in cloud di monitoraggio della web reputation.

v. Un metodo di preprocessing delle sequenze di navigazione web (125) finalizzato all'estrazione di un set di feature utile a descrivere il comportamento dell'operatore durante l'esecuzione dell'operazione (come da modalità di attuazione esemplificativa descritta in seguito)

vi. Un metodo di classificazione delle operazioni anomale svolte nel web (126), effettuata tramite reti neurali ricorsive (Long Short Term Memory) e convoluzionali concatenate.

c. Un modulo di monitoraggio operazioni su sistema informativo aziendale (es. ERP) (130) comprendente:

i. Un metodo di preprocessing dei dati riferiti ai records delle operazioni presenti nel sistema informativo aziendale (131).

ii. Un metodo di classificazione tramite Vertex Feature Classification per l'individuazione di operazioni anomale (132).

d. Un modulo di motore inferenziale (140) per la classificazione di anomalie di sicurezza dei dati secondo logiche fuzzy, comprendente:

i. Un metodo per il buffering dei dati (141) ottenuti dalle classificazioni dei moduli connessi (110,120,130);

ii. Un metodo per la progettazione e configurazione di regole inferenziali secondo logiche fuzzy (142) (ad esempio implementabile con strumenti tecnici esistenti come software CLIPS o libreria python Experta) ;

iii. Un metodo per il confronto (143) dei dati ottenuti (141) con le regole impostate (142).

iv. Un metodo per l'esecuzione (144) delle regole applicabili nel caso osservato (singola operazione).

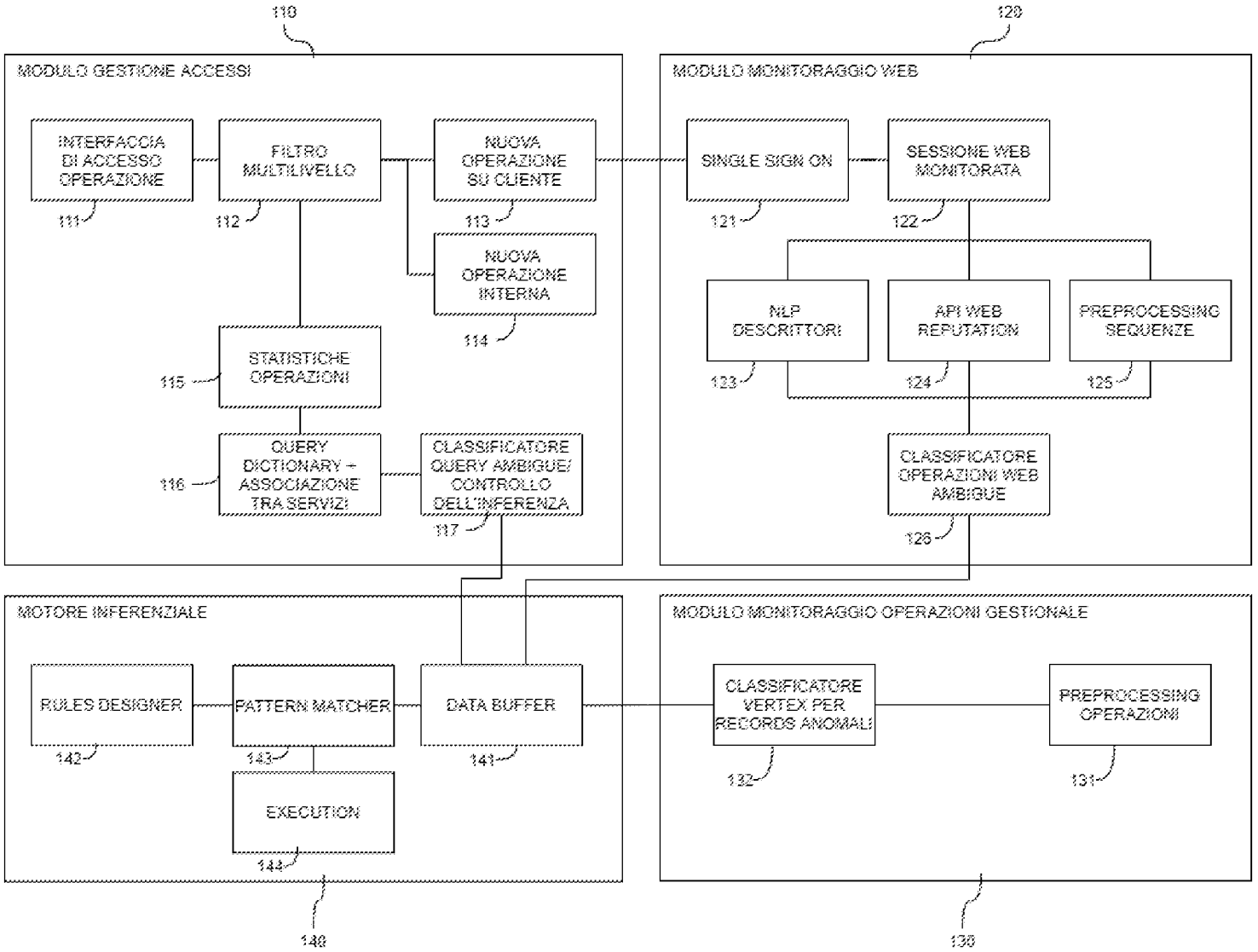
110
MODULO GESTIONE ACCESSI
INTERFACCIA DI ACCESSO OPERAZIONE
111
FILTRO MULTILIVELLO
112
NUOVA OPERAZIONE SU CLIENTE
113
NUOVA OPERAZIONE INTERNA
114
STATISTICHE OPERAZIONI
115
QUERY DICTIONARY + ASSOCIAZIONE TRA SERVIZI
116
CLASSIFICATORE QUERY AMBIGUE/ CONTROLLO DELL'INFERENZA
117
120
MODULO MONITORAGGIO WEB
SINGLE SIGN ON
121
SESSIONE WEB MONITORATA
122
NLP DESCRITTORI
123
API WEB REPUTATION
124
PREPROCESSING SEQUENZE
125
CLASSIFICATORE OPERAZIONI WEB AMBIGUE
126
MOTORE INFERENZIALE
RULES DESIGNER
142
PATTERN MATCHER
143
DATA BUFFER
141
EXECUTION
144
140
MODULO MONITORAGGIO OPERAZIONI GESTIONALE
CLASSIFICATORE VERTEX PER RECORDS ANOMALI
132
PREPROCESSING OPERAZIONI
131
130

FIG. 1

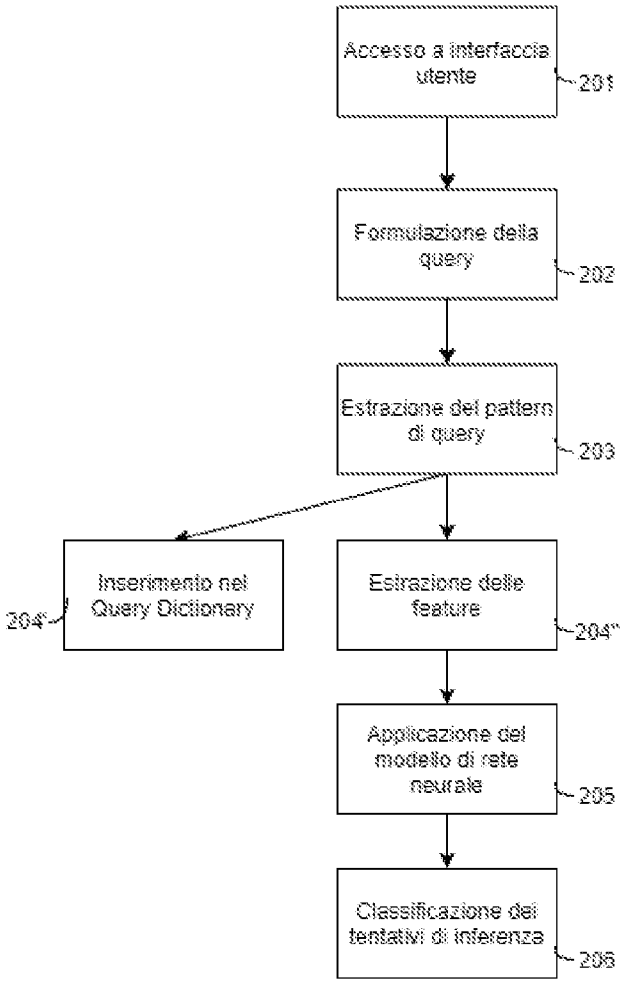
Accesso a interfaccia utente
201
Formulazione della query
202
Estrazione del pattern di query
203
Inserimento nel Query Dictionary
204'
Estrazione delle feature
204"
Applicazione del modello di rete neurale
205
Classificazione dei tentativi di inferenza
206

FIG. 2

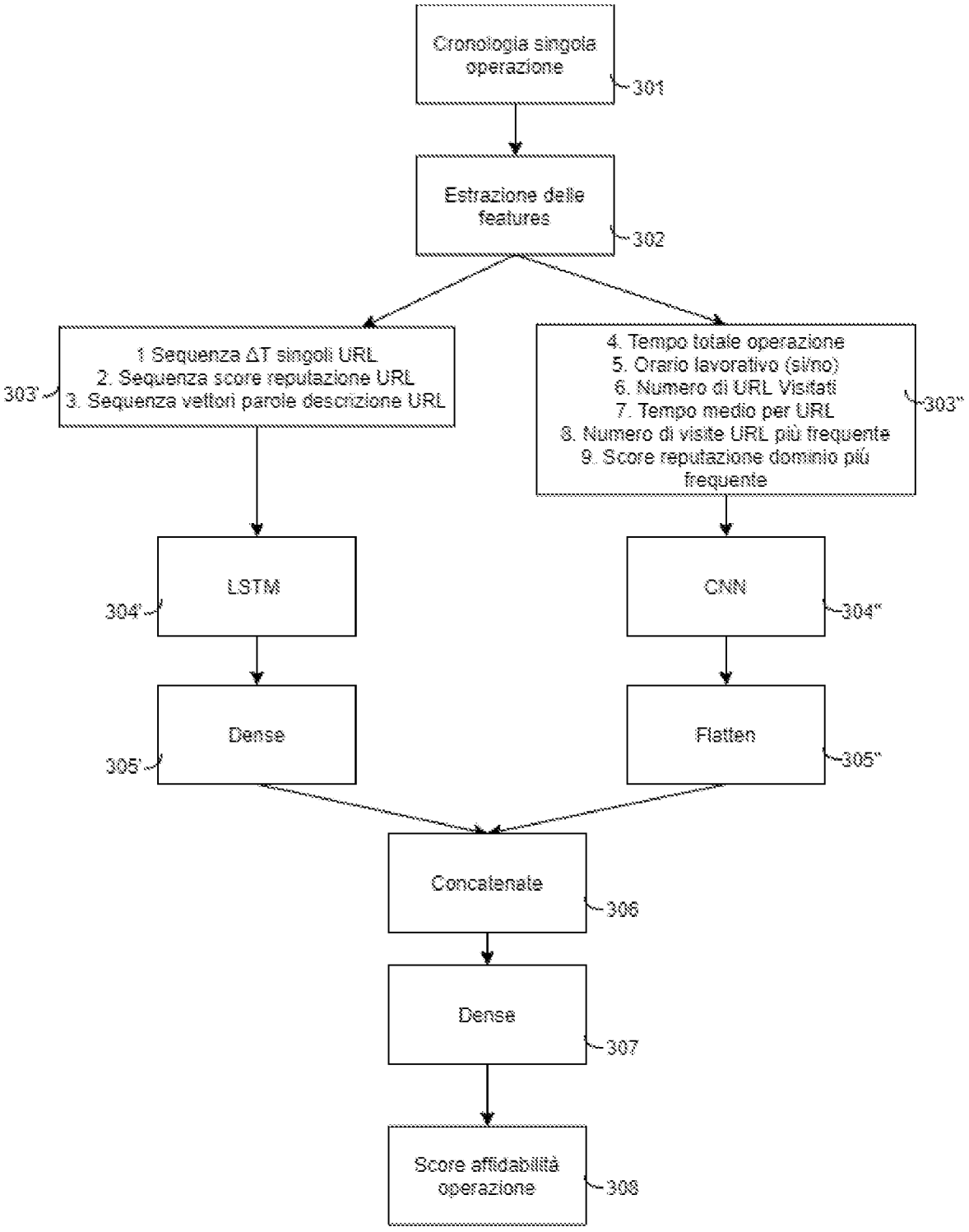
Cronologia singola operazione
301
Estrazione delle features
302
1. Sequenza ΔT singoli URL
2. Sequenza score reputazione URL
3. Sequenza vettori parole descrizione URL
303'
4. Tempo totale operazione
5. Orario lavorativo (si/no)
6. Numero di URL Visitati
7. Tempo medio per URL
8. Numero di visite URL più frequente
9. Score reputazione dominio più frequente
303''
LSTM
304'
CNN
304''
Dense
305'
Flatten
305''
Concatenate
306
Dense
307
Score affidabilità operazione
308

FIG. 3

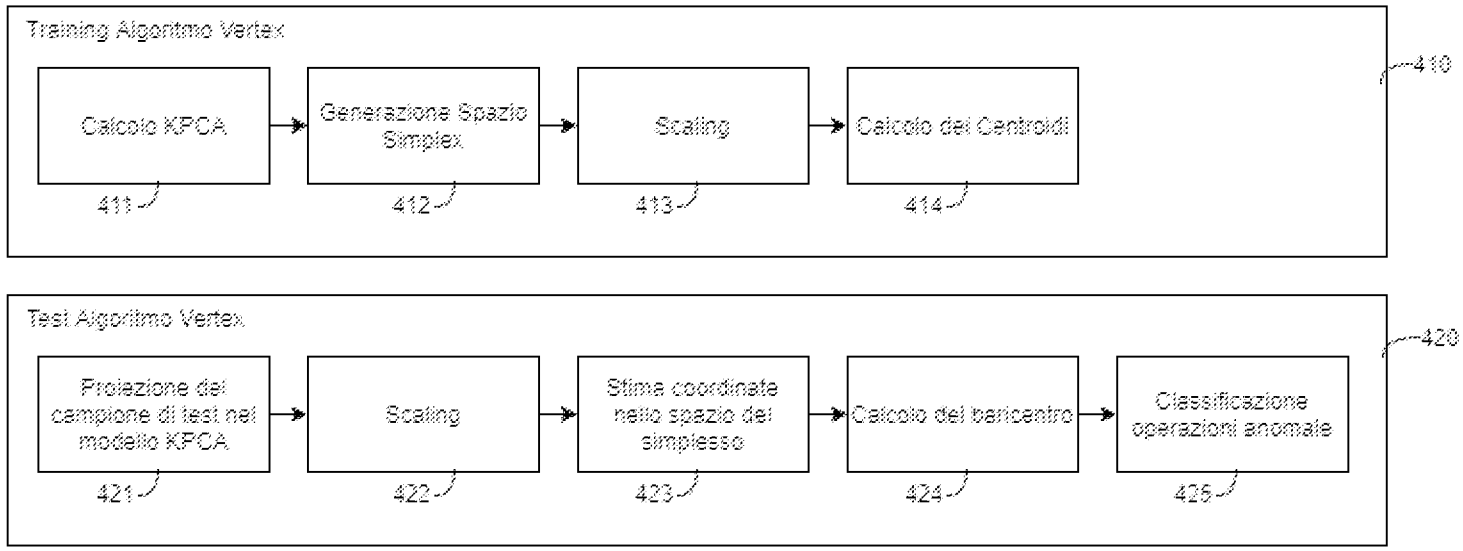
Training Algoritmo Vertex
Calcolo KPCA
Generazione Spazio Simplex
Scaling
Calcolo dei Centroidi
411
412
413
414
410
Test Algoritmo Vertex
Proiezione del campione di test nel modello KPCA
Scaling
Stima coordinate nello spazio del simplesso
Calcolo del baricentro
Classificazione operazioni anomale
421
422
423
424
425
420

FIG. 4