Innovations and Security Aspects in ICT Technologies

Raj Kumar

Innovations and Security Aspects in ICT Technologies

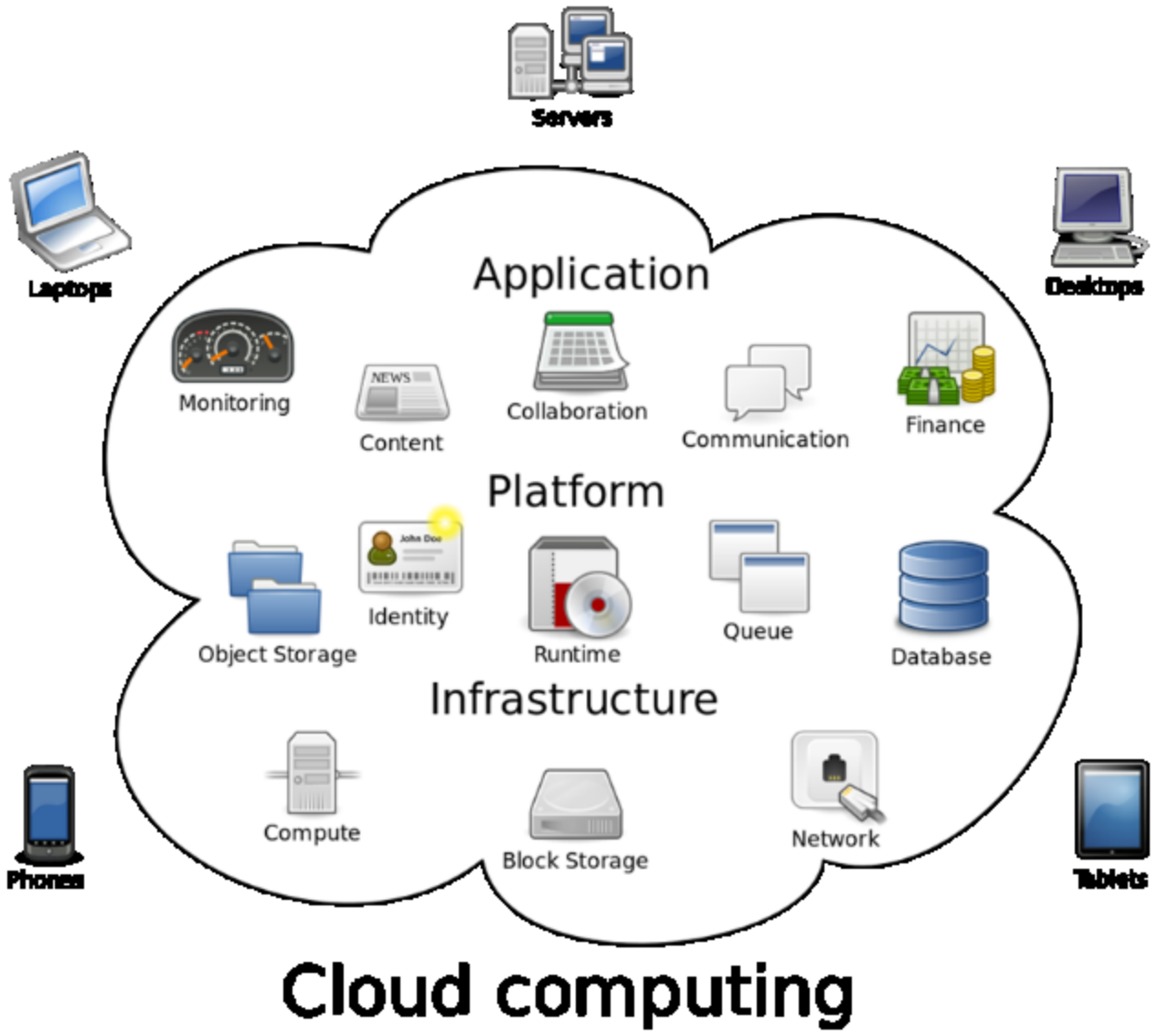
- Cloud Computing, IOT
- Block Chain
- Artificial Intelligence
- 5G Data Privacy and Security

Cloud Computing and IOT

- What is Cloud Computing?
- Benefits of Cloud Computing
- Private Cloud vs Public Cloud vs Hybrid Cloud
- Cloud Providers
- Obstacles of Cloud Computing
- Opportunities of Cloud Computing

What is Cloud C

- Cloud Computing - applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.
- Cloud computing enables sharing of computing resources on the internet and rids the need of relying on local servers for smooth functioning of business operations.

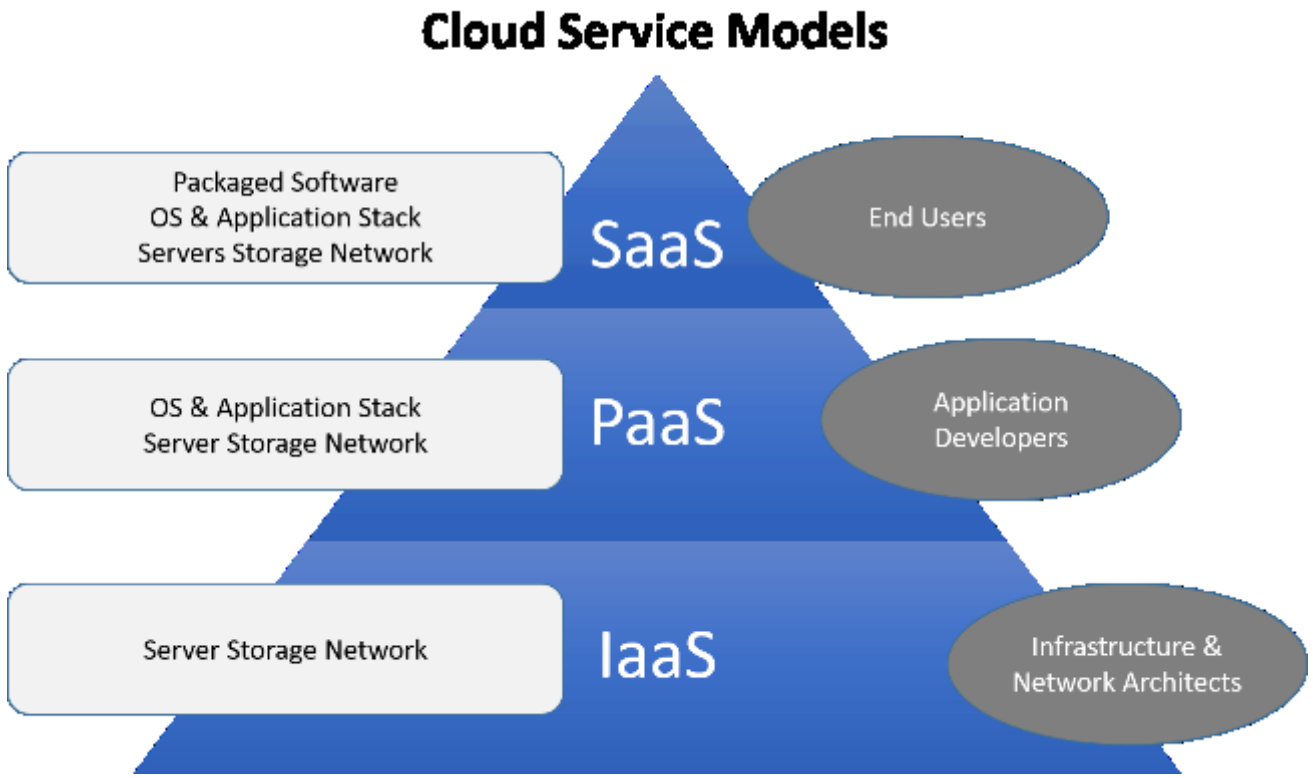


By Sam Johnston - Created by Sam Johnston using OmniGroup's OmniGraffle and Inkscape (includes Computer.svg by Sasa Stefanovic)

Cloud Computing Services

Cloud computing services are available under three categories:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (Iaas).



https://www.uniprint.net/en/7-types-cloud-computing-structures/

Benefits of Cloud Computing

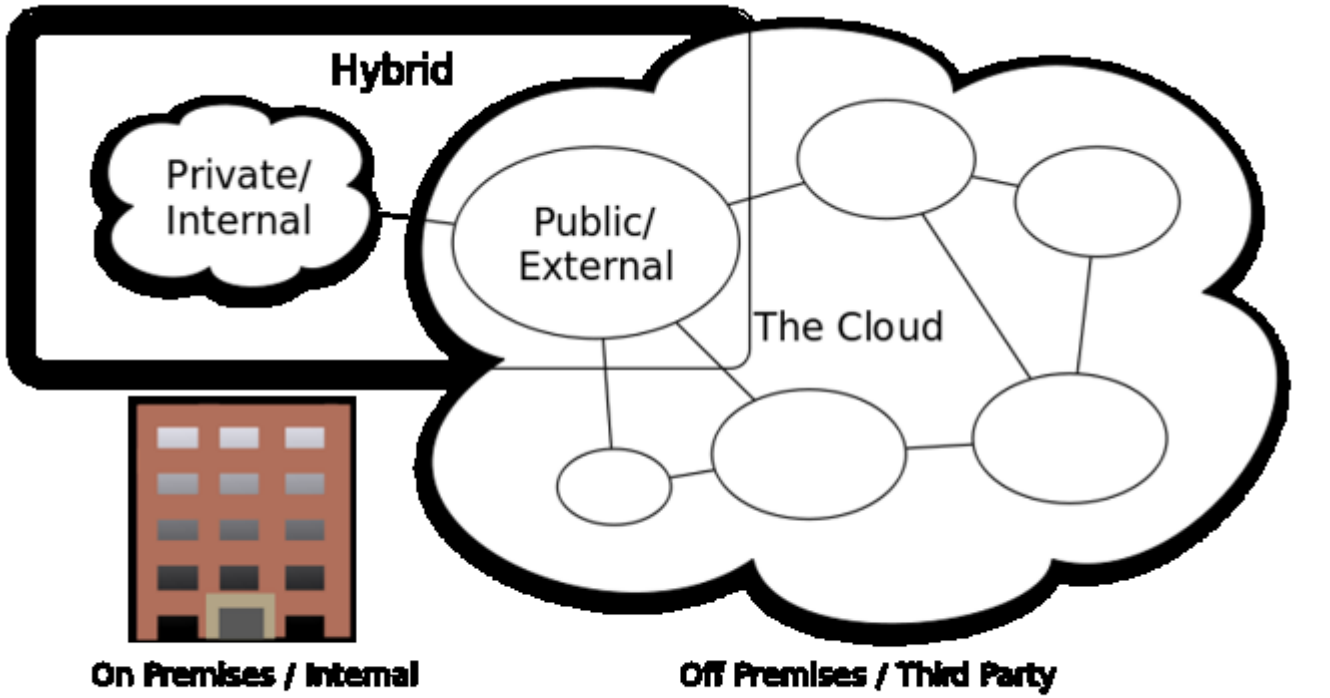
- Flexibility
- Disaster Recovery
- Software Updates
- Capital Expenditure- Free
- Increased Collaboration
- Work from anywhere
- Document control
- Security
- Competitiveness
- Environmental-Friendly

Private Cloud vs Public Cloud vs Hybrid Cloud

Public Cloud - When a cloud service is made available in a pay-as-you-go manner to the general public

Private Cloud - Internal datacenters of a business or other organization, not made available to the general public.

Hybrid Cloud – An environment where there is a mix of on-premise and public cloud with orchestration between both



Cloud Providers

Cloud Marketplace	AppDirect, APPIRIO, INGRAM MICRO Partner Smart, myGravitant, …
Cloud Broker Platform	cloudMatrix™, jamcracker, …
Cloud Management	apptio, cloudability, CLOUDSWITCH, Cloudyn, Gravitant, TECH, RIGHTSCALE, …
SaaS	Google Apps, NETSUITE, Salesforce, Taleo, …
PaaS	Azure, force.com platform as a service, Google, heroku, …
IaaS	amazon web services, GOGRID, Joyent, rackspace, SAVVIS, terremark, …
Cloud Platform	cloudstack open source cloud computing, cloud.com, ElasticStack Powering your own-brand cloud, enomaly, Eucalyptus, flexiant, onapp, openstack, vmware vCLOUD, …
Virtualization Software/Mgmt	Parallels, VirtualIron, Virtuozzo, vmware, Xen, CITRIX XenServer, Hyper-V, KVM, vSphere, …
Hardware	IBM BladeCenter®, DELL PowerEdge Blade Servers, ORACLE Sun Blade, hp BladeSystem, …

http://xyfon.com/how-to-pick-the-right-cloud-provider-your-business/

Obstacles of Cloud Providers

- Availability of Service
- Data Lock-In
- Data Confidentiality and Auditability
- Data Transfer Bottlenecks
- Performance Unpredictability
- Scalable Storage
- Bugs in Large-Scale Distributed Systems
- Scaling Quickly
- Reputation Fate Sharing
- Software Licensing

Opportunities of Cloud

- Use ICT for their business with low investment (no CAPEX; pay as you go)
- Buy ICT as Services (subscription model) such as SaaS
- Can focus on business
- Business Continuity
- New Business Opportunity

Security Aspects of Cloud Computing

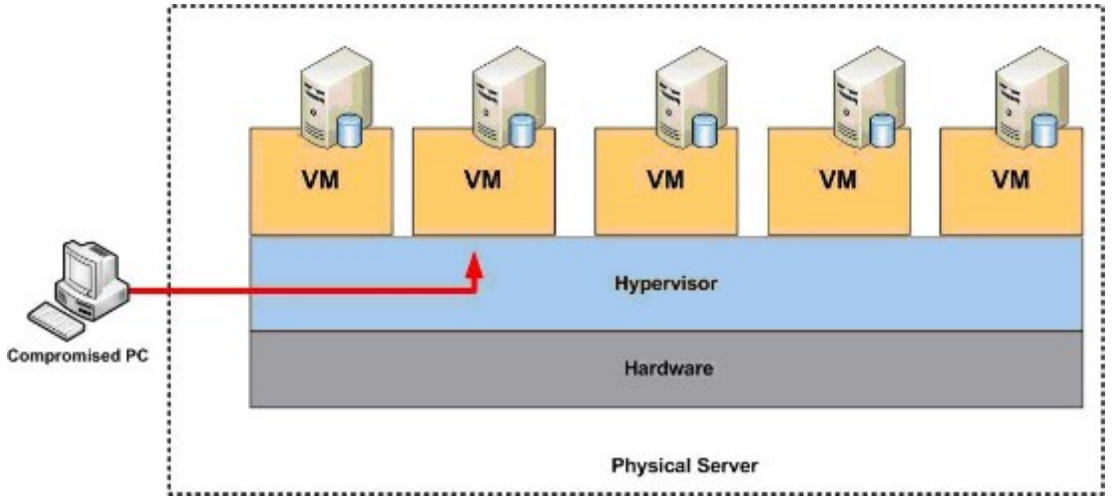
- Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time.
- Data could be accidentally or deliberately altered or deleted
- Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services.
- Solutions to privacy include policy and legislation, as well as end users' choices for how data is stored.
- Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access

According to the Cloud Security Alliance, the top three threats in the cloud are

- *Insecure Interfaces and API's*
- *Data Loss & Leakage*
- *Hardware Failure*—which accounted for 29%, 25% and 10% of all cloud security outages respectively.

Security Aspects of Cloud Computing

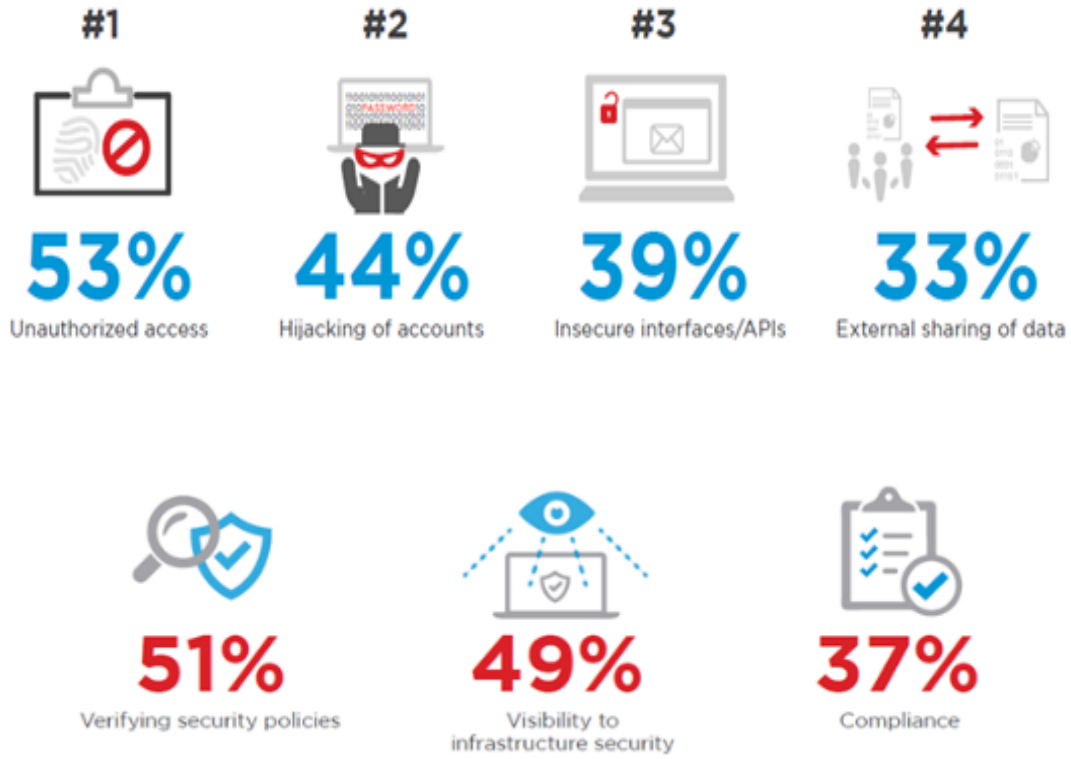
- Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack—a process he called "hyperjacking".
- Many companies shy away from adopting computing services on the cloud due to security threats.
- Many businesses fail to realize that the security concerns with cloud computing can be effectively addressed to successfully wipe off any data breach and abrupt obstacles to their business operations.



https://en.wikipedia.org/wiki/Hyperjacking

Biggest security concerns of Cloud Computing

- Data Loss
- Data Breach
- Insecure API
- Malicious Insiders
- Shared Technology Vulnerabilities
- Availability and Reliability Issues
- Lack of Risk Management
- Service Abuse



http://resources.infosecinstitute.com/security-barriers-adaptation-cloud-technology/#gref

Security Aspects of Cloud Computing

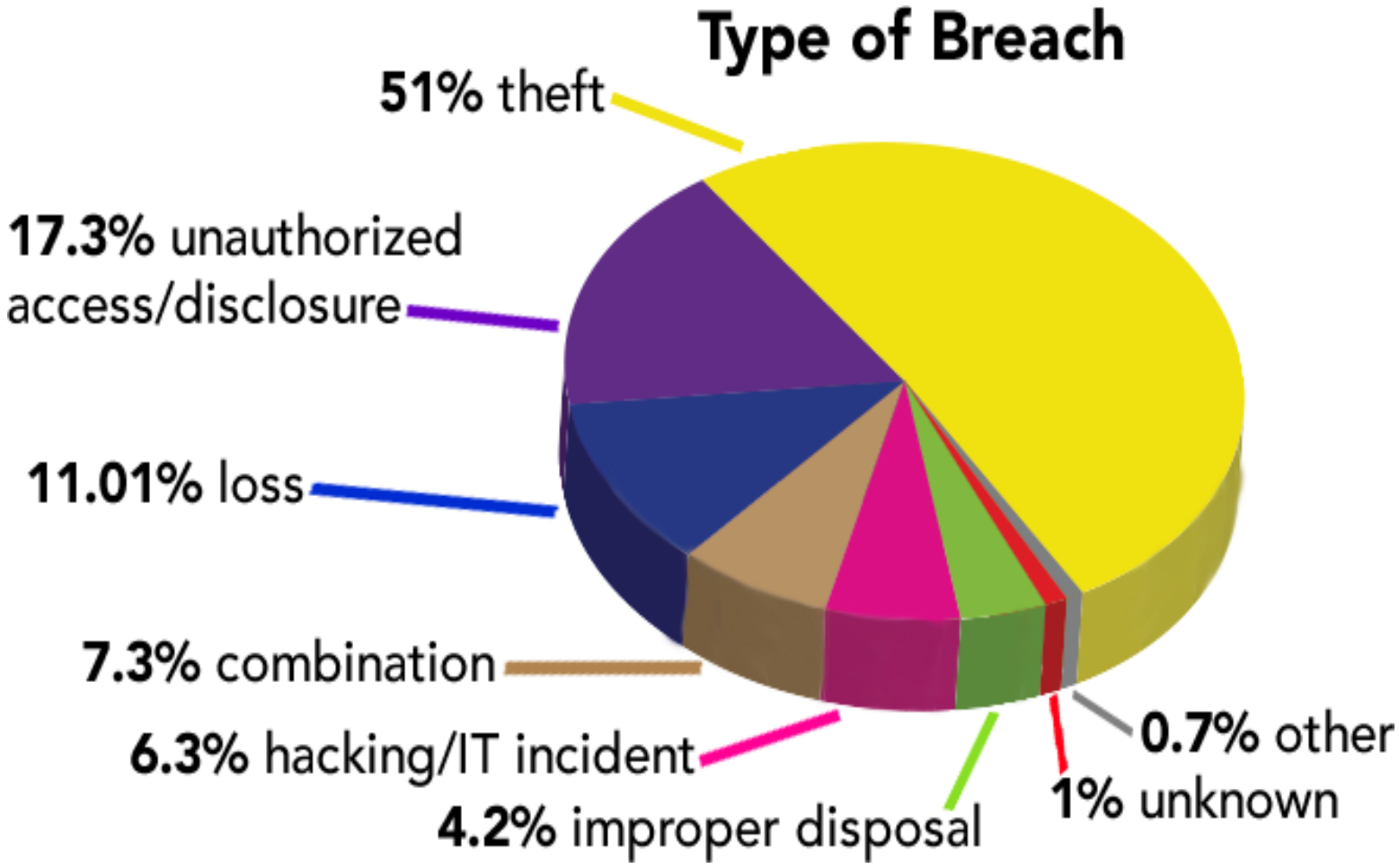


Image Credit: http://funnyvideoz.xyz/2016/02/21/cloud-computing-security-risks/

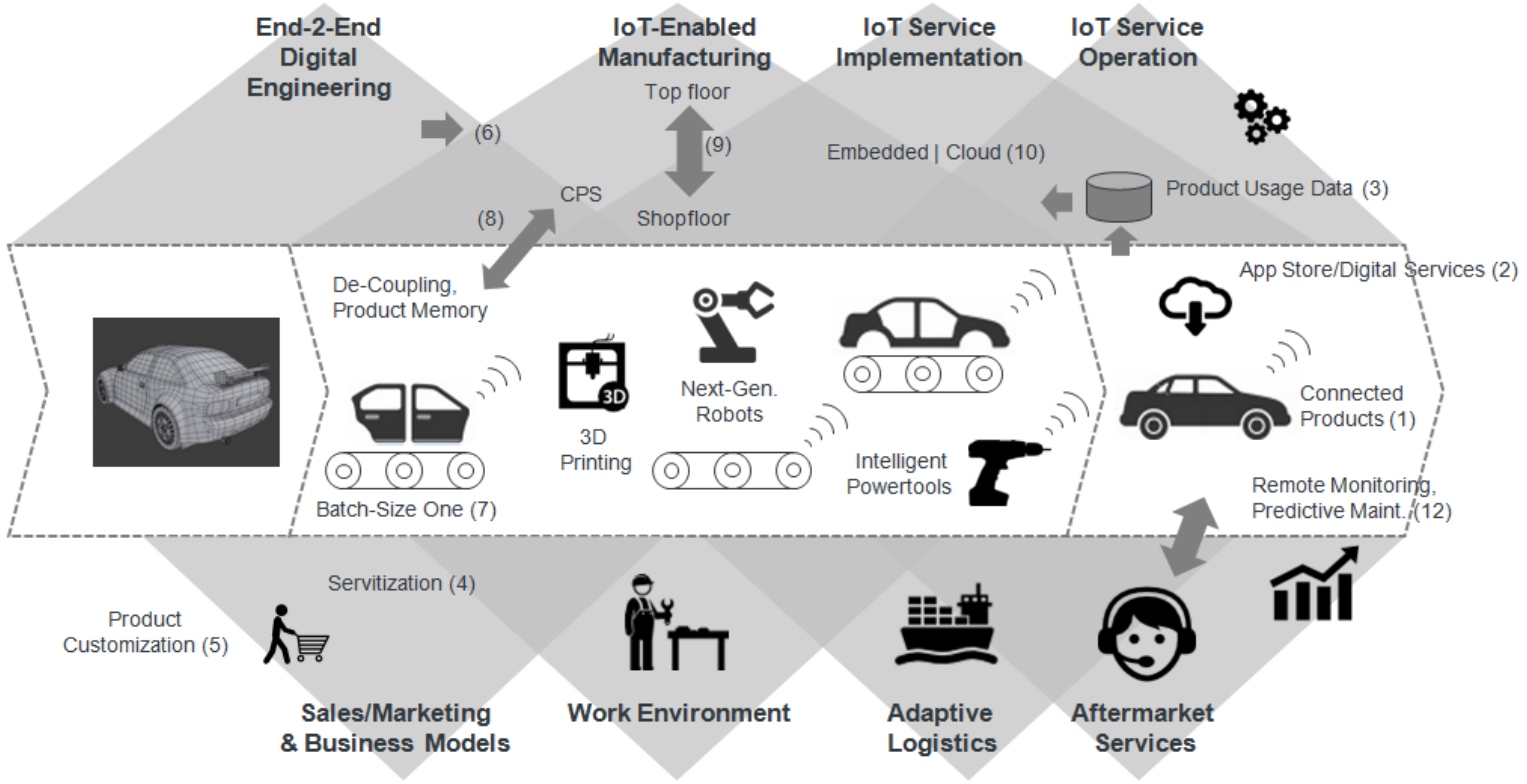
IoT Security

- The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data.
- Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.
- Experts estimate that the IoT will consist of about 30 billion objects by 2020.
- IoT allows devices to be controlled or sensed remotely using the network infrastructure

https://www.open-electronics.org/iot-gets-a-new-wireless-technology-backed-by-intel-nokia-and-ericsson-nb-lte/

IoT and Cyber-Physical System

When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems



http://enterprise-iot.org/book/enterprise-iot/part-i/manufacturing/

IoT Security Targets

IoT Security

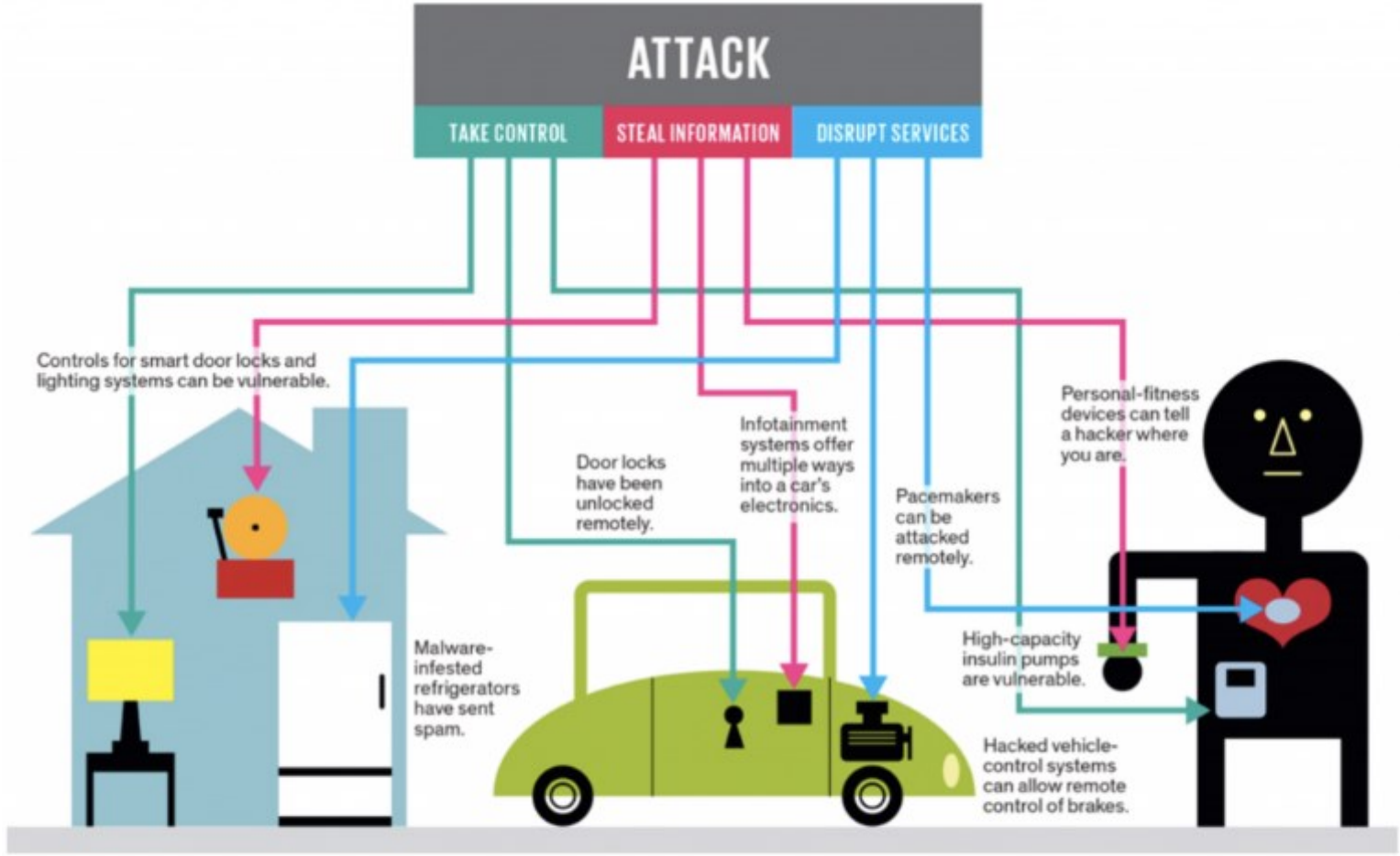
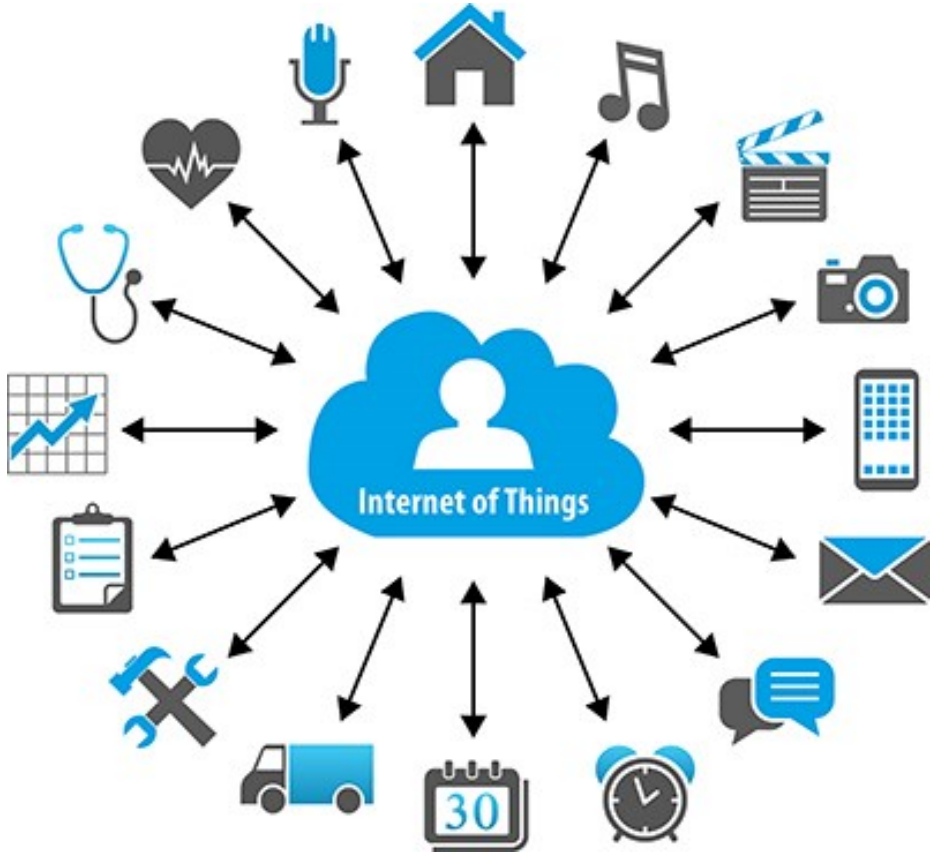


Illustration: J. D. King

- IoT Security is not well understood or defined
- Many industry are not clear about this, except for e-commerce and financial industry

Top 10 emerging IoT technologies by Gartner

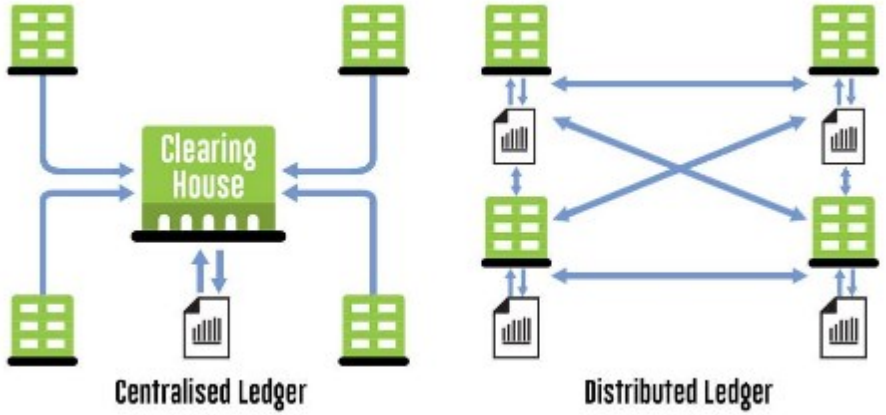
- IoT Security
- IoT Analytics
- IoT Device (Thing) Management
- Low Power, Short Range IoT Networks
- Low Power, Wide Area Networks
- IoT Processors
- IoT Operating System
- Event Stream Processing
- IoT Platforms
- IoT Standards and Ecosystem



http://www.kosbit.net/internet-things-iot-next-big-thing/

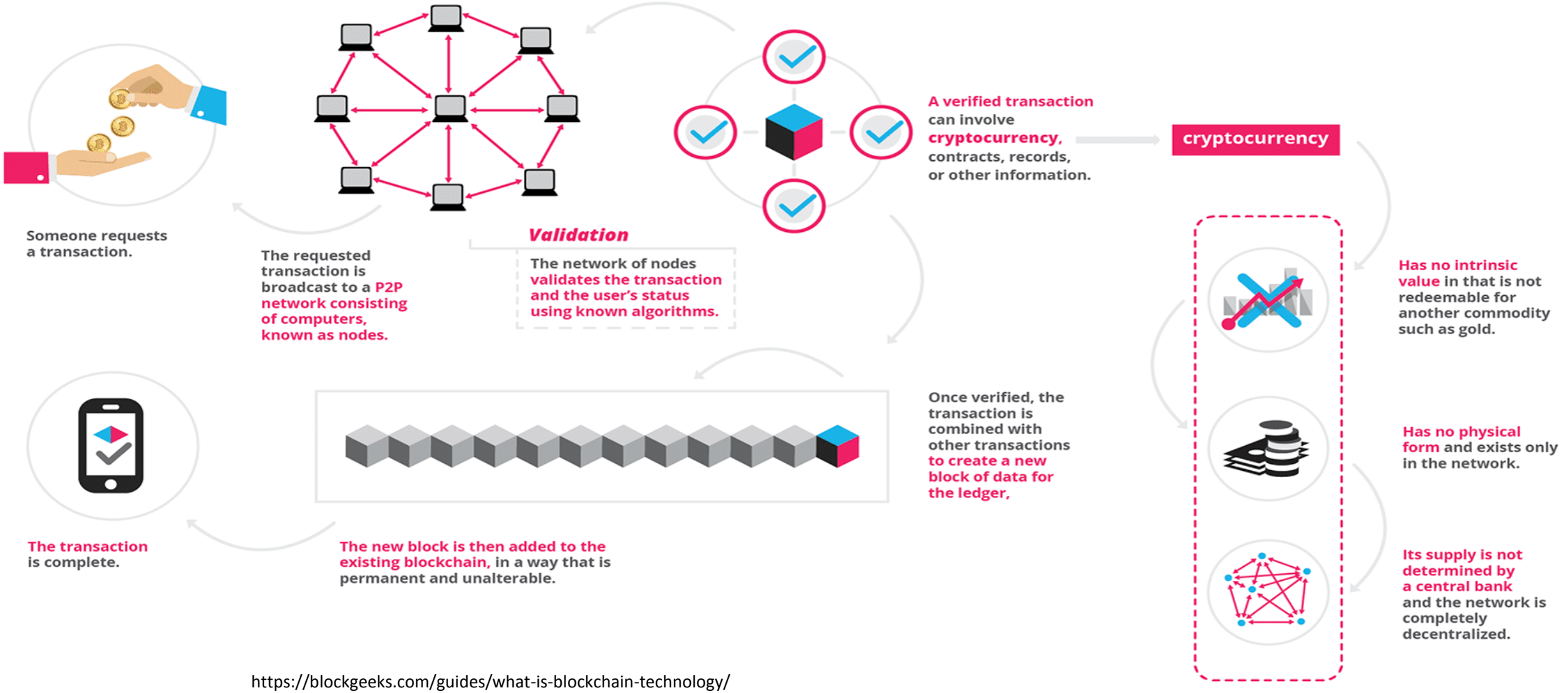
Block Chain

- “The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.” - Don & Alex Tapscott, authors Blockchain Revolution (2016)
- Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet. This is blockchain technology
- Information held on a blockchain exists as a shared — and continually reconciled — database.
- The blockchain database isn’t stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.



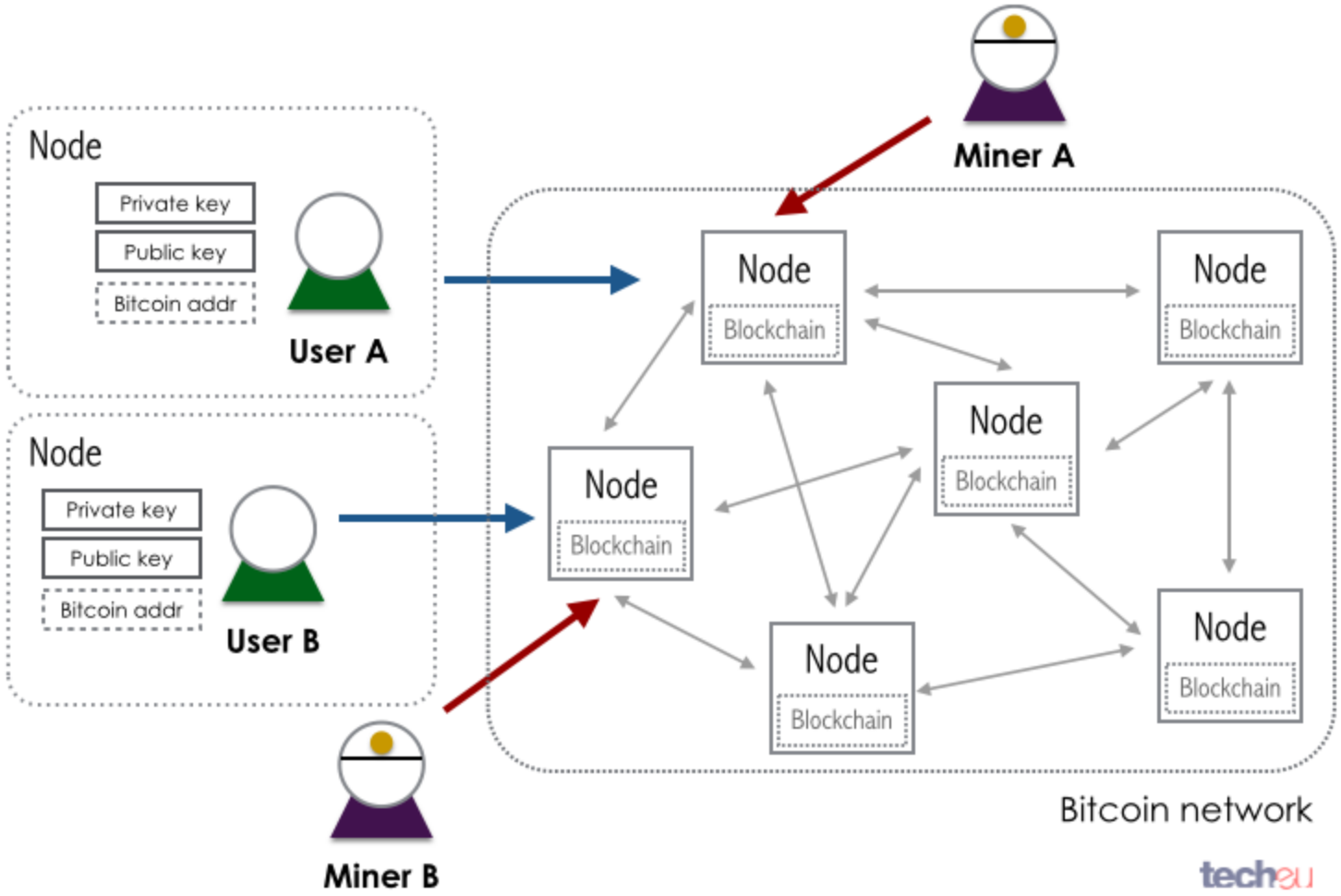
https://www.quantinsti.com/blog/will-blockchain-change-stock-markets/

Block Chain



https://blockgeeks.com/guides/what-is-blockchain-technology/

Block Chain



http://tech.eu/wp-content/uploads/2014/03/Bitcoin-network1.png

Artificial Intelligence

- In a cybersecurity context, AI is software that perceives its environment well enough to identify events and take action against a predefined purpose.
- AI is particularly good at recognizing patterns and anomalies within them, which makes it an excellent tool to detect threats.
- Machine learning is often used with AI - can “learn” on its own based on human input and results of actions taken.
- Together with AI, machine learning can become a tool to predict outcomes based on past events.

Analysing Threats with AI & ML

- Analysis – Study and understand collected data
- Analytic – Data analysis with predictability
- AI – Analytics with Intelligence
- AI will allow
  - Multiple sources of data
  - Dynamic context for data analysis
  - Low latency in prediction
- Machine Learning – Random Forest, Gradient Boosting engine, Deep Learning, Neural Networks

Challenge in cybersecurity

- Exposure of PII – Personal Identifiable Information – Banks, Govt, Corporations
- Enormous amount of data and compromises on network, on-premise and cloud
- Many apps, devices and platforms
- Threats are harder to detect and advancing quickly
- Attacker are collaborating
- Lack of advanced tools and technologies
- Human factor is not enough
- Responses to security events are not fast enough and labour-intensive
- Cybersecurity hiring crunch and shortage of skills
- Multiple attack vectors
- Many Zero day attack vectors

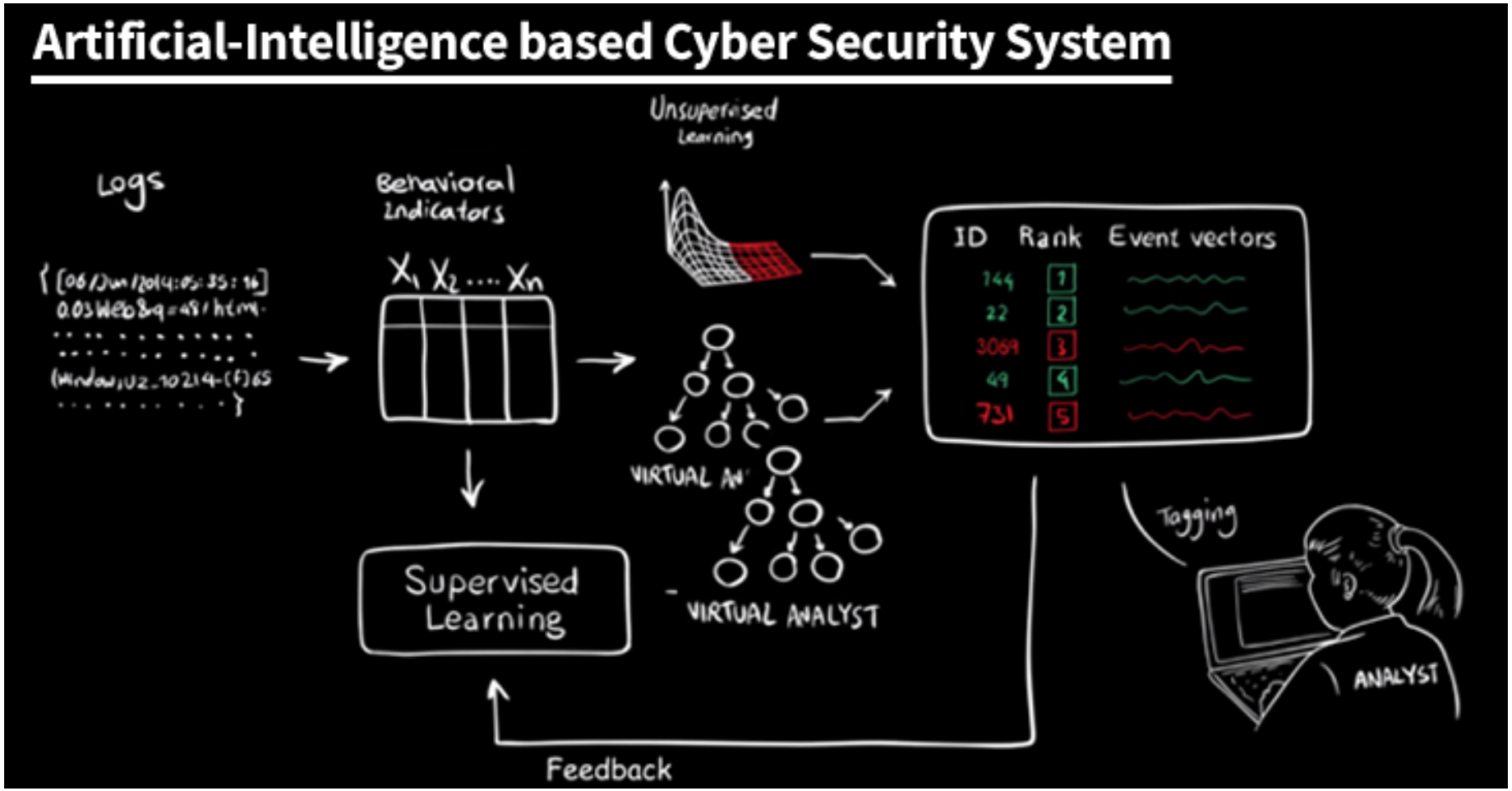
Benefits of AI in Cybersecurity

- AI and Machine learning automate tasks and can detect threats faster
- Look for patterns and anomalies for threats in networks, apps, devices and cloud
- Can predict based outcomes based on past events
- People can focus more on human-led tasks
- Overcome overload of security data

AI in Cybersecurity

Security researchers at MIT have developed a new Artificial Intelligence-based cyber security platform, called '**AI2**,' which has the ability to predict, detect, and **stop 85% of Cyber Attacks** with high accuracy.

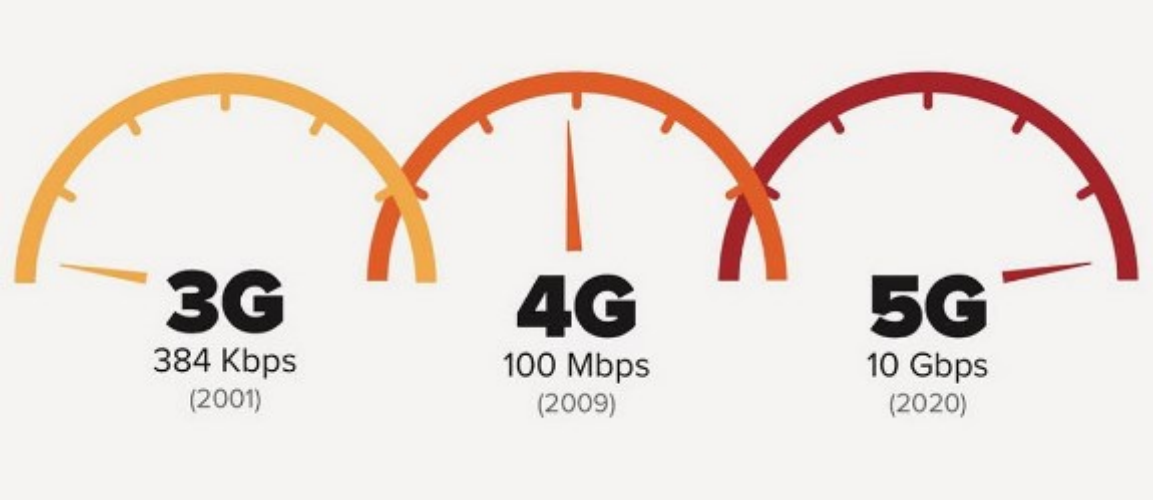
Can review data from more than *3.6 Billion lines of log files each day*



https://thehackernews.com/2016/04/artificial-intelligence-cyber-security.html

5G and Data Privacy and Security

- 5th generation mobile networks or 5th generation wireless systems, abbreviated 5G, are the proposed next telecommunications standards beyond the current 4G/IMT-Advanced standards.
- 5G planning aims at higher capacity than current 4G, allowing a higher density of mobile broadband users, and supporting device-to-device, more reliable, and massive machine communications.
- 5G research and development also aims at lower latency than 4G equipment and lower battery consumption, for better implementation of the Internet of things..
- There is currently no standard for 5G deployments



http://trak.in/wp-content/uploads/2017/10/5G-Network.jpg

Benefits of 5G

The Next Generation Mobile Networks Alliance defines the following requirements for 5G standard:

- Data rates of tens of megabits per second for tens of thousands of users
- Data rates of 100 megabits per second for metropolitan areas
- 1 Gb per second simultaneously to many workers on the same office floor
- Several hundreds of thousands of simultaneous connections for wireless sensors
- Spectral efficiency significantly enhanced compared to 4G
- Coverage improved
- Signaling efficiency enhanced
- Latency reduced significantly compared to LTE.

http://www.3gpp.org/about-3gpp/1824-logo_5g

Traditional Security Practice – 2G, 3G & 4G

- One way authentication – 2G
- Mutual authentication between network and user – 3G, 4G
- Focused on protection or voice and data
- User Identity Management based on U(SIM)
- Secure path between communication parties (hop by hop)
- Some SIM supported DES

Security Challenges for 5G

- New Services focused Business Model
  - Mobile IoT will require lightweight security
  - High speed secured mobile services
  - End to end security (E2E), hop to hop security will not be sufficient
  - More people will remotely “talk” to networked devices – Smart Homes
- IT-Driven Network Infrastructure
  - New Visualization and SDN (Software Driven Network)/Network Functions Visualization
  - Legacy networks focused on isolated systems for security
  - 5G Network elements (NE) will work as Virtual NE on cloud infrastructure with security consideration.
- Heterogenous Access
  - Different network access (WiFi and LTE) and also from multi-network environment
  - Network architecture varies from networks.
  - Security developers need to develop for various network architecture and access technologies
  - IoT have many choices to connect to networks – more efficient and lightweight – easier to establish trust between device and networks

Security Challenges for 5G

- Privacy Protection
  - Open networks will raise privacy leakage and concerns.
  - Data and signalling contains personal privacy information – identity, position, private content
  - To get quality service, the operator may need to sense what kind of service a user is using.
  - Privacy protection will be more challenging for 5G.

ITU : I Thank U