Rilevamento delle Intrusioni Attraverso Tecniche di Ensemble

Tesi di Laurea Magistrale in Ingegneria Informatica

Felice Maria D'Anna

Relatore: Prof. Giuseppe Lo Re

Correlatori: Ing. Vincenzo Agate

UNIVERSITÀ DEGLI STUDI DI PALERMO

FACOLTÀ DI INGEGNERIA

LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

RILEVAMENTO DELLE INTRUSIONI ATTRAVERSO TECNICHE DI ENSEMBLE

Tesi di Laurea di
Dott. Felice Maria D'Anna

Relatore:
Ch.mo Prof. Giuseppe Lo Re

Controrelatore:

Correlatore:
Ing. Vincenzo Agate

Anno Accademico 2022/2023

UNIVERSITÀ DEGLI STUDI DI PALERMO
FACOLTÀ DI INGEGNERIA

LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

RILEVAMENTO DELLE INTRUSIONI ATTRAVERSO TECNICHE DI ENSEMBLE

Tesi di Laurea di
Dott. Felice Maria D'Anna

Relatore:
Ch.mo Prof. Giuseppe Lo Re

Controrelatore:

Correlatore:
Ing. Vincenzo Agate

Sommario

Il continuo sviluppo di tecnologie e servizi digitali erogati attraverso Internet ha permesso all'informatica di permeare in molti aspetti fondamentali della nostra vita. Ciò si traduce in un aumento della quantità e del valore delle informazioni che transitano sulla rete, il quale spinge i criminali informatici a sviluppare tecniche di attacco sempre più avanzate e sofisticate. Conseguentemente l'interesse da parte delle società e delle organizzazioni governative nei confronti della sicurezza informatica ha subito un forte incremento. I sistemi di rilevamento delle intrusioni (IDS) svolgono un ruolo fondamentale nella sicurezza dell'ICT. Essi, infatti, sono in grado di rilevare degli attacchi informatici e talvolta anche di identificarne la tipologia ed hanno, inoltre, il compito di segnalare tempestivamente le intrusioni agli amministratori al fine di contrastare tali attacchi. Di conseguenza, è fondamentale che gli avvisi generati dagli IDS siano il più tempestivi e dettagliati possibile. In questo lavoro di tesi, viene presentato un *IDS behavior-based* strutturato su due livelli in grado di identificare gli attacchi che sfruttano la rete. Il primo layer del sistema proposto è costituito da un *Decision Tree* ed ha il compito di classificare in maniera binaria il traffico di rete, discriminando il traffico malevolo da quello benigno. Il secondo layer analizza il traffico etichettato come malevolo dal primo layer ed effettua una classificazione più dettagliata identificandolo tra 12 possibili classi di attacco, oltre a quella relativa al traffico benigno. Questo layer impiega un modello di *ensemble learning* per effettuare la classificazione. Tale modello è composto da quattro diversi *weak learner*: un *Random Forest*, un *XGBoost*, un *Extra Tree* ed un *k-NN*. Il sistema proposto permette, attraverso l'uso

del primo layer, di filtrare immediatamente il traffico benigno in modo da non sovraccaricare il sistema e conseguentemente permetterne una maggiore reattività nel rilevamento di intrusioni. La valutazione sperimentale eseguita utilizzando il dataset pubblico CIC-IDS2017 mostra che il sistema è in grado di rilevare gli attacchi in tempo reale e con prestazioni elevate in termini delle principali metriche di valutazione.

Indice

Introduzione

La crescente disponibilità di servizi offerti attraverso Internet e conseguentemente di dispositivi connessi in rete, genera un'immensa quantità di dati. I protocolli e le modalità di accesso e di interazione tra sistemi e servizi connessi a Internet creano per i malintenzionati nuove opportunità e metodologie di attacco.

Negli ultimi decenni si è assistito ad un continuo e crescente sviluppo di sistemi digitali connessi in rete, talvolta annegati in altri sistemi più grandi. Spesso si parla di *smart cities*, *smart home* ovvero di dispositivi digitali, nella maggior parte dei casi connessi in rete, che gestiscono e monitorano diversi processi fisici. I progetti riguardanti le *smart cities* generalmente comprendono sistemi di gestione automatica ed efficiente dell'energia, ed insiemi di sensori ed attuatori distribuiti in tutta la città che permettano ai sistemi centralizzati di aggregare dati ed analizzarli. La domotica permette di automatizzare e di gestire in maniera efficiente un ambiente domestico, ad esempio, un sistema domotico può gestire i processi di climatizzazione di un appartamento regolando in modo efficiente il consumo di energia. Altri sistemi intelligenti vengono utilizzati nelle industrie o nelle aziende. Oltre ai sistemi intelligenti, ogni giorno vengono utilizzati milioni di dispositivi come smartphone, computer, tablet. Gran parte di tali sistemi connessi in rete gestisce, genera o interagisce con dati e informazioni che hanno una rilevanza anche all'esterno del mondo digitale.

La vita di un uomo ormai è talmente legata a tali dispositivi che non può prescinderne in una società moderna. Certe infrastrutture connesse in rete e Internet stesso rivestono un ruolo così importante per gli stati da essere considerate *infrastrutture critiche*. Infrastrutture, quindi, la cui manomissione avrebbe conseguenze catastrofiche non su un singolo cittadino o utente, ma sulla stabilità economica e sociale di un intera nazione. Un'analisi specifica sull'impatto di attacchi cibernetici alle infrastrutture critiche viene svolto in [1].

La sicurezza di questi *device* e, più in generale, delle infrastrutture che compongono e che fanno parte di Internet assume un ruolo centrale nello sviluppo, nella manutenzione e nel

Figura 1: Attacchi informatici registrati a livello globale per anno dal 2018 al 2022 (**Immagine tratta da:** [2])

monitoraggio di nuovi sistemi.

La sempre maggiore interconnessione tra il mondo digitale e quello fisico rende le minacce informatiche ancora più serie e pericolose. L'intrusione da parte di un malintenzionato all'interno di tali dispositivi elettronici può, infatti, avere conseguenze anche fisiche sugli utenti. Si pensi, ad esempio, alla manomissione di un dispositivo di *healthcare*, o di un veicolo a guida autonoma connesso in rete.

Il Rapporto Clusit [1] 2023[2], analizza gli attacchi informatici che hanno colpito l'Italia e il resto del mondo nell'arco del 2022 e dei quattro anni precedenti evidenziando come negli ultimi anni il numero di attacchi informatici è in continua crescita, com'è possibile vedere nella Figura 1. Nel 2022 sono stati registrati 2489 attacchi, il numero di attacchi più alto di sempre, e come si può vedere dal grafico il trend non accenna a scendere.

È interessante ed importante notare come le situazioni geopolitiche si ripercuotano nel numero di attacchi e nella tipologia di attacchi. Osservando il grafico in Figura 2 è possibile notare, ad esempio, come nel 2020 gli attacchi di spionaggio/sabotaggio abbiano raggiunto il massimo degli ultimi quattro anni e questo è dovuto in particolare a causa delle azioni di spionaggio industriale legato al Covid nei confronti di laboratori, cliniche ed enti di ricerca. Un altro valore interessante è quello riguardante gli attacchi di *Information Warfare* ed *Attivismo*

[1] **Clusit**: Associazione Italiana per la Sicurezza Informatica. Link: https://clusit.it/rapporto-clusit/

Figura 2: Distribuzione dei tipi di attacchi informatici a livello globale per anno dal 2018 al 2022 (**Immagine tratta da:** [2])

che hanno raggiunto il loro picco proprio nel 2022. Fattore certamente legato almeno in parte alla guerra in Ucraina che oltre agli attacchi di information warfare ha stimolato attacchi da parte degli "hacktivisti".

Il dato più preoccupante però prescinde dalle situazioni geopolitiche o dallo spionaggio industriale ed è dovuto alla categoria del *cybercrime*, tale categoria è quella che negli ultimi quattro anni ha continuato ad avere una crescita costante, com'è possibile notare dal grafico. Il fatto che i crimini informatici siano in aumento evidenzia ancora di più quanto sia importante il ruolo della sicurezza informatica nelle infrastrutture e nei sistemi digitali. La maggior parte degli attacchi hanno come vittime "*multiple targets*" ovvero entità che non costituiscono obiettivi specifici dell'attacco, ma che rimangono vittime di attacchi che mirano a colpire una grande varietà di utenti, come ad esempio gli attacchi di *phishing*. Gli obiettivi più colpiti nel 2022 oltre a quelli appena citati, sono sistemi impiegati nell'ambito dell'*healthcare*, i sistemi governativi ed i sistemi e le infrastrutture ICT. Gli attacchi che hanno come obiettivo le tipologie di vittime appena descritte costituiscono il 57,7% della totalità degli attacchi rilevati nel 2022 a livello globale.

Alcune delle tecniche utilizzate non sono così all'avanguardia, ma costituiscono minacce che un utente medio dovrebbe essere in grado di riconoscere, un esempio sono gli attacchi di *phishing* o l'utilizzo di password deboli che vengono facilmente scoperte dai malintenzionati.

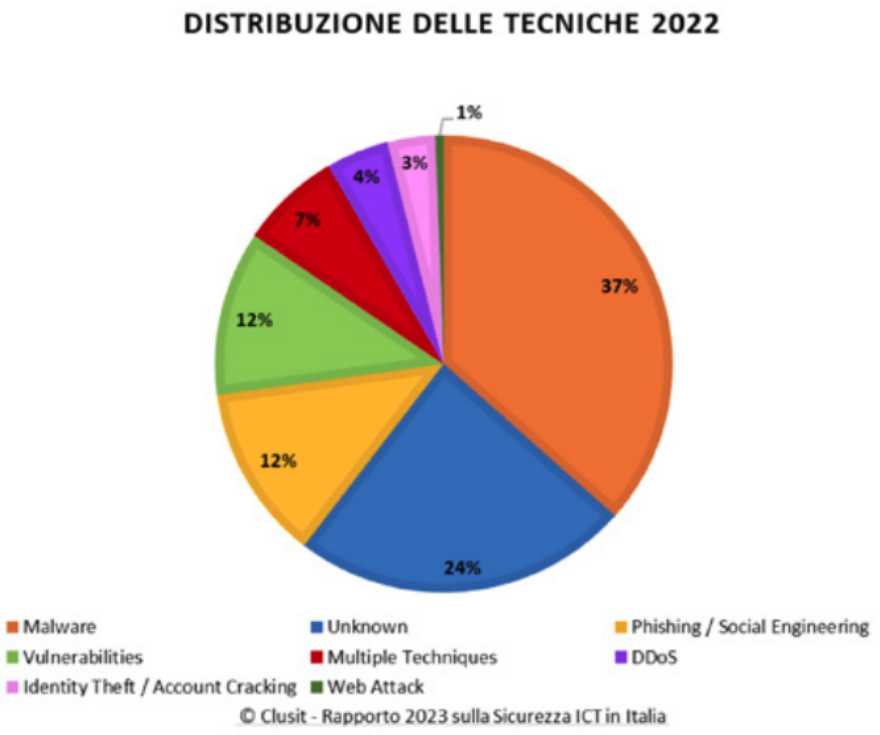

Figura 3: Distribuzione delle tecniche di attacchi informatici a livello globale relative al 2022 (**Immagine tratta da:** [2])

La Figura 3 riporta una distribuzione delle tecniche di attacco utilizzate a livello globale nel 2022. Il 37% degli attacchi globali è dovuto ai *malware*, il 12% ad attacchi di *phishing* o di *ingegneria sociale*.

Il Report Clusit mostra come gli attacchi informatici siano in crescita e conseguentemente quanto sia importante investire nella sicurezza dei sistemi informatici.

La *cybersecurity* ha, infatti, lo scopo di offrire protezione ad un sistema informatico e di preservarne la riservatezza, l'integrità e la disponibilità delle risorse. Queste tre proprietà garantiscono rispettivamente che i dati non siano accessibili o visibili ad entità non autorizzate, che questi non abbiano subito modifiche o manomissioni in maniera illegittima e che i servizi siano prontamente accessibili ed utilizzabili dalle entità legittimate.

Un attacco informatico, o intrusione, consiste in una qualsiasi azione offensiva che ha come obiettivo sistemi informatici, dispositivi elettronici o infrastrutture e la cui finalità sia il furto,

la manipolazione o, talvolta, la distruzione di informazioni o l'alterazione del normale funzionamento di un sistema informatico. I cyberattack possono essere categorizzati come passivi o attivi.

Gli attacchi passivi non prevedono nessuna manomissione, ma piuttosto un intenso monitoraggio dei canali di trasmissione. Lo scopo degli attacchi passivi è quindi quello di acquisire o inferire informazioni attraverso l'intercettazione di comunicazioni. Questi attacchi possono essere prevenuti utilizzando dei meccanismi di sicurezza quali la cifratura, che rende un messaggio intellegibile alle sole entità che conoscono la chiave segreta per decifrarlo, o altri servizi quali l'autenticazione e la verifica dell'integrità dei dati che usano opportuni meccanismi di sicurezza tra cui rispettivamente le *Digital Signature* o i *Message Authentication Code* (MAC).

A differenza di quelli passivi gli attacchi informatici attivi prevedono una qualche manomissione, come ad esempio, la modifica, l'inserimento o la cancellazione di informazioni o il sabotaggio di un servizio in modo da renderlo inaccessibile agli utenti legittimi. Gli attacchi attivi sono difficili da prevenire a causa delle molteplici possibili vulnerabilità della rete, dei software o dei protocolli. Per tali attacchi, l'obiettivo principale è quello di rilevarli ed agire immediatamente in modo da recuperare e riprendere quanto più velocemente il normale funzionamento del sistema.

Il rilevamento degli attacchi informatici viene effettuato utilizzando opportuni sistemi di monitoraggio chiamati *Intrusion Detection System* (IDS).

Gli IDS sono sistemi di rilevamento delle anomalie in grado di individuare deviazioni dal normale funzionamento nel traffico della rete o nel comportamento di un software riconducibili ad un attacco informatico o ad un *malware*. Per consentire a tali sistemi di rilevare possibili anomalie è necessario un continuo monitoraggio dei dispositivi o delle infrastrutture nei quali gli IDS sono installati.

Una volta rilevato un attacco, un IDS lo notifica agli amministratori dando informazioni sulla tipologia di attacco identificata in modo tale da consentire loro di intervenire nel modo più adeguato possibile. Il tempo costituisce un fattore di fondamentale importanza. Un attacco rilevato troppo tardi potrebbe, infatti, provocare danni catastrofici al sistema monitorato rendendo quindi vano il rilevamento da parte dell'IDS.

Gli *intrusion detection system* possono essere estesi in modo da effettuare anche operazioni orientate alla mitigazione dell'attacco, oltre al rilevamento dello stesso. Questi sono detti sistemi di rilevamento e prevenzione delle intrusioni (IDPS). Un IDPS, una volta rilevato un attacco,

può, oltre a mandare il segnale di allarme, effettuare delle azioni quali, ad esempio, il blocco di pacchetti provenienti da un certo indirizzo IP.

Questa tesi presenta un *Intrusion Detection System behavior-based*, progettato ed implementato utilizzando un'architettura *multi-layer*. Il sistema proposto è composto da due livelli, il primo, implementato attraverso un *Decision Tree*, effettua una classificazione binaria discriminando il traffico tra normale ed anomalo. Il secondo layer è costituito da quattro classificatori eterogenei le cui predizioni vengono aggregate da un algoritmo di *ensemble learning*. I classificatori che compongono il modello *ensemble* sono: un *Random Forest*, un *XGBoost*, un *Extra Tree* ed un *k-NN*. Lo scopo del secondo layer è quello di fornire una classificazione più dettagliata degli attacchi specificandone la tipologia tra 13 possibili classi, di cui 12 corrispondenti ad attacchi ed una relativa al traffico benigno. Una classificazione più dettagliata di un attacco è fondamentale al fine di consentire agli amministratori di operare per la mitigazione dello stesso.

I successivi capitoli di questa tesi sono organizzati come segue:

- Il **capitolo 1** presenta una panoramica sugli *Intrusion Detection System* e descrive le diverse categorie e le problematiche correlate.
- Il **capitolo 2** descrive lo stato dell'arte relativo ai sistemi di rilevamento delle intrusioni analizzando i pro e i contro relativi ai modelli proposti in letteratura ed analizzando i diversi dataset utilizzati per la costruzione degli IDS.
- Il **capitolo 3** presenta l'architettura del sistema proposto descrivendo il primo ed il secondo layer del sistema, i modelli che lo compongono ed il loro funzionamento.
- Il **capitolo 4** presenta le impostazioni sperimentali e le elaborazioni condotte sul dataset prima dell'effettiva fase di valutazione dei modelli.
- Il **capitolo 5** presenta la valutazione sperimentale condotta sui modelli che compongono il sistema, sul modello *ensemble* e sul sistema complessivo.

Capitolo 1

Gli Intrusion Detection System

Gli *Intrusion Detection System* sono dei sistemi di rilevamento delle anomalie specializzati nell'individuazione di irregolarità riconducibili ad un'intrusione informatica [3, 4]. Gli IDS sono sempre affiancati da esperti di *cybersecurity* o da sistemi che si occupano della mitigazione vera e propria di un attacco. I sistemi di rilevamento, infatti, si limitano soltanto ad individuare un attacco ed eventualmente ad identificarne la tipologia inoltrando una notifica riguardante l'attacco rilevato agli amministratori.

OMISSIS

Capitolo 2

Stato dell'arte

In questo capitolo verranno esaminati gli sviluppi più recenti riguardo gli *intrusion detection system* analizzando i sistemi proposti dalla comunità scientifica negli ultimi anni. Nella seconda parte del capitolo verranno descritti e analizzati i principali dataset utilizzati per l'addestramento e la valutazione dei modelli che compongono un sistema di rilevamento.

2.1 Stato dell'arte degli IDS

OMISSIS

2.2 Dataset esistenti

OMISSIS

Capitolo 3

Sistema proposto

In questo lavoro di tesi, viene proposto un IDS *behavior-based* a più livelli che utilizza l'*ensemble learning* per aggregare i risultati ottenuti dai classificatori che lo compongono. Tale sistema non classifica il traffico solamente come benigno o dannoso, come molti dei sistemi proposti, ma è in grado di identificare e categorizzare tale traffico tra 12 possibili classi di attacco in aggiunta alla classe relativa al traffico benigno. L'architettura del sistema proposto è strutturata su due livelli come illustrato nella Figura **??**.

In questo capitolo verrà esaminato il sistema proposto dal punto di vista architetturale analizzando nel paragrafo successivo il primo livello, passando poi all'analisi del secondo livello ci si soffermerà sui singoli modelli che compongono l'*ensemble* e, infine, sull'*ensemble* stesso.

OMISSIS

3.0.1 Decision Tree

OMISSIS

3.1 Secondo Layer

OMISSIS

3.1.1 Random Forest

OMISSIS

3.1.2 Extra Tree

OMISSIS

3.1.3 XGBoost

OMISSIS

3.1.4 K-Nearest Neighbors

OMISSIS

3.1.5 Ensemble

OMISSIS

Capitolo 4

Setting sperimentale

Questo capitolo, nel quale viene descritto il *setting sperimentale*, si apre con una introduzione riguardante le metriche di valutazione generalmente utilizzate per i modelli di classificazione. Verrà poi presentato il dataset e verranno descritte le elaborazioni eseguite in fase di *preprocessing* e di *feature selection* del dataset. Infine, verrà descritto il processo di analisi delle componenti principali e quello di generazione dei campioni sintetici.

4.1 Metriche di valutazione

OMISSIS

Confusion Matrix

OMISSIS

False Positive Rate (FPR)

OMISSIS

False Negative Rate (FNR)

OMISSIS

Accuracy

OMISSIS

Precision

OMISSIS

Recall

OMISSIS

F1-score

OMISSIS

4.2 Dataset utilizzato

OMISSIS

4.2.1 Principal Component Analysis

OMISSIS

4.2.2 Data Augmentation

OMISSIS

Capitolo 5

Valutazione sperimentale

In questo capitolo verranno trattate le valutazioni sperimentali condotte sul dataset CIC-IDS2017 e verranno analizzate l'influenza della *Principal Component Analysis* e dell'algoritmo di *Data Augmentation* sulle prestazioni dei modelli che costituiscono l'IDS proposto.

OMISSIS

5.1 Valutazione del primo layer

OMISSIS

5.1.1 Valutazione sul dataset standardizzato

OMISSIS

5.1.2 Valutazione sul dataset trasformato con PCA

OMISSIS

5.2 Valutazione del secondo layer

OMISSIS

5.2.1 Valutazione Random Forest

OMISSIS

5.2.2 Valutazione XGBoost

OMISSIS

5.2.3 Valutazione Extra Tree

OMISSIS

5.2.4 Valutazione k-NN

OMISSIS

Conclusioni

In questo lavoro è stato presentato un Sistema di Rilevamento delle Intrusioni *behavior-based* che analizza il traffico di rete per individuare eventuali attacchi informatici. L'IDS proposto è un sistema *multi-layer* composto da due livelli, di cui il primo, costituito da un *Decision Tree* effettua una classificazione binaria, discriminando il traffico benigno da quello malevolo. Mentre, il secondo effettua una classificazione a grana fine sul traffico classificato dal primo layer come malevolo ed è capace di identificare 12 possibili classi di attacco oltre alla classe relativa al traffico benigno. Questo layer, utilizza un *ensemble* di classificatori composto da quattro modelli:

OMISSIS

Elenco delle figure

Bibliografia

[1] K. Thakur, M. L. Ali, N. Jiang e M. Qiu. «Impact of Cyber-Attacks on Critical Infrastructure». In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. 2016, pp. 183–186.

[2] Clusit. *Rapporto Clusit 2023 sulla sicurezza ICT*. 2023.

[3] R. Bace e P. Mell. «NIST special publication on intrusion detection systems». In: *National Institute of Standards and Technology* 16 (2001).

[4] R. G. Bace, P. Mell et al. «Intrusion detection systems». In: (2001).

[5] Y.-X. Ding, M. Xiao e A.-W. Liu. «Research and implementation on snort-based hybrid intrusion detection system». In: *2009 International Conference on Machine Learning and Cybernetics*. Vol. 3. 2009, pp. 1414–1418.

[6] L. Xiao, Y. Li, G. Han, G. Liu e W. Zhuang. «PHY-Layer Spoofing Detection With Reinforcement Learning in Wireless Networks». In: *IEEE Transactions on Vehicular Technology* 65.12 (2016), pp. 10037–10047.

[7] K. Sethi, R. Kumar, N. Prajapati e P. Bera. «Deep Reinforcement Learning based Intrusion Detection System for Cloud Infrastructure». In: *2020 International Conference on COMmunication Systems and NETworkS (COMSNETS)*. 2020, pp. 1–6.

[8] V. Agate, A. De Paola, G. Lo Re e M. Morana. «A platform for the evaluation of distributed reputation algorithms». In: *2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*. IEEE. 2018, pp. 1–8.

[9] J. H. Friedman. «Greedy function approximation: a gradient boosting machine». In: *Annals of statistics* (2001), pp. 1189–1232.

[10] A. Khraisat, I. Gondal, P. Vamplew e J. Kamruzzaman. «Survey of intrusion detection systems: techniques, datasets and challenges». In: *Cybersecurity* 2.1 (2019), pp. 1–22.

[11] V. Agate, A. De Paola, S. Gaglio, G. Lo Re e M. Morana. «A framework for parallel assessment of reputation management systems». In: *Proceedings of the 17th International Conference on Computer Systems and Technologies 2016*. 2016, pp. 121–128.

[12] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin e K.-Y. Tung. «Intrusion detection system: A comprehensive review». In: *Journal of Network and Computer Applications* 36.1 (2013), pp. 16–24. URL: https://www.sciencedirect.com/science/article/pii/S1084804512001944.

[13] T. N. Rincy e R. Gupta. «Ensemble Learning Techniques and its Efficiency in Machine Learning: A Survey». In: *2nd International Conference on Data, Engineering and Applications (IDEA)*. 2020, pp. 1–6.

[14] L. Haripriya e M. Jabbar. «Role of Machine Learning in Intrusion Detection System: Review». In: *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. 2018, pp. 925–929.

[15] J. Lansky, S. Ali, M. Mohammadi, M. K. Majeed, S. H. T. Karim, S. Rashidi, M. Hosseinzadeh e A. M. Rahmani. «Deep Learning-Based Intrusion Detection Systems: A Systematic Review». In: *IEEE Access* 9 (2021), pp. 101574–101599.

[16] V. Agate, A. De Paola, P. Ferraro, G. Lo Re e M. Morana. «SecureBallot: A secure open source e-Voting system». In: *Journal of Network and Computer Applications* 191 (2021).

[17] G. Mylavarapu, J. Thomas e A. K. TK. «Real-Time Hybrid Intrusion Detection System Using Apache Storm». In: *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*. 2015, pp. 1436–1441.

[18] A. H. Halbouni, T. S. Gunawan, M. Halbouni, F. A. A. Assaig, M. R. Effendi e N. Ismail. «CNN-IDS: Convolutional Neural Network for Network Intrusion Detection System». In: *2022 8th International Conference on Wireless and Telematics (ICWT)*. 2022, pp. 1–4.

[19] M. Al-Qatf, Y. Lasheng, M. Al-Habib e K. Al-Sabahi. «Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection». In: *IEEE Access* 6 (2018), pp. 52843–52856.

[20] X. Yuan, C. Li e X. Li. «DeepDefense: Identifying DDoS Attack via Deep Learning». In: *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*. 2017, pp. 1–8.

[21] H. Liu, B. Lang, M. Liu e H. Yan. «CNN and RNN based payload classification methods for attack detection». In: *Knowledge-Based Systems* 163 (2019), pp. 332–341. URL: https://www.sciencedirect.com/science/article/pii/S0950705118304325.

[22] V. Agate, F. M. D'Anna, A. De Paola, P. Ferraro, G. Lo Re e M. Morana. «A behavior-based intrusion detection system using ensemble learning techniques». In: *ITASEC* (2022).

[23] S. Das, A. M. Mahfouz, D. Venugopal e S. Shiva. «DDoS Intrusion Detection Through Machine Learning Ensemble». In: *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. 2019, pp. 471–477.

[24] N. Moustafa, B. Turnbull e K.-K. R. Choo. «An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things». In: *IEEE Internet of Things Journal* 6.3 (2019), pp. 4815–4830.

[25] V. Agate, S. Drago, P. Ferraro e G. Lo Re. «Anomaly Detection for Reoccurring Concept Drift in Smart Environments». In: *2022 18th International Conference on Mobility, Sensing and Networking (MSN)*. IEEE. 2022, pp. 113–120.

[26] A. Khraisat e A. Alazab. «A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges». In: *Cybersecurity* 4.1 (2021), p. 18. URL: https://doi.org/10.1186/s42400-021-00077-7.

[27] I. Sharafaldin, A. H. Lashkari e A. A. Ghorbani. «Toward generating a new intrusion detection dataset and intrusion traffic characterization.» In: *ICISSp* 1 (2018), pp. 108–116.

[28] N. Koroniotis, N. Moustafa, E. Sitnikova e B. Turnbull. «Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset». In: *Future Generation Computer Systems* 100 (2019), pp. 779–796.

[29] M. Tavallaee, E. Bagheri, W. Lu e A. A. Ghorbani. «A detailed analysis of the KDD CUP 99 data set». In: *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*. 2009, pp. 1–6.

[30] K. Cup. *Available on: http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html*. 2007.

[31] N. Moustafa e J. Slay. «UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)». In: *2015 Military Communications and Information Systems Conference (MilCIS)*. 2015, pp. 1–6.

[32] R. Panigrahi e S. Borah. «A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems». In: *International Journal of Engineering & Technology* 7.3.24 (2018), pp. 479–482.

[33] I. F. Kilincer, F. Ertam e A. Sengur. «Machine learning methods for cyber security intrusion detection: Datasets and comparative study». In: *Computer Networks* 188 (2021), p. 107840. URL: https://www.sciencedirect.com/science/article/pii/S1389128621000141.

[34] H. Mennour e S. Mostefai. «A hybrid Deep Learning Strategy for an Anomaly Based N-IDS». In: *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*. 2020, pp. 1–6.

[35] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa e C. F. M. Foozy. «Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset». In: *IEEE Access* 9 (2021), pp. 22351–22370.

[36] V. Agate, A. De Paola, G. Lo Re e M. Morana. «Vulnerability Evaluation of Distributed Reputation Management Systems». In: *InfQ 2016 - New Frontiers in Quantitative Methods in Informatics*. ICST, Brussels, Belgium: ICST, 2016, pp. 1–8.

[37] X. Gao, C. Shan, C. Hu, Z. Niu e Z. Liu. «An Adaptive Ensemble Machine Learning Model for Intrusion Detection». In: *IEEE Access* 7 (2019), pp. 82512–82521.

[38] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot e E. Duchesnay. «Scikit-learn: Machine Learning in Python». In: *Journal of Machine Learning Research* 12 (2011), pp. 2825–2830.

[39] P. Geurts, D. Ernst e L. Wehenkel. «Extremely randomized trees». In: *Machine Learning* 63.1 (apr. 2006), pp. 3–42. URL: https://doi.org/10.1007/s10994-006-6226-1.

[40] V. Agate, P. Ferraro e S. Gaglio. «A Cognitive Architecture for Ambient Intelligence Systems». In: *AIC*. 2018, pp. 52–58.

[41] L. Breiman. «Random Forests». In: *Machine Learning* 45.1 (ott. 2001), pp. 5–32. URL: https://doi.org/10.1023/A:1010933404324.

[42] V. Agate, A. De Paola, G. Lo Re e M. Morana. «DRESS: A Distributed RMS Evaluation Simulation Software». In: *International Journal of Intelligent Information Technologies (IJIIT)* 16.3 (2020), pp. 1–18.

[43] T. Chen e C. Guestrin. «Xgboost: A scalable tree boosting system». In: *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*. 2016, pp. 785–794.

[44] W. S. McCulloch e W. Pitts. «A logical calculus of the ideas immanent in nervous activity». In: *The bulletin of mathematical biophysics* 5 (1943), pp. 115–133.

[45] V. Agate, A. De Paola, G. Lo Re e A. Virga. «Reliable Reputation-Based Event Detection in V2V Networks». In: *International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability*. Springer. 2023, pp. 267–281.

[46] J. Schmidhuber. «Deep learning in neural networks: An overview». In: *Neural Networks* 61 (2015), pp. 85–117. URL: https://www.sciencedirect.com/science/article/pii/S0893608014002135.

[47] T. Cover e P. Hart. «Nearest neighbor pattern classification». In: *IEEE transactions on information theory* 13.1 (1967), pp. 21–27.

[48] V. Agate, A. De Paola, G. Lo Re e M. Morana. «A simulation framework for evaluating distributed reputation management systems». In: *Distributed Computing and Artificial Intelligence, 13th International Conference*. Springer. 2016, pp. 247–254.

[49] J. R. Quinlan. «Induction of decision trees». In: *Machine learning* 1 (1986), pp. 81–106.

[50] I. T. Jolliffe. *Principal component analysis for special types of data*. Springer, 2002.

[51] N. V. Chawla, K. W. Bowyer, L. O. Hall e W. P. Kegelmeyer. «SMOTE: synthetic minority over-sampling technique». In: *Journal of artificial intelligence research* 16 (2002), pp. 321–357.

[52] A. De Paola, P. Ferraro, S. Gaglio, G. Lo Re e S. K. Das. «An adaptive bayesian system for context-aware data fusion in smart environments». In: *IEEE Transactions on Mobile Computing* 16.6 (2016), pp. 1502–1515.

[53] A. De Paola, P. Ferraro, S. Gaglio, G. Lo Re, M. Morana, M. Ortolani e D. Peri. «A context-aware system for ambient assisted living». In: *International Conference on Ubiquitous Computing and Ambient Intelligence*. Springer. 2017, pp. 426–438.

[54] H. He, Y. Bai, E. A. Garcia e S. Li. «ADASYN: Adaptive synthetic sampling approach for imbalanced learning». In: *2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence)*. Ieee. 2008, pp. 1322–1328.

[55] V. Agate, P. Ferraro, G. Lo Re e S. K. Das. «BLIND: A privacy preserving truth discovery system for mobile crowdsensing». In: *Journal of Network and Computer Applications* (2023), p. 103811.

[56] A. Gosain e S. Sardana. «Handling class imbalance problem using oversampling techniques: A review». In: *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2017, pp. 79–85.

[57] N. Thockchom, M. M. Singh e U. Nandi. «A novel ensemble learning-based model for network intrusion detection». In: *Complex & Intelligent Systems* (apr. 2023). URL: https://doi.org/10.1007/s40747-023-01013-7.

[58] V. Agate, F. Concone, A. De Paola, P. Ferraro, G. Lo Re e M. Morana. «Bayesian Modeling for Differential Cryptanalysis of Block Ciphers: A DES Instance». In: *IEEE Access* 11 (2023), pp. 4809–4820.

[59] P. Ferraro e G. Lo Re. «Designing ontology-driven recommender systems for tourism». In: *Advances onto the Internet of Things*. Springer, 2014, pp. 339–352.

[60] A. Thakkar e R. Lohiya. «Attack Classification of Imbalanced Intrusion Data for IoT Network Using Ensemble-Learning-Based Deep Neural Network». In: *IEEE Internet of Things Journal* 10.13 (2023), pp. 11888–11895.

[61] V. Agate, F. Concone e P. Ferraro. «A Resilient Smart Architecture for Road Surface Condition Monitoring». In: *The Proceedings of the International Conference on Smart City Applications*. Springer. 2021, pp. 199–209.

[62] Y. Freund e R. E. Schapire. «A desicion-theoretic generalization of on-line learning and an application to boosting». In: *European conference on computational learning theory*. Springer. 1995, pp. 23–37.

[63] T. Hastie, S. Rosset, J. Zhu e H. Zou. «Multi-class adaboost». In: *Statistics and its Interface* 2.3 (2009), pp. 349–360.