AI-Powered Cybersecurity & Public-Private Synergy

Presented by- Alok Verma
Cyber World Organization

Introduction

It is nothing new when we discuss artificial intelligence in cyber security. Two years ago, people in forums, used to discuss how artificial intelligence and machine learning would change the future of cyber security because data is at the heart of cyber security trends.

Cybersecurity “So What?”

Did You Know?

Antivirus software is available for mobile devices, which are an easy, common target for hackers and other bad actors.

Cybersecurity Common Sense

- Being safe online isn’t so different from being safe in the physical world!
- Keep Calm and Trust Your Gut!

it can also serve as a new weapon for cybercriminals who can use this technology to speed up their techniques and improve their cyberattacks.

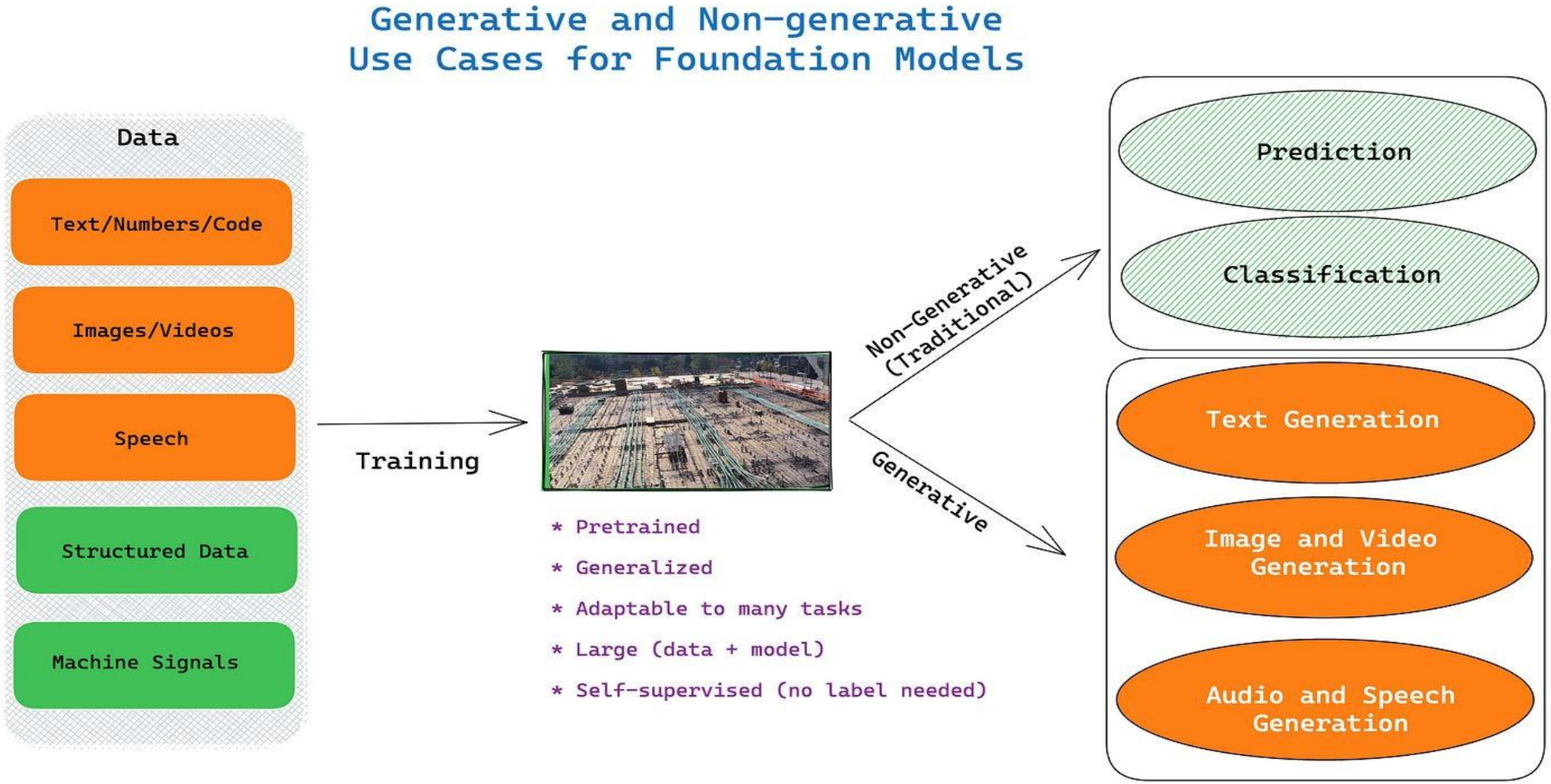
Do Your Part.

#BeCyberSmart

Cybersecurity starts with YOU and is everyone's responsibility.

There are currently an estimated 5.2 billion internet users or 63% of the world's population.

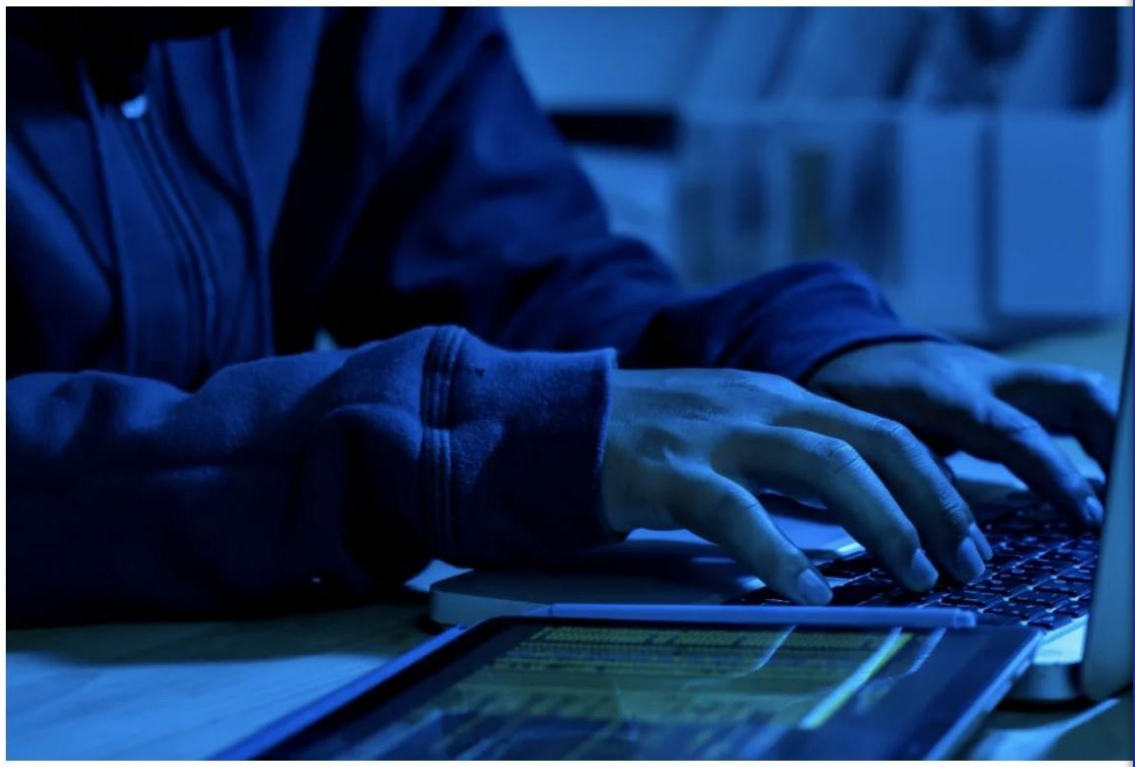
GenAI Performs in Multiple Contexts



Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024



Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company’s chief financial officer in a

CYBER WORLD

TECHNOLOGY

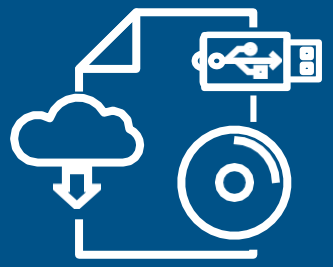
That Colleague or Customer on Zoom Might Be an AI Deepfake. Here's How You Can Tell

Think it can't happen? A Hong Kong company just lost $25.6 million to a deepfake version of its CFO.

EXPERT OPINION BY MINDA ZETLIN, AUTHOR OF 'CAREER SELF-CARE: FIND YOUR HAPPINESS, SUCCESS, AND FULFILLMENT AT WORK' @MINDAZETLIN

FEB 8, 2024

Fake News in Elections!



PHYSICAL CYBER ATTACKS

Did You Know?

Anything connected to the internet is potentially vulnerable, from e-scooters to laptops to cargo ships.

What is it?

Physical cyber attacks use hardware, external storage devices, or other physical attack vectors to infect, damage, or otherwise compromise digital systems. This can include…

- USB storage devices
- CD/DVD
- Internet of Things (IoT)

Why should you care?

- Easy to overlook
- Difficult to identify and detect
- Extremely difficult to remove
- Can do anything from installing ransomware, to sending copies of or modifying information systems, to dismantling networks

Would This Email Fool You?

New message

From Legitimate-Looking-Source@notquiteyourworkemail.com

Subject Ugent IT Update: Software Vulnerability

Software Update

Good afternoon Tom,

A vulneribility has been identified in “Big Name Software” that allows an attacker to record calls and videos from your computer without your knowldge. Please install the attacked update by the end of the day or your workstation will be locked.

We have also created app for all employees to determan if they been affected by this vulnerability. Click here to run the app.

www.fakewebsite.com/gotcha.exe
Click or tap to follow link.

Sincerely,
BossMann
Your Company IT Department

REPLY

OTHER AVENUES OF ATTACK

What is it?

- Internet of everything
- Any device connected to your network
- Information collection
- Remote access
- Bluetooth
- Open ports

Why should you care?

- Your network can be used to attack someone else
- Any device that stores information or is connected to the internet can be a vulnerability
- Assume that you are vulnerable, and take measures to understand and mitigate risk
- Don‘t be the “low-hanging fruit”

Examples

- Smart devices
- Mobile phone
- Thermostat
- Vehicles
- Gaming consoles
- Printers
- Medical equipment
- Industrial systems

How Can You Better Protect Yourself Online?

Secure your networks.

Wireless routers are a way for cybercriminals to access online devices.

Stay up to date.

Keep software updated to the latest versions and set security software to run regular scans.

If You Connect It, Protect It.

One proven defense against intrusion is updating to the latest virus protection software.

Double your login protection.

Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you.

“Cybersecurity is an ongoing journey, not a final destination—continuous vigilance, adaptation, and innovation are key to staying ahead of evolving threats.”

Mr. Alok Verma
alokverma.cyber4u@gmail.com
+91 6386949793