Machine Learning Algorithms in Cyber Security: Protecting Networks and Detecting Attacks

Assoc. Prof. Emil SIMION

UNSTPB, Centre for Research and Training in Innovative Techniques of Applied Mathematics in Engineering & Advisor of Director of DNSC

Email: emil.simion@upb.ro

joint work with Assist. Prof. Ioana-Corina BOGDAN

Transilvania University of Brașov & CiTi, Email: corina.bogdan@unitbv.ro

Agenda

- What is Ransomware?
- Why Machine Learning in Cybersecurity?
- Machine Learning Algorithms for Ransomware Detection
- Case Study – WannaCry
- The Ransomware Detection Process
- Challenges and Vulnerabilities in ML for Cybersecurity
- Mitigation Strategies
- The Future of AI in Cybersecurity
- Conclusions

What is Ransomware?

Ransomware explained: How it works and how to remove it | CSO Online

- Type of malware that encrypts users' files

and demands a ransom for their release

- Examples of ransomware attacks
- Ransomware targets individuals and organizations, hospitals, banks, or government institutions.
- The main challenge is that traditional security solutions often fail to detect modern ransomware, which evolves rapidly.

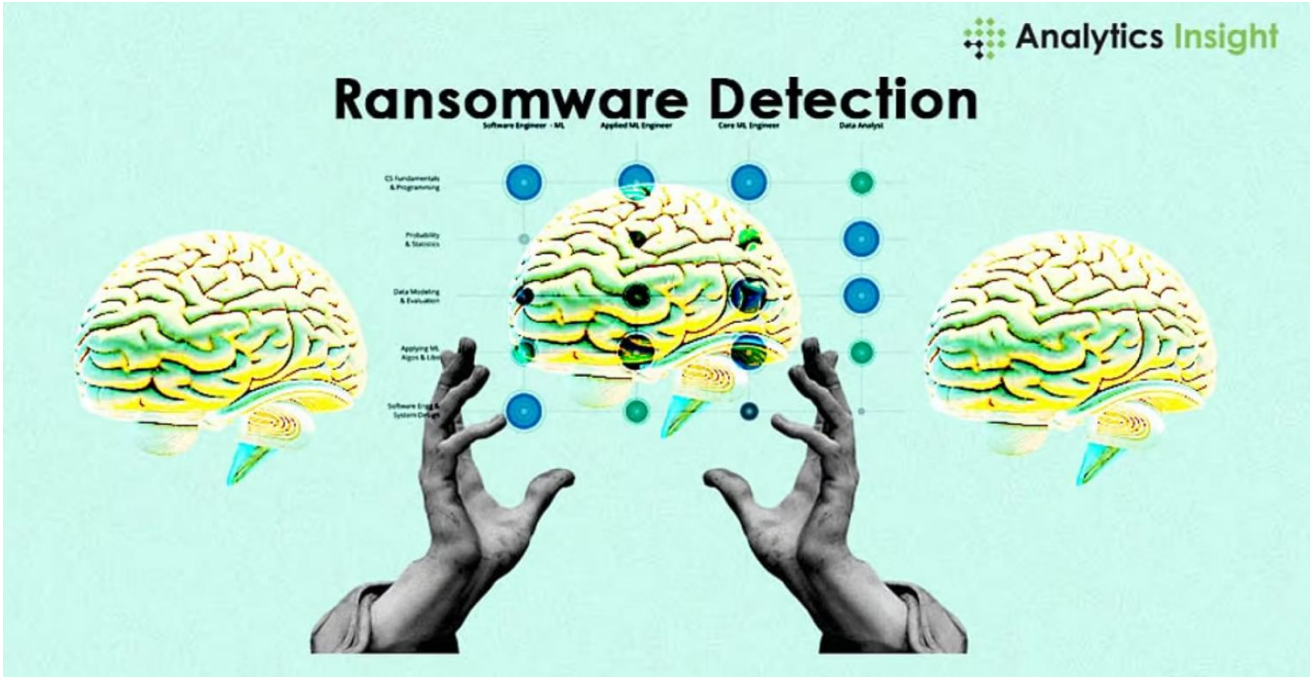
Why Machine Learning in Cybersecurity?

- Traditional security methods rely on detecting known signatures, which is ineffective against evolving malware
- Machine Learning advantages
- Mandiant report reveals : 91% of cyberattacks do not trigger initial alerts

Machine Learning in Cybersecurity: A Proactive Approach | PECB

Machine Learning Algorithms for Ransomware Detection

- Classification Algorithms
- Anomaly Detection
- Neural Networks



Essential Machine Learning Algorithms for Ransomware Detection

Case Study – WannaCry

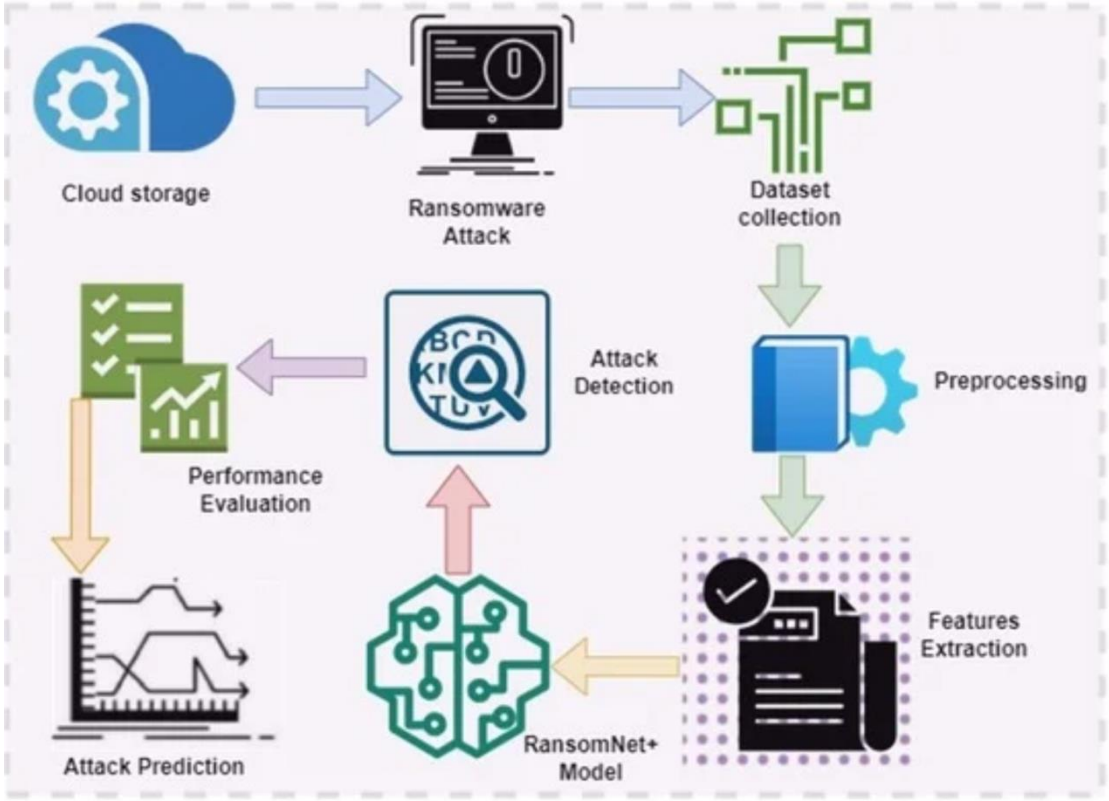
- The most devastating ransomware attacks.
- How was it detected using ML?

ML can significantly shorten response times !

Countries initially affected in WannaCry ransomware attack - WannaCry - Wikipedia

The Ransomware Detection Process

- Data Collection
- Data Preprocessing
- Data, Knowledge, Insight, Wisdom (DIKW) model
- ML Model Training
- Model Testing and Validation
- Deployment in Security Systems



Enhancing Ransomware Attack Detection Using Transfer Learning and Deep Learning Ensemble Models on Cloud-Encrypted Data

Challenges and Vulnerabilities in ML for Cybersecurity

- Despite its advantages, Machine Learning has security challenges:
  - Training Data Poisoning
  - Attacks on ML Models
  - Cloud Dependency Risks
- Conclusion: **ML must be combined with other security measures to remain effective.**

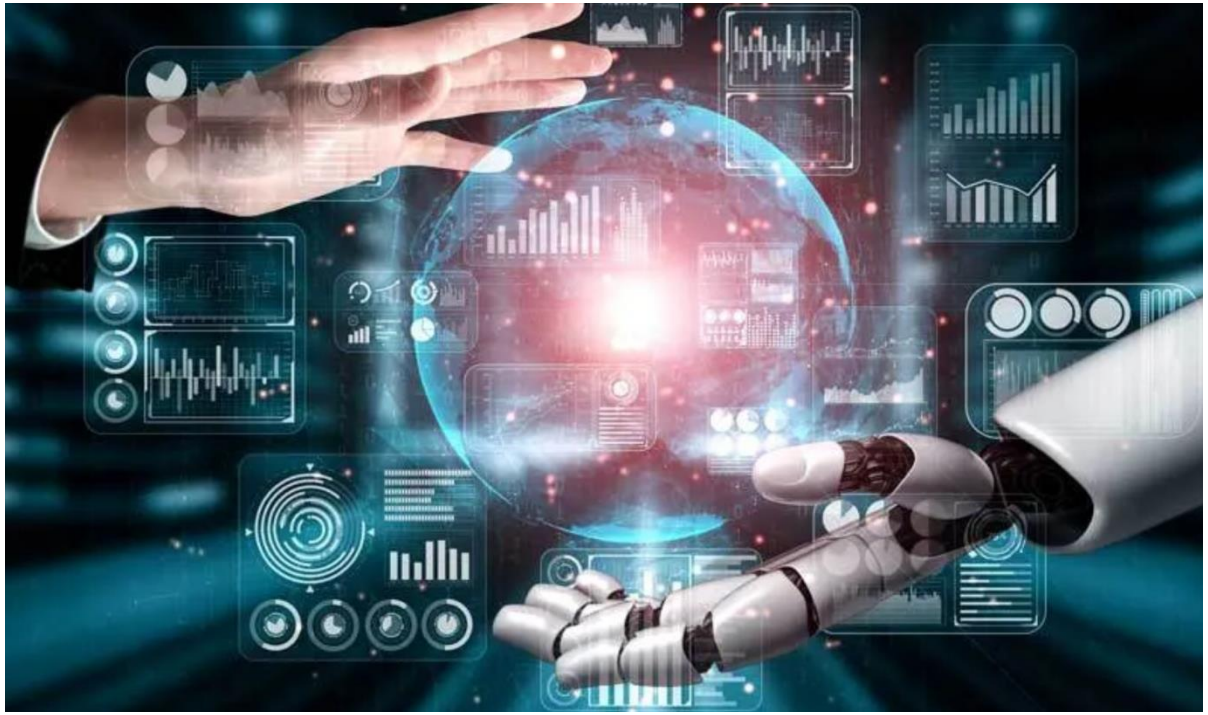
Mitigation Strategies

- Secure Training Data
- Protecting ML Models
- Continuous Monitoring and Updates
- These strategies significantly enhance ML-based cybersecurity effectiveness.

S. Hakak, W. Z. Khan, M. Imran, K. -K. R. Choo and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," in *IEEE Access*, vol. 8, pp. 124134-124144, 2020.

The Future of AI in Cybersecurity

- AI and Quantum Computing
- The Risk of Self-Replicating AI
- AI Regulations and Ethics



The Future of AI and Its Impact on Cybersecurity | Bluefin

Conclusions

- Machine Learning improves ransomware detection and response time.
- Machine Learning-based security must be protected from adversarial attacks.
- Future depends on balancing technology, regulation, and security.

Thank you!
Q&A