



Funded by the  
Erasmus+ Programme  
of the European Union

Introduction to Cybersecurity

# Background – Challenges of the 4th Industrial Revolution

**Safeguarding against Phishing in the age of 4<sup>th</sup> Industrial Revolution**

**[www.cyberphish.eu](http://www.cyberphish.eu)**

*This project has been funded with support from the European Commission.*

*This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*



# Learning Goals



- Recall the concept of Cybersecurity together with the normal challenges faced by businesses
- List the cyber-attack challenges individuals and businesses are witnessing with the advent of Industry 4.0

# Student Workload



Lecture	1,5 h
Audio and video material	1,5 h
Case studies	1,5 h
Further reading	4 h
Preparation for exam	1,5 h

# Wide Use of Technology



Software and information systems play an important role in different areas of human life

The need to secure information becomes a necessity than an option

Definition

# Cybersecurity

a.k.a.,

**Computer Security, Information Technology Security or IT Security**

*The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users*

[Schatz et al. 2017]



# Table of Contents

- Business Challenges
- Growth of Cybersecurity Attacks
- Use of Technology and Security Challenges
  - *Internet of Things*
  - *Cloud Computing*
  - *Intelligent Infrastructure*
  - *Smart Home*
  - *Blockchain Technology*
  - *Big Data*
- The Challenge of Growing Threats
- Nation-State Threats



# Business Challenges

- Digital Transformation
- The Cloud
- Compliance
- Automation
- Internet of Things
- Integration and Upgrades
- Artificial Intelligence and Machine Learning




- Remote Work Support
- Data Management
- Focus on Mobility
- Social Media
- Project Management
- Infrastructure Changes
- Lack of Technical Training

# Business Challenges

- Digital Transformation
- The Cloud
- Compliance
- Automation
- Internet of Things
- Integration and
- Artificial Intelligence and Machine Learning

- Remote Work Support
- Data Management
- Focus on Mobility
- Social Media
- Project Management
- Infrastructure Changes
- Technical Training



**Third-party risk** – the risk arising from an organization's connections with outside parties to provide business-related supplies or services

- *Regulatory/ Compliance*
- *Financial*
- *Operational*
- *Reputational*
- *Strategic*

<https://hyperproof.io/resource/author/hyperproof-team/>



# Business Challenges

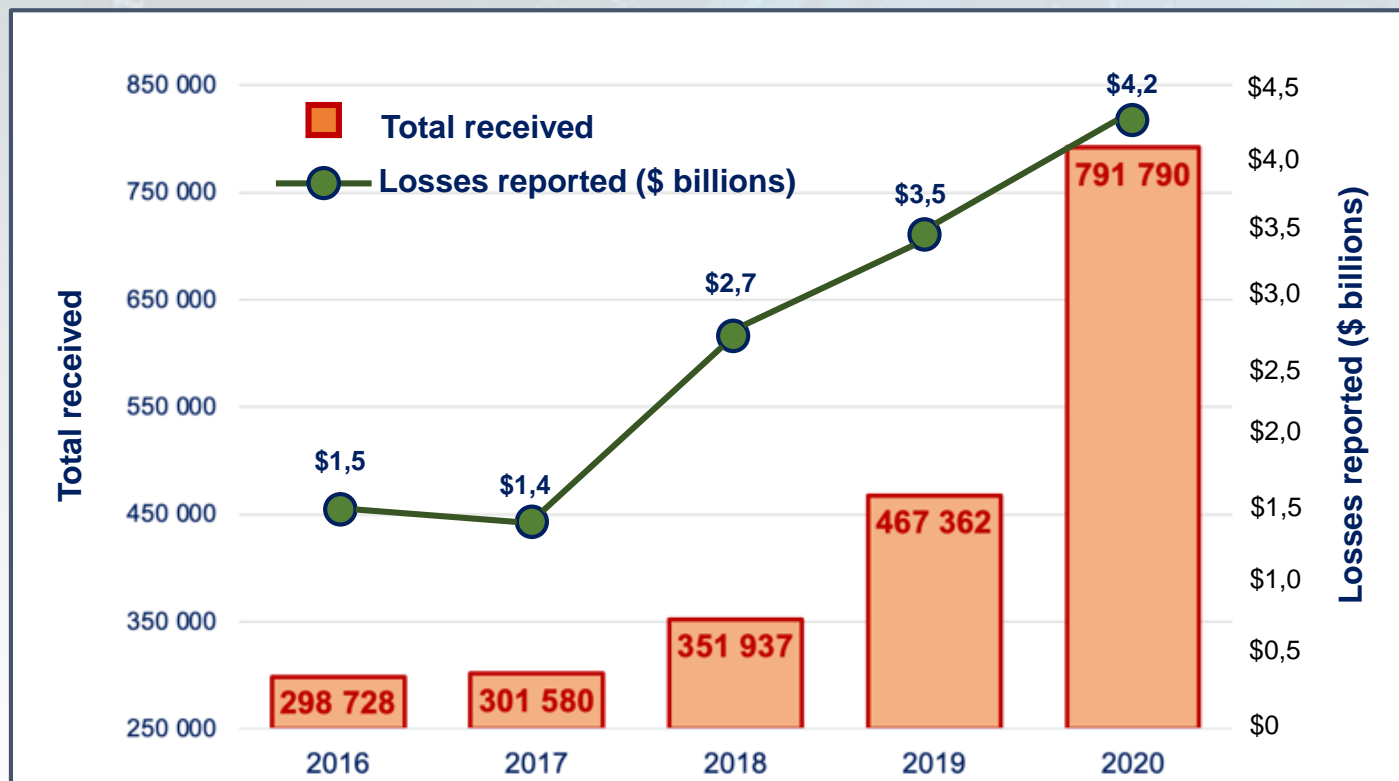
- Digital Transformation
- The Cloud
- Compliance
- Automation
- Internet of Things
- Integration and Upgrades
- Artificial Intelligence and Machine Learning



- Remote Work Support
- Data Management
- Focus on Mobility
- Social Media
- Project Management
- Infrastructure Changes
- Technical Training

**Information Security**

# Growth of Cybersecurity Attacks

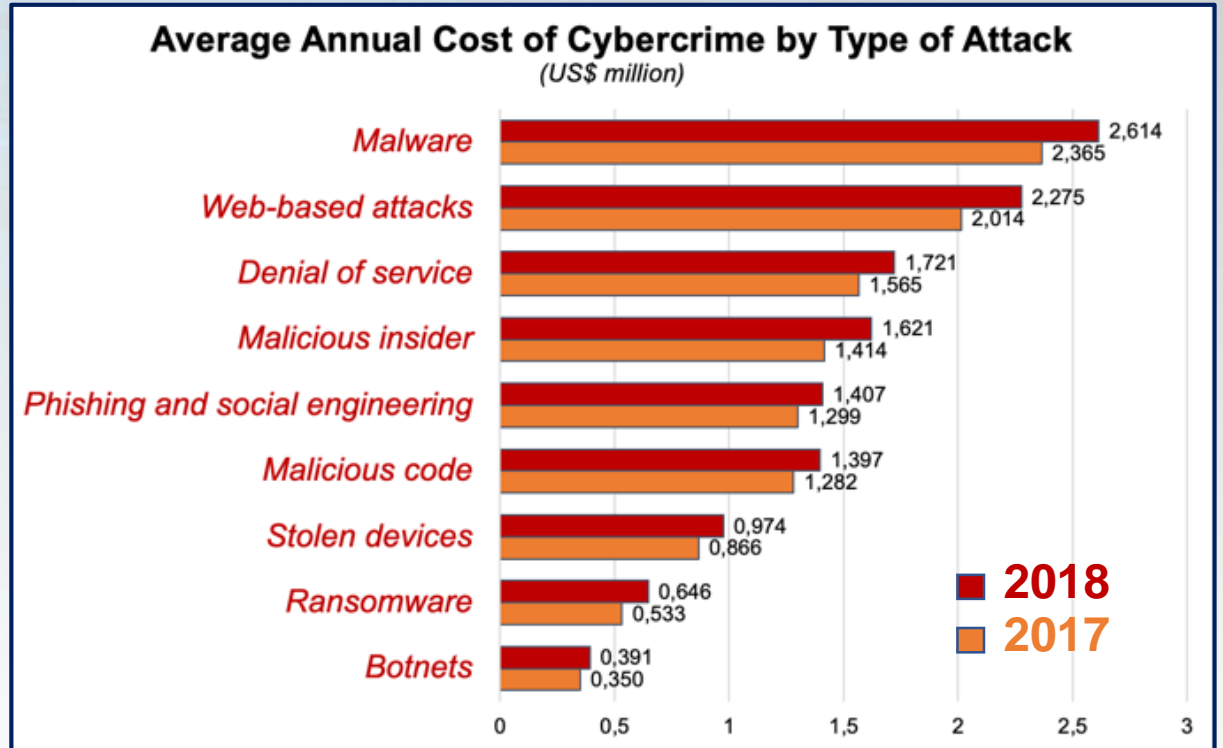
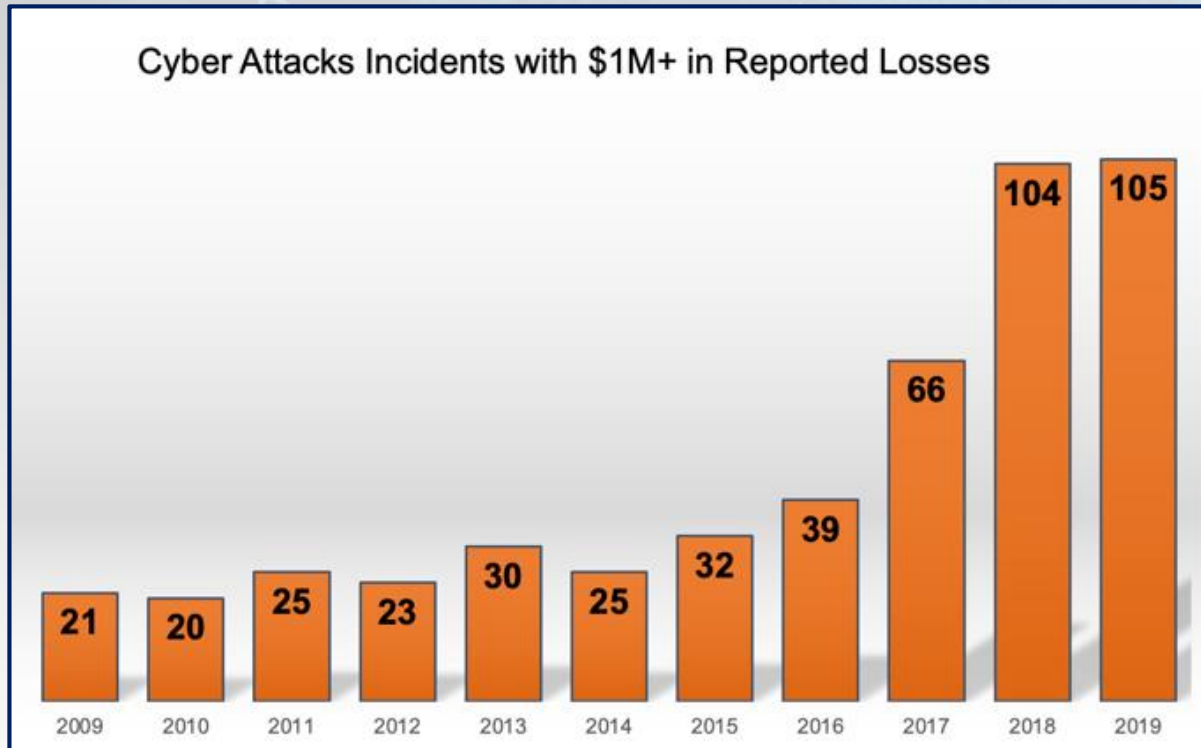


- Targeting people
- Doing the homework
- It is a numbers game
- Scams keep evolving
- Criminals sell stolen information
- Patience and persistence pay off
- Criminals can operate from anywhere

<https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>

<https://www.forbes.com/sites/forbestechcouncil/2019/12/23/seven-reasons-for-cybercrimes-meteoric-growth/?sh=17cfbc8c5fa2>

# Cost of Cybersecurity Attacks



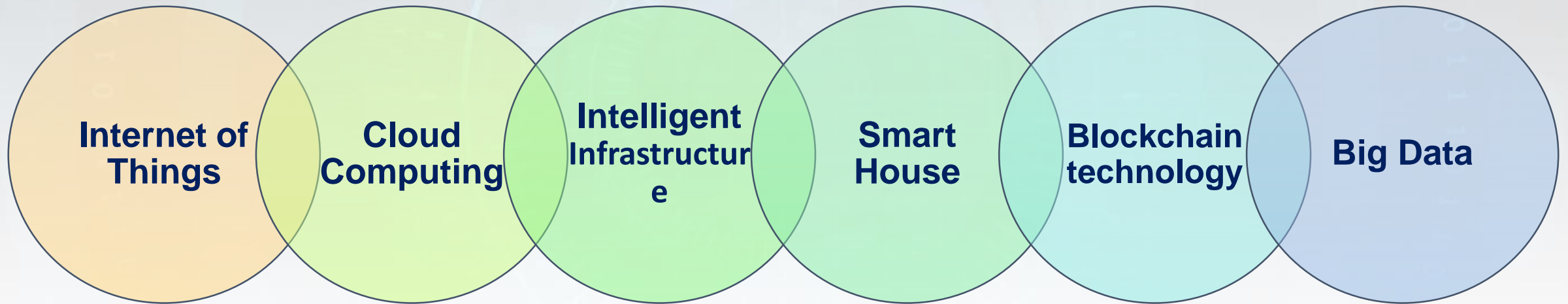
Over the past decade – **490** significant cyber incidents

2018 total = US\$ **13** million

<https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/>

<https://www.digitalmarketingcommunity.com/researches/ninth-annual-cost-of-cybercrime-research-2019/>

# *Security Challenges in Wide Use of Mobile Technology*



# Security Challenges in Internet of Things

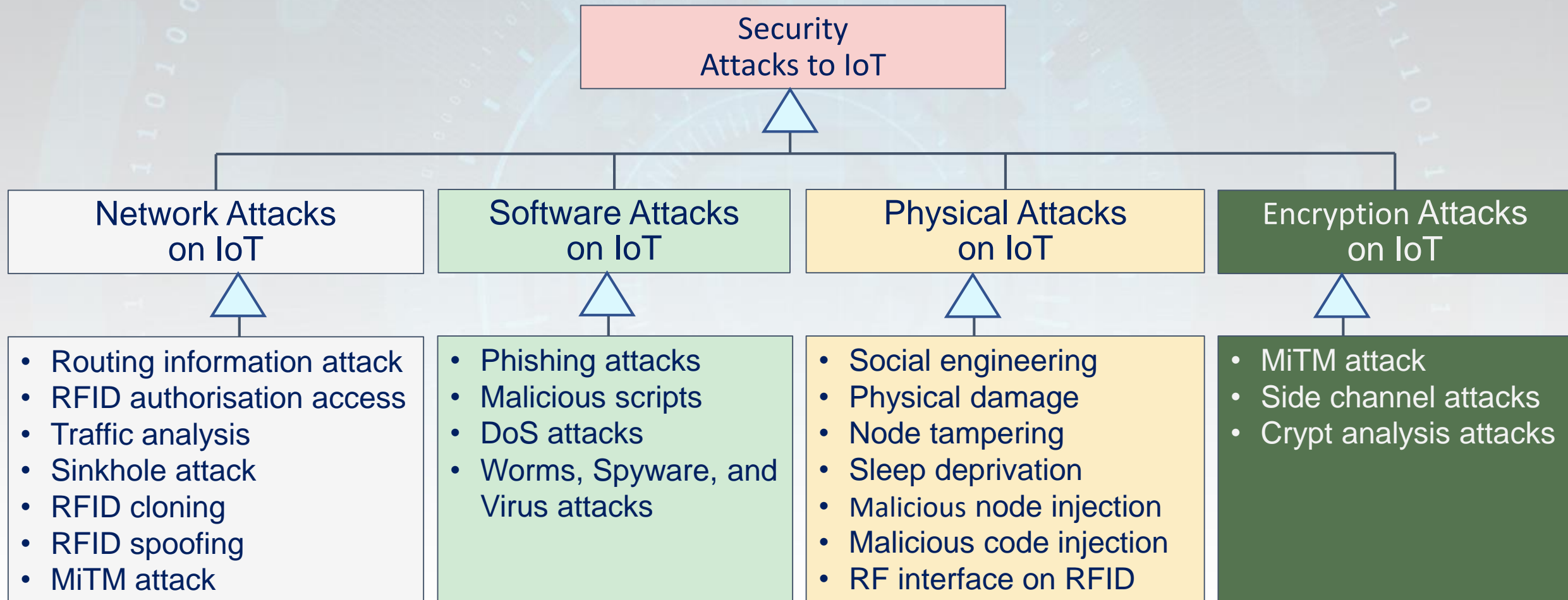
**Internet of Things (IoT)** describes the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet

- *The "things", i.e., technologies, devices, objects, animals , or humans*
- *The networks of communication that connect the device*
- *The computer networks through data streaming from Internet to device*

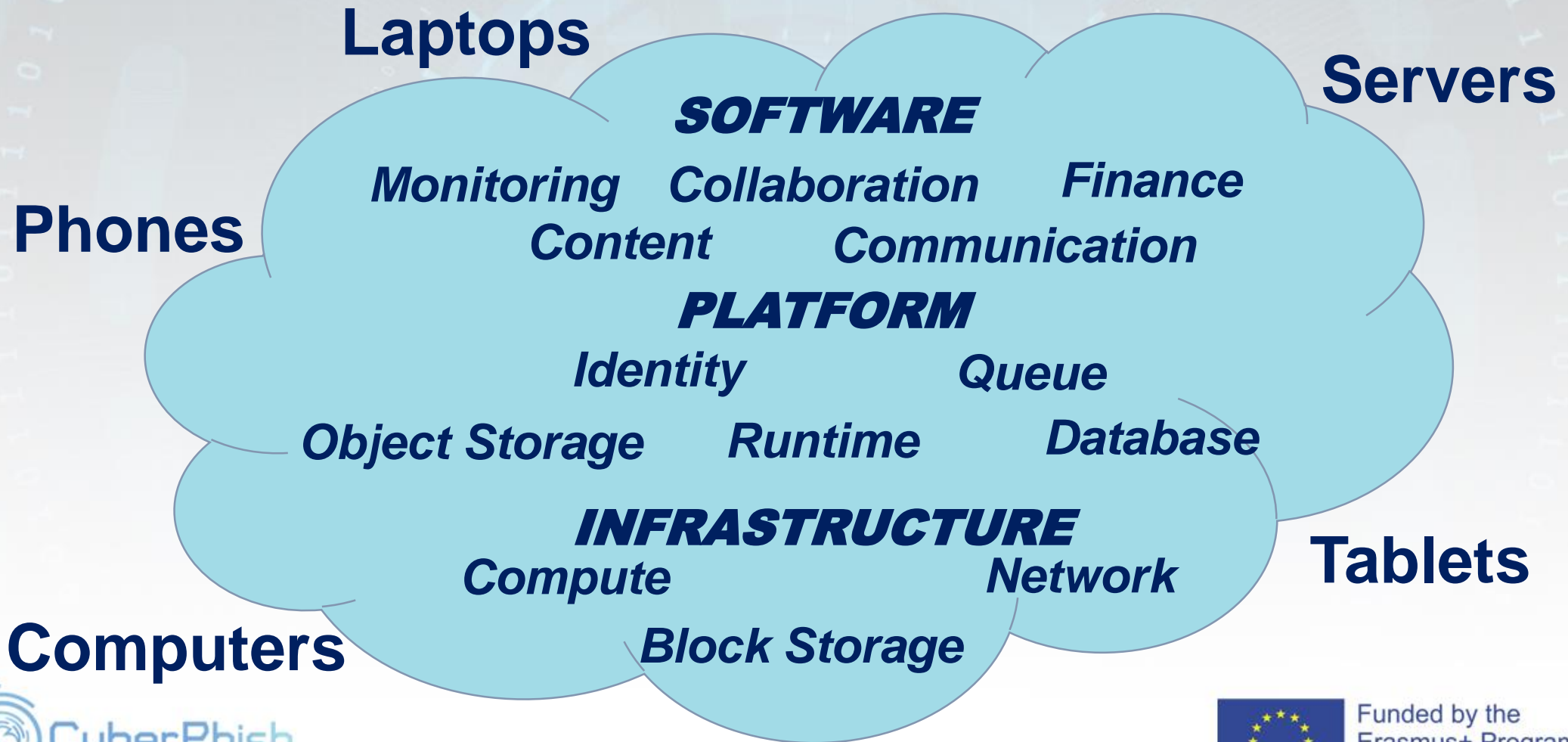
<b>Year</b>	<b>World Population</b> <i>(in billion)</i>	<b>IoT Connected Devices</b> <i>(in billion)</i>	<b>Ratio</b>
<b>2003</b>	6,3	0,5	0,08
<b>2010</b>	6,8	12,5	1,84
<b>2015</b>	7,2	25	3,47
<b>2020</b>	7,6	50	6,58



# Security Challenges in Internet of Things



# Security Challenges in Cloud Computing



# Security Challenges in Cloud Computing

**Laptops**

**Servers**

**Phones**

*Abuse and Misuse of Cloud Computing*

*Interfaces and Unsecure API*

*Internal Threats*

*Problems Derived from Shared Technologies*

*Loss or Leakage of Information*

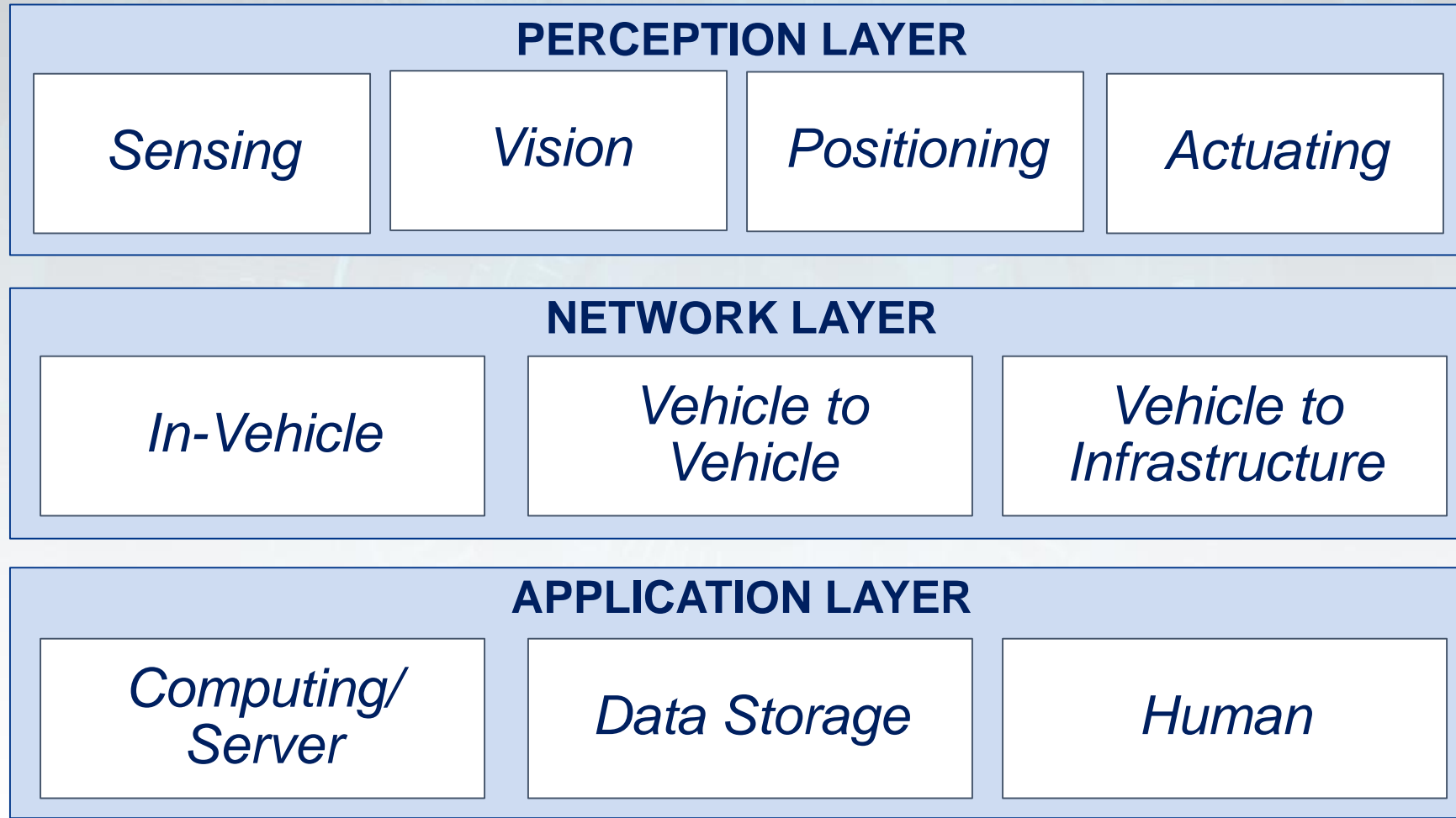
*Session or Service Hijacking*

*Risks Due to Lack of Knowledge*

**Tablets**

**Computers**

# Security Challenges in Intelligent Systems

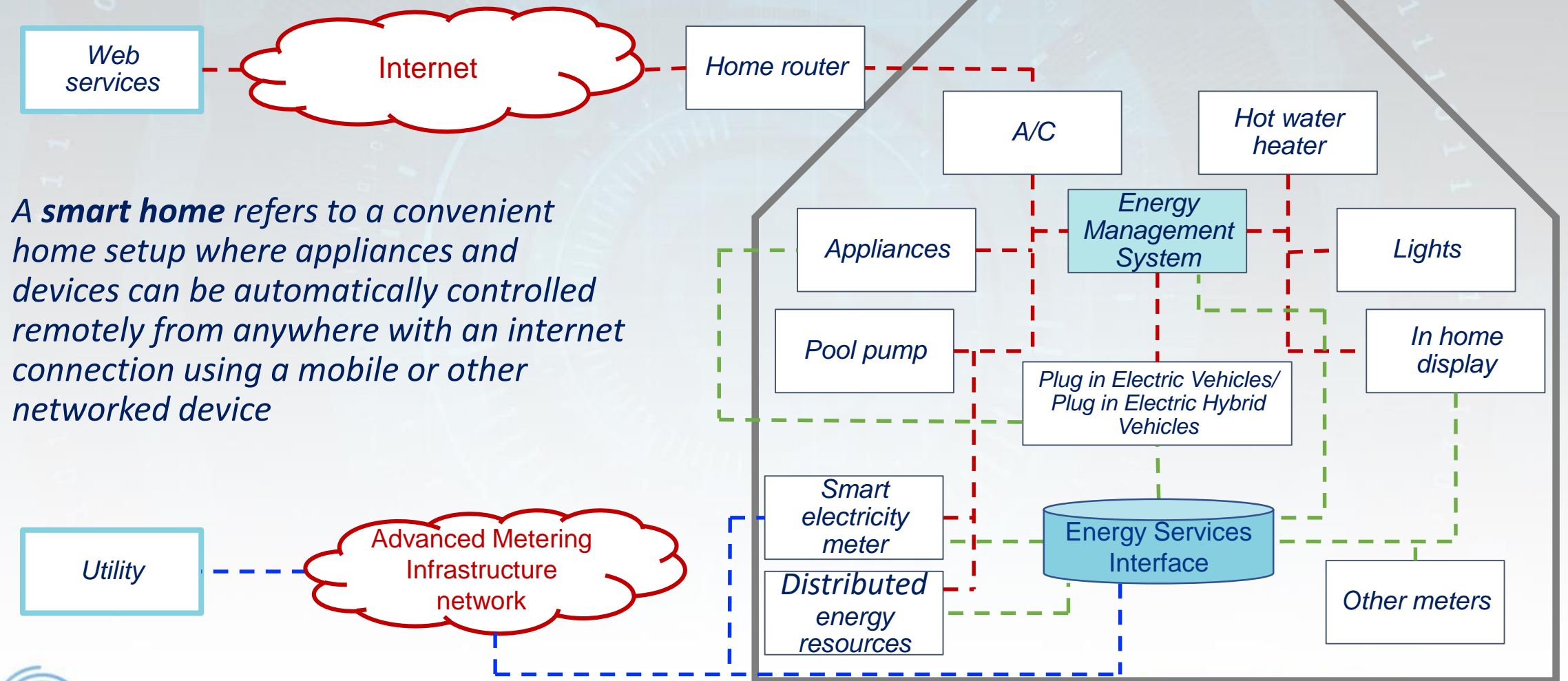


## SECURITY THREATS

<b>System Assets</b>	<b><i>Spooftng</i></b>	<b><i>Tampering</i></b>	<b><i>Repudiation</i></b>	<b><i>Information disclosure</i></b>	<b><i>Denial of service</i></b>	<b><i>Elevation of privileges</i></b>
<b>Sensing, Positioning, Vision technologies</b>	Spooftng, Node impersonation, Illusion, Replay, Sending deceptive messages, Masquerading	Forgery, Data manipulation, Tampering, Falsification of readings, Message injection	Bogus message	Stored attacks, Eavesdropping	Message saturation, Jamming, Denial of service (DoS), Disruption of system	Backdoor, Unauthorized access, Elevation of privilege, Remote update of ECU
<b>In-vehicle network, Vehicle-to-vehicle (V2V), Vehicle-to-Infrastructure (V2I)</b>	Sybil, Spooftng, Replay attack, Masquerading, Fingerprinting, Wormhole, Camouflage attack, Impersonation attack	Timing attacks, Injection, Manipulation, Routing manipulation, Tampering, Forgery, Malicious update	Bogus messages, Rogue Repudiation, Loss of event traceability	Eavesdropping, MiTM, ID disclosure, Location tracking, Message interception, Information disclosure	DoS/DDoS, Spam, Jamming, Flooding, Message suppression, Channel interference, Black hole	Malware, Brute Force, Gaining control, Social engineering, Logical attacks, Unauthorized access, Session Hijack
<b>Application server, Edge data center, Human</b>	Spooftng, Sybil, Illusion attack	Malicious update	--	Eavesdropping, Location tracking, Privacy leakage	Deny of Service	Jail-breaking OS, Social engineering, Rogue data-center, malware



# Security Challenges in Smart House Systems

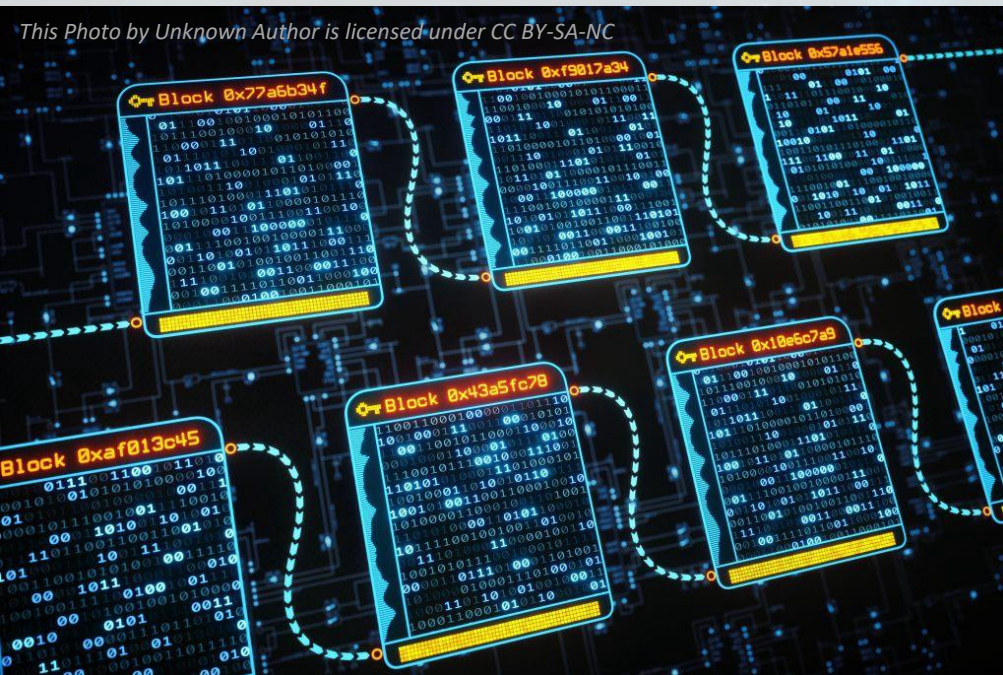


A **smart home** refers to a convenient home setup where appliances and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device

# Security Challenges in Smart House Systems

Scenario	Possible threat (N – networking domain, SH – smart home concept)	Security criterion negated
<b>AS1:</b> Attacks Threatening Successful Device Energy– Consumption Reporting	Eavesdropping (N), Traffic analysis (N), Message modification (N), Reply attack (N), Energy management system impersonation (SH)	Confidentiality, Integrity, Authentication
<b>AS2:</b> Attacks Aiming Energy Import/ Export Signals at the Energy service interface or Home area network	Repudiation (N), Message modification (N), Replay attack (N)	Non-repudiation, Integrity, Authentication
<b>AS3:</b> Physical Meter Tampering/ Reversal or Removal	Tampering/ Reversal, Removal of meter (SH), Illegal software modification / update (SH)	Authentication, Integrity
<b>AS4:</b> Attacks Against Remote Home Monitoring and Control	Customer impersonation (N), Device impersonation (SH), Message modification (N), Replay attack (N), Repudiation (N)	Integrity, non-repudiation, Authentication
<b>AS5:</b> Attacks Aiming the Requests for Energy Usage Data	Customer impersonation (N), Eavesdropping (N), Interception (N), Message modification (N)	Confidentiality, Integrity, Availability

# Security Challenges in Blockchain Technology



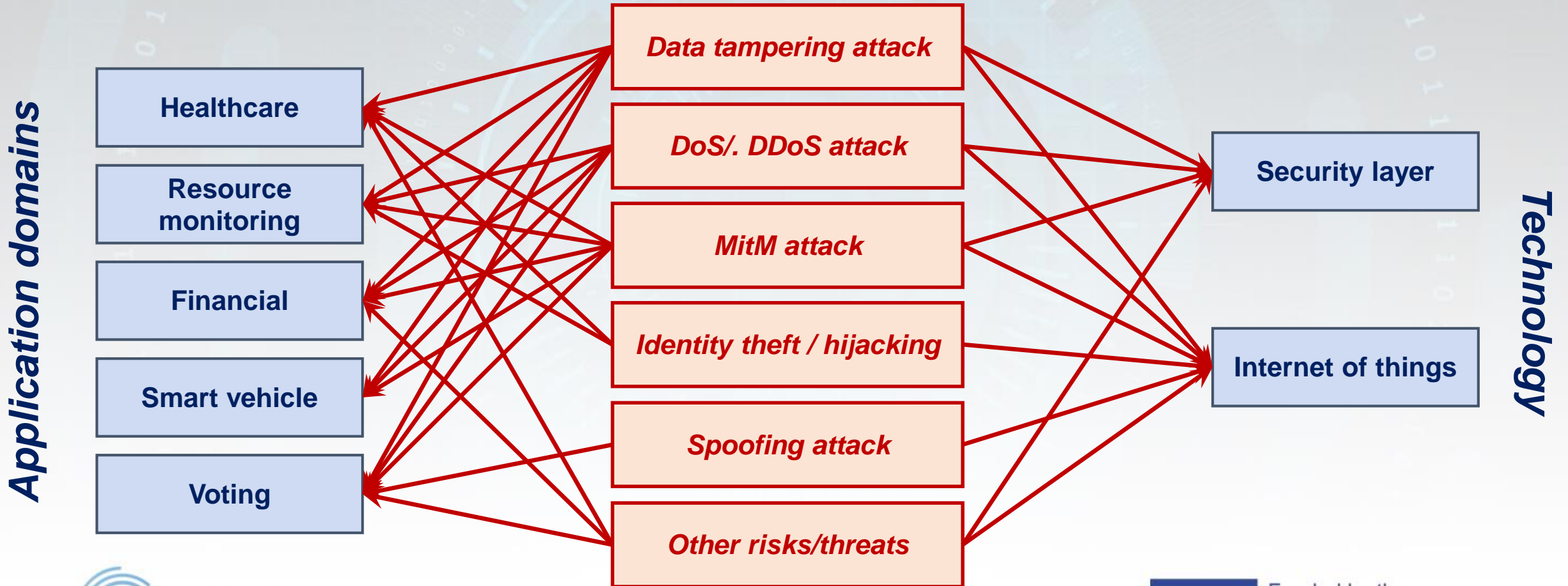
**Blockchain** is a distributed immutable ledger technology, which gives participants an ability to share a ledger by peer-to-peer replication and updates every time when a transaction occurs

[Lewis , 2015; Sato and Himura, 2018]



# Security Challenges in Blockchain Technology

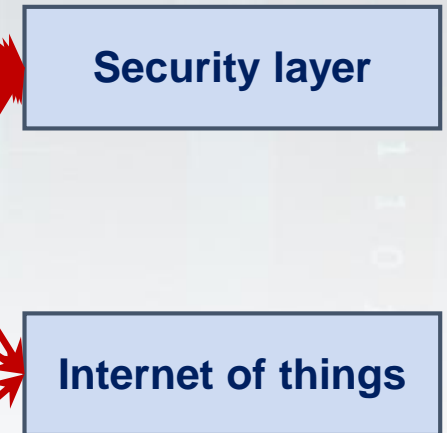
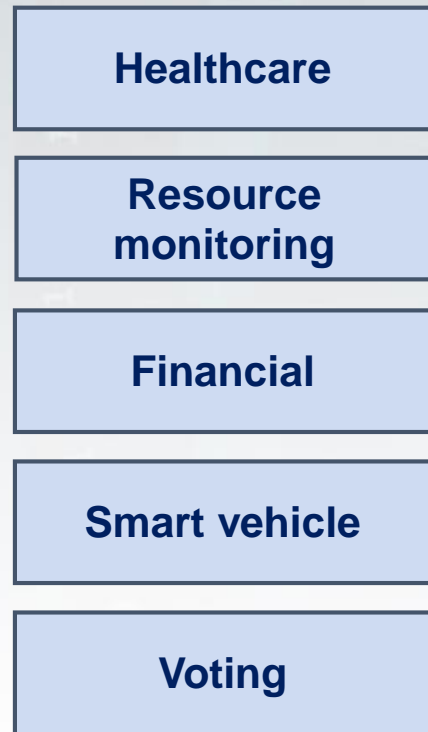
Security risks in different application domains mitigated using Blockchain applications



# Security Challenges in Blockchain Technology

*Security risks to Blockchain applications*

*Application domains*



*Technology*



# Security Challenges in Big Data Ecosystem

## CHALLENGES

### HUMAN

*Business, Information,  
Social, Professional*

Lack of Consent, Social Misuse of Knowledge, Unauthorised Access, Data Deluge, Inappropriate Analytics, Availability, Accuracy

### TECHNOLOGY

*Application, Platform, Data  
Infrastructure*

Multiple Uses of Data, Technology Gap, Agreed Data Usage, data, Timeliness, Data Provenance, Device Heterogeneity, Availability, Data Collection management & transfer, Data types and formats, Incomplete & Inconsistent data

### FACILITY

*Spatial, HVAC, Energy,  
Ancillary*

Storage and Processing  
Diverse Data Sources, Availability

### ENVIRONMENT

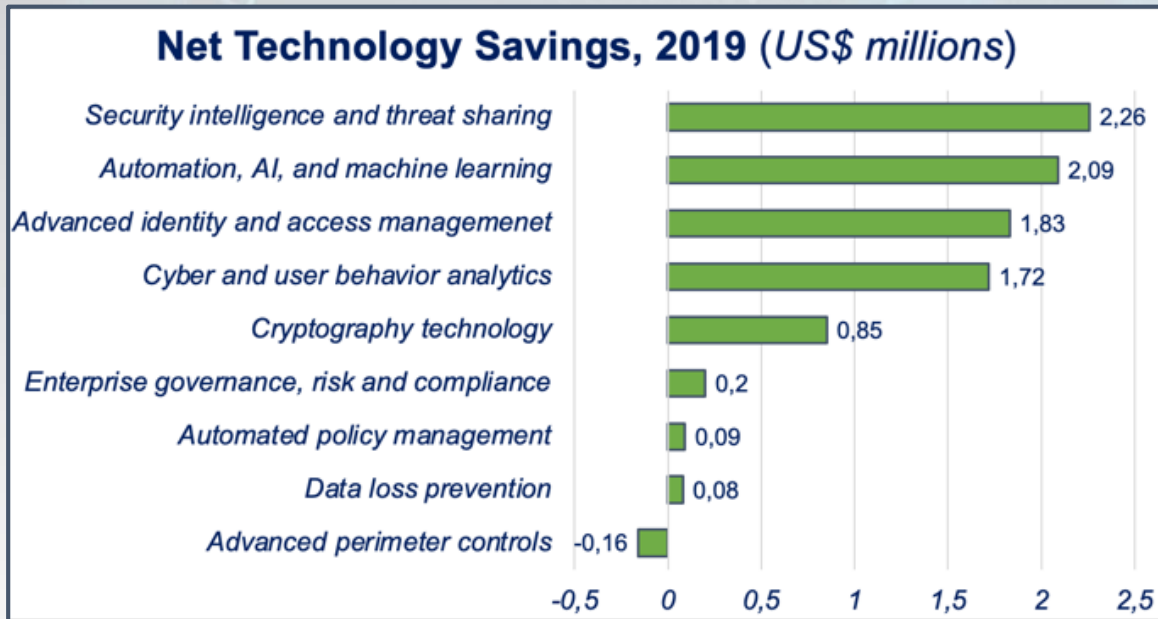
*Political, Environmental, Social,  
Technological, Legal*

Lack of Governance, Policies, Laws, Organisational Resistance, Establishing data driven culture

# Security Challenges in Big Data Ecosystem

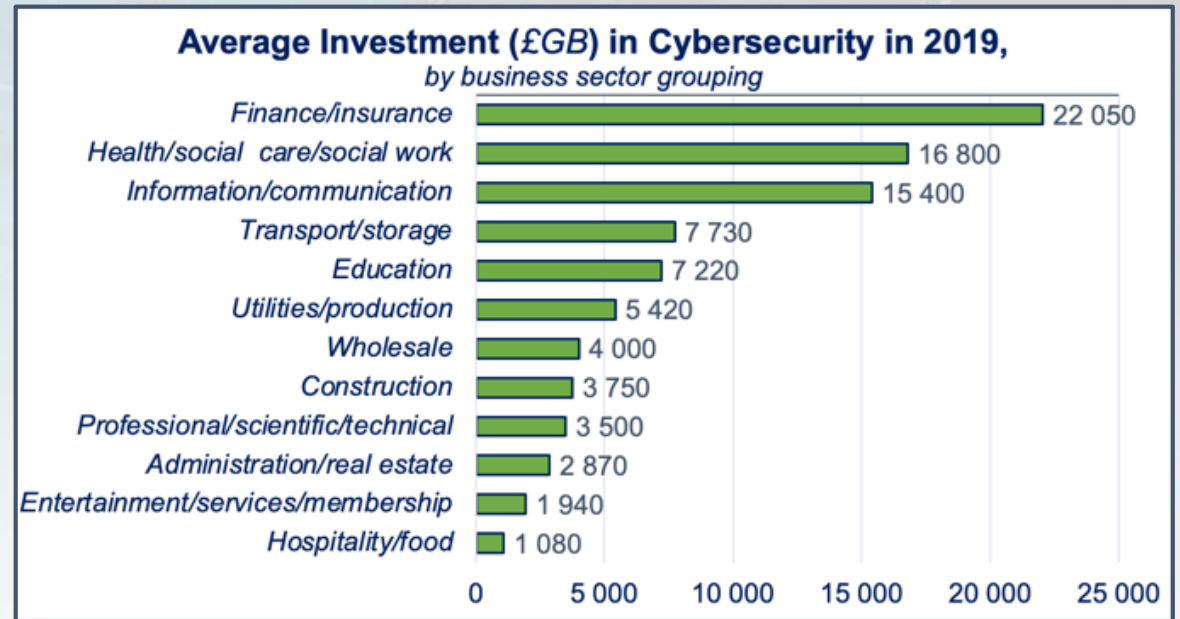
SOLUTIONS	
<b>HUMAN</b> <i>Business, Information, Social, Professional</i>	User Validation, Skills, Access Control, User Education, Audits, Communications Security, Threat Modelling, Risk Assessment, Data Classification, Data driven privacy preserving, Privacy at Social Networks
<b>TECHNOLOGY</b> <i>Application, Platform, Data Infrastructure</i>	End point validation & encryption, Secure Queries, Differential Privacy, Latent Data Privacy, Secure data Collection, Storage & Transformation, Machine Learning Algorithms, Intrusion Recognition, Data Anonymisation
<b>FACILITY</b> <i>Spatial, HVAC, Energy, Anciliary</i>	Distributed sources for data Backup and Recovery Storage of Encrypted Header Information
<b>ENVIRONMENT</b> <i>Political, Environmental, Social, Technological, Legal</i>	Governance and Legal Support

# Investment to Security



**Security intelligence and threat sharing** are ranked as the most used security technology

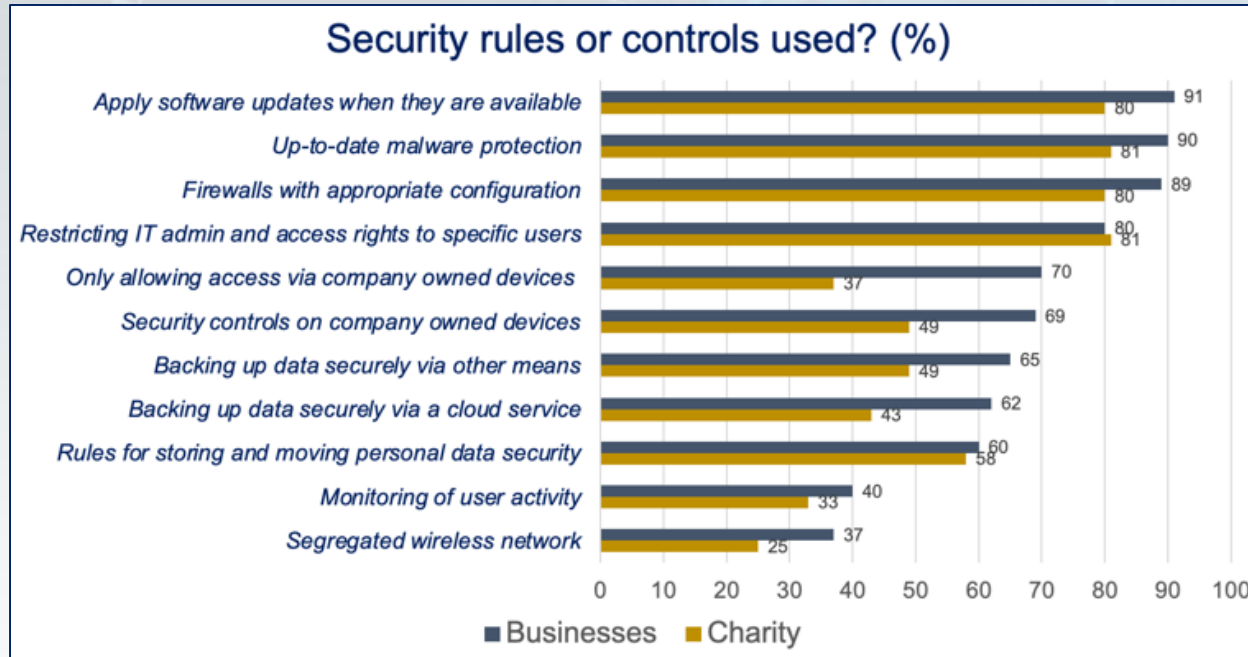
<https://www.digitalmarketingcommunity.com/indicators/security-technologies-cost-saving-2019/>



**Finance and insurance** are ranked as the top business sectors that invested in cybersecurity

<https://www.digitalmarketingcommunity.com/indicators/cyber-security-investment-2019/>

# The Challenge of Growing Threats



<https://www.digitalmarketingcommunity.com/indicators/preventing-minimizing-cyber-security-2019/>

- Do not deny that there is a threat as this will result in failures
- Expect accidental information breaches to be more likely than malicious attacks
- Do not wait to take action until you've been attacked or leak information
- Apply policies consistently
- Address cultural issues at a variety of levels
- Balance investment between outsider and insider threats
- Accept the maxim "*education, education, education*"!

[Colwill, 2009]

# Nation-State Threats

- Cyber espionage targets
  - *industrial sectors*
  - *critical and strategic infrastructures*
  - *government entities*
  - *railways*
  - *telecommunication providers*
  - *energy companies*
  - *hospitals*
  - *banks*

Data breaches motivated by cyber espionage

**20%**

Malicious actors connected with nation-states

**38%**

Incidents motivated by cyber espionage

**11,2%**

Cyber espionage incidents involving phishing

**63%**



# Nation-State Threats

- Cyber espionage focuses on
  - *driving geopolitics*
  - *stealing state and trade secrets*
  - *intellectual property rights*
  - *proprietary information in strategic fields*



- In 2019, *the number of nation-state-sponsored cyber attacks targeting the economy increased and it is likely to continue this way*
- Nation-state-sponsored attacks on Industrial Internet of Things (IIoT) are increasing in
  - *utilities*
  - *oil and natural gas*
  - *manufacturing sectors*

# Nation-State Threats

- Cyber espionage focuses

- driving geopolitics
- stealing sensitive information
- intellectual property
- proprietary data
- strategic

- In 2019, the number of nation-state-sponsored attacks on the economy continued to rise

*Identify mission critical roles in the organisation and estimate their exposure to espionage risks*

*Create security policies*

*Establish corporate practices to communicate and train staff*

*Develop evaluation criteria (KPIs) to benchmark the operation*

*Create a Whitelist for critical application services*

*Assess vulnerabilities and patch the software regularly*

*Implement the need-to-know principle for defining access rights*

*Establish content filtering for all inbound and outbound channels*

➤ *manufacturing sectors*

# Summary

- Business Challenges
- Growth of Cybersecurity Attacks
- Use of Technology and Security Challenges
- The Challenge of Growing Threats
- Nation-State Threats



# Assignments



Discuss what the second biggest business challenge is (*after information security, of course*)

What is, in your opinion, the most dangerous security threat/attack?

Do you use any (mobile) technology in your everyday life? Which one? Is it secured?

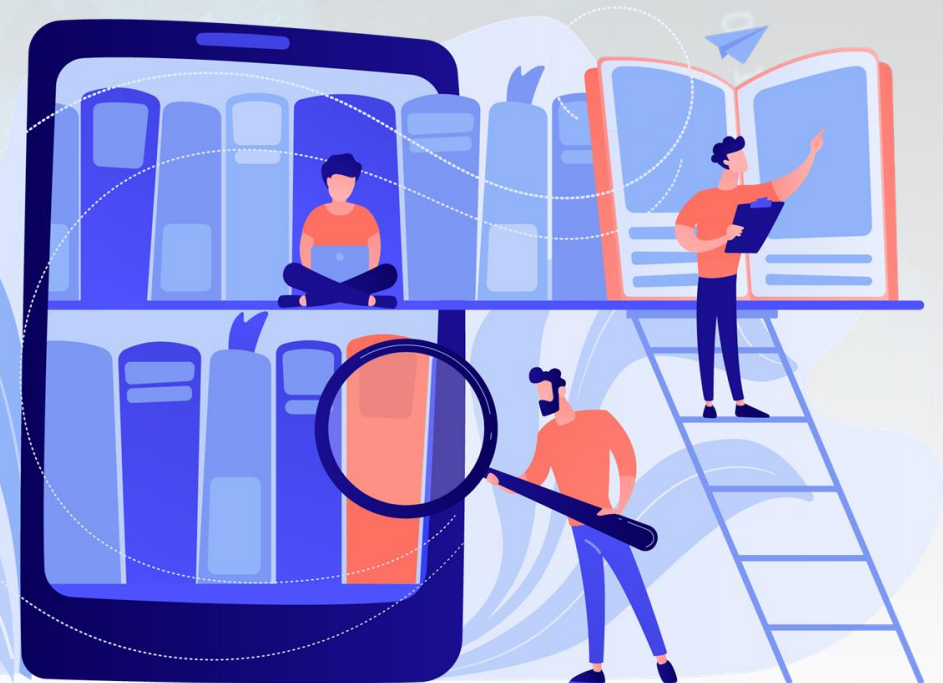
Do you know or have read about any Nation-State threat? Could you tell about it and explain what is the case?



# Further Reading

## Material used in preparation of this lecture

- **Abiodun O. I. A., Abiodun E. O., Alawida M., Alkhawaldeh R. S., Arshad H.,** (2021). A Review on the Security of the Internet of Things: Challenges and Solutions. *Wireless Personal Communications* 119:2603–2637 <https://doi.org/10.1007/s11277-021-08348-9>
- **Affia A-a. O., Matulevičius R., Nolte A.** (2019): Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review. *Panetto H. et al. (eds.), LNCS 11877, CoopIS 2019, Springer*
- **Anwar M. J. Gill A. Q., Hussain F. K., Imran M.** (2021), Secure big data ecosystem architecture: challenges and solutions. *J Wireless Com Network* 2021:130 <https://doi.org/10.1186/s13638-021-01996-2>
- **Colwill C.** (2009) Human factors in information security: The insider threat e Who can you trust these days? *Information Security Technical Report* 14,186-196
- **Iqbal, M., Matulevičius, R.** (2019) Blockchain-Based Application Security Risks: A Systematic Literature Review, *Proceedings of CAiSE 2019 International Workshops, 2019 Workshop, LNBIP 349, 176-188*
- **Komninos N., Philippou E., Pitsillides A.** (2014). Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures, *IEEE Communication Surveys & Tutorials*, 16(4)

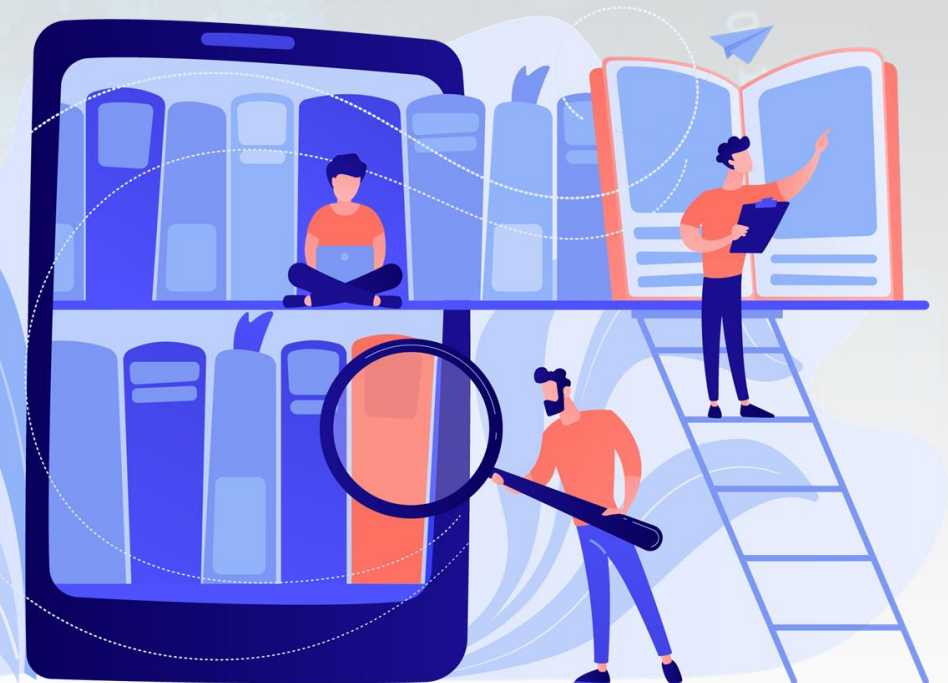




# Further Reading

## Material used in preparation of this lecture

- **Lewis, A.** (2015): Blockchain technology explained (2015). <http://www.blockchaintechnologies.com/blockchain-definition>
- **Orantes-Jimenez A.D., Aquirre E.** (2020): A Survey on Information Security in Cloud Computing, *Computation y Sistemas* 24(2)
- **Perdomo R.** (2021): 15 Technology Challenges Business May Face in 2021, URL: <https://blog.systems-x.com/author/rubens-perdomo>
- **Sato, T., Himura, Y.** (2018): Smart-contract based system operations for permissioned blockchain. *NTMS 2018, vol., 1–6*
- **Schatz, D., Bashroush, R., Wall, J.** (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law.* 12 (2).
- **Tahirkheli, A.I.; Shiraz, M.; Hayat, B.; Idrees, M.; Sajid, A.; Ullah, R.; Ayub, N.; Kim, K.-I. A.** (2021). Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics* 2021, 10, 1811. <https://doi.org/10.3390/electronics10151811>



# Short Videos

- Business Technology Trends  
<https://youtu.be/DOAnYtqhXBU>
- The Internet of Things Security  
<https://youtu.be/IQkRscixagM>
- Cloud Cybersecurity  
<https://youtu.be/k2684fuzHLs>
- Hacking your Home  
<https://youtu.be/iRQPfISsG9k>
- Introduction to Blockchain Security  
<https://youtu.be/dl8HI91siM8>
- Challenges of Securing Big Data  
<https://youtu.be/3xlulcPzMVs>
- What are the Current Data Security Threats?  
<https://youtu.be/WugGZaT2oHE>
- Top 7 Most Elite Nation State Hackers  
[https://youtu.be/S\\_IPgHbondk](https://youtu.be/S_IPgHbondk)



# Thank you!

