# AI MODELS IN CYBERSECURITY

NASANTOGTOKH AMARSAIKHAN
MNCERT/CC

MN CERT/CC
Mongolian Cyber Emergency Response Team / Coordination Center

# CONTENTS

# CHALLENGES

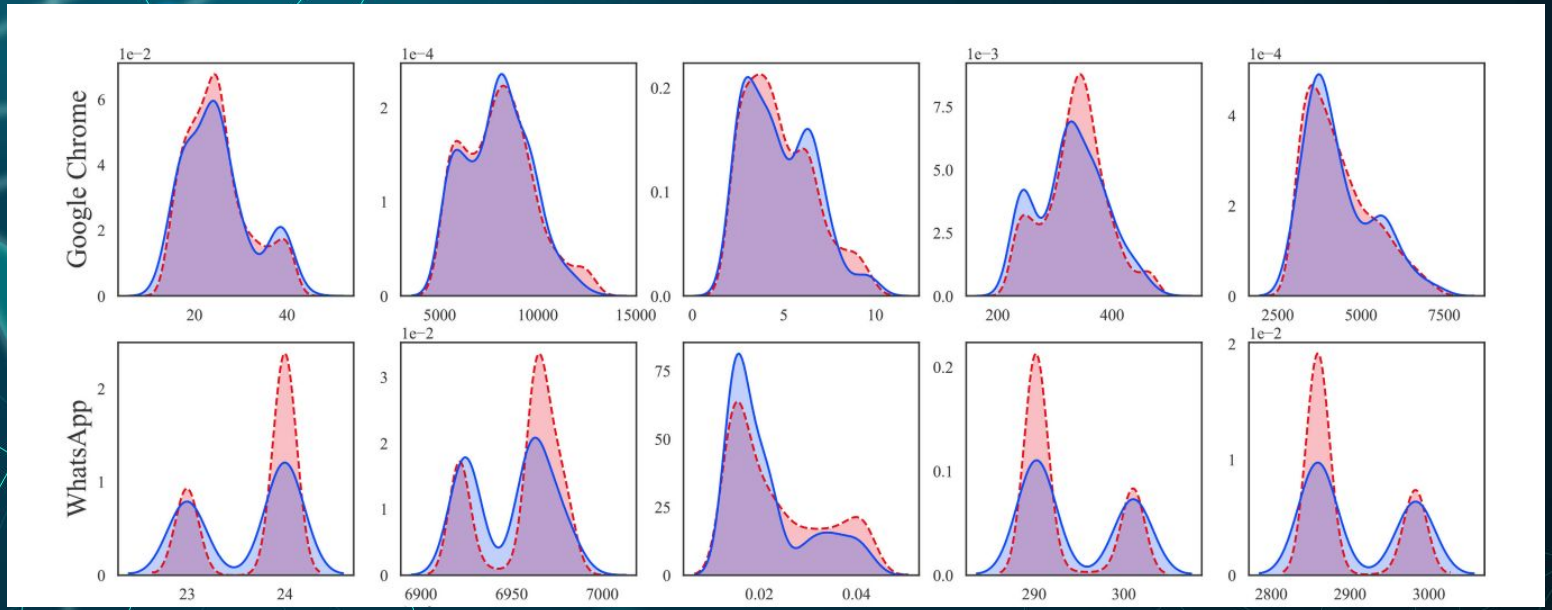
**Cloud Resources** - Geographically-distant IT resources
Complexity, Shared responsibility

**Speed of technical advancement**, and software development
Agile development etc

IoT devices - **Everything is connected** to internet

Hackers who have **AI/ML skillset**

Can you guess which one of the photo is real?




Source: Sina and Roberto, 2020. “GAN tunnel”

Can you tell which **network traffic sampling** is Real application?

Are you confident that your IDS/IPS can differentiate between real and fake data?


With proper tuning **AI/ML** can do myriad of things for you

# AI/ML

Algorithm that can **learn** and operates **on its own** with its learnt behaviour

*Supervised, Unsupervised, Semi-supervised, Reinforced*

Trained models (in general) can do **clustering**, **classification**, **regression**, **prediction**, or even they can **generate** things

AI/ML is **double-edged sword**.

# AI-WIELDED HACKER

What they can do with AI/ML?

# AI POWERED ATTACKS

Fake voice scamming

**DEEP FAKE VOICE**

Exploiting Firewall, IDS and IPS

**CLUSTERING MODEL**

Password Cracking with AI Powered Tools

**PassGAN**

# AI POWERED ATTACKS

Smart malware, no C&C

**DECISION TREE MODELS**

Custom crafter phishing emails

**NLP**

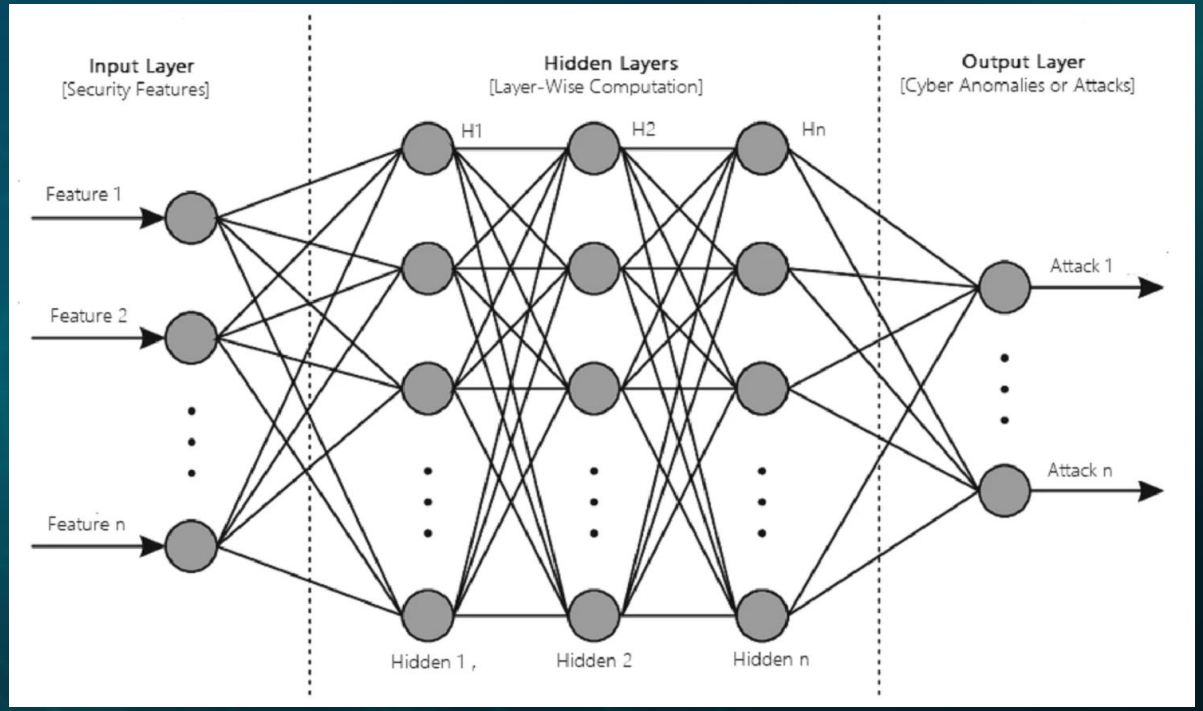
Traffic Stegno

**GAN TUNNEL**

Mining Zero-Day Vulnerabilities

**INTELLIGENT PENTESTING**

# AI POWERED ATTACKS




Source: Iqbal, Hasan and Raza, 2021. “AI-Driven Cybersec”

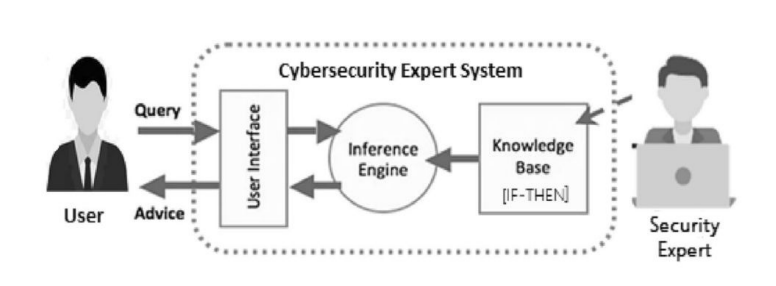
# How to overcome those challenges?

# Automation, AI/ML ...

# AI-DRIVEN CYBERSECURITY

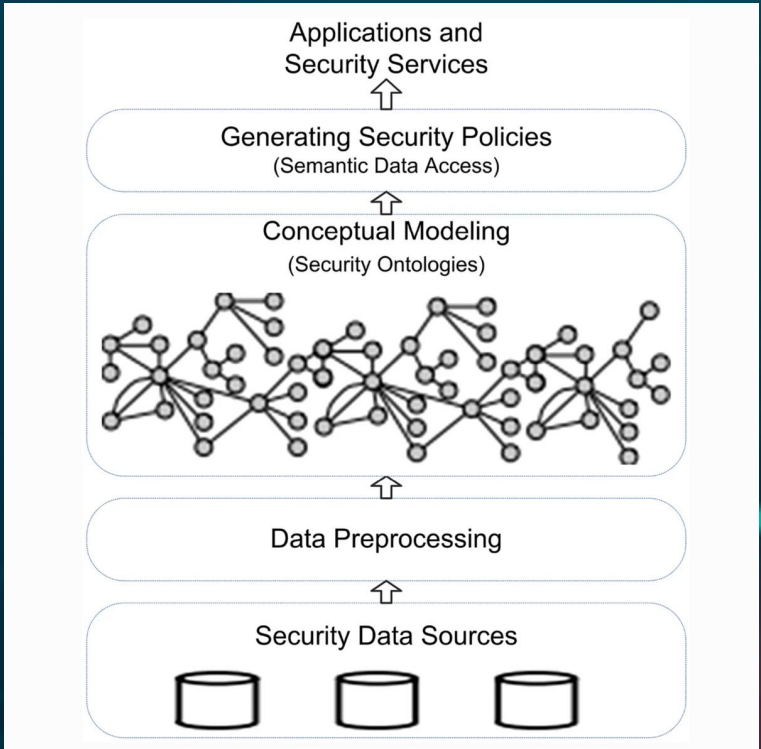
What we can do with AI/ML?

# TRADITIONAL

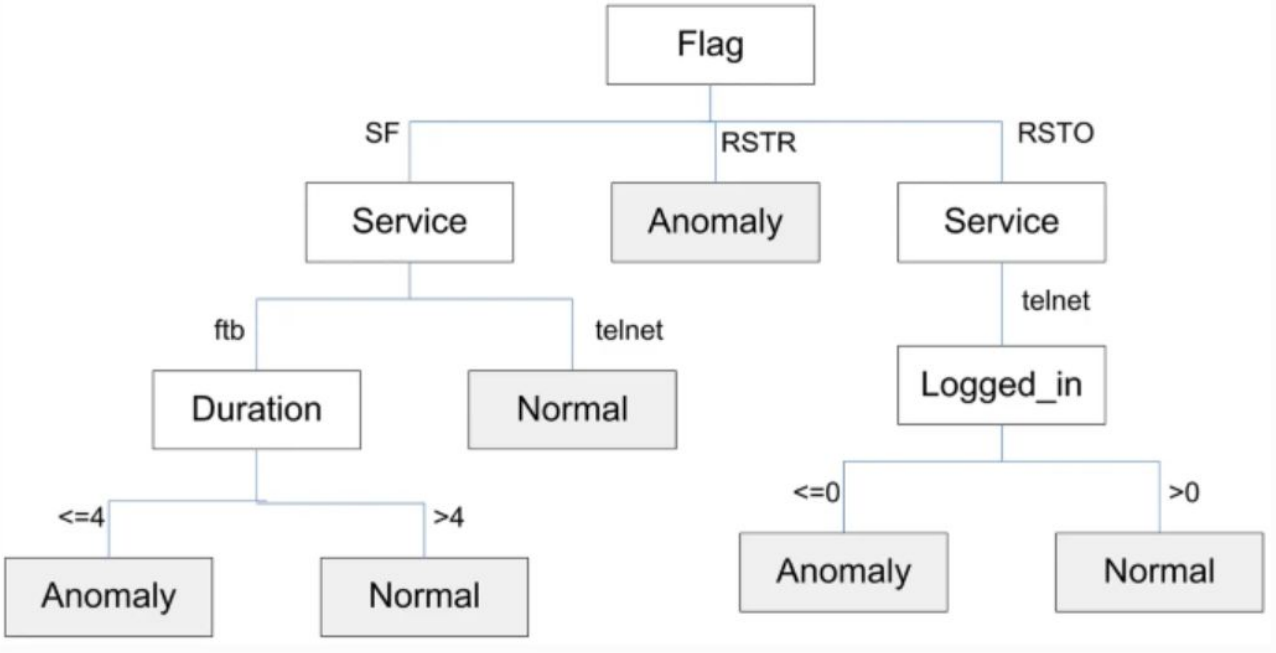



IF
<antecedent>
<antecedent> THEN
<consequent>

# AI-DRIVEN



# Decision tree-based detection model




An example of detecting cyber anomalies based on a decision tree-based machine learning model

Source: Iqbal, Hasan and Raza, 2021. "AI-Driven Cybersec"

# Detection/Prevention with AI/ML

Example of those systems.
Intrusion Prevention System (IPS) with **optimal stopping** (reinforcement learning). IPS will choose optimal stopping point

# Conclusion

Speed of development, Cloud infrastructure

Offensive usage of AI/ML would make defense difficult

AI/ML defense mechanism is required

Attack on AI/ML defense mechanism would be more critical

# THANK YOU!