SECURITY AND PRIVACY CONCERNS IN IOT

Session 4

OBJECTIVES

In this session, you will learn to:

- Describe the role of IoT in the future
- Explain the Security and Privacy issues and Challenges involved
- Explain Subscription based charges
- Explain the concept of Trust in IoT

INTRODUCTION 1/3

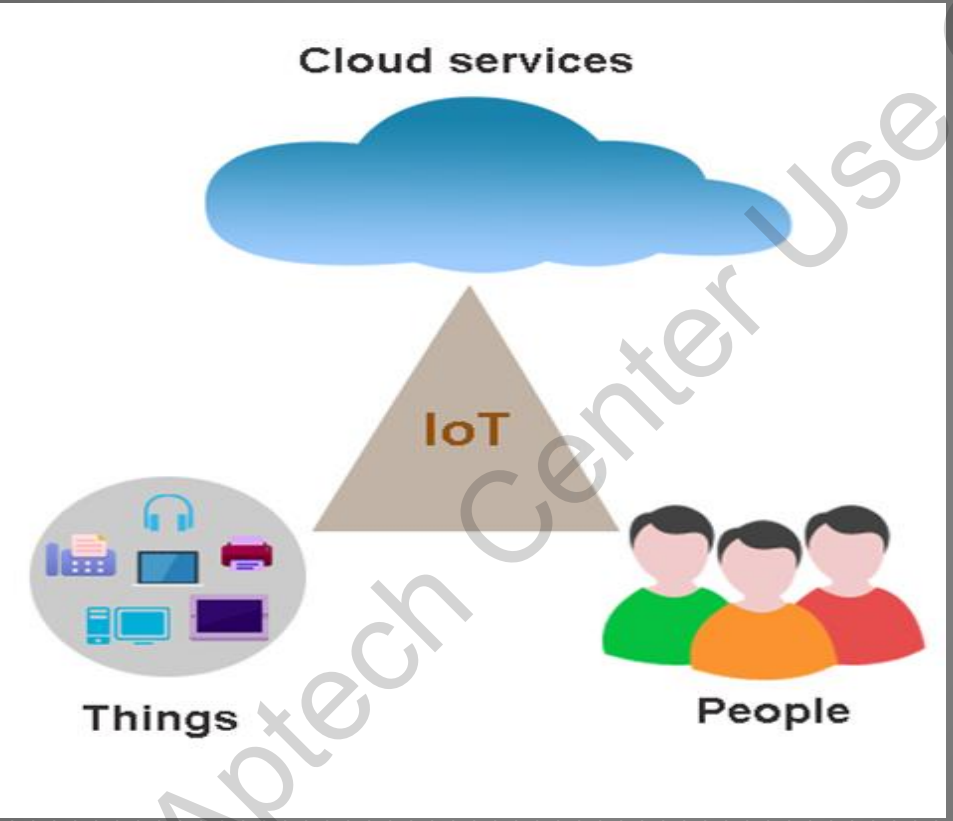
- IoT is an information network connecting virtual and physical objects
- Closely linked to sensitive infrastructures and strategic services
- Enables people and objects to interact with each other
- Protects the information of users from exposure

INTRODUCTION 2/3

- Provides integrated services
- The ‘things’ in the IoT environment transmits data
- Interoperability of things is essential for functioning
- Fragmented data produce sensitive information

Fundamentals of IoT

INTRODUCTION 3/3



FUTURE OF IOT 1/3

- Major channel for interconnecting devices
- Far-reaching access to all products
- Applications are independent
- Improve productivity and users' life

FUTURE OF IOT 2/3

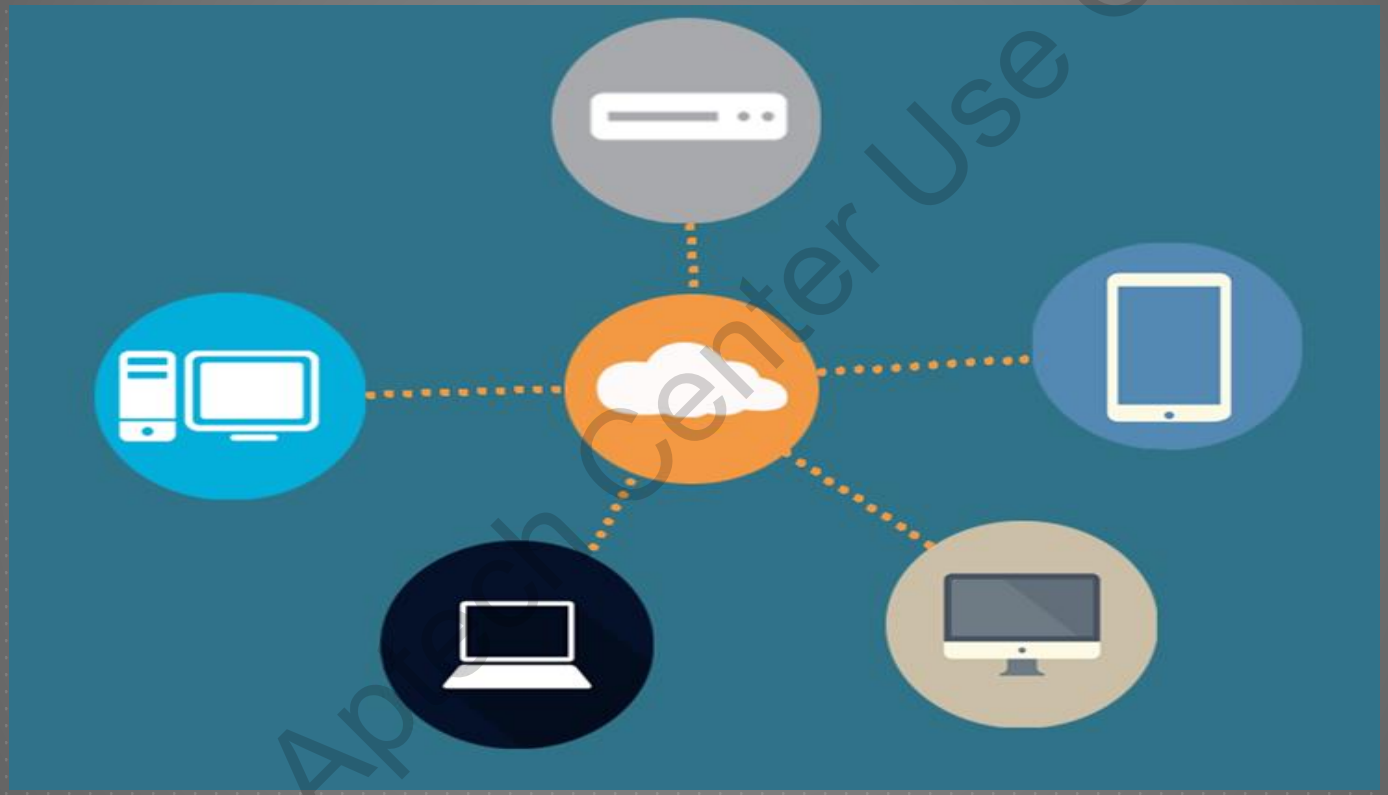
Monitoring and Reporting

Plants and Animals

Utility

Information

FUTURE OF IOT 3/3

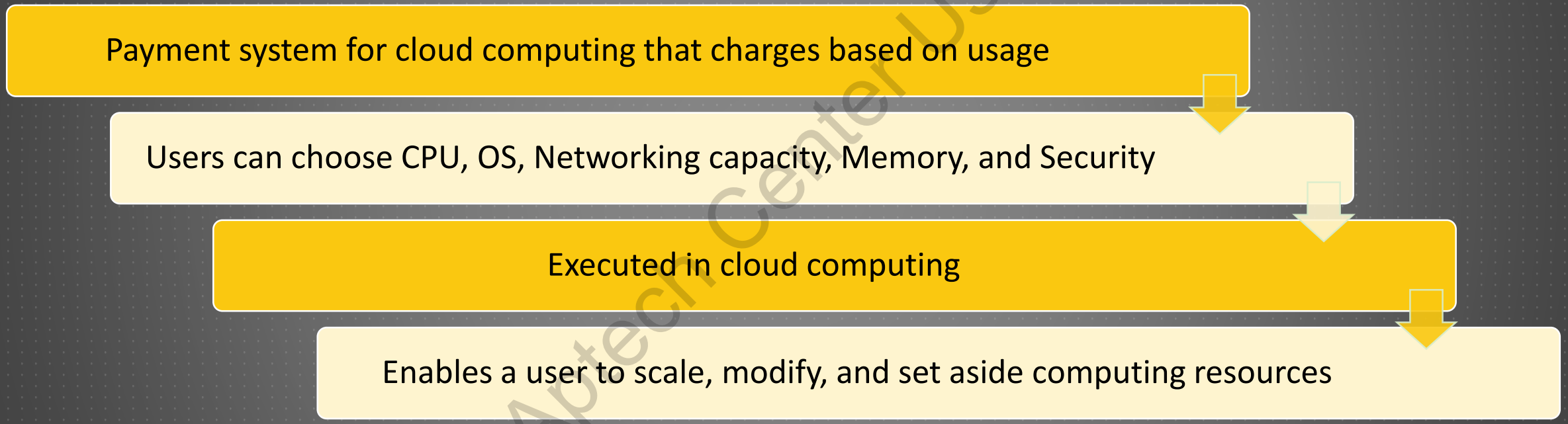


SUBSCRIPTION BASED SERVICES 1/2

- Allows a customer or organization to purchase or subscribe the IT services
- Monitors operational and diagnostic information in real-time
- Provides ‘As-a-Service’ model, which is centered on a pay-per-month/use business
- Anticipate on-going value and inimitable experiences

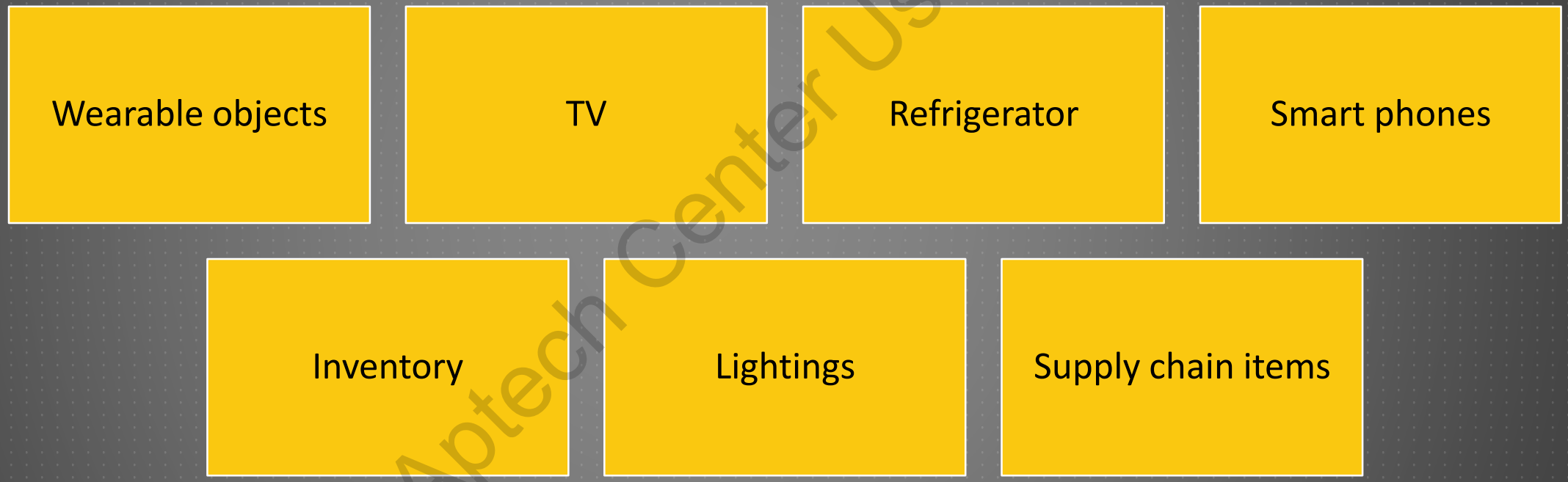
SUBSCRIPTION BASED SERVICES 2/2

- ‘Pay-As-You-Go’ Model



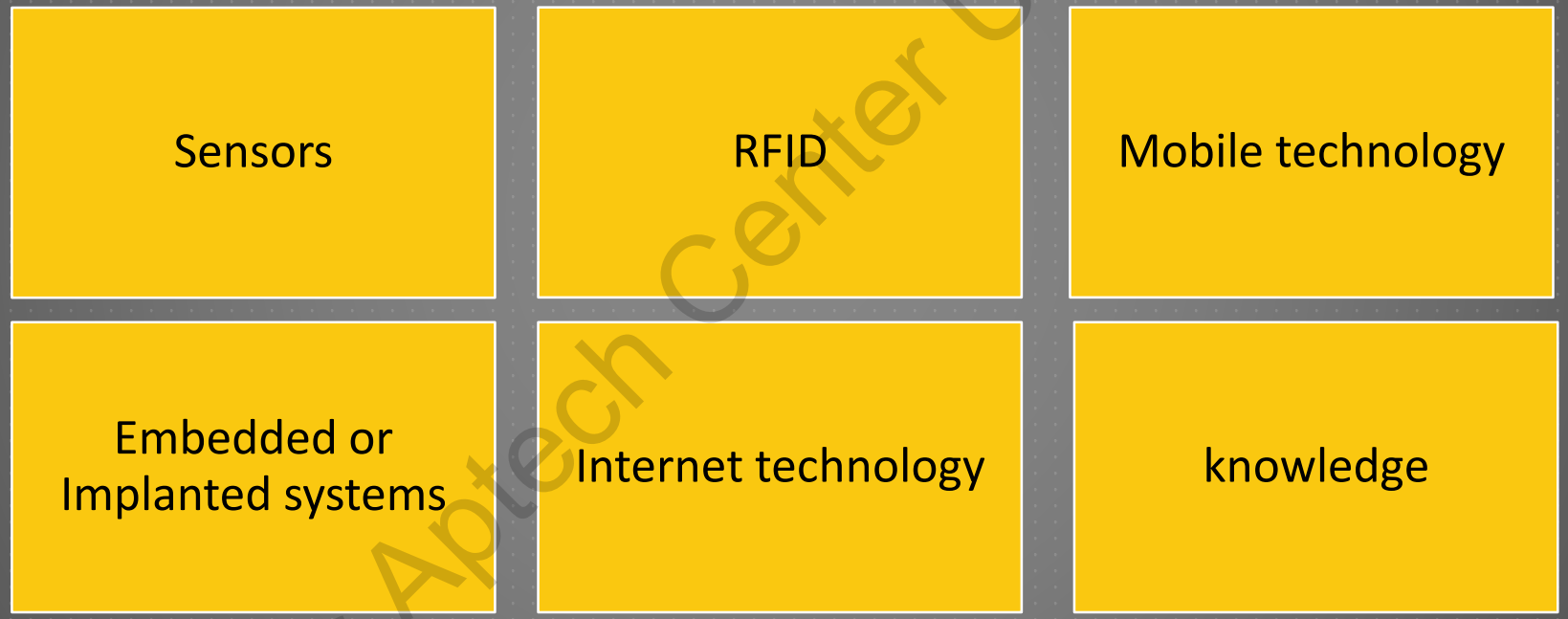
PRIVACY AND SECURITY ISSUES AND CHALLENGE 1/13

- IoT envisages as a universal network

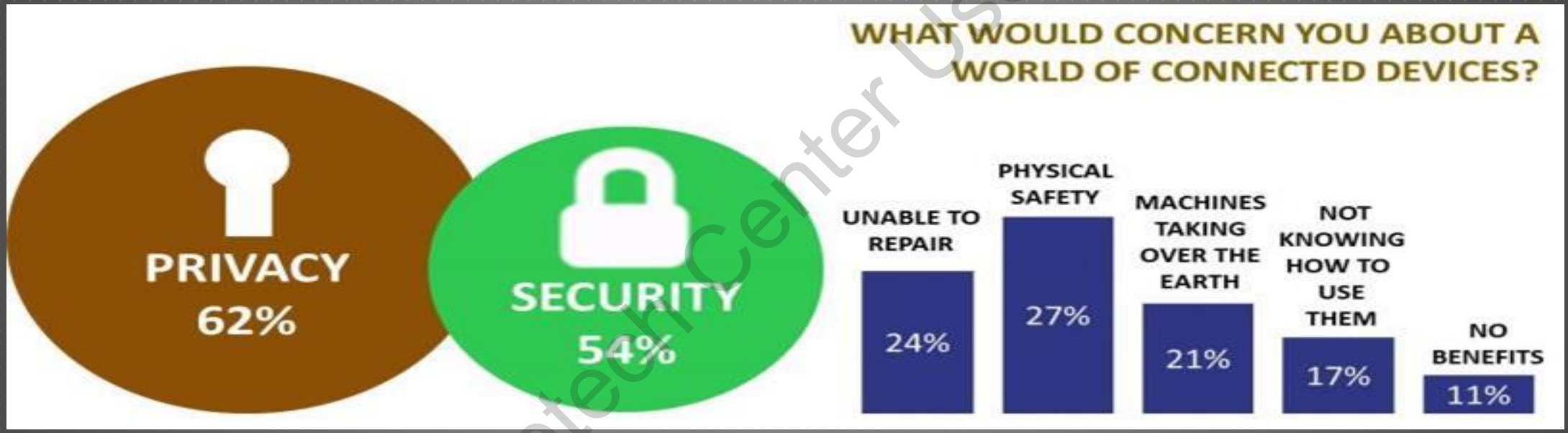


PRIVACY AND SECURITY ISSUES AND CHALLENGE 2/13

- **IoT Infrastructure**

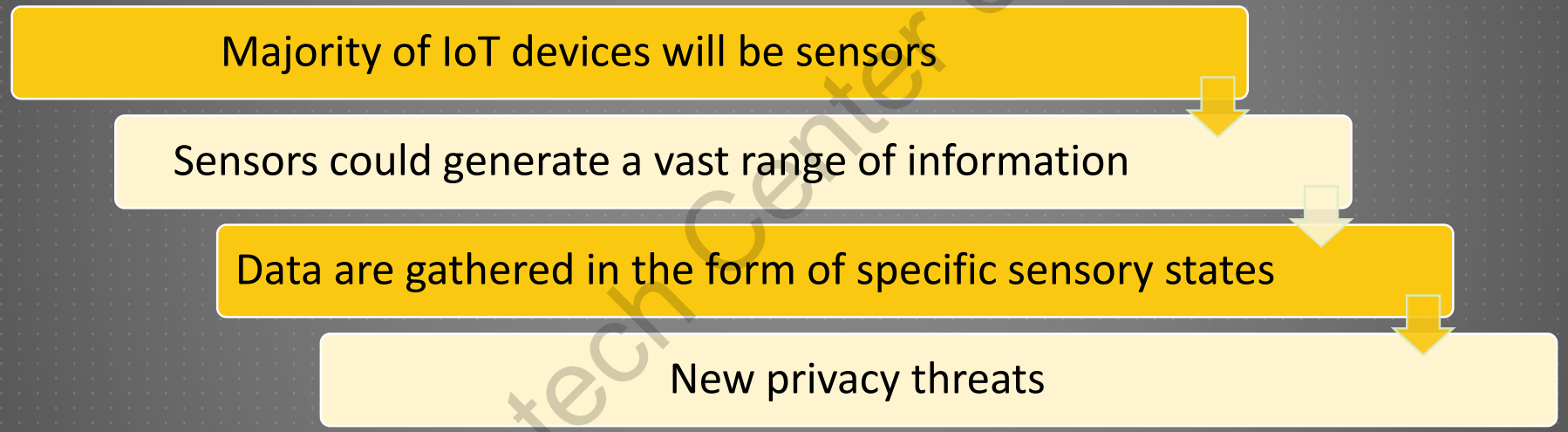


PRIVACY AND SECURITY ISSUES AND CHALLENGE 3/13



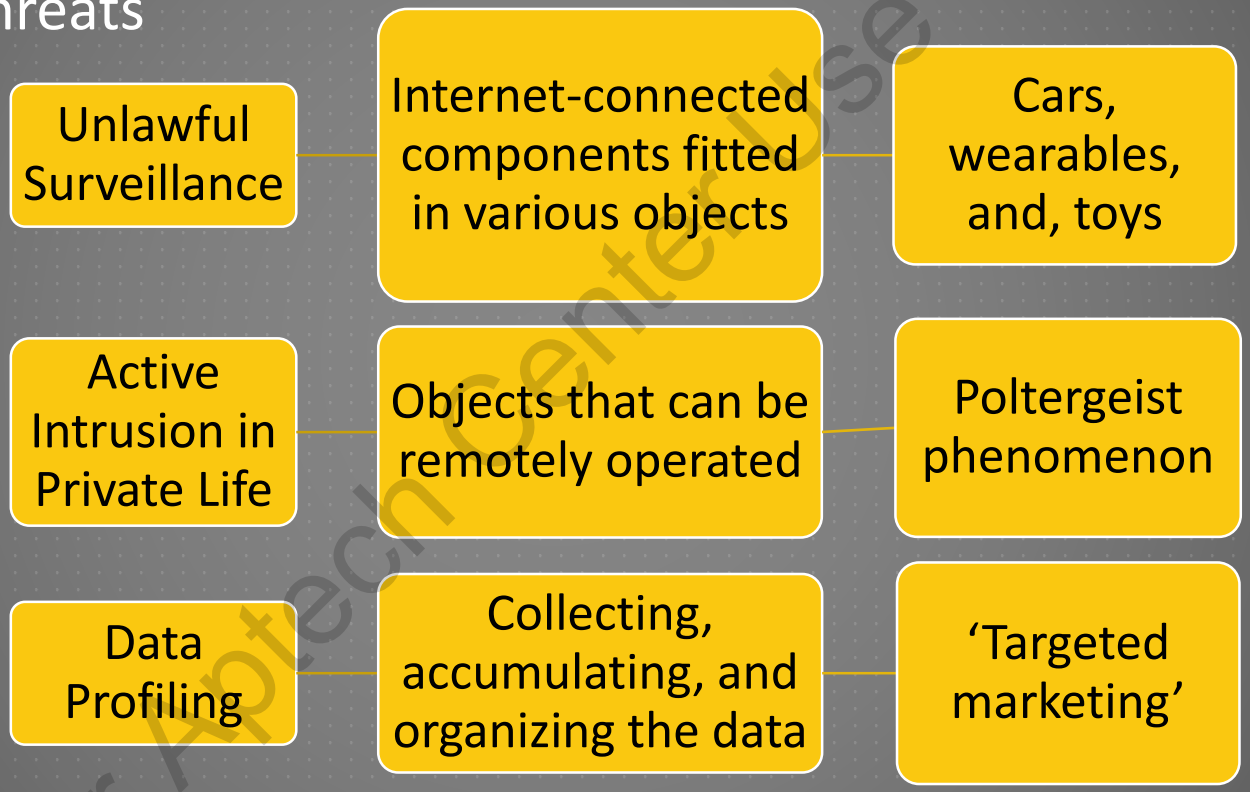
PRIVACY AND SECURITY ISSUES AND CHALLENGE 4/13

- Privacy for IoT



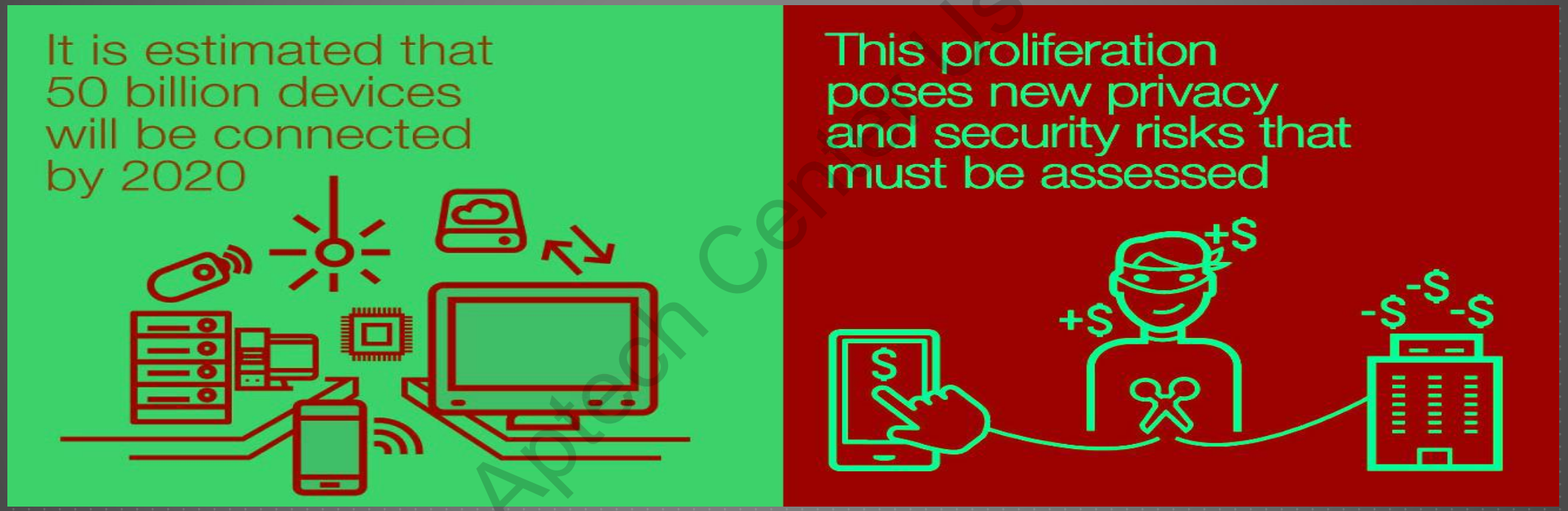
PRIVACY AND SECURITY ISSUES AND CHALLENGE 5/13

- Major Privacy Threats



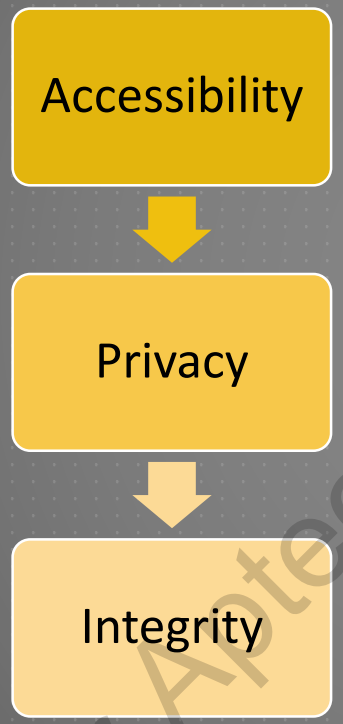
PRIVACY AND SECURITY ISSUES AND CHALLENGE 6/13

- Privacy Risks Exposed to Users



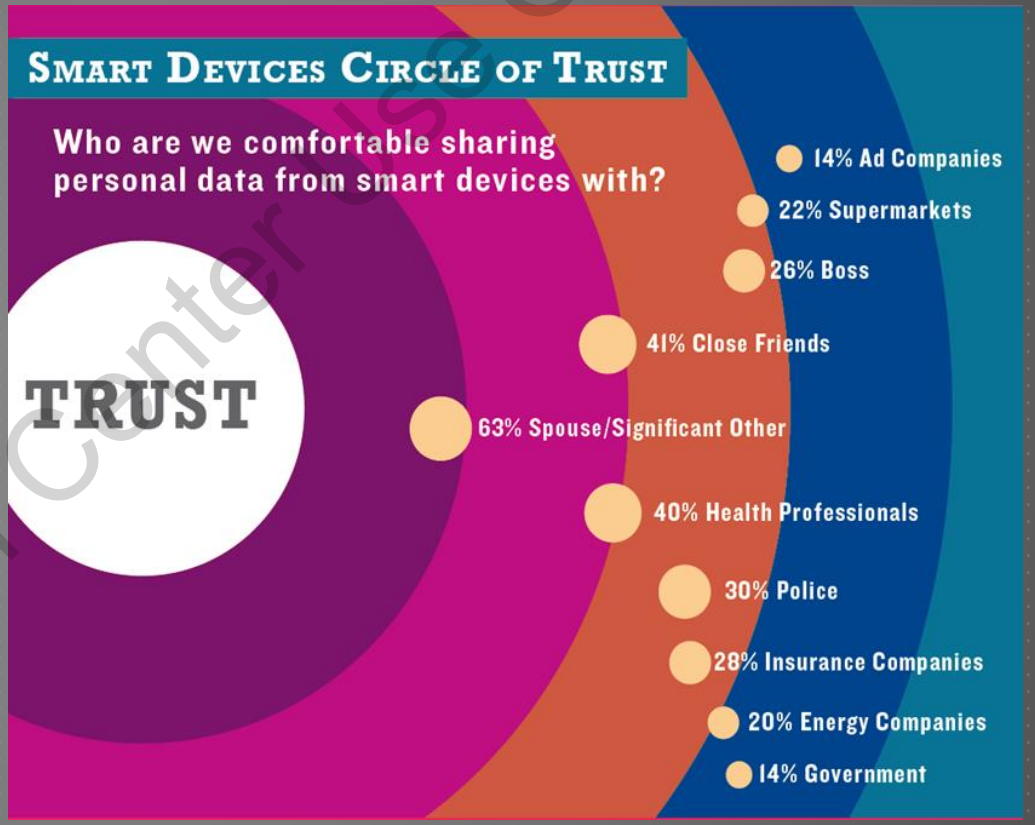
PRIVACY AND SECURITY ISSUES AND CHALLENGE 7/13

- Trust in IoT



PRIVACY AND SECURITY ISSUES AND CHALLENGE 8/13

- Trust in IoT



PRIVACY AND SECURITY ISSUES AND CHALLENGE 9/13

- Security for IoT

Protecting connected devices and networks in the IoT

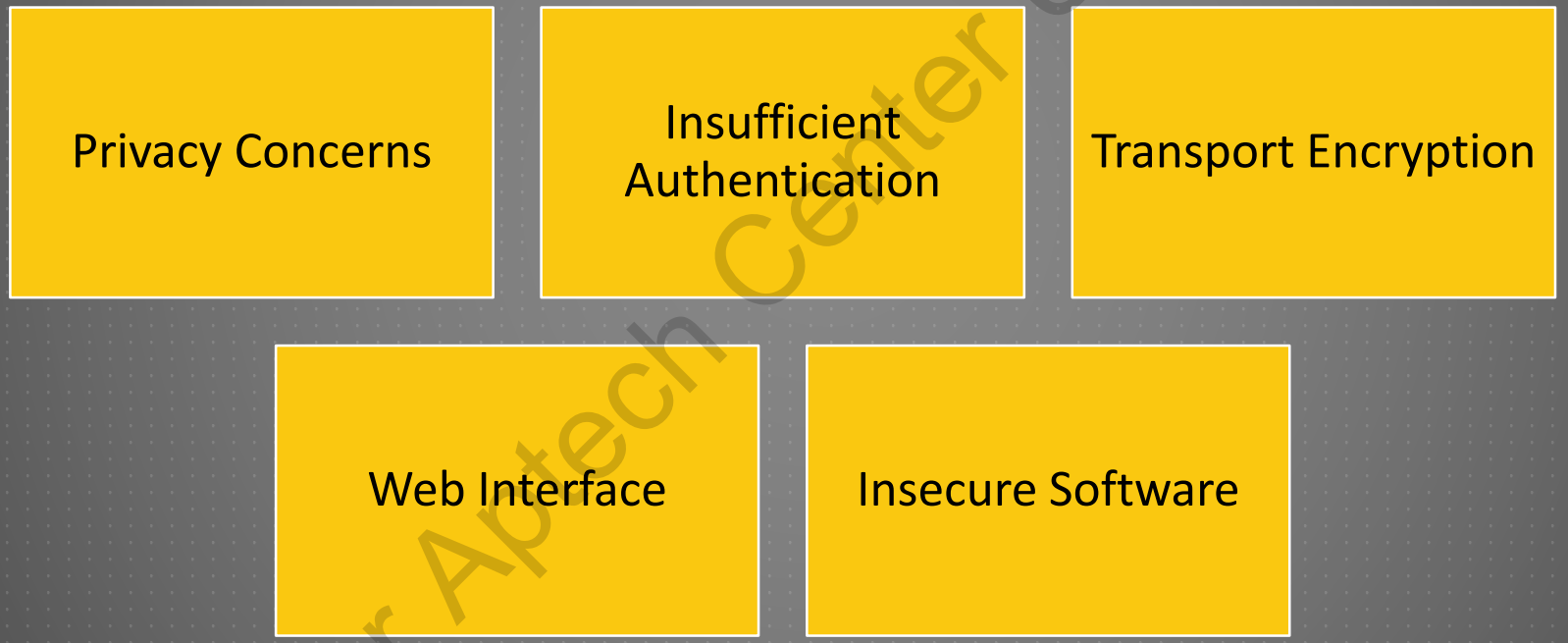
Provides unique Identifiers

Conventional and unpatched embedded O/S and S/W

Advent of Internet Protocol version 6 (IPv6) and Wifi

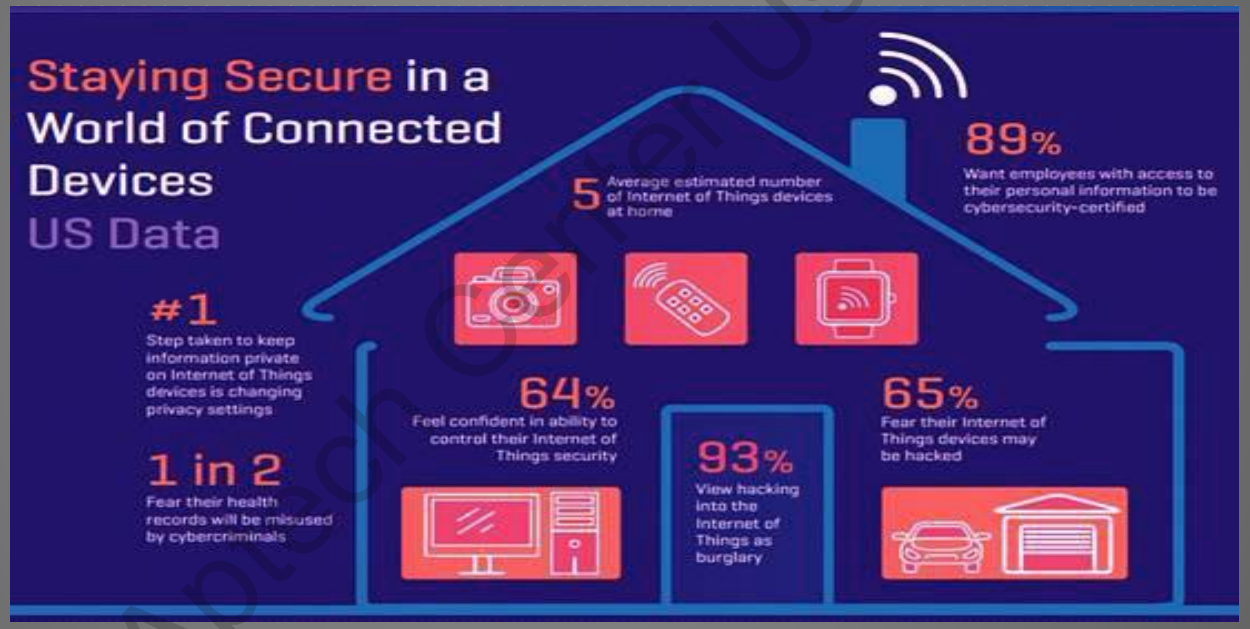
PRIVACY AND SECURITY ISSUES AND CHALLENGE 10/13

- Security Issues in IoT



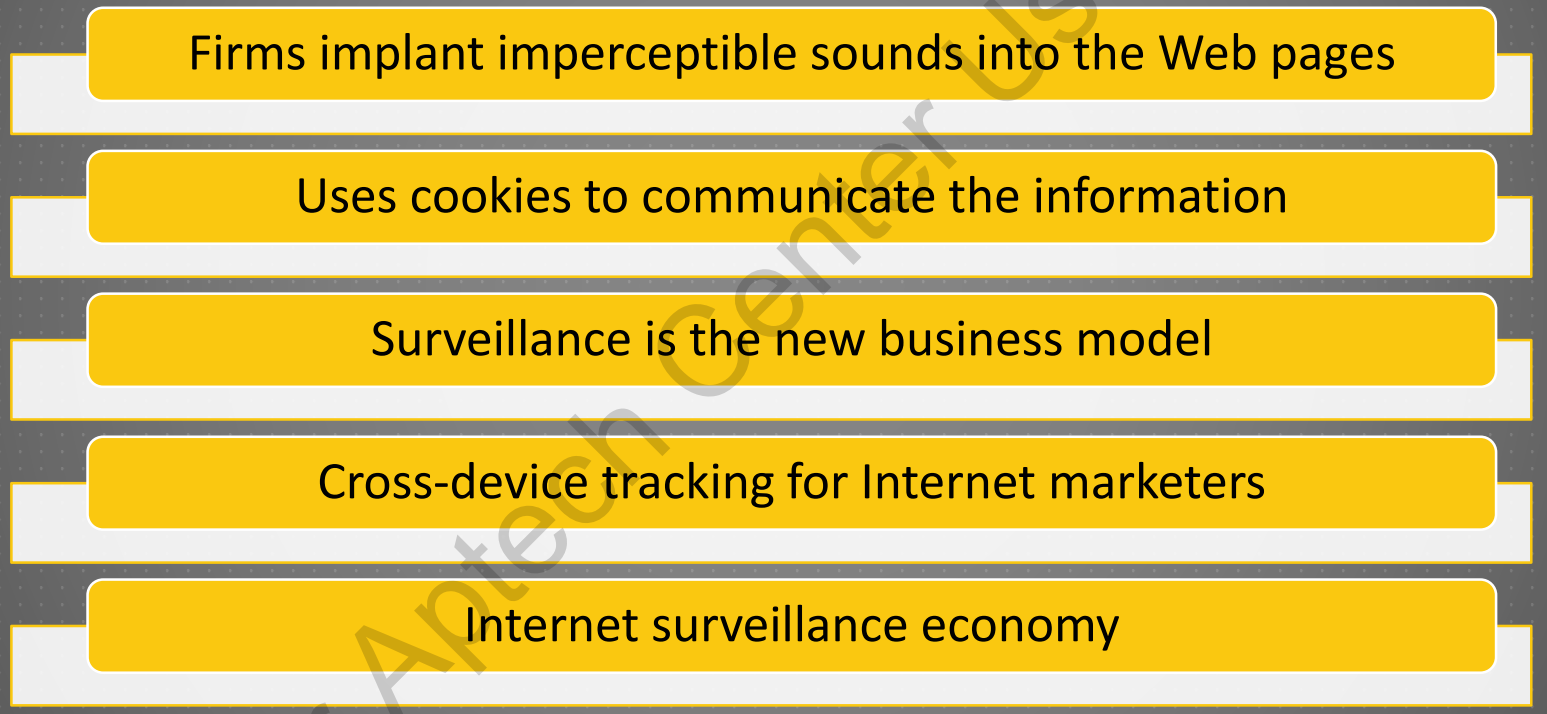
PRIVACY AND SECURITY ISSUES AND CHALLENGE 11/13

- Data for Security Issues



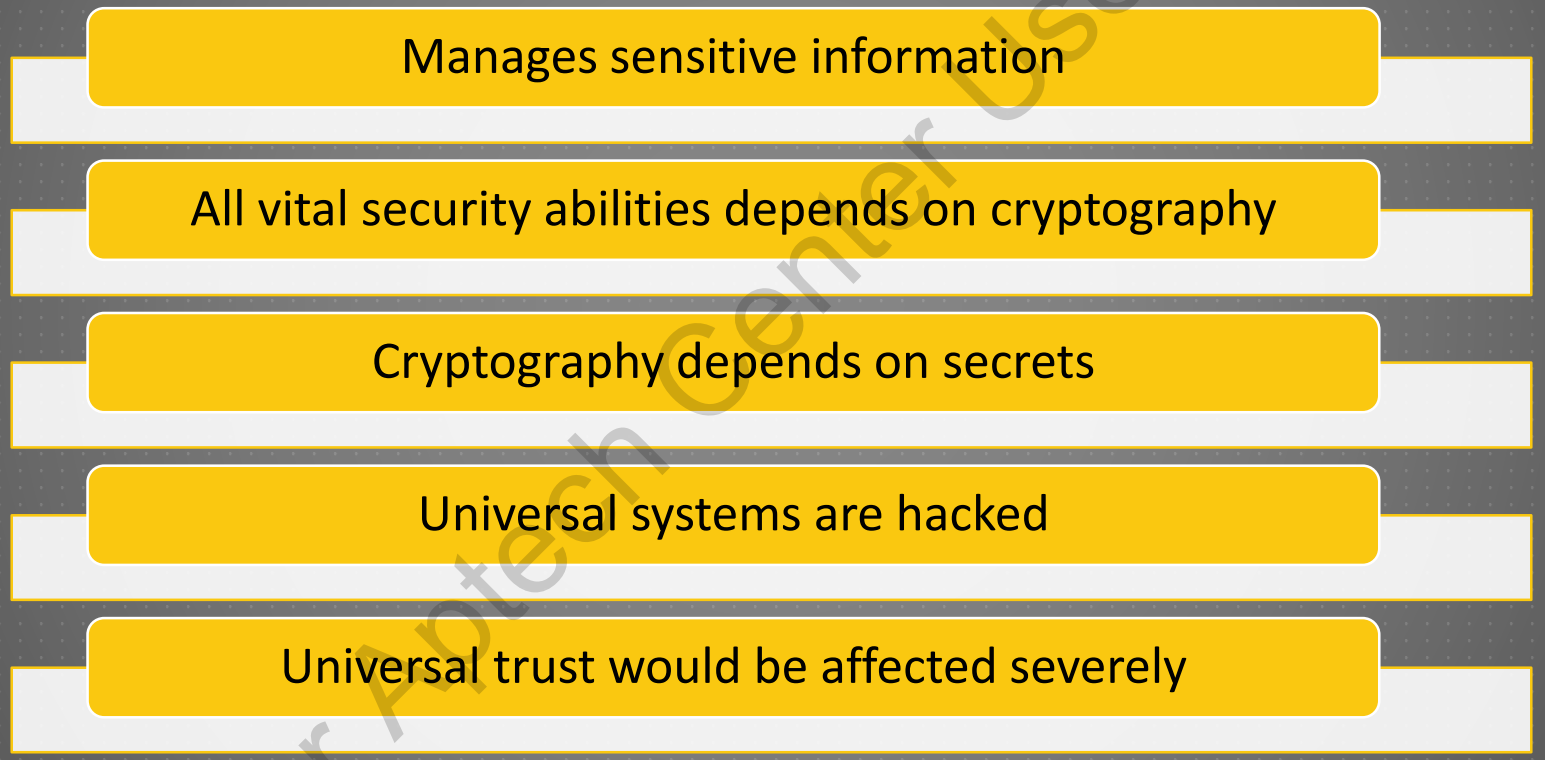
PRIVACY AND SECURITY ISSUES AND CHALLENGE 12/13

- Nobody is Anonymous



PRIVACY AND SECURITY ISSUES AND CHALLENGE 13/13

- Keeping Secrets

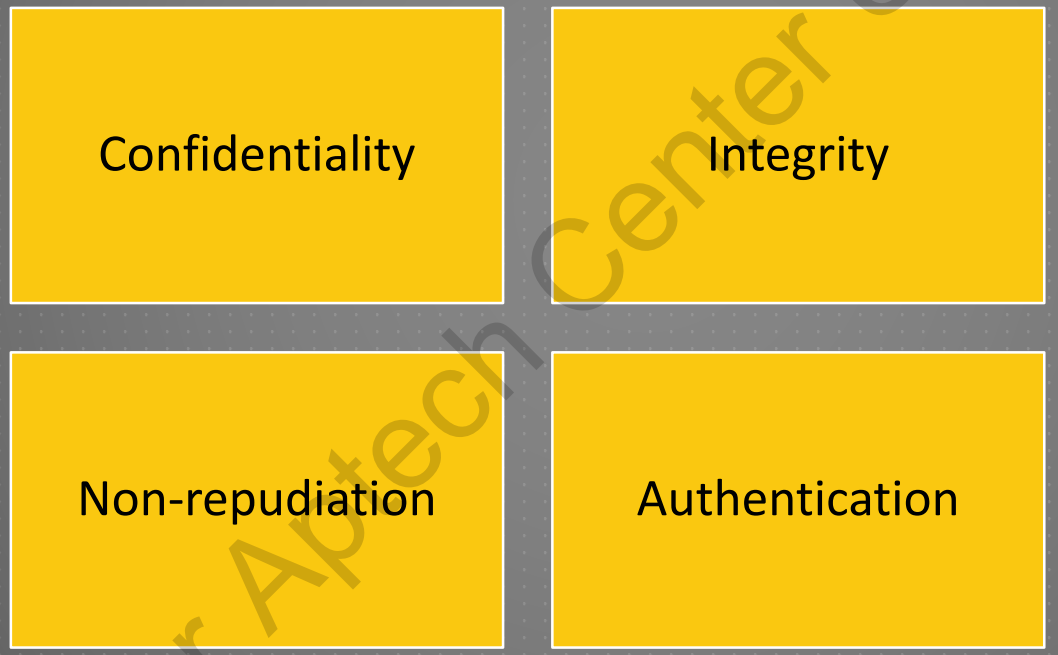


CRYPTOGRAPHY 1/7

- Preserve secrets in the IoT
- Method of storing and transmitting data communication partners do not change frequently

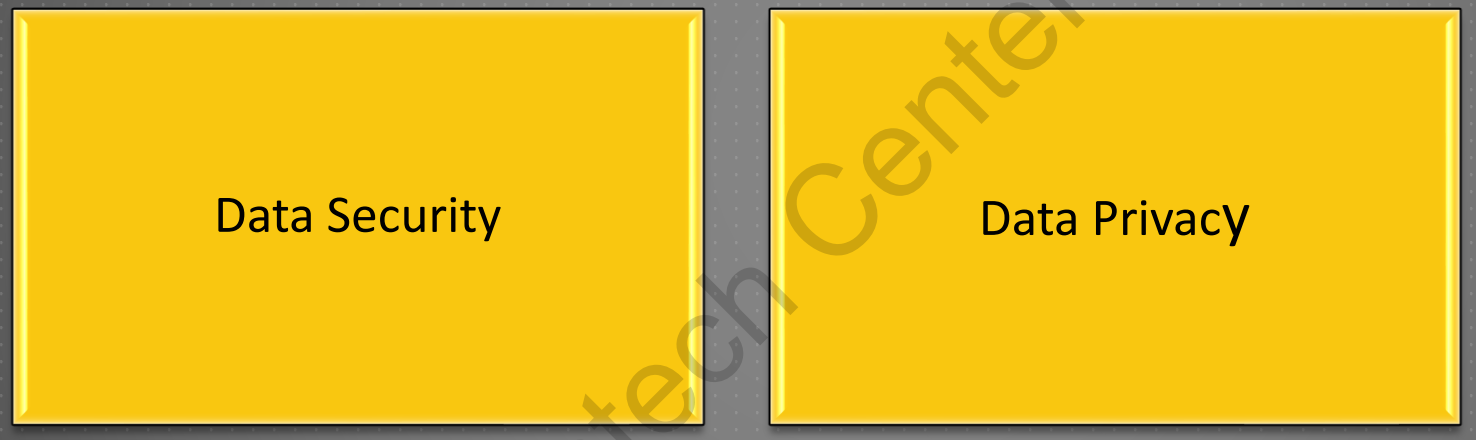
CRYPTOGRAPHY 2/7

- Objectives



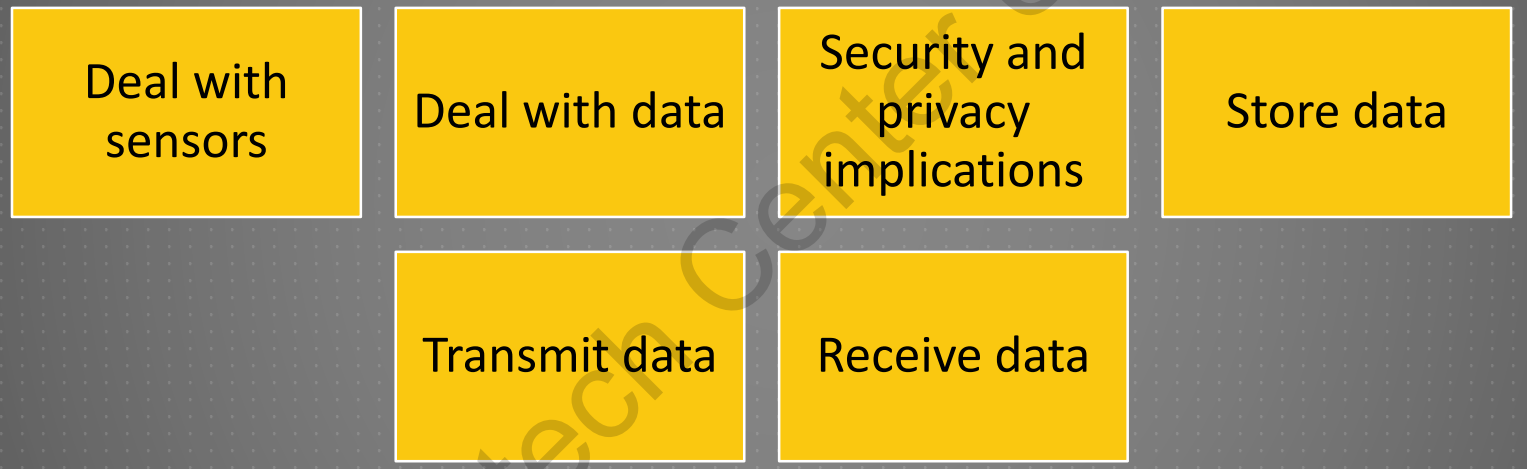
CRYPTOGRAPHY 3/7

- Requirements



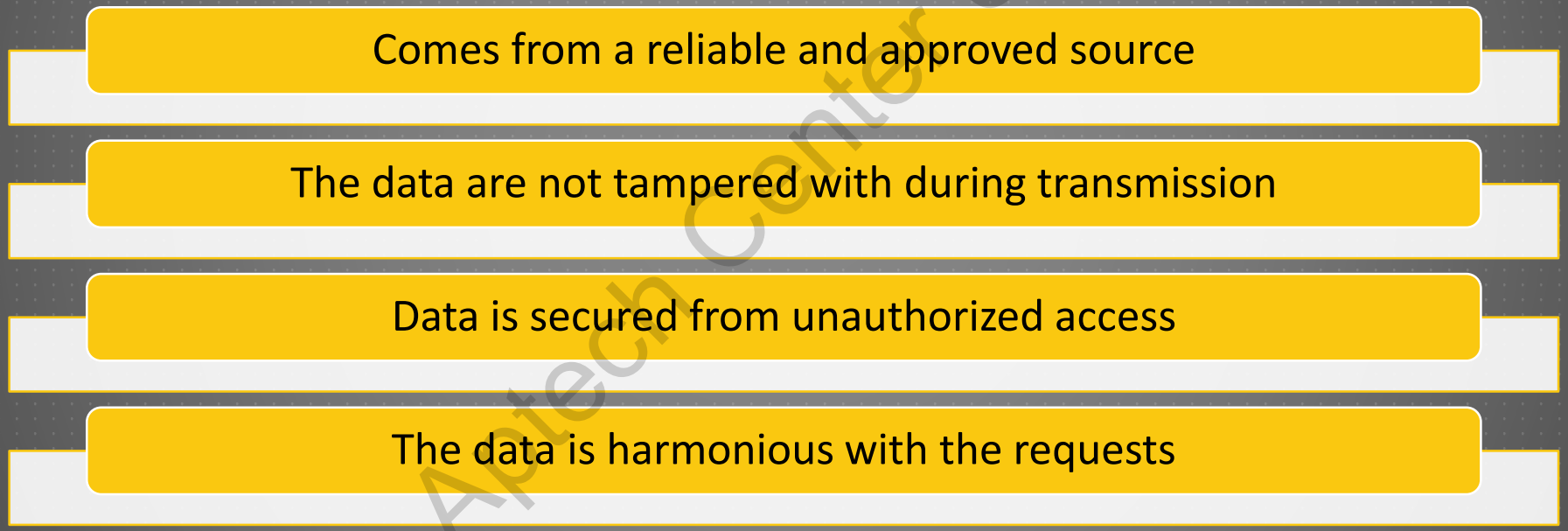
CRYPTOGRAPHY 4/7

- Role and Assumptions



CRYPTOGRAPHY 5/7

- Data Transmission



CRYPTOGRAPHY 6/7

- Processor Time and Resources

More time and resources

Use of long keys in encryption is related to political or costs constrain

Encryption offers on network package

Key exchange issues can be: Static and Dynamic

CRYPTOGRAPHY 7/7

- Data Storage

Data should be protected when transmitting and storing it

Permanent, semi-permanent, and volatile

Capability of the system

DIGITAL SIGNATURE 1/4

- Validating the authenticity and integrity
- Based on public key cryptography
- Private and Public key algorithm

DIGITAL SIGNATURE 2/4

- Public key cryptography

Verifies the reliability and authenticity of digital content

Reliability - digital content is not altered

Authenticity - same digital content has been issued by a well-recognized entity

DIGITAL SIGNATURE 3/4

- Public key cryptography
- Secure Hash Algorithm

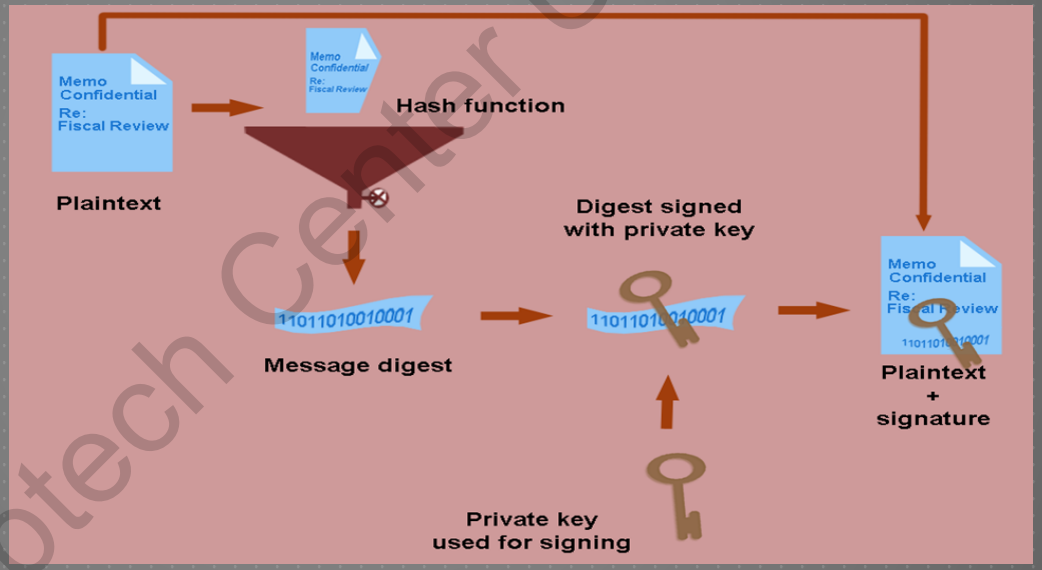
Digests the Message

Difficult to forge digital content that generates a predefined hash value

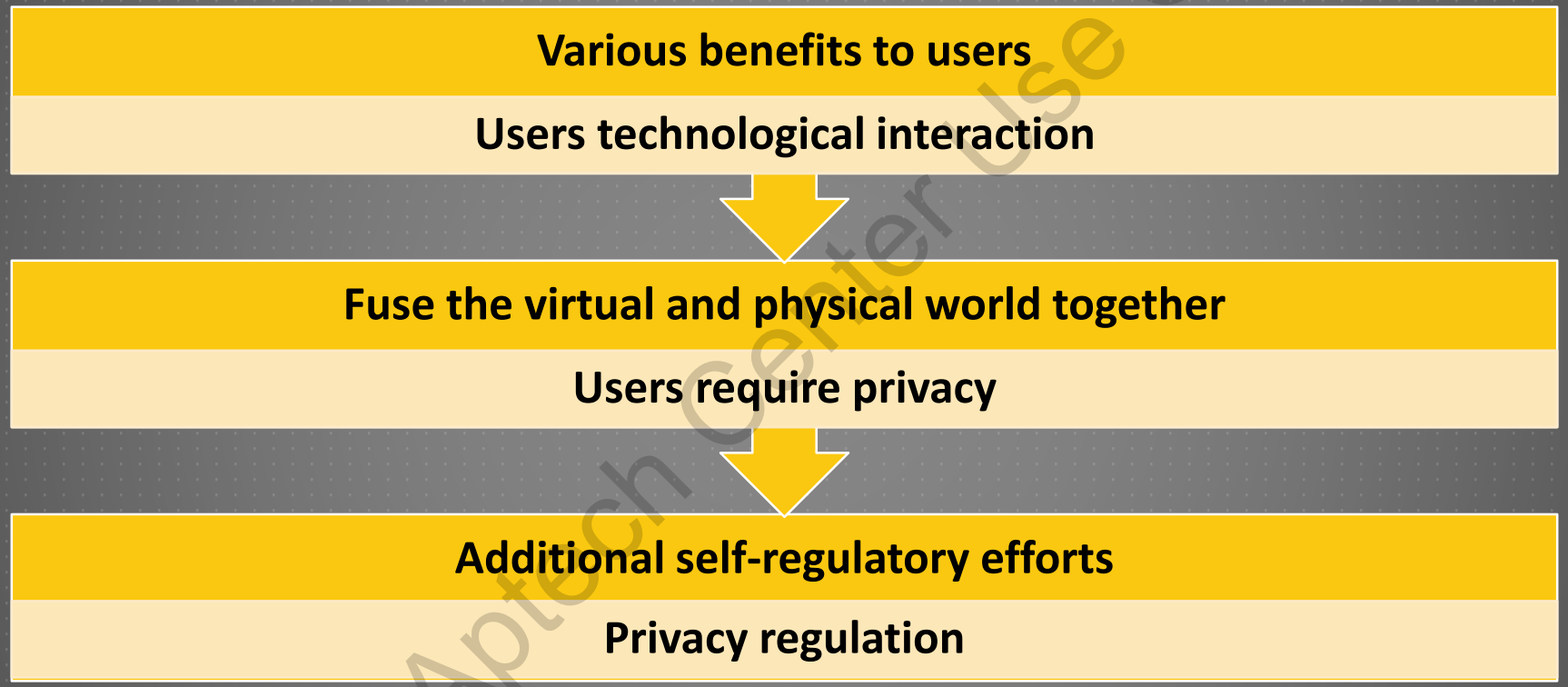
Two different digital contents generating the same hash value is nil

DIGITAL SIGNATURE 4/4

- Public key cryptography
- Digital Signature Process



CONCLUSION



SUMMARY

- IoT privacy and security issues are the special considerations essential to protect the information of users from exposure in the IoT environment, in which any physical or object can be given a unique identifier and the ability to communicate freely over the Internet or any other similar network. The ‘things’ in the IoT environment transmits data autonomously and works in conjunction with ‘other things’ and communicates with them.
- IoT will lead to increased awareness about environmental and social issues, as increasing users will have access to the Internet and thus, will have access to new techniques and solutions for education, environmental hazards, and health hazards.
- The On-going use of IoT devices is currently creating serious issues related to the privacy of users, on the IoT security, and the possible threat of cyber criminals controlling sensors and smart devices connected to the Internet.

SUMMARY

- Trust management plays a significant role in IoT for consistent data fusion and data mining, competent services with context-awareness, and improved user privacy and information security. It helps users to overcome uncertainty and risk and take part in user approval and utilization on IoT services and applications.
- Security concerns for the IoT are developing at a faster pace than the IoT itself. Tackling IoT related concerns requires identifying the issues related to IoT security. The main issues relating to security of IoT are privacy concerns, insufficient authorization; Web interfaces risks, transport encryption, and insecure software.
- Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Digital signatures are based on public key cryptography, also known as asymmetric cryptography.