



Cybersecurity ed Industria 4.0

Le nuove sfide della sicurezza nell'era dell'IA

Prof. F. Benedetto

francesco.benedetto@uniroma3.it
fbenedetto@ieee.org

Chair of "Machine Learning and Data Processing" - University of Roma Tre
Chair of the IEEE VTS Italian Chapter - IEEE Vehicular Technology Society

- Digital Revolution towards Industry 4.0
- AI, CyberSecurity and Industry 4.0
- Fundamentals of CyberSecurity
- AI and Cyber Attacks
- Conclusions and Future Directions



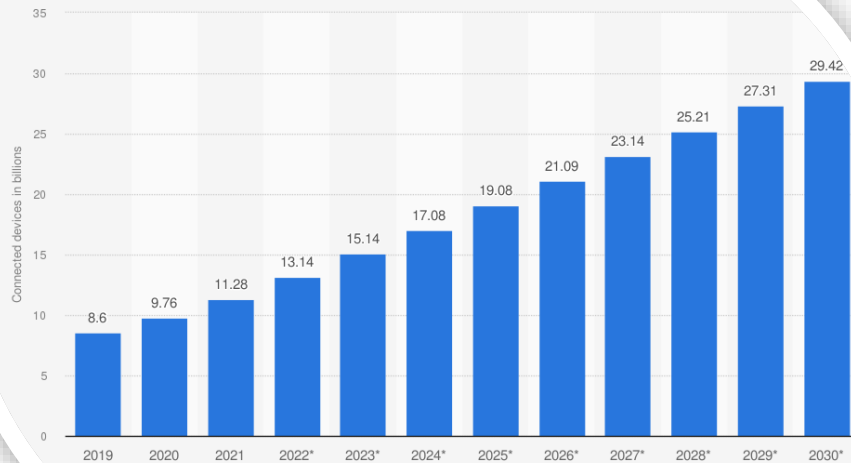
SETTING SIGHTS ON GENERATIONAL LEAP



Evoluzione nel tempo di Industry 4.0 e Cybersecurity

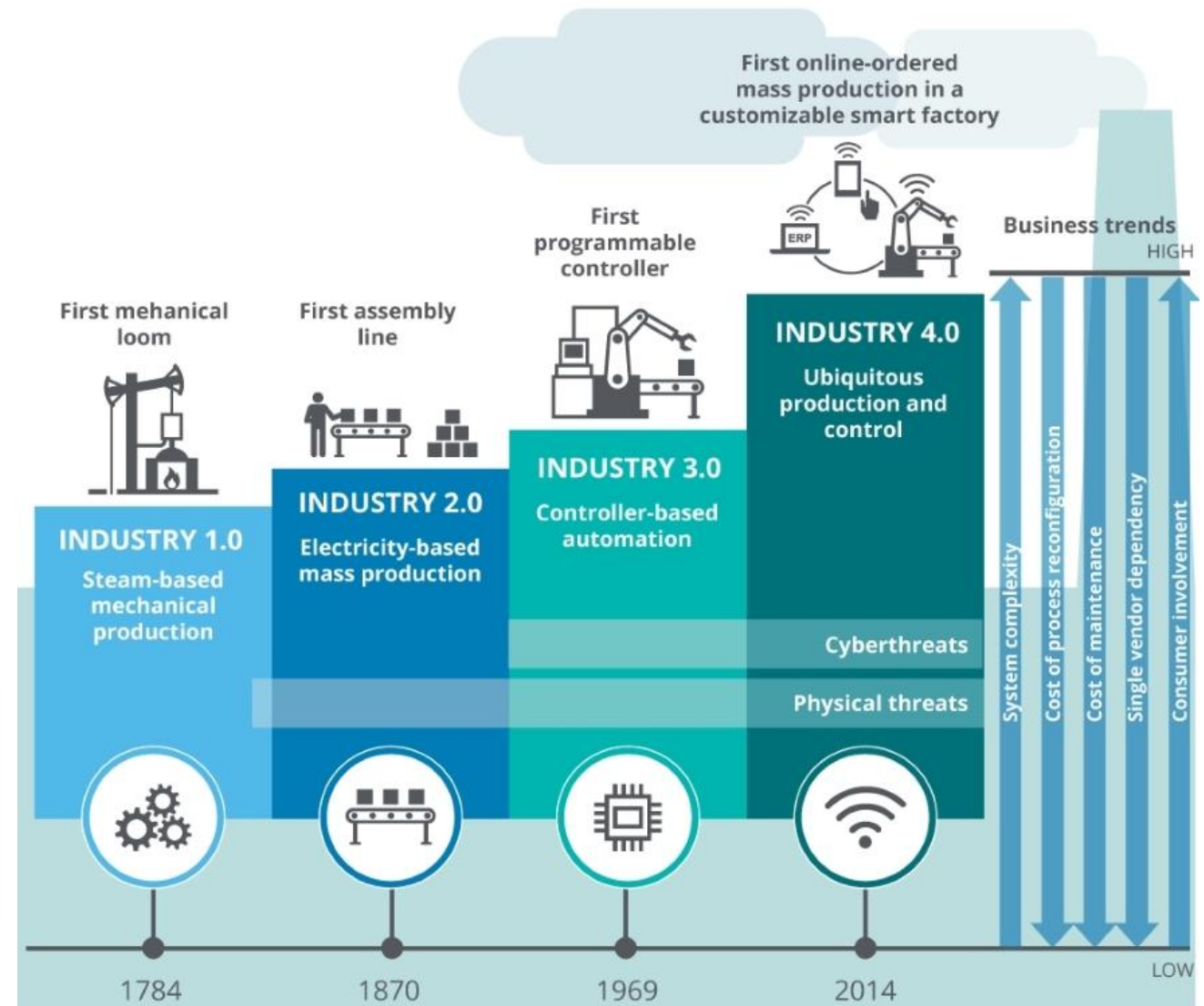
Cyberspace technologies are shifting human history from a linear and continuous development to a non-linear and discontinuous progression that widely indicates that the world we live in will never be the same.

Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030* with forecasts from 2022 to 2030 (in billions)



Additional Information:
Worldwide; 2019 to 2022

Source: Statista.com

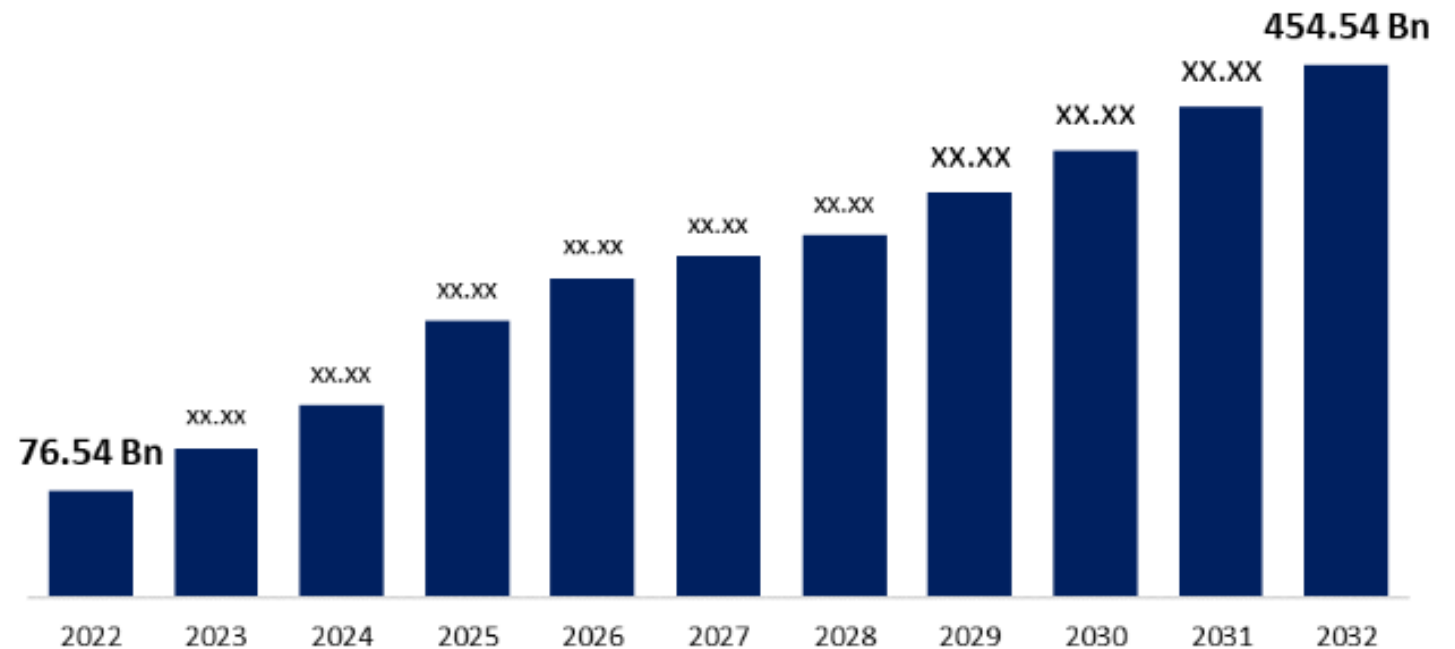


Source: Deloitte.

Deloitte University Press | dupress.deloitte.com 4

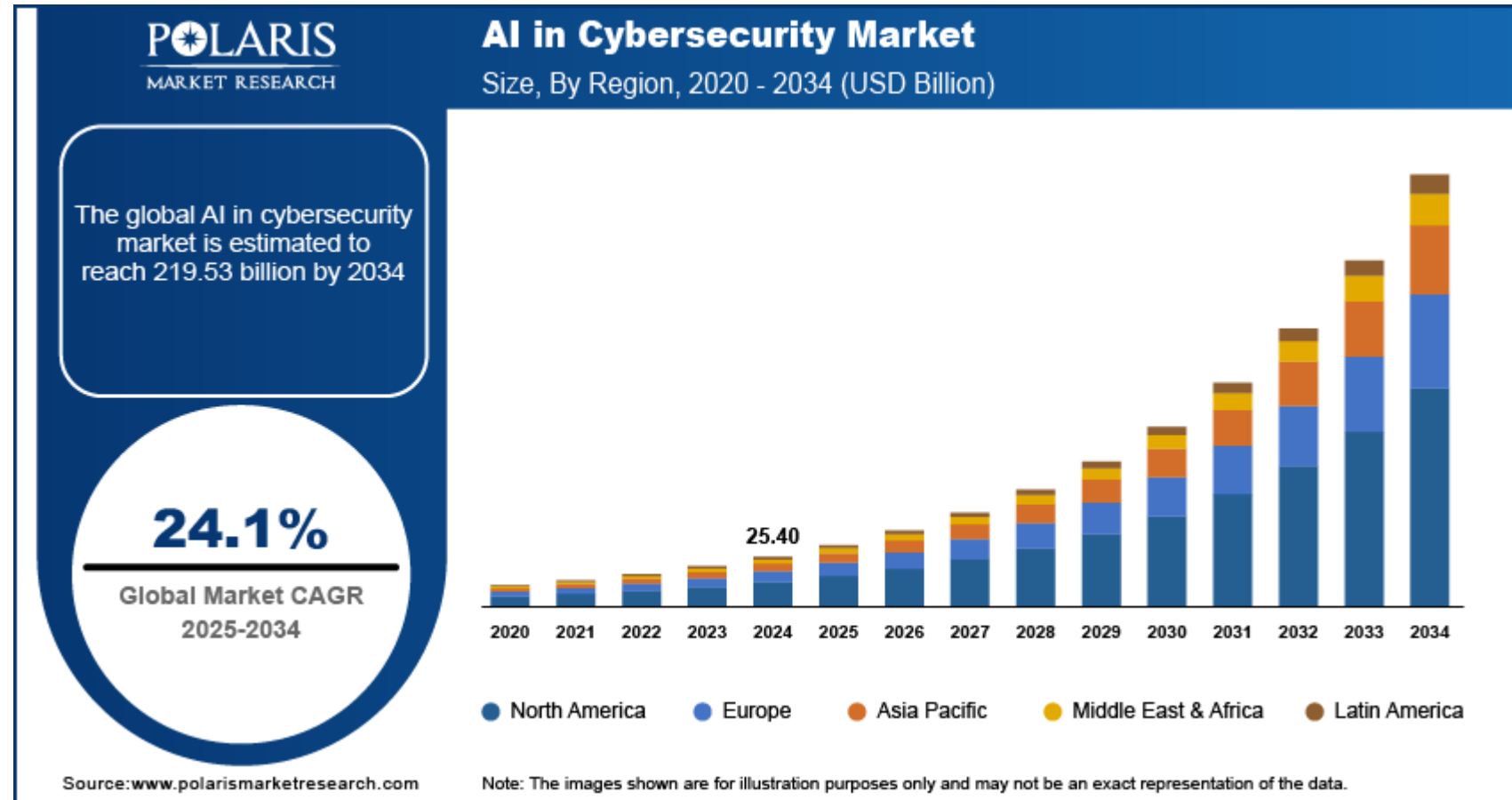
•Secondo Spherical Insights, il mercato globale di Industry 4.0 è stato valutato **76,54 miliardi di USD nel 2022** e si prevede che raggiungerà **454,54 miliardi di USD entro il 2032**, con un tasso di crescita annuale composto (CAGR) del **19,5%** dal 2023 al 2032.

Global Industry 4.0 Market Size



Stime di crescita: Cybersecurity

- Il mercato dell'IA applicata alla cybersecurity è stato valutato a **25,4 miliardi di USD nel 2024** e si prevede che raggiungerà **219,5 miliardi di USD entro il 2034**, con un CAGR del **24,1%**.



AI in Industry 4.0 e Cybersecurity



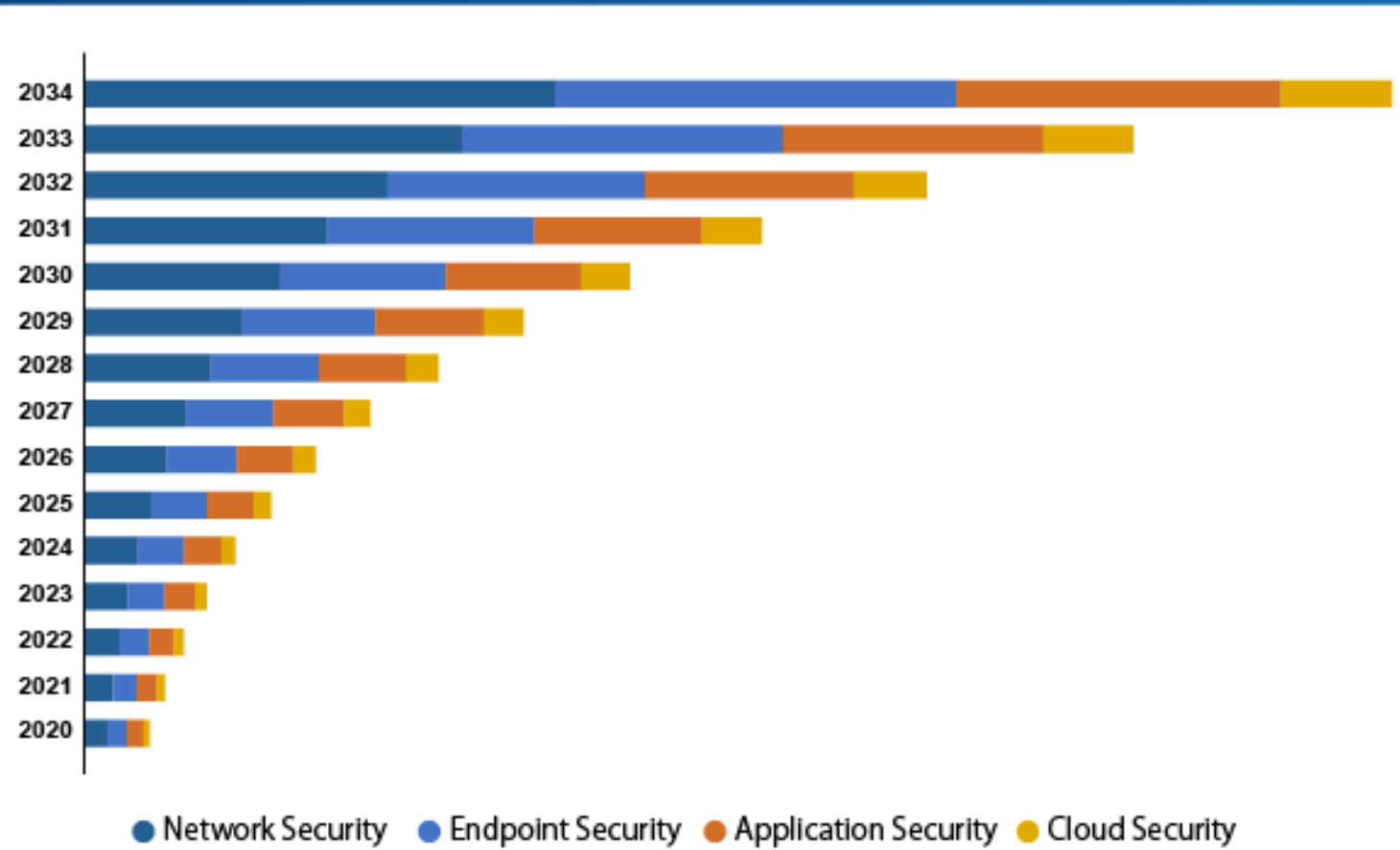


Based on type, the AI in cybersecurity market is divided into network security, endpoint security, application security, and cloud security.

The network security segment dominated the AI in cybersecurity market expansion in 2024 due to the critical need to safeguard organizational networks from evolving cyber threats.

AI in Cybersecurity Market

By Type Analysis 2020 - 2034 (USD Billion)



Source: www.polarismarketresearch.com

Note: The images shown are for illustration purposes only and may not be an exact representation of the data.

La cybersicurezza rappresenta una delle principali sfide dell'era digitale. Con l'evoluzione dell'intelligenza artificiale (IA), nuove opportunità e minacce emergono nel panorama della sicurezza informatica.

L'IA ha trasformato la cybersicurezza in diversi modi:

- **Rilevamento delle Minacce:** Algoritmi di machine learning analizzano enormi quantità di dati per identificare modelli di attacchi informatici.
- **Automazione della Risposta agli Incidenti:** Sistemi basati su IA possono reagire automaticamente a intrusioni sospette, riducendo il tempo di risposta.
- **Analisi Predittiva:** L'IA può prevedere potenziali minacce prima che si verifichino, migliorando la proattività della sicurezza informatica.
- **Autenticazione e Accesso Sicuro:** Tecnologie basate su IA, come il riconoscimento biometrico e il comportamento utente, migliorano i sistemi di autenticazione.

Cybersecurity

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Application Security

Information Security

Network Security

Operational Security

Disaster Security

End-user Education

CIA Triad



Confidentiality



Confidentiality is about preventing the disclosure of data to unauthorized parties.



Integrity



Integrity refers to protecting information from being modified by unauthorized parties.



Availability



Availability is making sure that authorized parties are able to access the information when needed

Nonostante i benefici, l'uso dell'IA nella cybersicurezza presenta anche rischi significativi:

- **Attacchi Adversariali:** Gli hacker possono manipolare i modelli di IA per ingannare i sistemi di sicurezza.
- **Deepfake e Inganno:** L'IA può essere utilizzata per creare contenuti falsi (deepfake) per attacchi di phishing avanzati.
- **Automazione degli Attacchi:** I cybercriminali possono usare l'IA per sviluppare malware più sofisticati e adattivi.
- **Problemi Etici e Privacy:** L'uso di IA nella cybersicurezza può sollevare questioni legate alla sorveglianza e alla protezione dei dati personali.

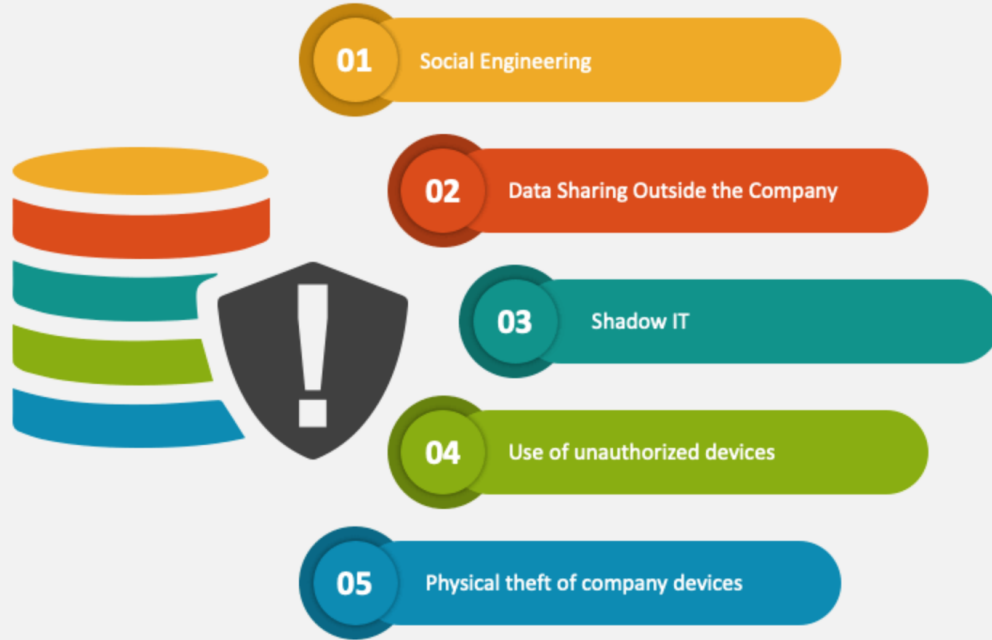


CIA Triad Broken Down

	 Confidentiality	 Integrity	 Availability
Attacks	• Cracking Encrypted Data • Man In The Middle • Installing Spyware • Doxxing	• Web Penetration • Unauthorised Scans • Remote Controlling	• DDoS attacks • Ransomware Attacks • Disrupting Server
Countermeasures	• Access Control • Encryption • Biometric Verification	• Intrusion Detection • Cryptography • Hashing	• Regular Backup • Data Replication • Adequate communication bandwidth



Most Common Threat to a Company's Data Security



Technical Data Threats





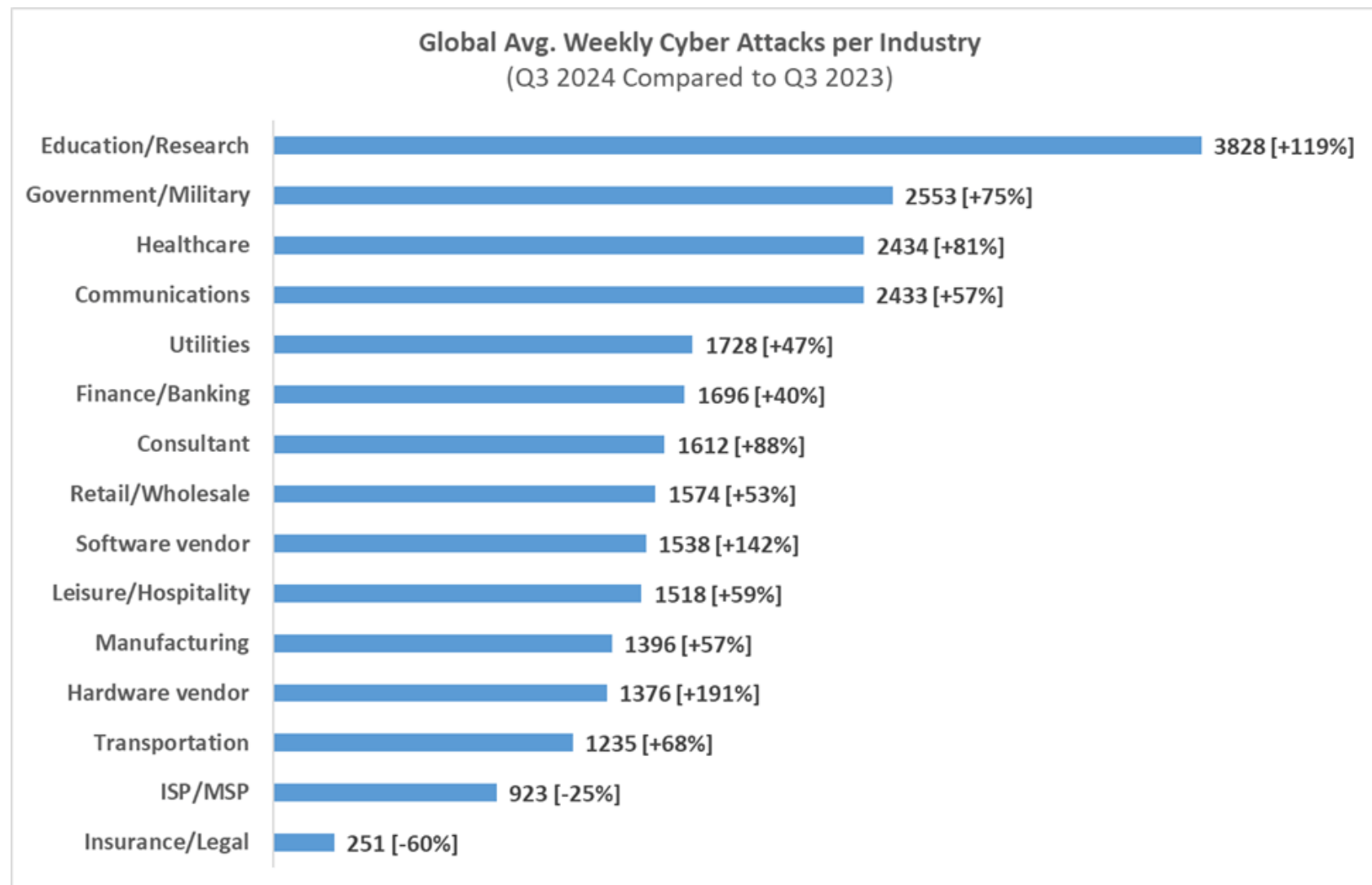
Sources of Cyber Security Threats



Top Cyber Threats



Aumento del 75% a livello mondiale: Nel terzo trimestre del 2024, gli attacchi informatici globali sono aumentati del 75% rispetto allo stesso periodo del 2023, raggiungendo una media di 1.876 attacchi settimanali per organizzazione

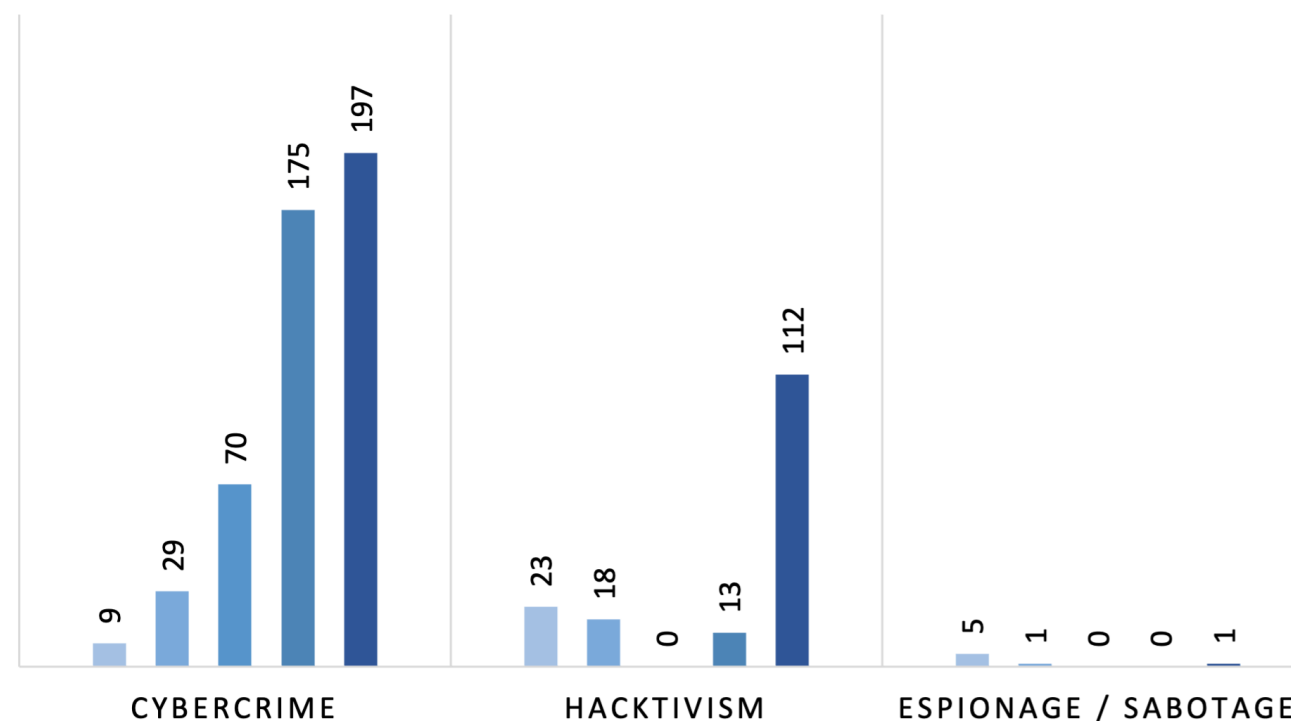


ATTACCANTI IN ITALIA 2019 - 23

■ 2019 ■ 2020 ■ 2021 ■ 2022 ■ 2023

Situazione in Italia

Incremento del 115%: In Italia, nello stesso periodo, si è registrato un aumento del 115% degli attacchi informatici, con una media di 2.301 attacchi settimanali per organizzazione.



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

- **Ransomware in aumento:** Nel secondo trimestre del 2024, gli attacchi ransomware ai sistemi di controllo industriale (ICS) sono aumentati del 20% rispetto al trimestre precedente.

- **Presenza persistente di spyware:** Il 4,08% dei computer ICS è stato colpito da spyware, in aumento rispetto al 3,9% del primo trimestre del 2024.

- **Malware predominante:** Il malware rappresenta il 34% degli attacchi a livello globale e il 51% in Italia, confermandosi come la tecnica di attacco più utilizzata.

Incidenti per semestre H1 2019 - H1 2024



Manufacturing Cybersecurity: Stats, Risks & DataGuard Solutions 2024

Il settore manifatturiero italiano è stato il più colpito nel primo semestre del 2024, rappresentando il 19% degli attacchi IT, in crescita rispetto al 13% del 2023. Inoltre, oltre un quarto (28%) degli attacchi globali al settore manifatturiero ha riguardato realtà italiane.

Over 60%

Experienced cyberattacks

30%

Increase in security incidents after IoT integration

\$1M

Average cost of a cyber breach

70%

breaches is due to internal vulnerabilities primarily human error

50%

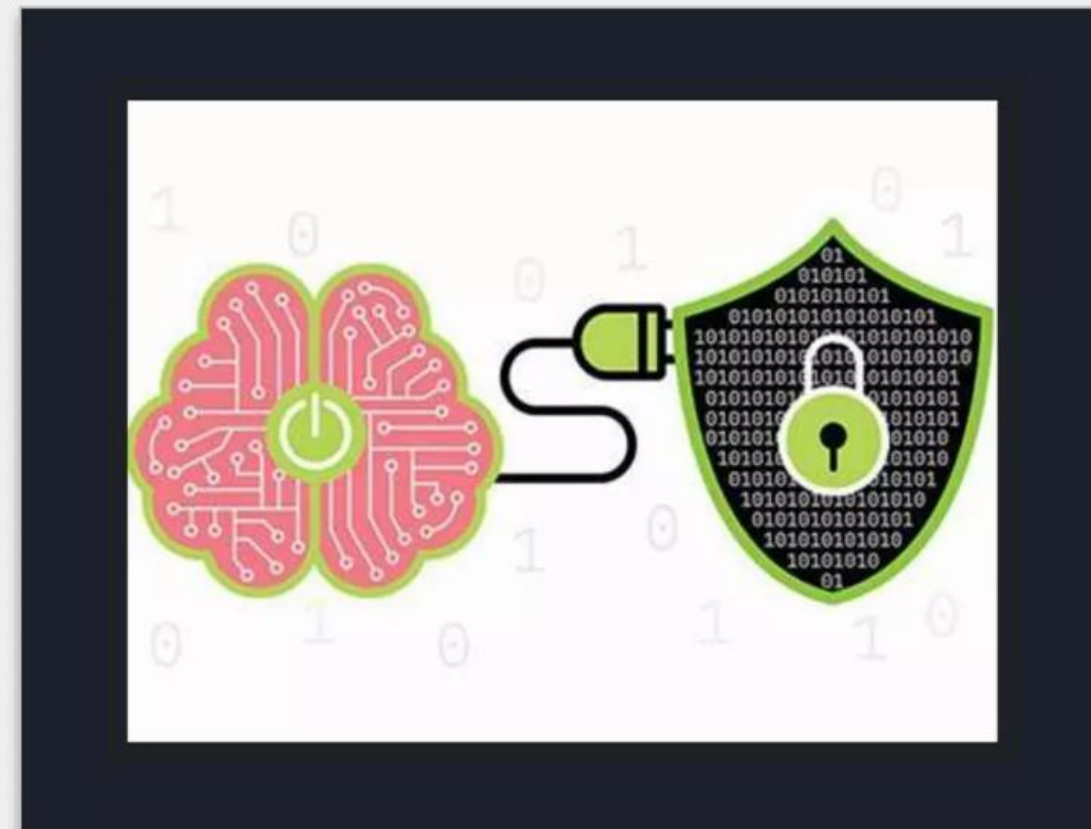
of firms does not comply with standard cybersecurity protocols



Why Machine Learning used in Cyber Security?

- DDoS on Github 1.3 terabytes per second
- 16.7 million identity theft 16.8 billion dollars stolen.
- 50 million users compromised Facebook developer API's breach.

All these breaches if were detected and terminated by the machine itself huge losses could be prevented.





What is AI in Cybersecurity?

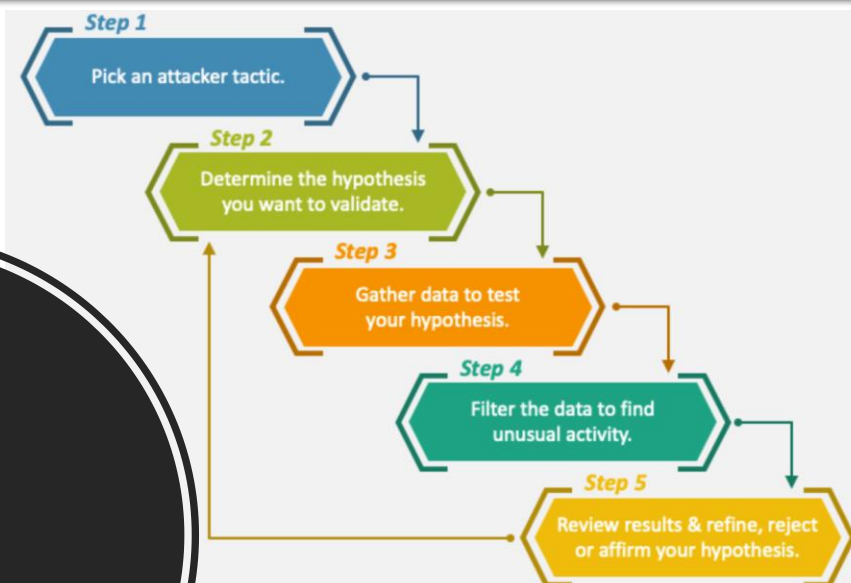
AI in cybersecurity refers to the use of AI & machine learning algorithms & techniques to enhance the security of computer systems & networks. The goal of AI in cybersecurity is to automate the process of detecting, preventing, & mitigating security threats, thereby making cybersecurity more efficient & effective.

Some of the ways AI is being used in cybersecurity include:

- *Threat detection*
- *Intrusion prevention*
- *Malware detection*
- *Fraud detection*
- *Vulnerability mgmt.*



Cyber Threats Hunting



Information and enriching automated analytics is key to successful hunts. Ensure to record and leverage new findings as encountered during hunting.

Discover new malicious patterns and reconstruct complex attack paths to reveal an attacker's Tactics, Techniques, and Procedures (TTP's).



A hunt starts with creating an educated guess about various types of activities in the IT environment.

Linked Data Analysis is an effective technique for laying out data in an understandable way. This includes visualization, statistical analysis, and machine learning.

Per affrontare le sfide della cybersicurezza nell'era dell'IA, è necessario adottare strategie adeguate:

- **Sviluppo di Modelli IA Robusti:** Implementare tecniche di difesa contro attacchi avversariali.
- **Monitoraggio e Aggiornamento Costante:** Aggiornare continuamente i modelli di IA per prevenire exploit e vulnerabilità.
- **Collaborazione tra Settori:** Favorire la cooperazione tra enti governativi, aziende e ricercatori per sviluppare standard di sicurezza condivisi.
- **Educazione e Consapevolezza:** Formare gli utenti e i professionisti della sicurezza informatica sulle minacce emergenti e sulle contromisure disponibili.

AI e Cybersicurezza: benefici e sfide

Benefits of Using AI in Cybersecurity



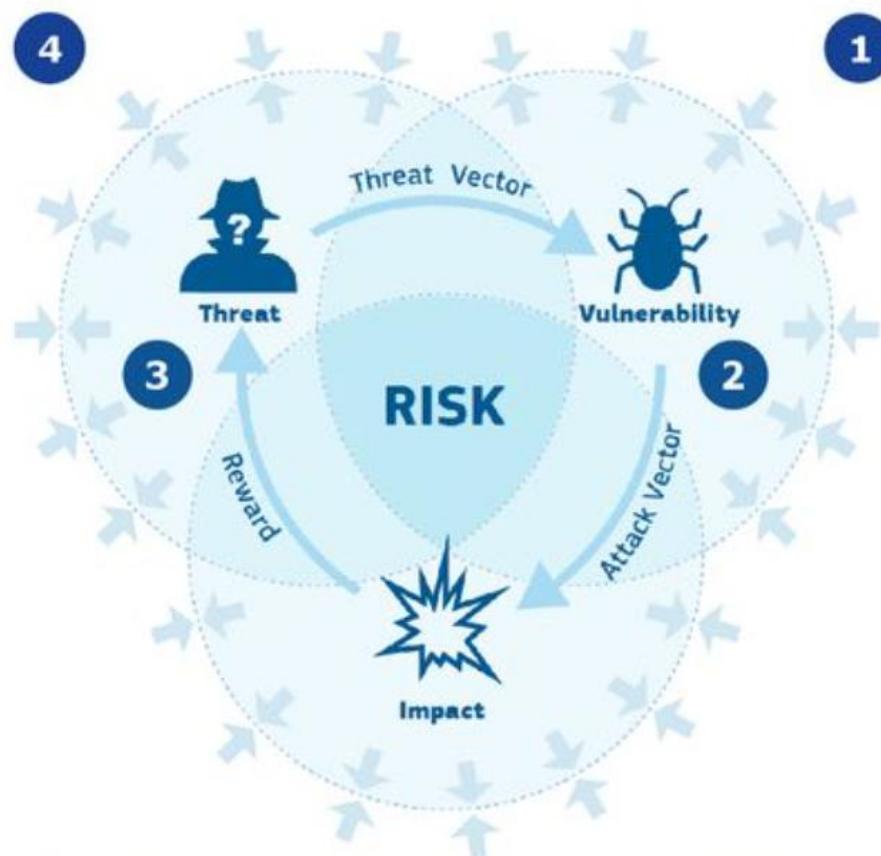
Challenges



AI Applications in Cybersecurity



Cybersecurity and AI & DT: 4 angles of influence



	Opportunities	Challenges
Resilience	1. AI to create smarter cybersecurity E.g. more effective security controls (antivirus, intrusion detection and prevention, email scanning), automatic discovery of vulnerabilities, automatic malware analysis, smarter cyber defence, etc.	2. Robustness/Vulnerability of AI algorithms E.g. adversarial machine learning (i.e. exploitation of weaknesses in AI algorithms to change their behavior), attacks against AI powered cyber-physical systems, etc.
Deterrence	4. Use of AI to fight cyber attackers & criminals E.g. better biometrics, smarter forensics, fraud analysis, encryption challenge, fight against fake news, etc.	3. Misuse of AI E.g. creation of deep audio video fakes, AI powered malware, smarter social engineering attacks, etc.

Conceptual model depicting the logical links between the different components of the cybersecurity risk in the context of the influence of AI and Digital Transformation

New countermeasures and attacks with AI



I covert channels (canali nascosti) rappresentano un metodo per trasferire informazioni in modo non autorizzato o inosservato, sfruttando canali di comunicazione non destinati a tale scopo.

L'intelligenza artificiale (IA) sta rivoluzionando sia la creazione che il rilevamento di questi canali, aumentando le possibilità di attacco e difesa nei sistemi informatici.

- **Definizione:** Un covert channel è un mezzo di comunicazione segreto che utilizza risorse condivise di un sistema per trasmettere informazioni senza essere rilevato.
- **Tipologie:**
 - **Covert Storage Channels:** Utilizzano variabili di stato di un sistema per nascondere dati.
 - **Covert Timing Channels:** Manipolano il tempo di risposta di un sistema per trasmettere dati in modo nascosto.

Clever misuse of legitimate, existing channel

Easy to design and nearly undetectable

Perfect for patient long term data exfiltration

Not a commonly used technique

- Bypass security or policy by compromised/malicious computer processes
- Evade Surveillance
- Bypass Communication
- Etc.



Classification



Storage Channel

Data transmitted by writing or abstaining from writing e.g to a ram



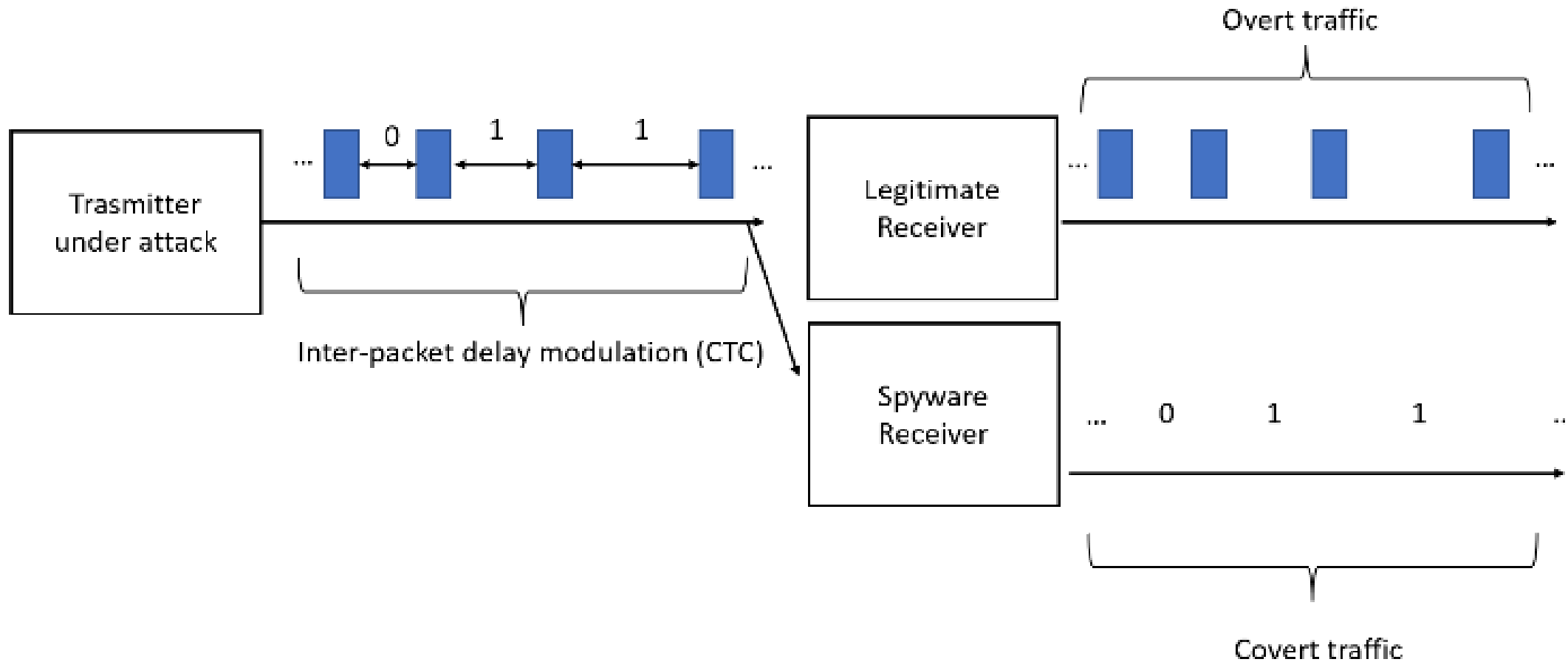
Timing Channel

Data modulated into the timing or occurrence of events, e.g., the times between network packets

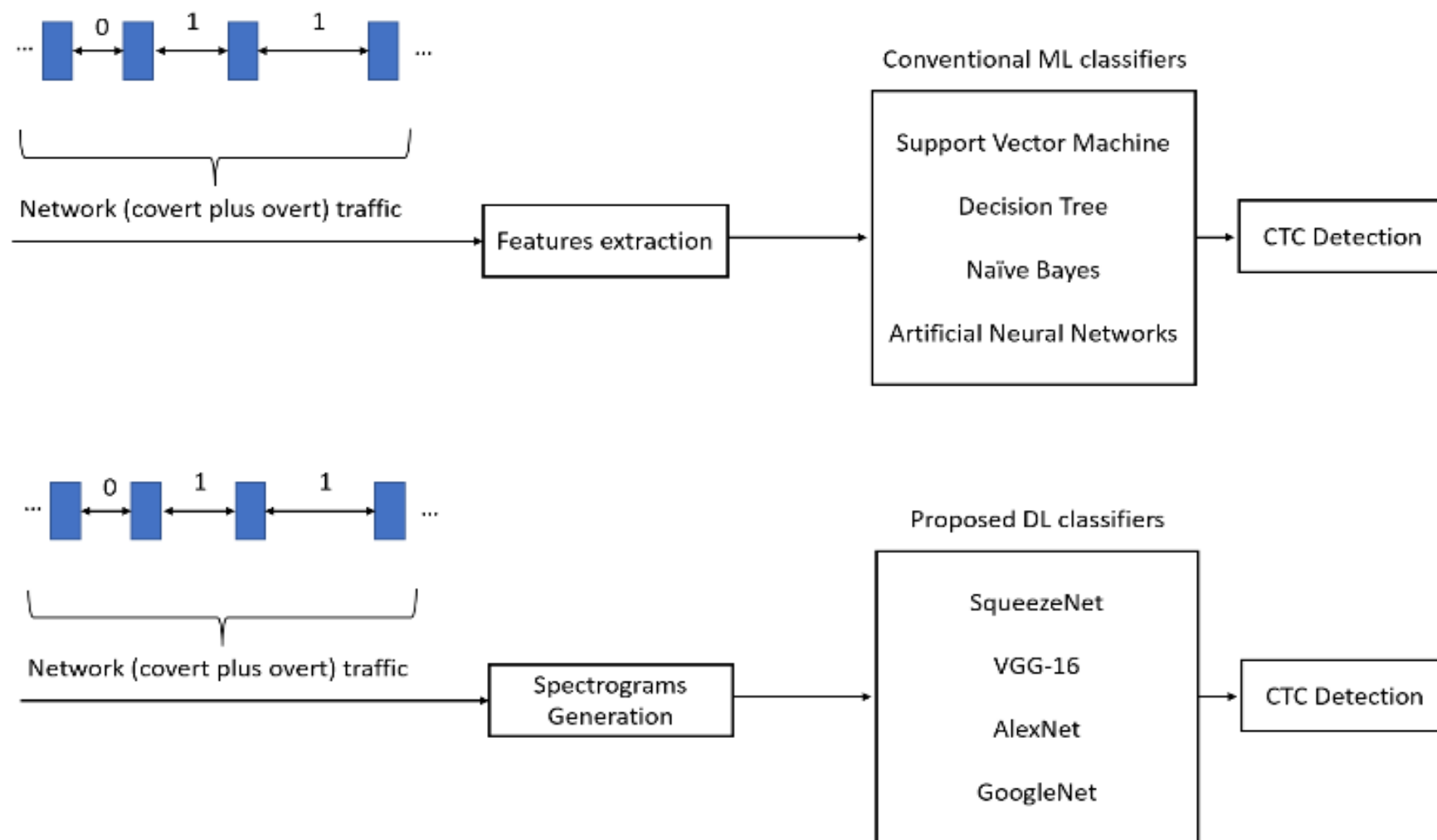
Other types in research:

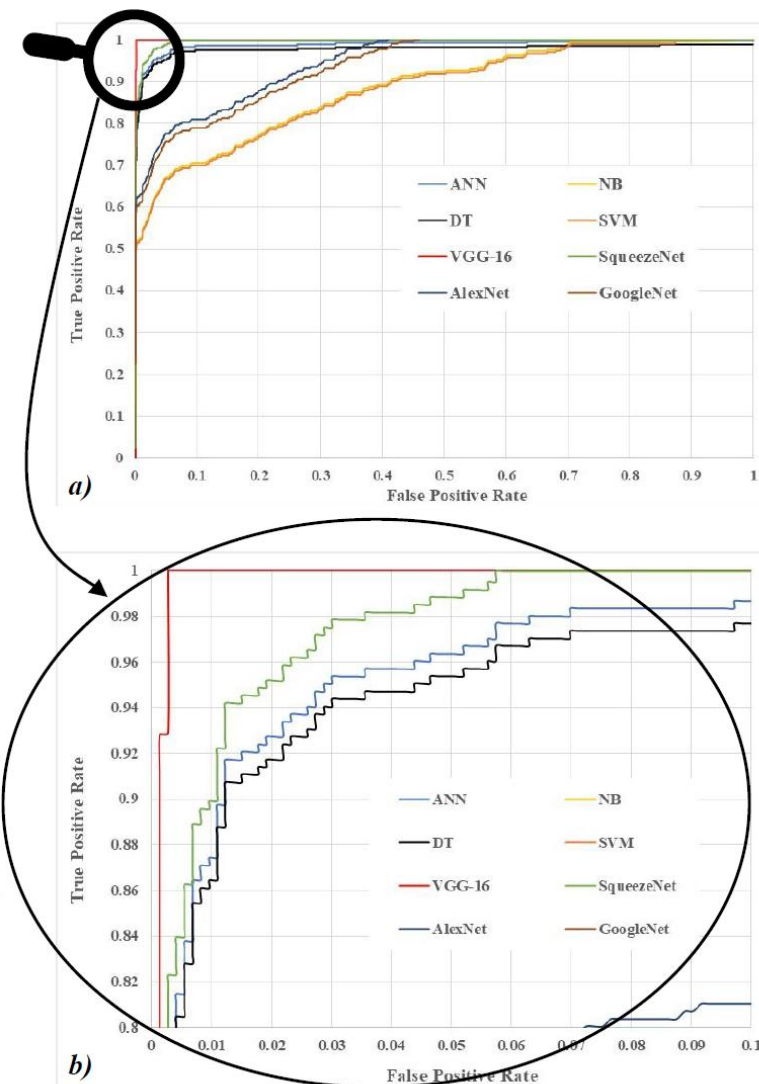
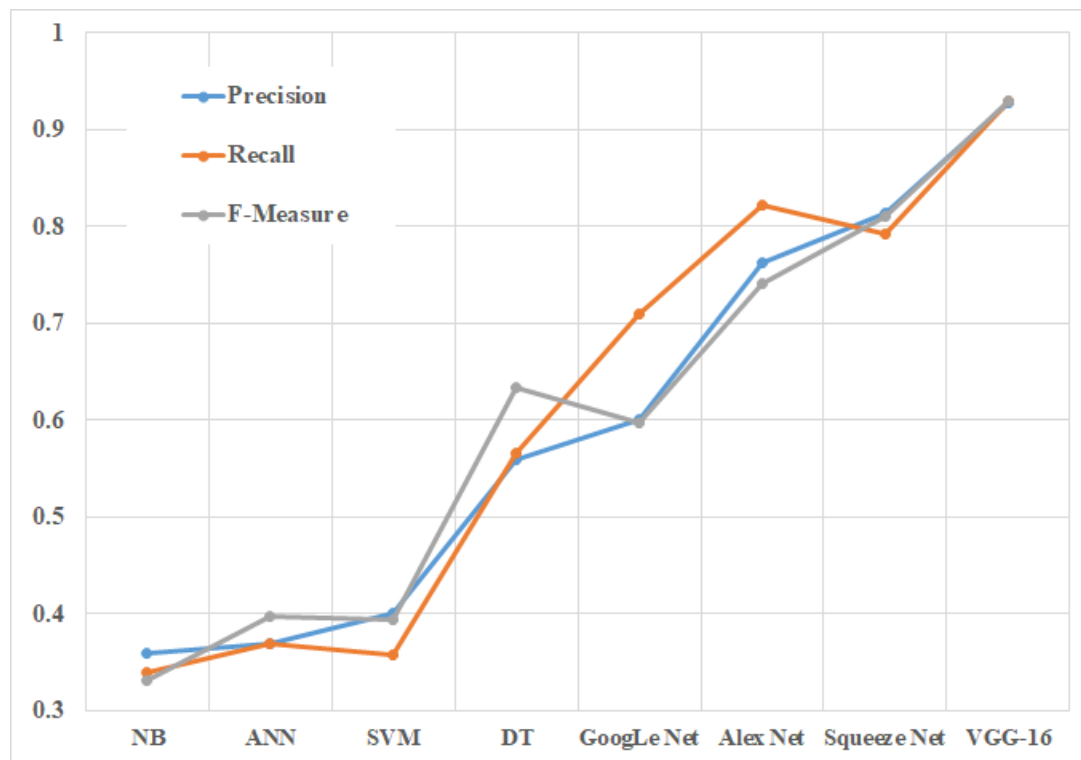
- Temperature based Covert Channels
- Hybrid Covert Channels

Covert Timing Channel



How ML/DL
can help...





```
import time
import threading
import random

# Parametri del covert channel
time_slot = 0.1 # Tempo base di trasmissione
bit_0_delay = 0.05 # Ritardo per il bit 0
bit_1_delay = 0.15 # Ritardo per il bit 1

# Messaggio da trasmettere
message = "10101010" # Messaggio binario

def sender():
    """Simula il mittente che trasmette il messaggio con ritardi
    temporali"""
    print("[Sender] Inizio trasmissione...")
    for bit in message:
        if bit == '0':
            time.sleep(bit_0_delay)
        else:
            time.sleep(bit_1_delay)
        print("[Sender] Bit trasmesso:", bit)
    print("[Sender] Trasmissione completata.")
```

```
def receiver():
    """Simula il ricevente che misura i tempi tra i messaggi"""
    received_bits = ""
    prev_time = time.time()
    print("[Receiver] In attesa di dati...")
    for _ in range(len(message)):
        time.sleep(time_slot) # Simula il controllo dei
        messaggi
        current_time = time.time()
        delta = current_time - prev_time
        prev_time = current_time
        if delta < (bit_0_delay + bit_1_delay) / 2:
            received_bits += '0'
        else:
            received_bits += '1'
        print(f"[Receiver] Tempo misurato: {delta:.3f} s, Bit
        ricevuto: {received_bits[-1]}")
    print("[Receiver] Messaggio ricevuto:", received_bits)
```

```
# Creazione dei thread per il sender e il
receiver

sender_thread =
threading.Thread(target=sender)

receiver_thread =
threading.Thread(target=receiver)

# Avvio della trasmissione

sender_thread.start()

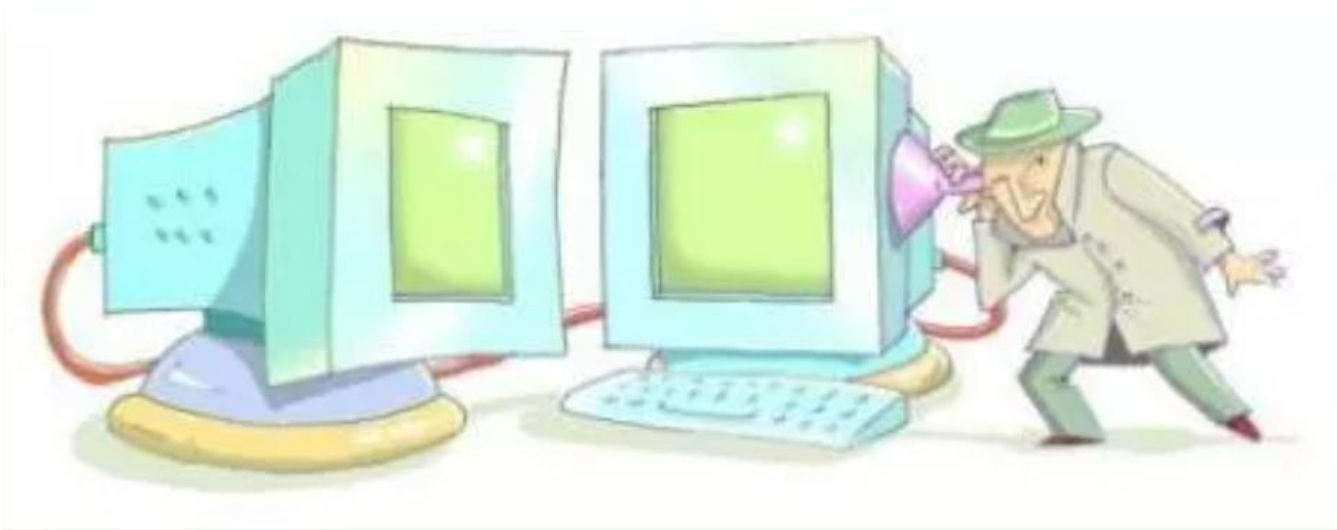
time.sleep(0.05) # Leggero ritardo per
sincronizzazione

receiver_thread.start()

# Attendere la fine della trasmissione

sender_thread.join()
receiver_thread.join()

print("[System] Comunicazione terminata.")
```

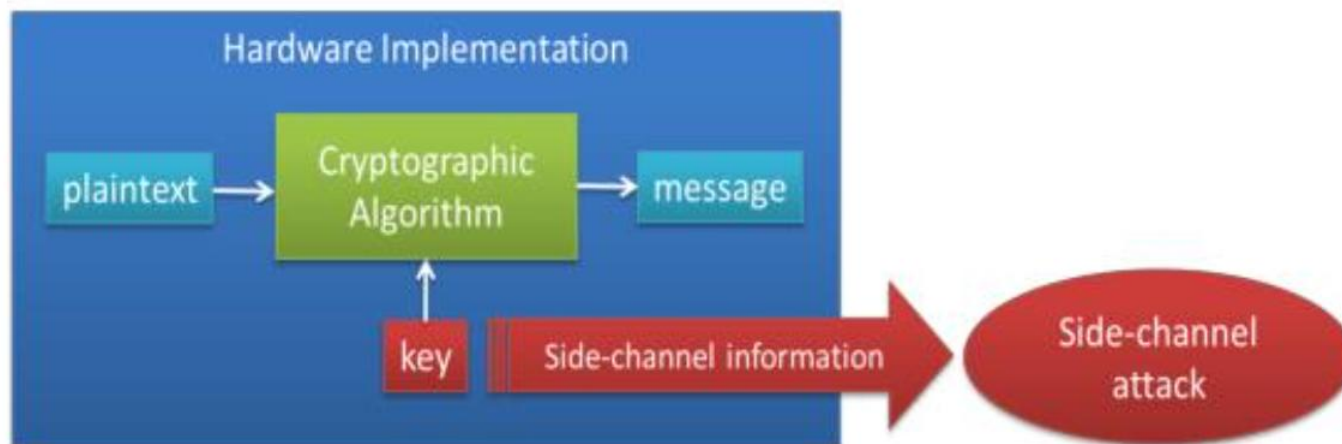


I side channels (canali laterali) rappresentano una classe di vulnerabilità informatica che sfrutta informazioni indirette derivanti dall'esecuzione di un sistema, come consumo energetico, tempi di risposta e segnali elettromagnetici, per estrarre dati sensibili.

Definizione: Un side channel è un meccanismo di acquisizione di informazioni basato su segnali collaterali emessi da un sistema durante il suo funzionamento.

- **Tipologie di side channels:**

- **Temporal:** Analizzano le variazioni nei tempi di esecuzione di operazioni crittografiche.
- **Elettromagnetici:** Sfruttano emissioni EM per inferire operazioni interne.
- **Acustici:** Analizzano suoni generati dai dispositivi elettronici.
- **Energetici:** Studiano i consumi di potenza per dedurre operazioni interne.
- **Cache-Based:** Esaminano le interazioni con la cache di un processore per estrarre dati.



a. Power Analysis Attacks

Questi attacchi analizzano il consumo di potenza del dispositivo durante l'esecuzione di AES.

- **Simple Power Analysis (SPA)**: Osservazione diretta del consumo di potenza per individuare pattern di esecuzione.
- **Differential Power Analysis (DPA)**: Analisi statistica delle variazioni di potenza per dedurre le operazioni crittografiche e recuperare la chiave segreta.
- **Correlation Power Analysis (CPA)**: Variante più avanzata del DPA, che utilizza modelli precisi del consumo energetico per correlare i dati con le operazioni eseguite.

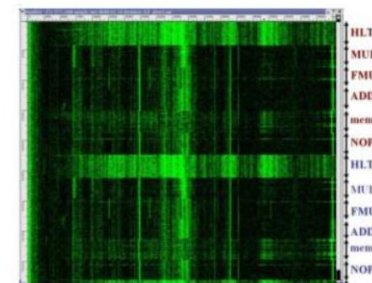
Esempio di attacco DPA su AES:

- L'attaccante raccoglie migliaia di tracce di consumo di energia mentre il dispositivo esegue la crittografia AES.
- Viene analizzato il comportamento dei registri interni per trovare correlazioni tra i dati crittografati e il consumo di potenza.
- Attraverso analisi statistica, si estrae la chiave AES parzialmente e si ricostruisce completamente con attacchi iterativi.

Types of Side Channel Attacks

Simple Power Analysis(SPA) Attacks

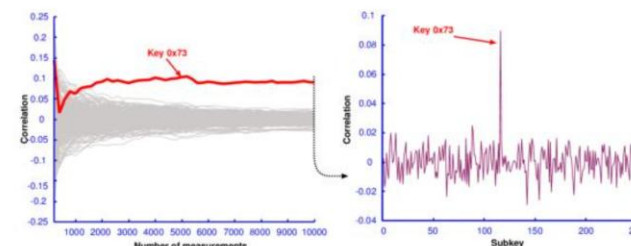
- ▣ Involves direct interpretation of power consumption measurements collected during cryptographic operations.
- ▣ SPA can reveal the sequence of microprocessor instructions executed.
- ▣ Sonic spectrum measured using an ultrasonic microphone.



Types of Side Channel Attacks

Differential Power Analysis

- ▣ Involves statistical analysis of power consumption measurements from a cryptosystem.
- ▣ Have signal processing & error correction properties.



Per mitigare questi attacchi, esistono diverse contromisure hardware e software.

a. Protezione contro Power Analysis Attacks

✓ **Randomizzazione del consumo energetico:** introduzione di variazioni casuali nel consumo di potenza per rendere inefficace il DPA.

✓ **Masking Techniques:** aggiunta di valori casuali nei dati elaborati per nascondere la correlazione con il consumo energetico.

✓ **Dual-rail logic e circuiti bilanciati:** hardware che consuma energia in modo costante per impedire l'analisi di consumo.

b. Protezione contro Timing Attacks

✓ **Constant-Time Implementations:** garantire che tutte le operazioni AES impieghino lo stesso tempo di esecuzione indipendentemente dai dati in ingresso.

✓ **Avoidance of Data-Dependent Branching:** evitare istruzioni condizionali basate sui dati in ingresso.

Prevention

□ General countermeasures:

- Data Independent Calculations
- Binding
- Licensing Modified Algorithms

□ Countermeasures against timing attacks:

- Adding Delays
- Time Equalization of Multiplication & Squaring

□ Countermeasures against power analysis attacks

- Power Consumption Balancing
- Reduction of Signal Size
- Addition of Noise
- Shielding
- Modification of Algorithm Design

□ Countermeasures against fault attacks

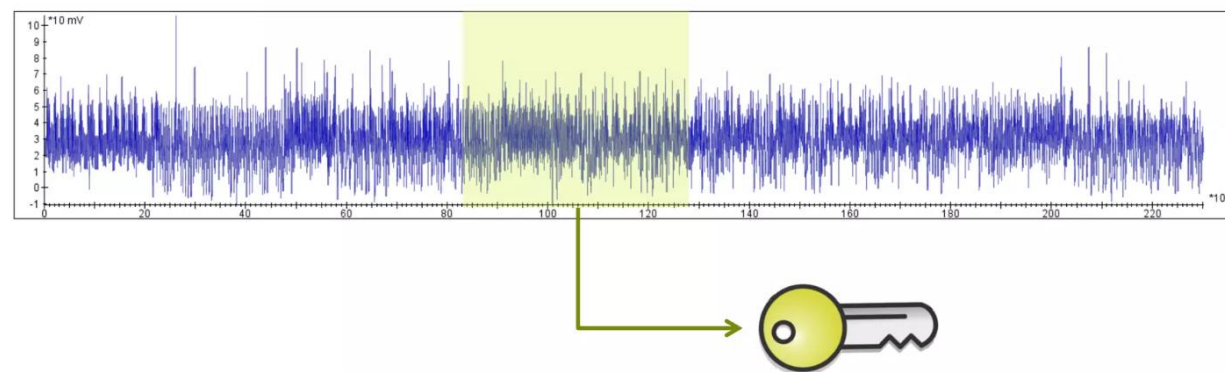
- Running the encryption twice



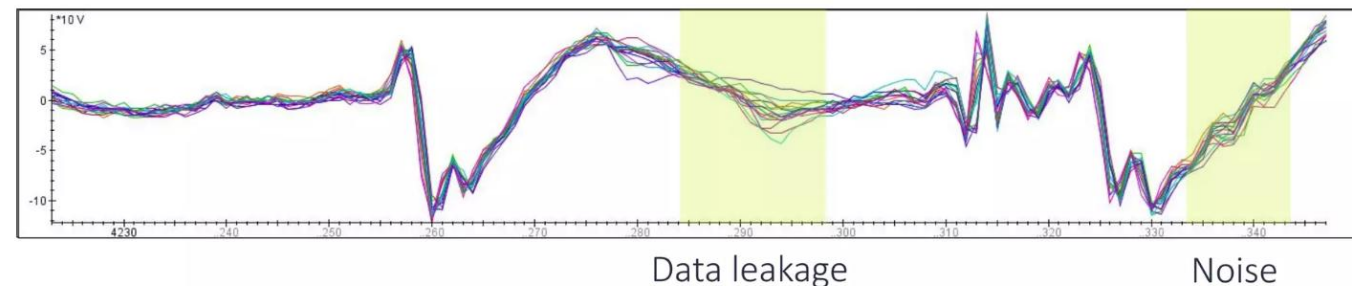
- Supponiamo di avere un dispositivo embedded che esegue AES su diversi blocchi di testo.
- Acquisiamo i tracciati di consumo di energia durante la cifratura.
- Utilizziamo un attacco DPA per estrarre la chiave segreta.

Power analysis

Some crypto algorithm



Example (huge) leakage



Primo grafico: Tracciato di Potenza Singolo

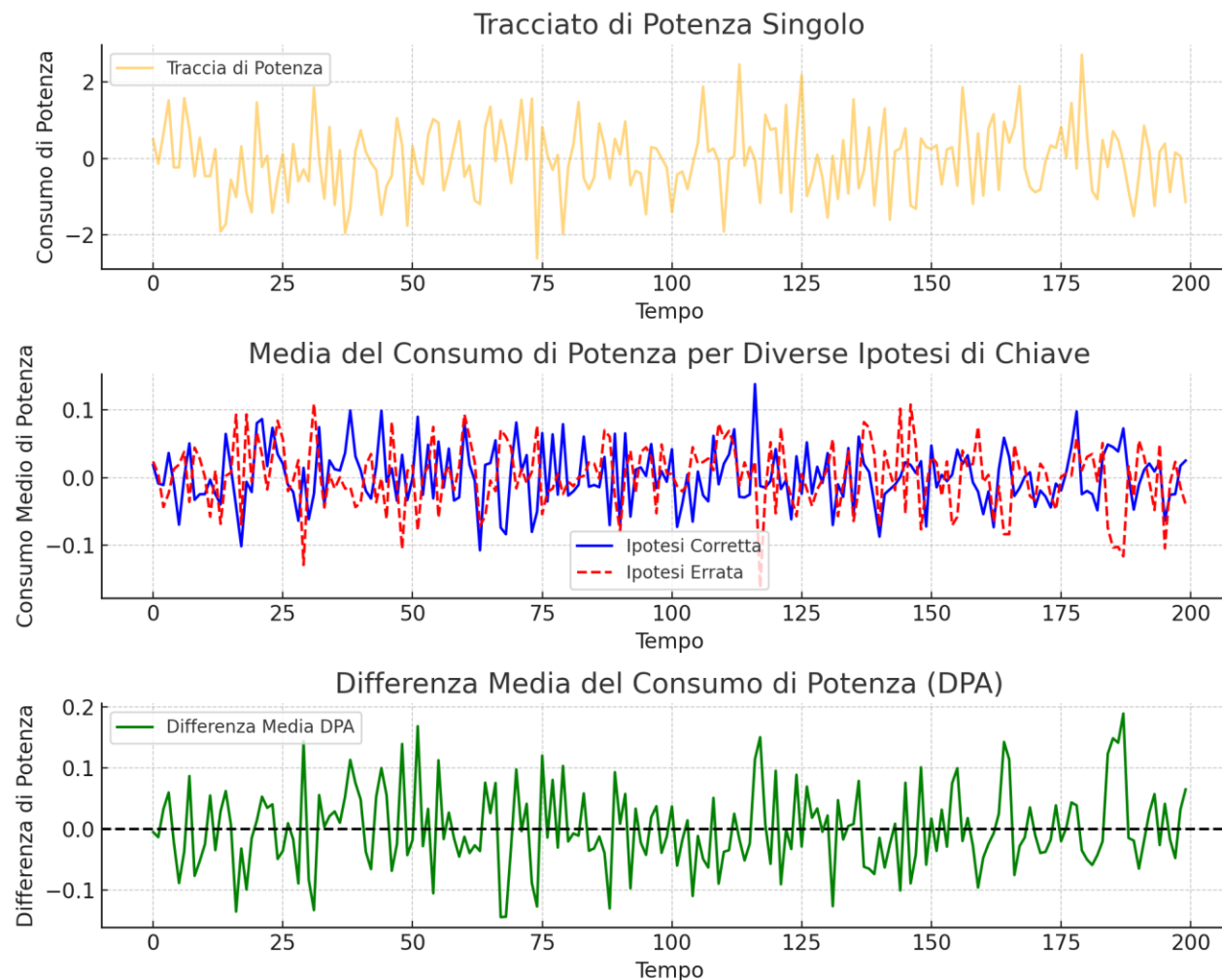
- Mostra una singola acquisizione del consumo di potenza durante un'operazione AES.
- Il consumo varia in base alle istruzioni eseguite.

Secondo grafico: Media del Consumo di Potenza per Due Ipotesi di Chiave

- La linea blu rappresenta il consumo medio per un'ipotesi di chiave corretta.
- La linea rossa tratteggiata mostra l'ipotesi errata.
- Le differenze tra le due curve indicano un possibile **leakage** di informazioni.

Terzo grafico: Differenza Media del Consumo di Potenza (DPA)

- Il picco verde indica la presenza di una correlazione significativa tra il consumo energetico e la chiave segreta.
- Questo consente all'attaccante di **identificare il byte corretto della chiave AES**.



Attacco DPA:

```
import numpy as np

import matplotlib.pyplot as plt

# Simulazione di un attacco DPA su AES

# Generiamo dati sintetici che rappresentano il consumo di potenza durante l'esecuzione di AES

np.random.seed(42)

num_traces = 1000 # Numero di tracciati di potenza raccolti

num_samples = 200 # Numero di punti per traccia

# Simuliamo un consumo di potenza casuale con una componente dipendente dalla chiave

true_key_byte = 42 # Byte della chiave segreta (valore casuale)

power_traces = np.random.normal(0, 1, (num_traces, num_samples)) # Rumore casuale

# Aggiungiamo un pattern di consumo energetico dipendente dalla chiave segreta

for i in range(num_traces):

    if (i % 256) == true_key_byte: # Simuliamo una dipendenza della potenza dalla chiave segreta

        power_traces[i, 50:100] += 0.5 # Incremento nel consumo di potenza

# Calcoliamo la media delle tracce per due ipotesi di chiave (una corretta, una errata)

hypothesis_correct = power_traces[:500].mean(axis=0) # Media per l'ipotesi corretta

hypothesis_wrong = power_traces[500:].mean(axis=0) # Media per l'ipotesi errata
```

```
# Calcoliamo la differenza media (DPA)
```

```
dpa_differential = hypothesis_correct -
hypothesis_wrong
```

```
# Generazione grafici
```

```
fig, axs = plt.subplots(3, 1, figsize=(10, 8))
```

```
# Tracce di potenza grezze
```

```
axs[0].plot(power_traces[0], alpha=0.5,
label="Traccia di Potenza")
```

```
axs[0].set_title("Tracciato di Potenza Singolo")
```

```
axs[0].set_xlabel("Tempo")
```

```
axs[0].set_ylabel("Consumo di Potenza")
```

```
axs[0].legend()
```

```
# Confronto tra le ipotesi di chiave
```

```
axs[1].plot(hypothesis_correct, label="Ipotesi
Corretta", color="blue")
```

```
axs[1].plot(hypothesis_wrong, label="Ipotesi
Errata", color="red", linestyle="dashed")
```

```
axs[1].set_title("Media del Consumo di Potenza per Diverse
Ipotesi di Chiave")
```

```
axs[1].set_xlabel("Tempo")
```

```
axs[1].set_ylabel("Consumo Medio di Potenza")
```

```
axs[1].legend()
```

```
# Differenza media del DPA
```

```
axs[2].plot(dpa_differential, label="Differenza Media DPA",
color="green")
```

```
axs[2].axhline(y=0, color="black", linestyle="dashed")
```

```
axs[2].set_title("Differenza Media del Consumo di Potenza (DPA)")
```

```
axs[2].set_xlabel("Tempo")
```

```
axs[2].set_ylabel("Differenza di Potenza")
```

```
axs[2].legend()
```

```
plt.tight_layout()
```

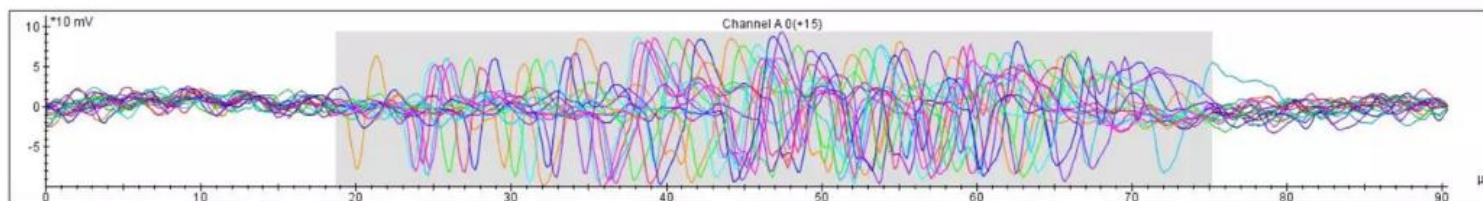
```
plt.show()
```

Bypassing Misalignment with CNNs

Neural Network: Input Layer > ConvLayer > 36 > 36 > 36 > Output Layer

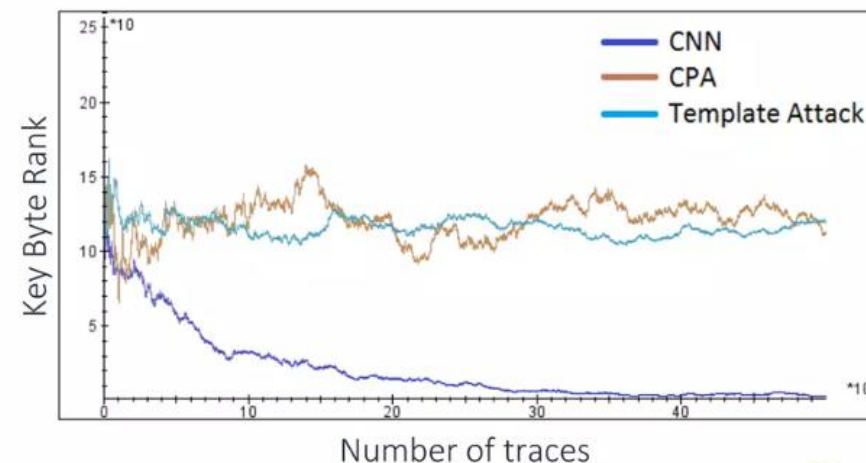
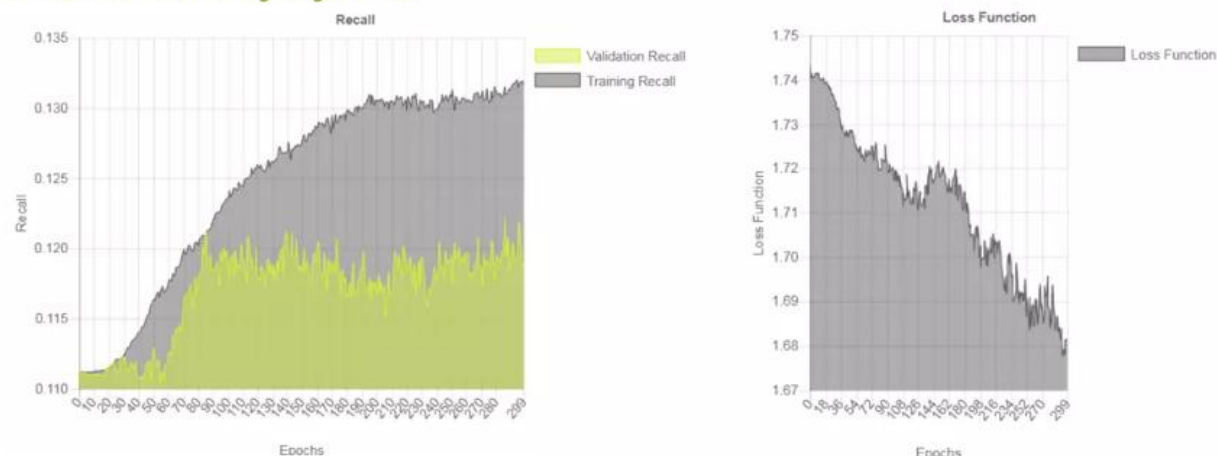
Training/validation/test sets: 90000/5000/5000 traces of 500 samples

Leakage Model: HW of S-Box Out (Round 1) → 9 classes

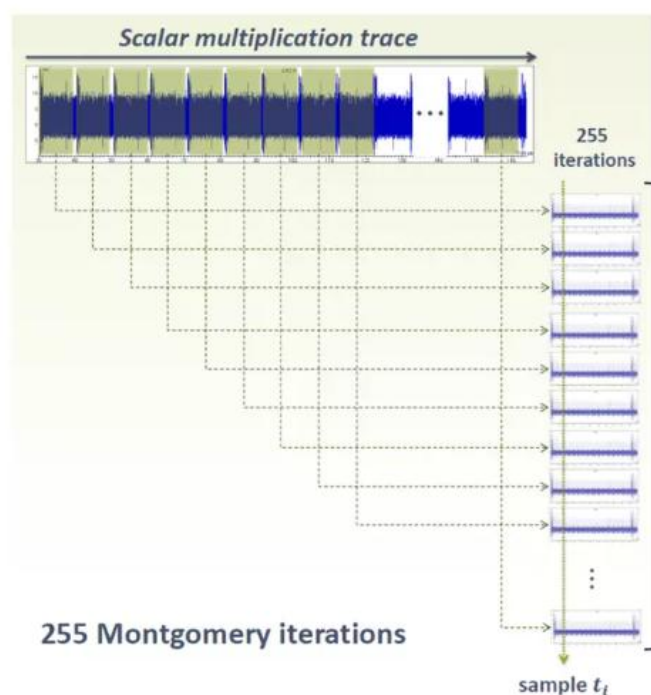


Use Data Augmentation
as regularization
technique to improve
generalization

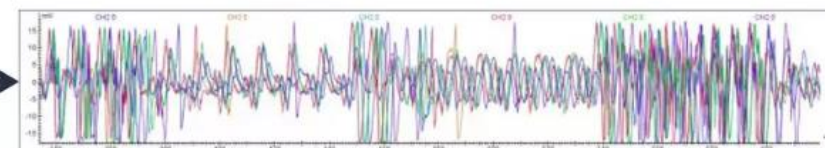
Results for key byte 0:



Breaking protected ECC



Misaligned traces

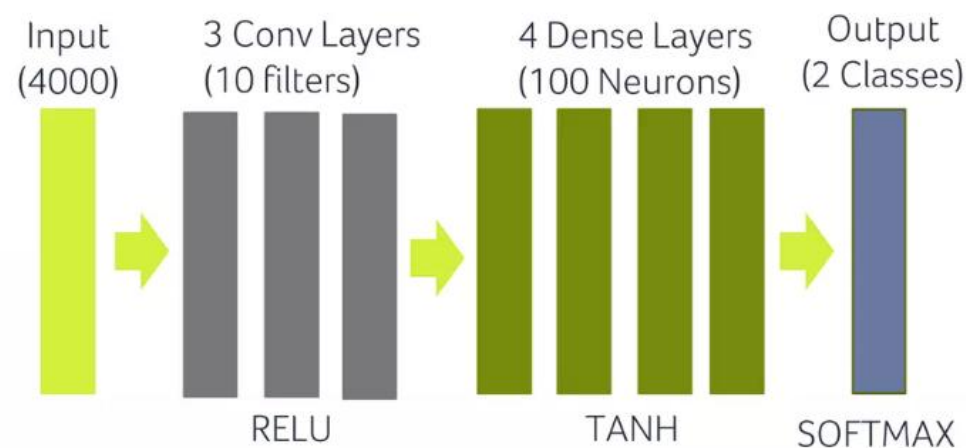


Unsupervised/Supervised Horizontal Attack: 60% success rate

Deep learning: 90% success rate

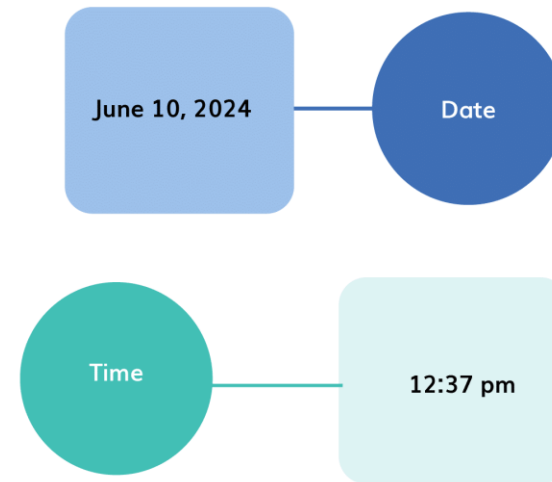
Deep learning(+ data augmentation): 99.4% success rate

Data augmentation: 25k $\rightarrow$ 200k traces.

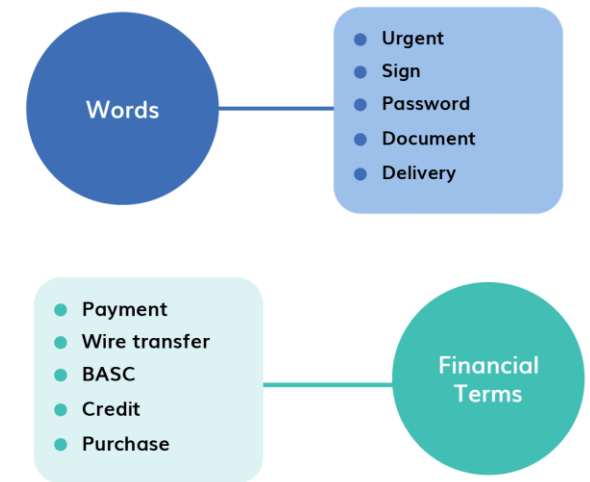


- Nel 2024, gli attacchi di phishing hanno registrato una crescita significativa a livello globale, sia in termini di volume che di sofisticazione.
- Il 10 giugno 2024, esattamente alle 12:37, ha segnato il picco dell'attività di phishing dell'anno. Tra il 1° aprile e il 30 giugno, le e-mail di phishing hanno registrato un'impennata del 28% rispetto al primo trimestre del 2024.
- I truffatori si sono affidati a parole che attirano l'attenzione come "urgente", "firma", "password", "documento" e "consegna" per attirare le persone, insieme a termini finanziari come "pagamento", "bonifico", "BACS", "credito" e "acquisto".

The most phished day of 2024:



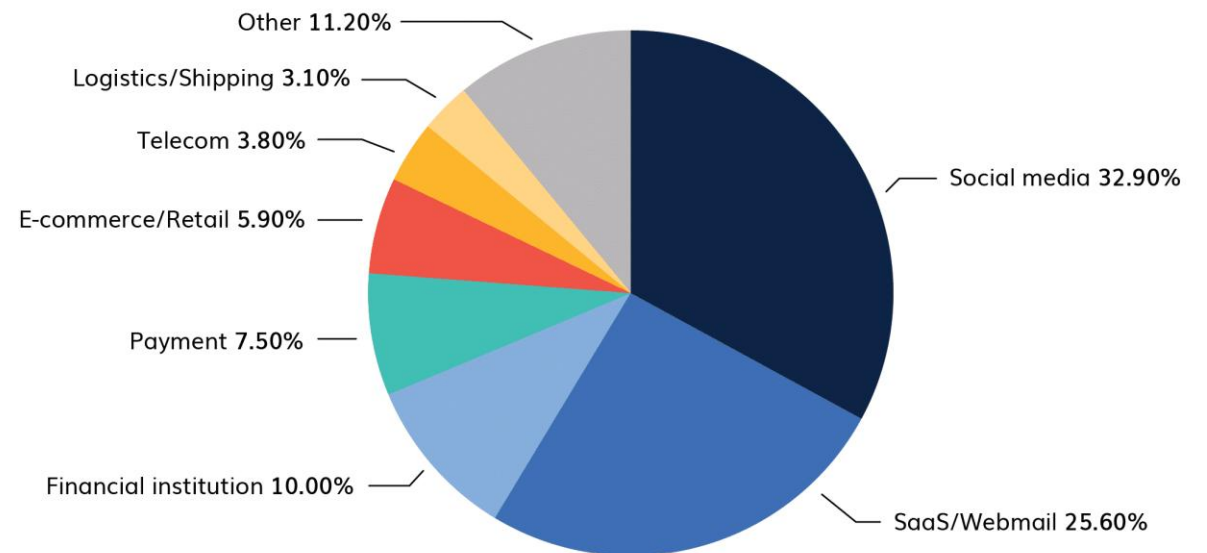
Top phishing indicators:



POWERDMARC

- Quarto trimestre 2024: Secondo l'APWG (Anti-Phishing Working Group), sono stati osservati 989.123 attacchi di phishing, in aumento rispetto ai 877.536 del secondo trimestre e ai 932.923 del terzo trimestre dello stesso anno.
- Aumento complessivo: Il numero totale di attacchi di phishing nel 2024 ha superato i 3,7 milioni, segnando un incremento del 60% rispetto all'anno precedente-
- Gli attacchi di phishing nel secondo trimestre del 2024 hanno preso di mira soprattutto i social media (32,9%), seguiti da SaaS/Webmail (25,6%) e dalle istituzioni finanziarie (10%). Questi settori sono probabilmente presi di mira a causa dell'ampia base di utenti e dei dati preziosi associati a queste piattaforme.

Phishing most targeted industry sectors worldwide Q2 2024



- Il 95% dei responsabili IT afferma che i cyberattacchi sono oggi più sofisticati che mai.
- Le e-mail di phishing realizzate manualmente richiedono in media 16 ore per essere prodotte.
- Con l'intelligenza artificiale, un'e-mail di phishing ingannevole può essere generata in soli 5 minuti. Questo salto di efficienza apre la strada ad attacchi su larga scala con un investimento minimo di tempo.
- Il tempo medio impiegato dagli utenti per cadere nelle e-mail di phishing è allarmante, spesso inferiore ai 60 secondi.
- L'errore umano è una vulnerabilità critica, che gioca un ruolo nel 74% di tutte le violazioni.
- Nonostante la formazione in materia di sicurezza, le persone sono ancora propense a cliccare sui link di phishing a causa di abitudini radicate o di tattiche di social engineering ben congegnate.
- Solo un dipendente su quattro ritiene che le proprie organizzazioni siano pienamente preparate ad affrontare le minacce di phishing attraverso i vari canali. Ad aggravare il problema, solo il 29% delle e-mail di phishing viene segnalato con precisione dai dipendenti, sottolineando le lacune sia nella consapevolezza che nelle capacità di rilevamento.

- L'integrazione tra **intelligenza artificiale**, **cybersicurezza** e **Industria 4.0** rappresenta una delle sfide più complesse e strategiche del panorama industriale contemporaneo.
- L'automazione spinta, l'interconnessione tra dispositivi (IoT) e la digitalizzazione dei processi produttivi offrono enormi vantaggi in termini di efficienza, flessibilità e competitività, ma espongono le imprese a nuovi e crescenti rischi di natura informatica.
- L'**intelligenza artificiale**, se ben implementata, si sta rivelando una risorsa chiave per la difesa delle infrastrutture industriali: consente di rilevare minacce in tempo reale, anticipare comportamenti anomali e automatizzare le risposte agli attacchi, aumentando la resilienza dei sistemi.

- Tuttavia, l'IA stessa può diventare un bersaglio o addirittura uno strumento nelle mani di attori malevoli, richiedendo un approccio etico e sicuro al suo sviluppo e impiego.
- I dati mostrano chiaramente che il settore manifatturiero, uno dei pilastri dell'Industria 4.0, è oggi tra i più colpiti dagli attacchi informatici, in particolare in Paesi come l'Italia. Questo evidenzia l'urgenza di adottare strategie di **cybersicurezza by design**, che integrino la sicurezza fin dalla fase progettuale delle soluzioni digitali.
- In sintesi, il futuro dell'Industria 4.0 dipenderà dalla capacità delle imprese di **conciliare innovazione tecnologica e sicurezza digitale**, facendo dell'IA non solo un motore di trasformazione, ma anche una sentinella intelligente a difesa dell'ecosistema produttivo.

Crittografia Post-Quantistica

- Nuovi algoritmi di crittografia resistenti agli attacchi quantistici e side-channel.

Uso dell'Intelligenza Artificiale per la Cybersecurity

- Machine learning per il **rilevamento di anomalie nei consumi energetici e nei segnali elettromagnetici**.
- AI che monitora il comportamento dei dispositivi crittografici e rileva tentativi di attacco in tempo reale.

Tecnologie di Sicurezza Hardware Avanzate

- Sviluppo di processori crittografici **completamente resistenti ai side/cover-channel attacks**, per applicazioni di intelligence e difesa.

➤ Formazione e consapevolezza informatica, etica e giuridica

- **Approccio multidisciplinare** che unisca:
 - ✓ **Protezione fisica (schermatura, jamming)**
 - ✓ **Difese software (OS sicuri, randomizzazione dei tempi)**
 - ✓ **Analisi avanzata con AI per il rilevamento di anomalie**

