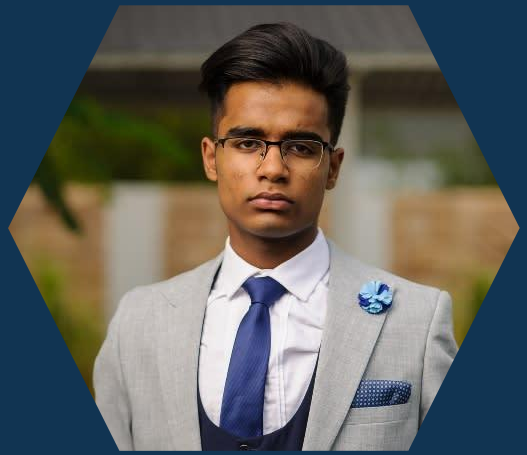
Recent Developments in Cybersecurity

HyperionDev

Welcome



Lecturer: Liano Naidoo

Moderator: Zahir Junjeo

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Covered some basic operations using OpenSSL and GnuPG

Objectives

- Have a look at why Cyber Security is important
- Explore the recent developments within the industry
- Take a peek in to some events that have transpired in 2023 already

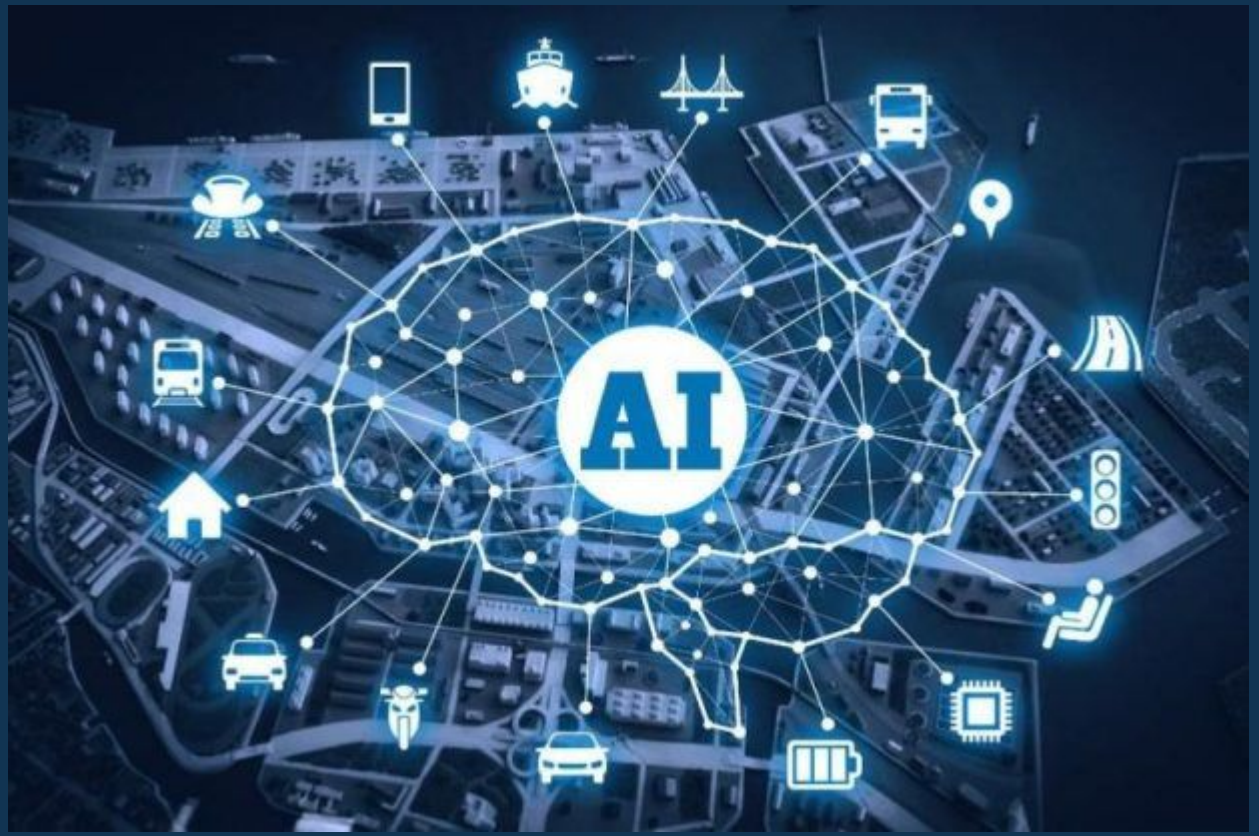
Importance of Cyber

- Cybersecurity is crucial in the digital age. In order to protect people, organizations, and governments from cyber threats, cybersecurity has become increasingly important as a result of our society's growing reliance on digital technologies and interconnected systems.

- Cybersecurity protects systems and networks from unauthorized access, attacks, and data breaches while ensuring the confidentiality, integrity, and availability of data.

- Cybercriminals use sophisticated methods like ransomware, phishing, social engineering, and advanced persistent threats (APTs), and the threat landscape is constantly changing as a result.

- The threat landscape has been expanded by the emergence of nation-state actors and cyberwarfare, which poses risks to critical infrastructure, governmental institutions, and geopolitical stability.



https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fwww.udayavani.com%2Fwp-content%2Fuploads%2F2023%2F05%2FAI-artificial-intelligence-iStock-2-620x413.jpg&f=1&nofb=1&ipt=3a25aa517cdaec267f02adac791731a9b6087d819677c7e6228b93b60b176994&ipo=images

Artificial Intelligence

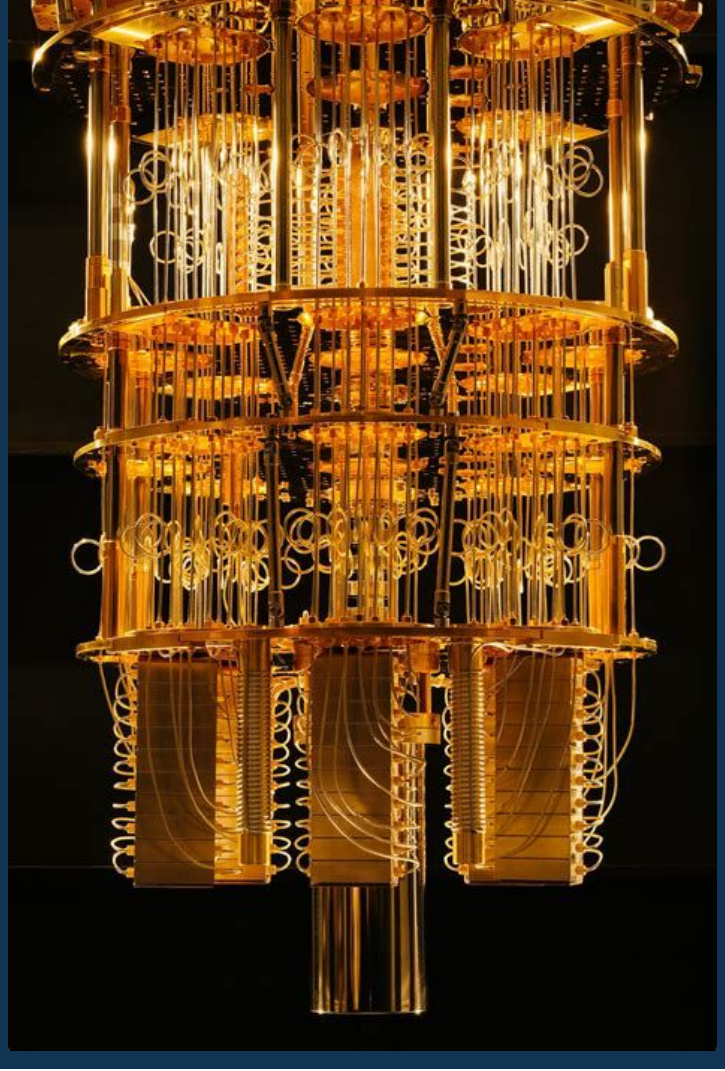
- AI algorithms and machine learning techniques make it possible to spot patterns and outliers in massive amounts of data, enabling proactive threat detection and quicker reaction times.

- AI-powered security systems can continuously analyze network traffic, behavior, and user activity to identify potential threats and trigger alerts or automated response actions.

- By monitoring user behavior and analyzing contextual data, AI-driven behavioral analytics can detect suspicious activities, such as unauthorized access attempts, privilege escalation, or insider threats.

- These analytics systems can help identify and respond to potential security incidents in real-time, reducing the impact of cyber attacks.

-



https://newsforkids.net/wp-content/uploads/2019/10/40786969122-9a55880199-b-d.jpg

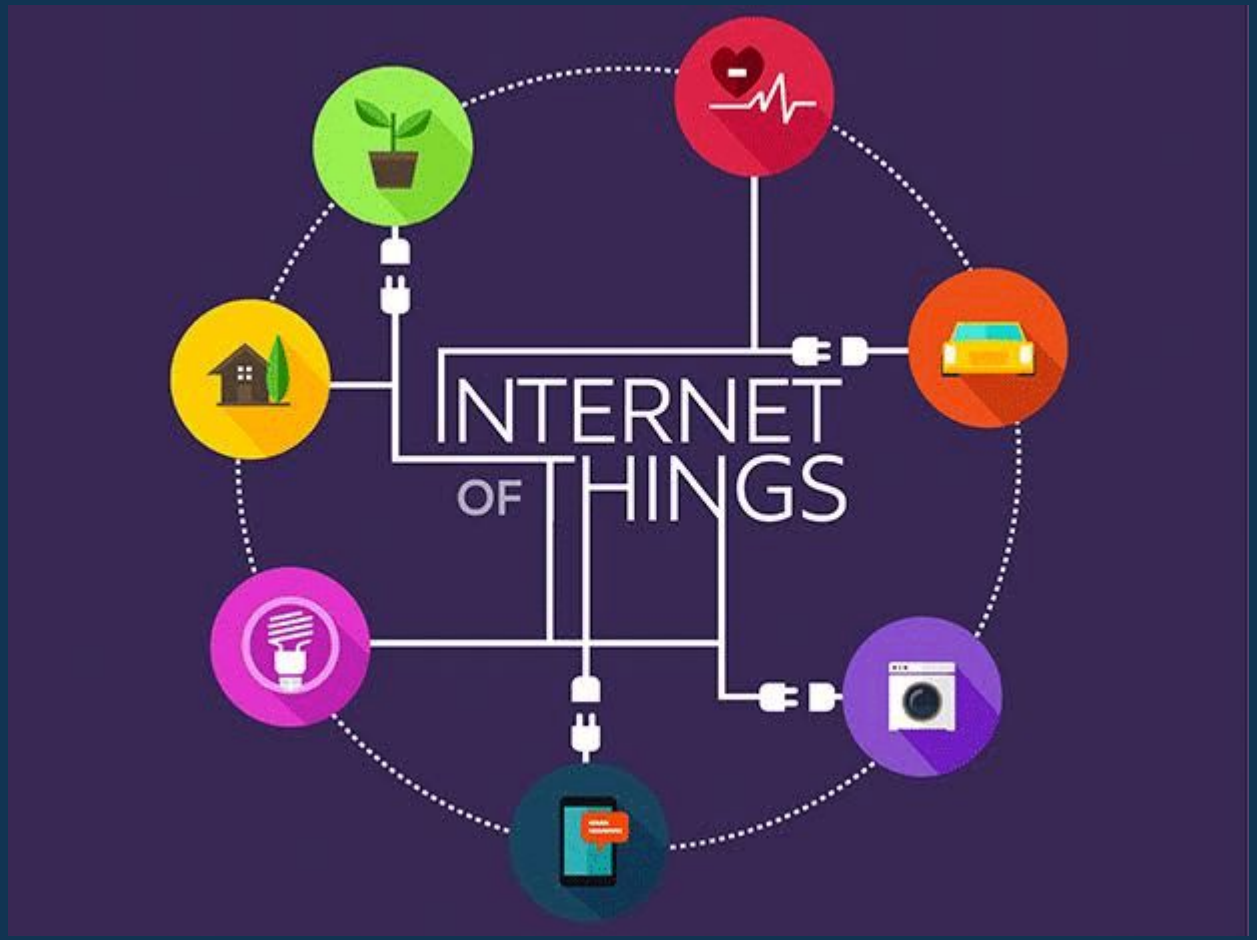
Quantum Computers

- Many of the cryptographic algorithms currently in use, such as RSA and elliptic curve cryptography (ECC), are susceptible to being broken by quantum computers. The security of sensitive data may be jeopardized by the enormous computational power of quantum computers, which may render conventional encryption techniques useless.

- To create cryptographic algorithms that can withstand attacks from quantum computers, post-quantum cryptography was created.

Homework:

Research the term Post-Quantum Cryptography.



https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Felectronicsmaker.com%2Fwp-content%2Fuploads%2F2016%2F08%2FInternet-of-Things.png&f=1&nofb=1&ipt=5f6e163330e14444fe5dcd49a72f50a261d312def0691f89262bceaa5524c5f6&ipo=images

Internet of Things(IoT)

Due to their extensive attack surfaces and frequently insufficient security measures, the proliferation of interconnected IoT devices poses serious security risks.

IoT devices can be exploited, which could result in data breaches, privacy violations, and the possible interruption of vital services.

Robust authentication mechanisms and access control policies are essential to prevent unauthorized access to IoT devices and networks.

Implementing strong authentication protocols, such as two-factor authentication, certificates, and secure communication protocols, can enhance IoT security.

Encrypting data transmitted between IoT devices and storage systems can protect against interception and unauthorized access.

Employing secure communication protocols, such as Transport Layer Security (TLS), can safeguard the integrity and confidentiality of IoT data.

Cloud Security

Cloud computing introduces unique security challenges, including data breaches, unauthorized access to cloud resources, and shared infrastructure vulnerabilities.

Organizations must understand and address these risks when migrating to the cloud and ensure the adoption of robust security measures.

Sensitive data is protected from unauthorized access and data leaks in the cloud by encrypting data both at rest and in transit.

Strong access control strategies, like identity and access management (IAM) solutions, can be implemented to make sure that only authorized users can access cloud resources.


LOGIN
Password
*****
ONLINE
PRIVACY
****
100%
PROTECTION
DATA
Card ***
- Autonomy
- Security
search ?

Privacy & Data Protection

Cloud computing introduces unique security challenges, including data breaches, unauthorized access to cloud resources, and shared infrastructure vulnerabilities.

Organizations must understand and address these risks when migrating to the cloud and ensure the adoption of robust security measures.

Sensitive data is protected from unauthorized access and data leaks in the cloud by encrypting data both at rest and in transit.

Strong access control strategies, like identity and access management (IAM) solutions, can be implemented to make sure that only authorized users can access cloud resources.

Wrapping up

To effectively reduce risks and defend against new threats, it is crucial to keep up with technological developments and develop creative cybersecurity solutions. This is because cyber threats are becoming more sophisticated and targeted.

Democratic processes promote transparency and accountability in the formulation and implementation of cybersecurity laws and regulations. Open discussions, public consultations, and legislative debates ensure that the decision-making process is transparent and subject to scrutiny.

Next up

Workshop Series! (Hands on Linux)

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

Questions and Answers