Securing IoT in the AI and Quantum Era

É-EGC, Anglet, 26/01/2026

Theme 1: From reactive defense to predictive autonomy

Theme 2: When quantum decryption meets classical vulnerability

Theme 3: Harnessing quantum intelligence to secure the next generation of IoT

EGC 2026

About me- Degrees

B.Eng. in **HW computer architecture**
ESIR Rennes.

M.Eng. in critical **computer systems** and **networks**
INP + INSA of Toulouse.

PhD in **Software engineering**
ETS-University of Quebec.

About me-current affiliations

- Associate Professor and head of the Digital Transformation & Innovation engineering program.

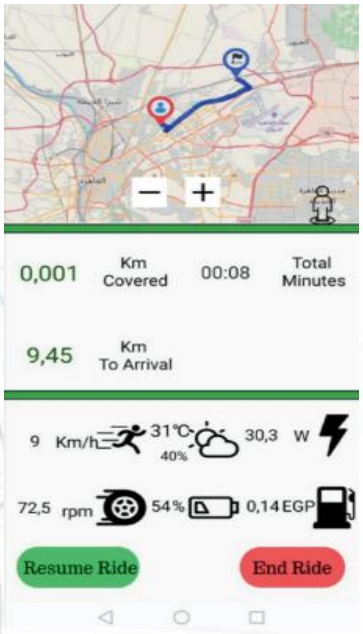
https://www.ece.fr/en/program/engineering-degree-bac4-digital-industry-major/
https://www.ece.fr/les-membres-du-lyrids/

- Nominated member of the Measurement Practices Committee and the International Advisory Council at **COSMIC-ISO 19761** the Common Software Measurement International Consortium.

https://cosmic-sizing.org/organization/committees/measurement-practices-committee/
https://cosmic-sizing.org/cosmic-projects/

About me-Previous experience

- Associate Professor CSEN and head of the IoT Lab



About me-Previous experience

- Associate Professor

ESTACA
ECOLE D'INGENIEURS

- Software Engineering Courses' Coordinator
- Consulting for different OEMs
- Head of Intelligent Transportation Systems program

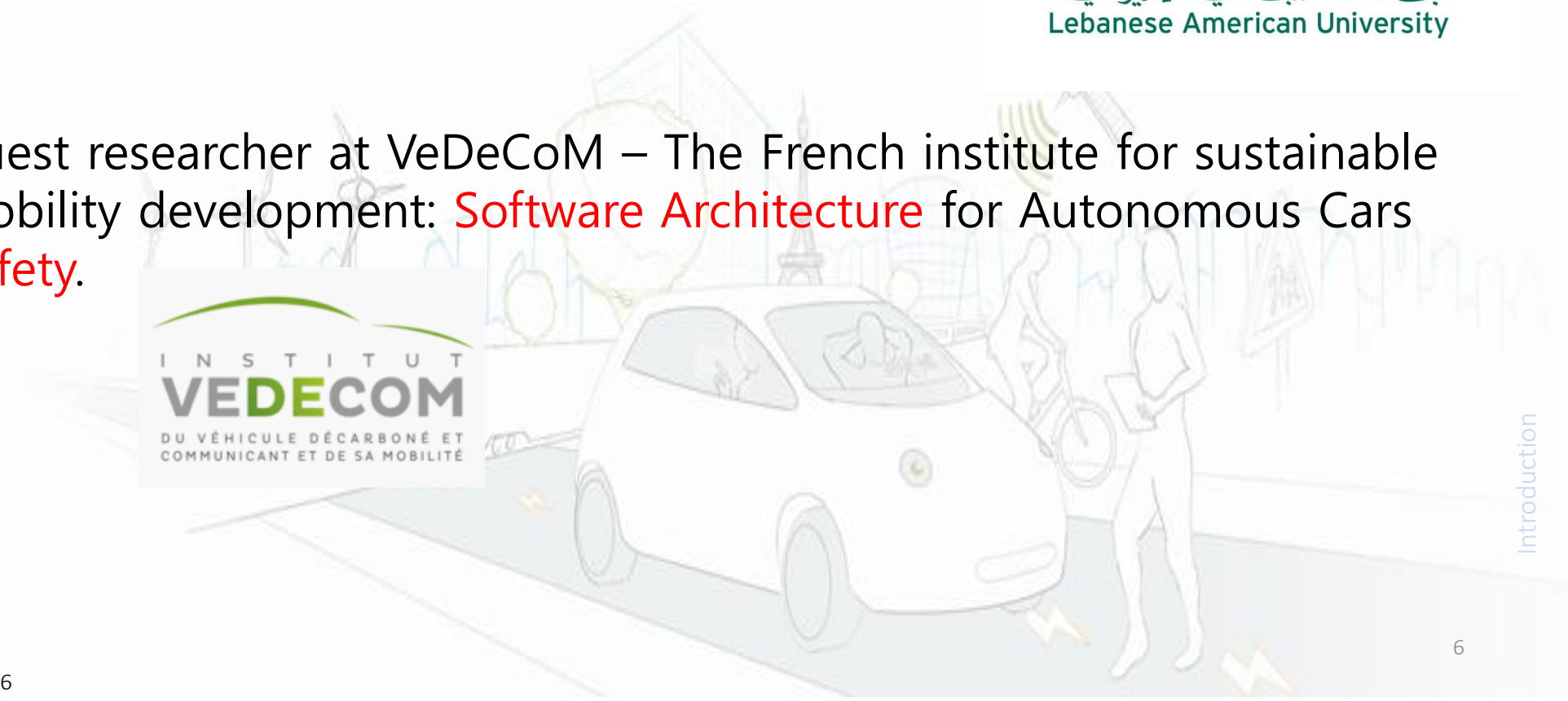
About me-Previous experience

- Guest Part-time lecturer in Computer Science (Sabbatical Leave)

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

- Guest researcher at VeDeCoM – The French institute for sustainable mobility development: Software Architecture for Autonomous Cars Safety.

INSTITUT VEDECOM
DU VÉHICULE DÉCARBONÉ ET COMMUNICANT ET DE SA MOBILITÉ



About me-Industry experience

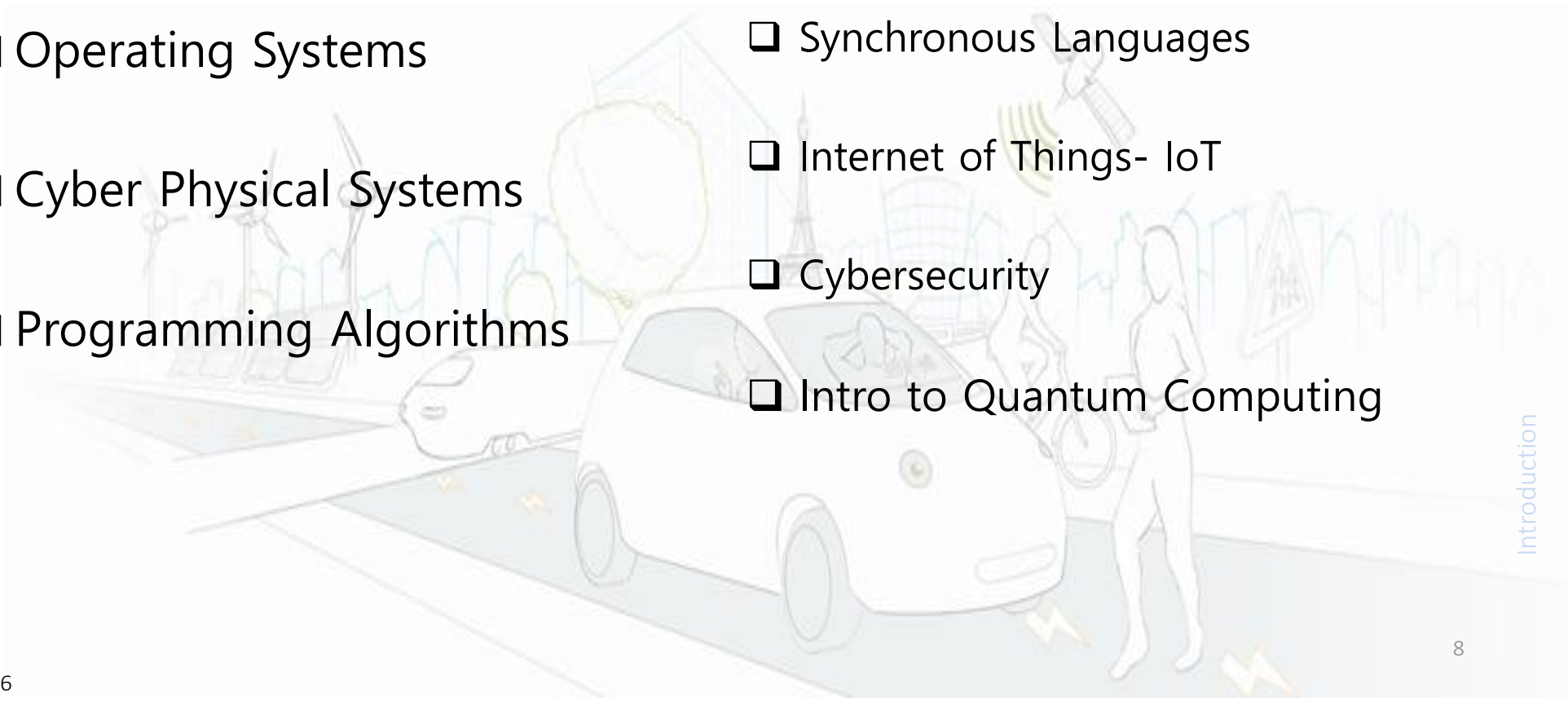
- R&D engineer in Emb. Software

- R&D engineer at Thomson Multimedia (now Technicolor SA)

- Researcher at LAAS CNRS in collaboration with Thales Avionics.

About me- Teachings

- Embedded Systems Design
- Computer System Architecture
- Operating Systems
- Cyber Physical Systems
- Programming Algorithms
- Microcontrollers
- Autonomous Vehicles
- Synchronous Languages
- Internet of Things- IoT
- Cybersecurity
- Intro to Quantum Computing



About me- Research Fields

- ❑ Software Metrics and Measurement.
- ❑ Quantum SE
- ❑ Smart Cities and Intelligent Transportation Systems

Google Scholar

IEEE COMPUTER SOCIETY QTC
Quantum Technical Community

2 patents + >66 papers including **3 best paper awards**

Looking for contributors-- pls Reach out!!

https://cosmic-sizing.org/cosmic-projects/

About me- Quantum Taskforce

Software product & project management chair
École de technologie supérieure - Montréal

COSMIC

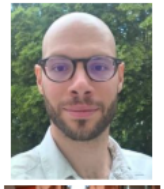
ÉTS
Le génie pour l'industrie

mitacs

With the advent of large-scale software development came the need to better plan, monitor and control the economics of software development, including in new software development paradigms. The COSMIC organization has initiated five task forces to tackle current industry challenges in software measurement:

- Quantum software sizing
- Artificial Intelligence software sizing
- Non-functional requirements sizing and Technical Debt
- Sizing for DevOps
- Educational Simulator for Software Estimation

The COSMIC taskforces are led by international experts in the respective areas of expertise:



Dr. Hassan Soubra
Quantum software

Dr. Sylvie Trudel
DevOps portfolio

Dr. Thomas Fehlmann

About me- Submit your work !

Special Issue

New Insights into Network Security in the AI and Quantum Era

Guest Editor

Dr. Hassan Soubra

Deadline

10 February 2026

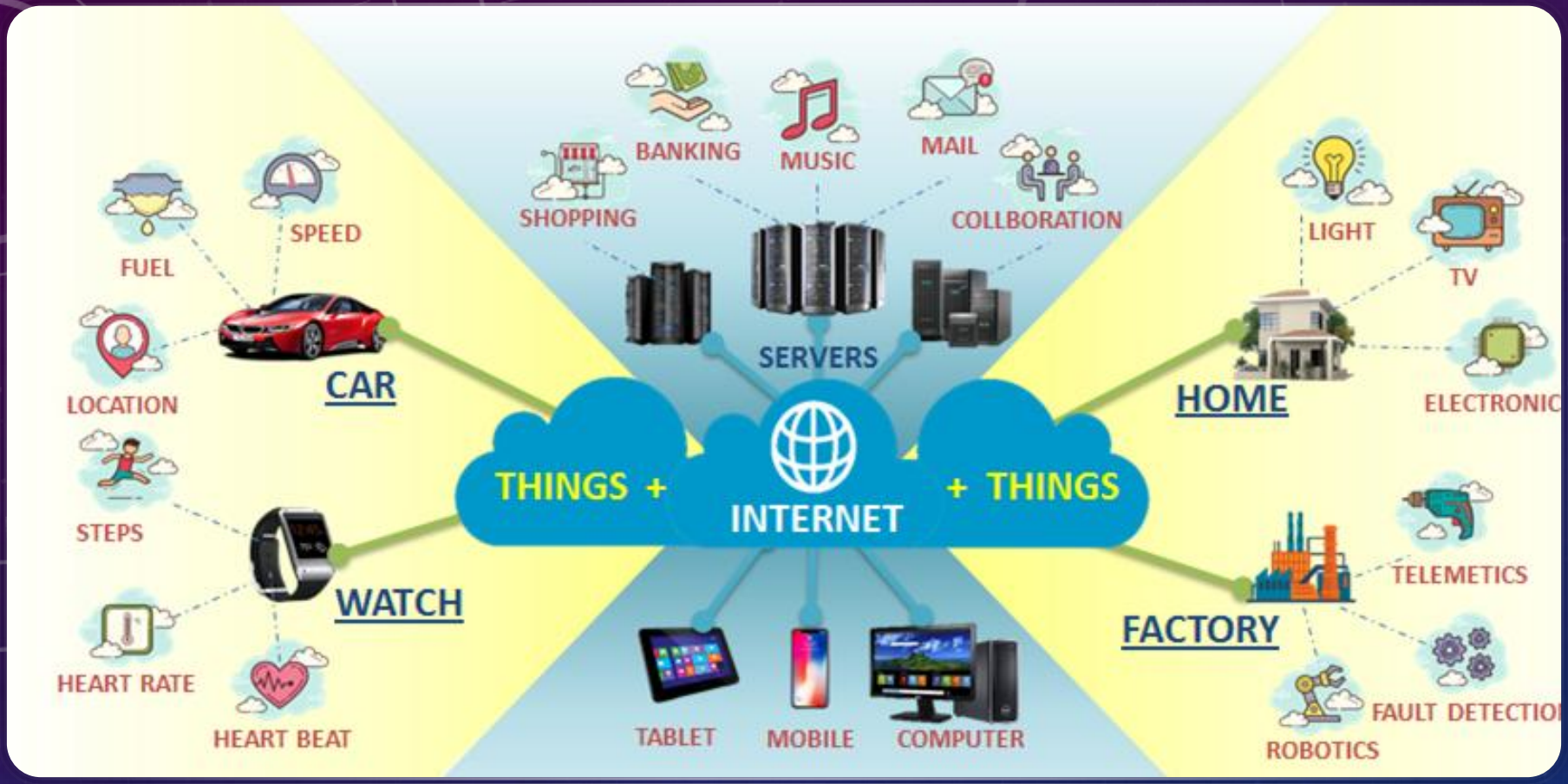
applied sciences

IMPACT FACTOR 2.5

CITESCORE 5.5

DISCLAIMER

This presentation contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. They are used strictly for educational purposes. The principle of fair use applies.



Source: simplycoding.in

WHY IOT NEEDS AI

Brief History of IoT

1993
The first online webcam is used at Cambridge

1994
Steve Mann creates WearCam

1999
Kevin Ashton coins the term Internet of Things

2000
LG announces the first smart refrigerator

2005
UN publishes its first report on the Internet of Things

2007
First iPhone is launched

2008
The number of connected devices overtakes the number of people in the world and IoT is 'born'

2009
The original Fitbit activity tracker is released

2011
IIoT comes into being

2014
Seoul becomes the world's first smart city

2015
IoT goes Mobile with smartphones

2016
AWS IoT core is launched

2020
The number of IoT device connections increased more than 50% of the active connected devices

2021
More than 10 billion active IoT devices active

2022
World Economic Forum names IoT as one of the three most impactful technological advancements

BYTEBEAM

medium.com

Facts & Insights

How can defenders stay one step ahead of threats without compromising operational efficiency and security effectiveness?

The problem is the need for intrusion detection systems that react to known threats and anticipate and adapt to emerging threats in real-time.

Villegas-Ch, William, et al. "Effectiveness of an Adaptive Deep Learning-Based Intrusion Detection System." IEEE Access (2024).

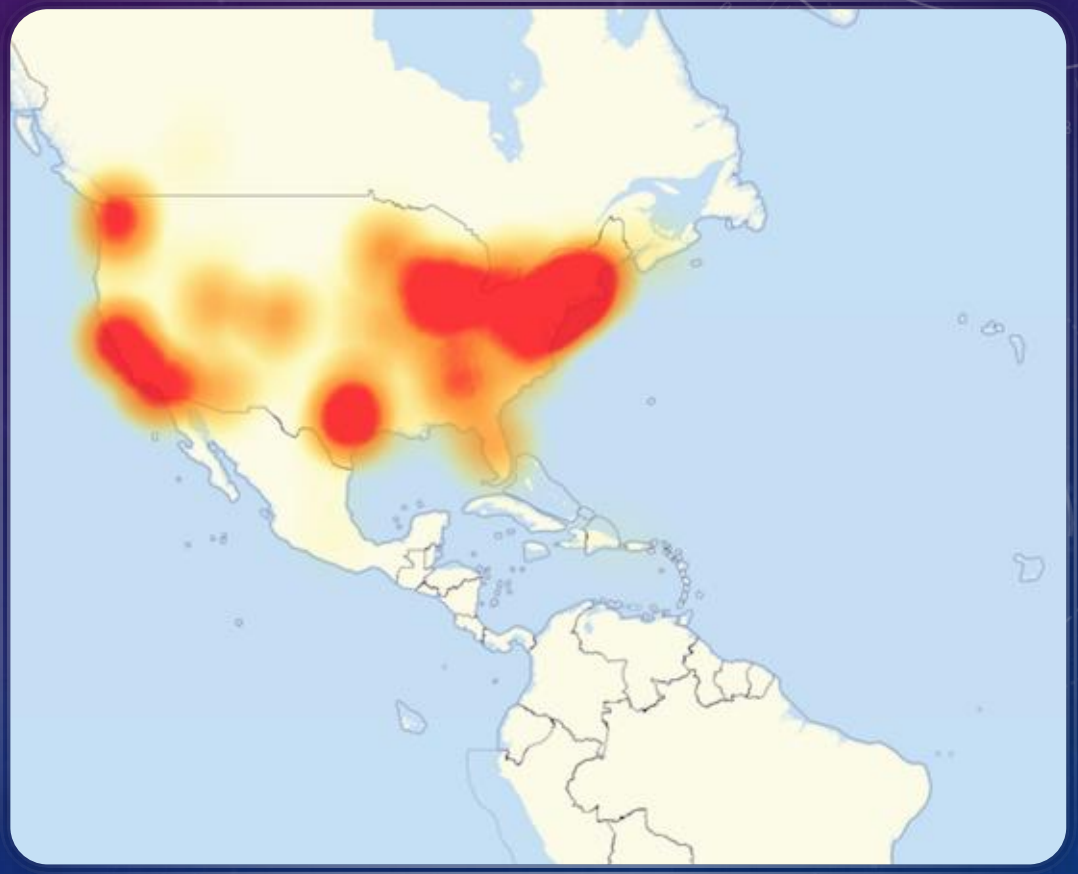
The Internet of Things (IoT) is now the nervous system of modern infrastructure—smart cities, autonomous vehicles, healthcare, and industry. However, this connectivity expands the attack surface exponentially.

Over **29 billion IoT devices** expected by 2030 (Statista, 2024).
Traditional security mechanisms (e.g., static firewalls, signature-based IDS) fail under real-time, heterogeneous IoT conditions.

AI allows *behavioral baselining*, *context-aware monitoring*, and *self-learning protection*.

MIRAI-DYN ATTACK

- On October 21st 2016, millions of household IoT devices were infected with the malware Mirai and instructed to send data requests to Dyn, a widely used Domain Name Server (DNS) that acts like a switchboard for the Internet.
- This tidal wave of requests crashed over 175,000 domains—including including GitHub, Twitter, Reddit, Netflix, Airbnb and many others—for several hours, affecting tens of millions of users.

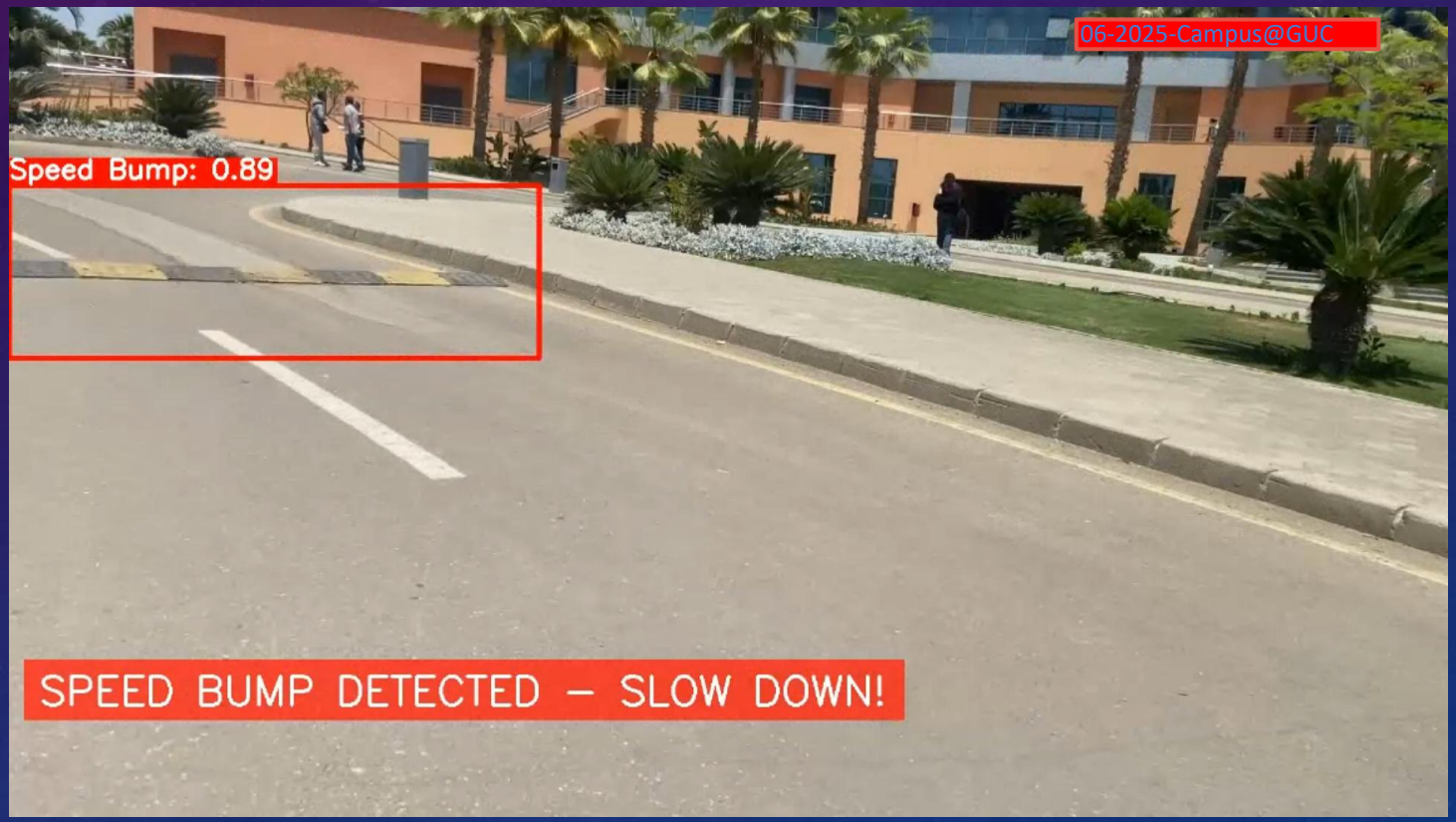


www.cylab.cmu.edu

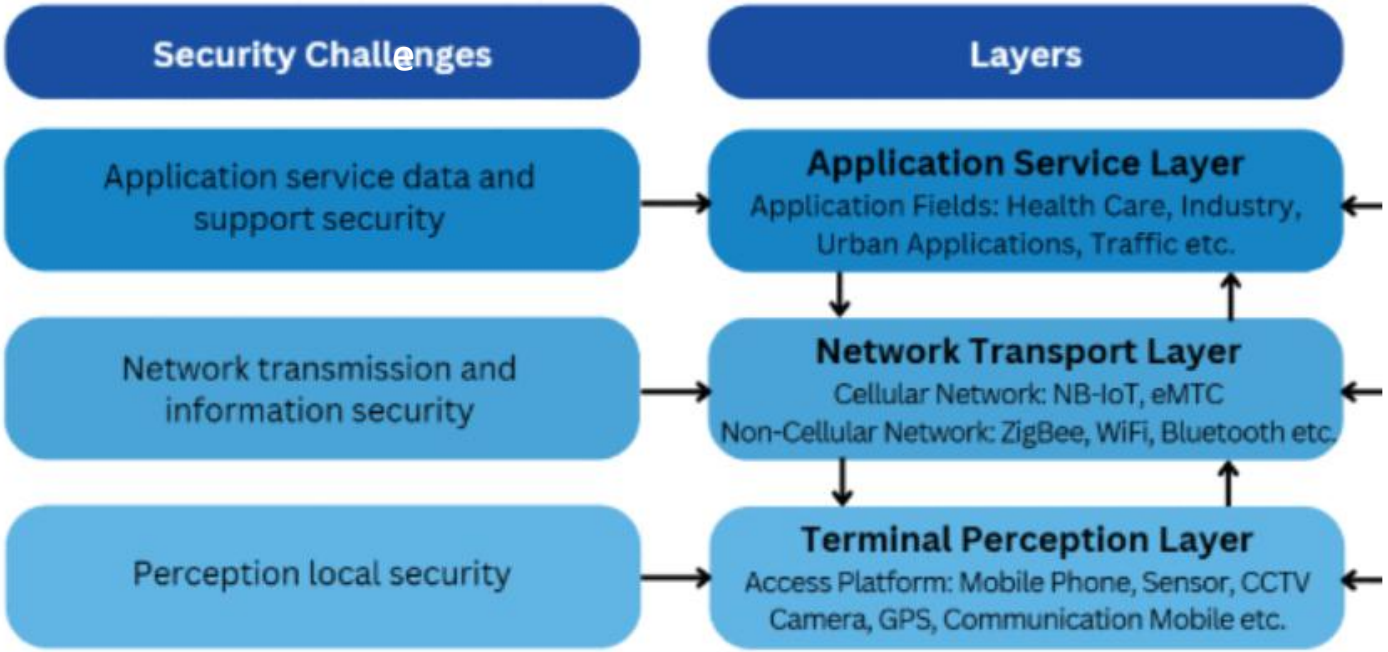
IOT EXAMPLE : CONNECTED AUTONOMOUS E-BIKE

CONNECTED AUTONOMOUS E-BIKE

CONNECTED AUTONOMOUS E-BIKE

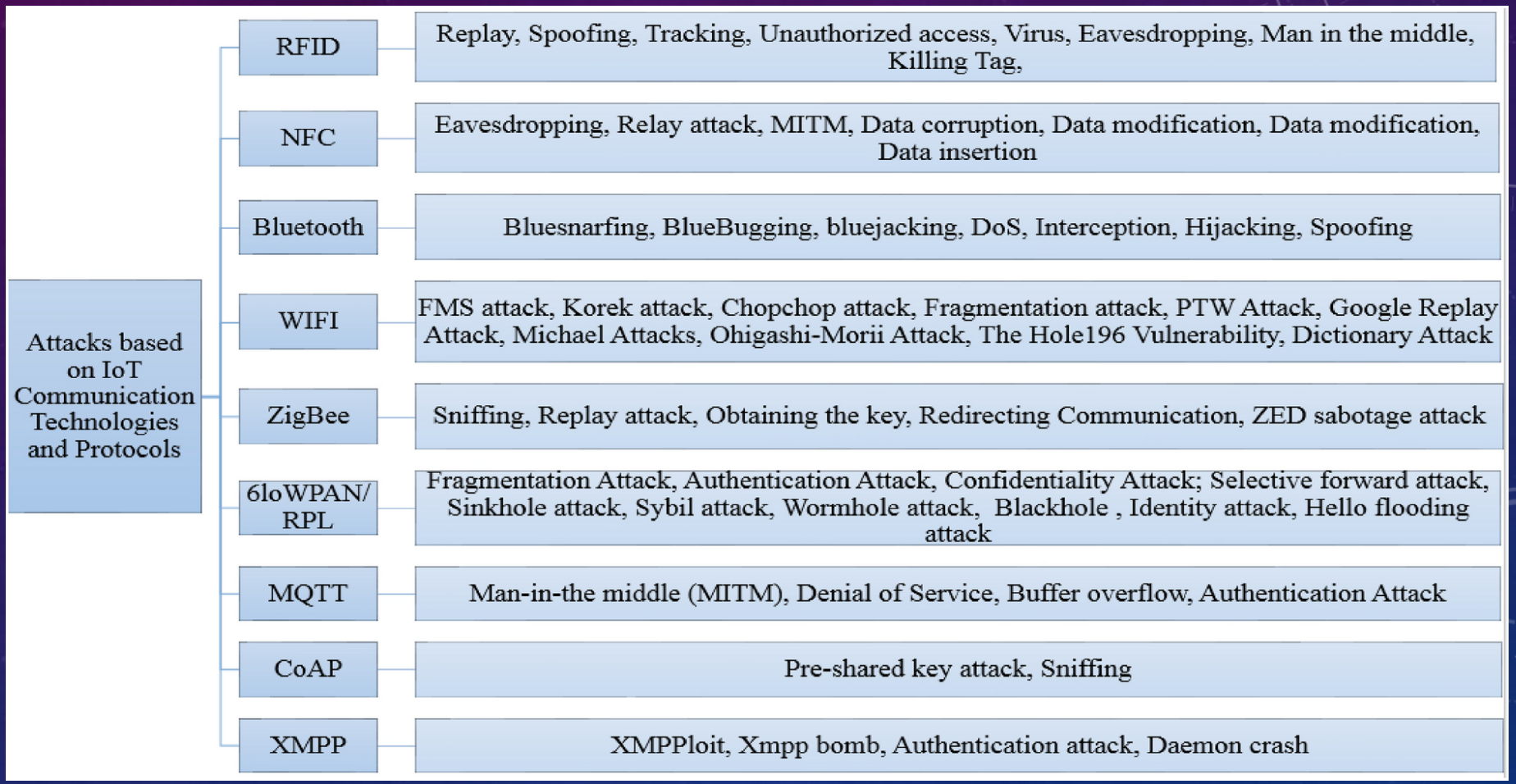


comprehensive representation of security challenges, layers, and associated attacks in IoT systems



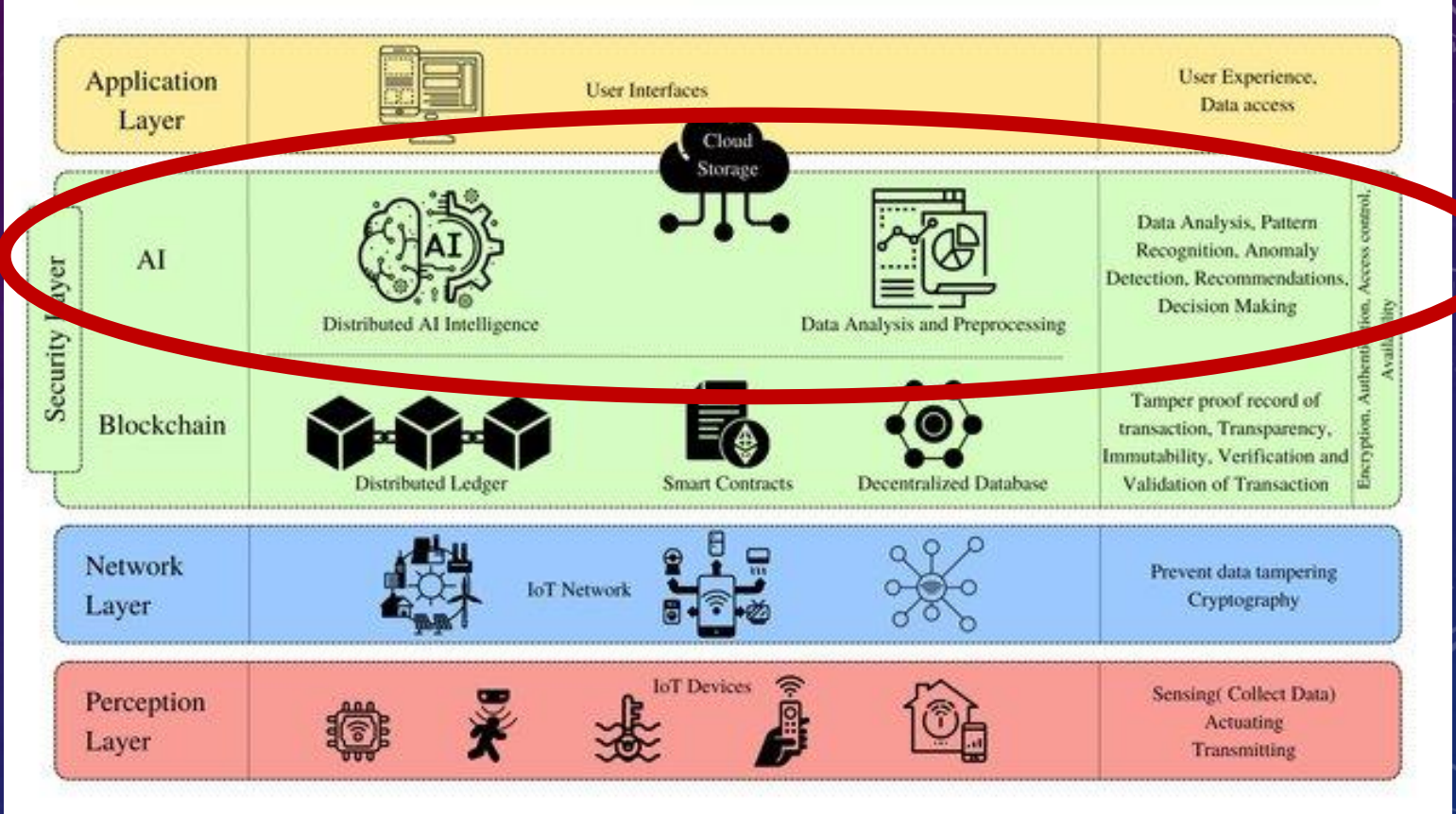
Sharma, Shashi Bhushan, and Amit Kumar Bairwa. "Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study." IEEE Access (2025).

Taxonomy of IoT Attacks

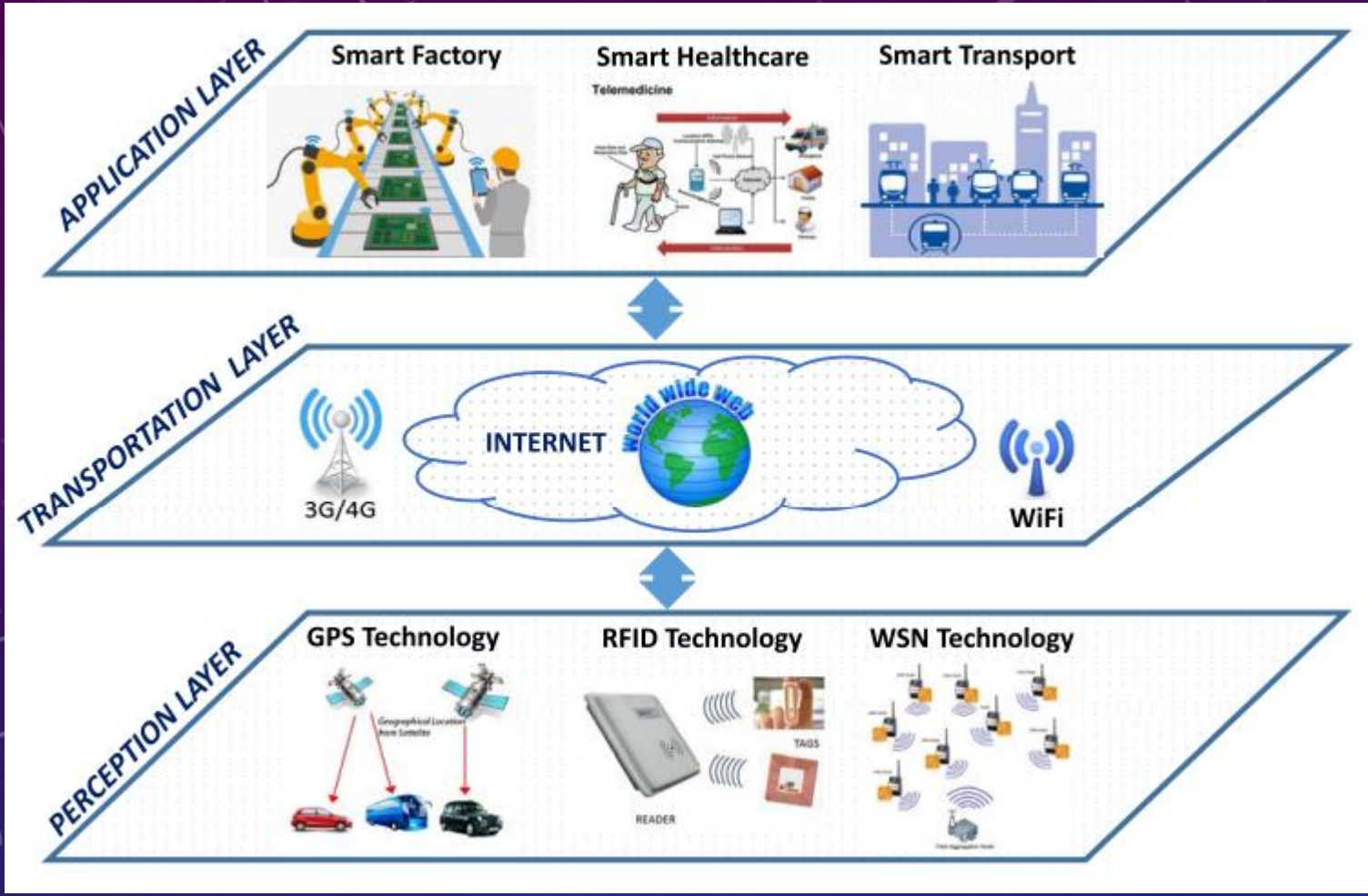


https://scifiniti.com/3104-4719/1/2024.0008

AI-driven security layer



Tauseef, Md, et al. "Exploring the joint potential of Blockchain and AI for securing Internet of things." International Journal of Advanced Computer Science and Applications 14.4 (2023).



cryptiot.de

AI'S ROLE IN IOT SECURITY

EXCERPTS FROM MEZIANE, H., OUERDI, N. A SURVEY ON PERFORMANCE EVALUATION OF ARTIFICIAL INTELLIGENCE ALGORITHMS FOR IMPROVING IOT SECURITY SYSTEMS. *SCI REP* **13**, 21255 (2023). HTTPS://DOI.ORG/10.1038/S41598-023-46640-9

DEEP LEARNING FOR THREAT DETECTION

- HIDS (Host Intrusion Detection System),
- NIDS (Network Intrusion Detection System),
- and anomaly detection

are common IoT security application fields where DL has been applied prominently.

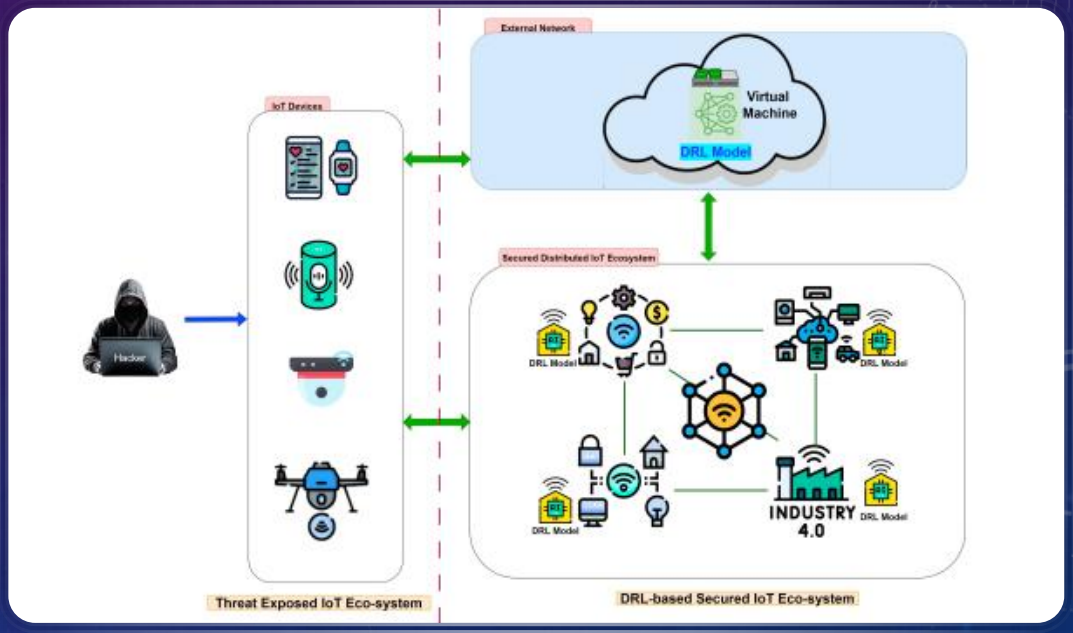
ANOMALY-BASED INTRUSION DETECTION MODEL USING DEEP LEARNING FOR IOT NETWORKS

Alsoufi, Muaadh A., et al. "Anomaly-based intrusion detection model using deep learning for IoT networks." Computer Modeling in Engineering & Sciences 141.1 (2024): 823-845.

- A novel anomaly-based intrusion detection system (AIDS) for IoT networks.
- Sparse Autoencoder (SAE) is applied to reduce the high dimension and get a significant data representation by calculating the reconstructed error.
- Convolutional Neural Network (CNN) technique is employed to create a binary classification approach.
- The proposed SAE-CNN approach is validated using the Bot-IoT dataset. The proposed models exceed the performance of the existing deep learning approach in the literature with an accuracy of 99.9%, precision of 99.9%, recall of 100%, F1 of 99.9%, False Positive Rate (FPR) of 0.0003, and True Positive Rate (TPR) of 0.9992.
- In addition, alternative metrics, such as training and testing durations, indicated that SAE-CNN performs better.

REINFORCEMENT LEARNING FOR ADAPTIVE DEFENSE

- RL-based agents continuously optimize firewall and routing policies based on threat evolution.
- For expl : Jagatheesaperumal, Senthil Kumar, et al. "Distributed reinforcement learning for iot security in heterogeneous and distributed networks." Computing&AI Connect 1.1 (2024): 1-10=.
- Advantage: Self-learning and decentralized adaptation.



FEDERATED LEARNING FOR PRIVACY-PRESERVING IOT SECURITY

- Enables collaborative model training across IoT devices without sharing raw data.
- Protects data sovereignty in healthcare, smart home, and industrial contexts.

- Awan, Kamran Ahmad, et al. "Privacy-preserving big data security for IoT with federated learning and cryptography." *IEEE Access* 11 (2023): 120918-120934.

> *"…when compared to current methods at the same noise level, the proposed method offers better privacy guarantees"*

COMPARISONS OF RELATED STATE-OF-THE-ART MODELS

Authors	Key Concept	Findings
Parisa Raoufi et. al [12]	Comprehensive review of deep learning applications in IoT, analyzing 56 articles from 2019 to April 2024.	Identified current challenges and potential breakthroughs at the intersection of deep learning and IoT, providing a roadmap for future research.
Pushpa R P et. al [67]	Development of an optimized deep learning framework for real-time intrusion and anomaly detection in IoT networks.	Achieved high accuracy (98.5%) and low latency (50 ms) in detecting anomalies, with a 40% reduction in energy consumption, enhancing security and efficiency in large-scale IoT deployments.
Mei Liu et. al [68]	Literature review and implementation of ensemble deep learning models for IoT network traffic anomaly detection.	Demonstrated over 98% accuracy in detecting anomalies using ensemble techniques, highlighting the effectiveness of deep learning in monitoring complex IoT networks.
Amrik Singh et. al [69]	Exploration of deep learning techniques for anomaly detection in IoT systems across various applications.	Discussed the integration of models like CNNs and LSTMs for real-time anomaly detection, emphasizing the need for adaptive learning techniques to enhance IoT security.
Nadia Ansar et. al [70]	Proposal of an intrusion detection system for IoT environments using a hybrid CNN-LSTM deep learning model.	Achieved 99.52% accuracy in classifying network traffic as benign or malicious, offering a robust solution for enhancing IoT network security.

https://ieeexplore.ieee.org/abstract/document/10921642

SECURITY CHALLENGES IN IOT ENVIRONMENTS

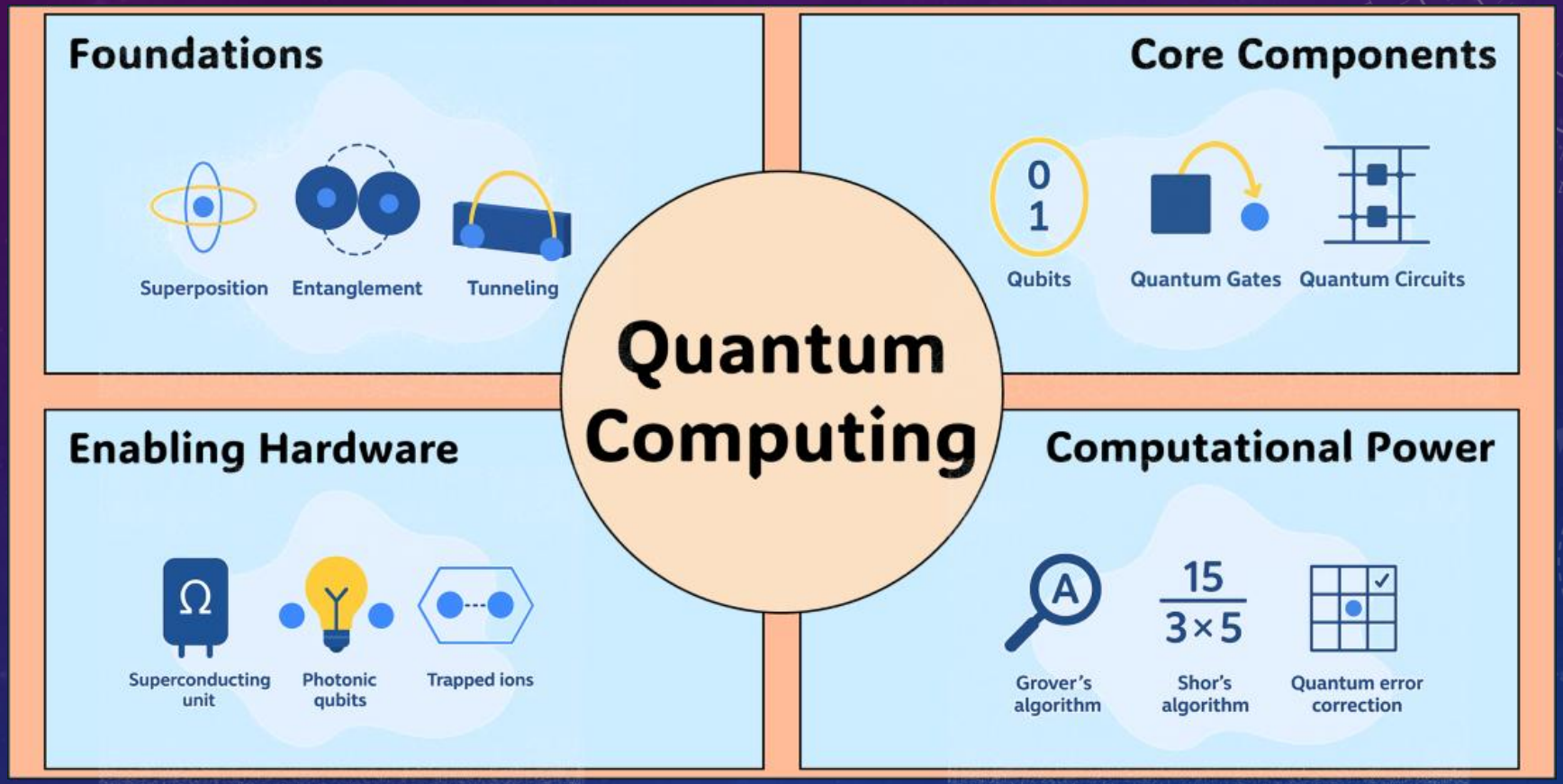
Characteristics	Description
Inadequate Authentication and Authorization	some IoT devices may need more robust authentication mechanisms due to resource constraints. Weak or non-existent authentication can lead to unauthorized access, data breaches, and the compromise of entire IoT networks [10].
Insufficient Encryption	Ensuring the confidentiality of data transmitted between IoT devices is challenging. Inadequate encryption can expose sensitive information to eavesdropping and interception, leading to privacy violations.
Lack of Standardization	The absence of standardized security protocols across IoT devices and platforms creates vulnerabilities. A lack of uniform security standards hampers interoperability and makes it challenging to implement consistent security measures [10].
Physical Vulnerabilities	Many IoT devices are deployed in physically accessible environments, making them susceptible to tampering and physical attacks. This is particularly relevant in industrial settings and critical infrastructure.
Limited Update Mechanisms	IoT devices often lack efficient mechanisms for software updates and patches. This limitation can result in devices running outdated, vulnerable software, making them attractive targets for exploitation [10].
Privacy Concerns	The extensive collection of personal and sensitive data by IoT devices raises privacy concerns. Unauthorized access to this data can lead to identity theft, stalking, or other privacy breaches.
Denial-of-Service (DoS) Attacks	The massive scale of IoT networks makes them susceptible to DoS attacks, where attackers flood the network with traffic, rendering it inaccessible. Such attacks can disrupt critical services and compromise the functionality of IoT devices [10].

https://ieeexplore.ieee.org/abstract/document/10921642

iotforall.com

PART 2 – QUANTUM COMPUTING AND IOT SECURITY IN THE QUANTUM ERA

OVERVIEW OF QC



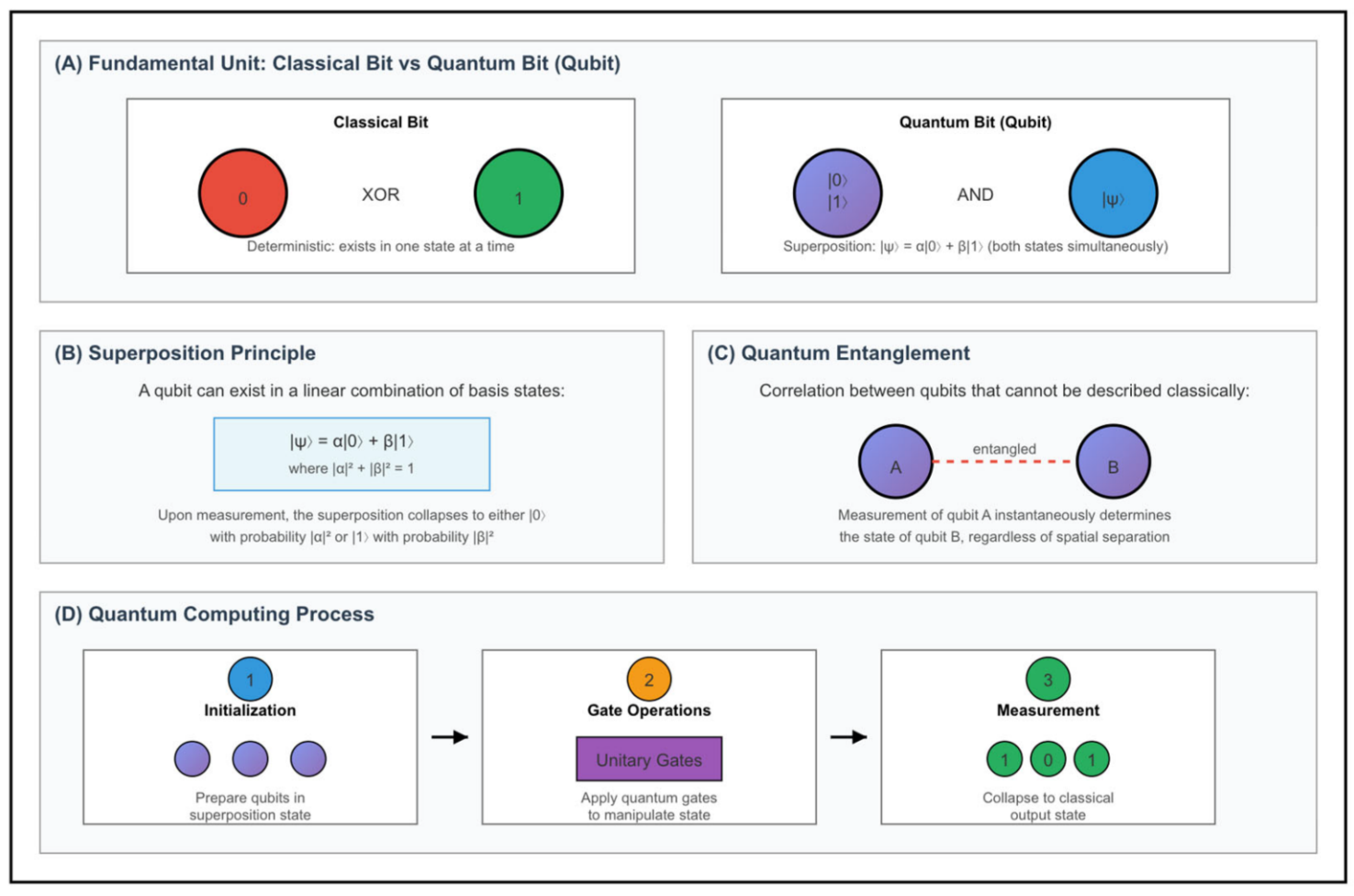
Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173. https://doi.org/10.3390/encyclopedia5040173

QC PLATFORMS AND SDKS: STRENGTHS, LIMITATIONS, AND MATURITY

Category	Platform	Type	Connectivity	Strengths	Limitations	Maturity
Hardware	Google Willow [4]	Superconducting (transmon)	Planar grid and nearest-neighbor	Fast gates; advanced calibration & benchmarking pipelines	Cryogenics; crosstalk; fidelity scaling	Research & Noisy intermediate-scale quantum computing (NISQ)-class flagship devices
Hardware	IBM Quantum [5]	Superconducting (transmon)	Coupling-map topologies (planar)	Cloud access; strong toolchain	Coherence & connectivity constraints typical of superconductors	Broad device family; leading NISQ access
Hardware	IonQ [6]	Trapped ions (hyperfine/optical)	All-to-all within a single chain	Long coherence; high single/two-qubit fidelities	Slower gates; scaling across chains needs photonic links	Commercial cloud systems; strong small to medium-circuit performance
Software	Qiskit [7]	SDK (Python)	IBM devices; providers for others; simulators	Rich transpiler; visualization; pulse-level access	IBM-centric by default	Actively maintained; wide community use
Software	Cirq [8]	SDK (Python)	Google devices and compatible simulators	Native abstractions; noise models; calibration workflows	Google-centric	Research & production tooling within Google ecosystem
Software	Microsoft QDK [9]	SDK (Q#, Python & C# interop)	Azure Quantum ecosystem; simulators; resource estimation	High-level Q# language; resource estimation; heterogeneous backend routing	Heavier tooling stack; best within Azure flow	Active tooling; growing backend support

Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173. https://doi.org/10.3390/encyclopedia5040173

QC FUNDAMENTAL PRINCIPLES



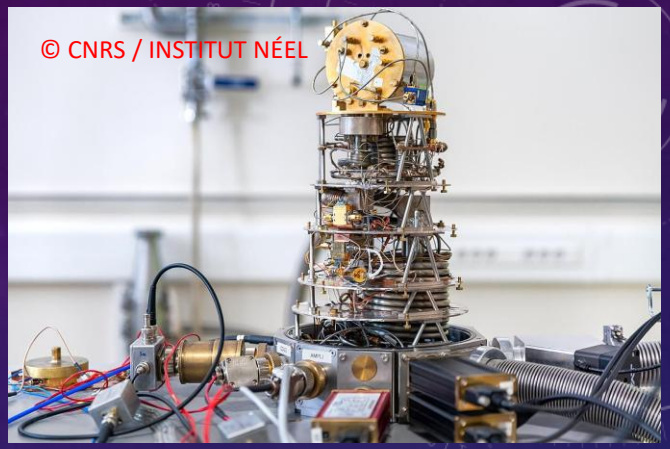
Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173. https://doi.org/10.3390/encyclopedia5040173

FUNDAMENTAL DIFFERENCES BETWEEN CLASSICAL AND QC FOR INFORMATION PROCESSING

Feature	Classical Computing	Quantum Computing
Basic Unit	Bit (0 or 1)	Qubit (a coherent quantum state in superposition of basis states)
Key Phenomena	Binary Logic	Quantum gates
Processing	Sequential/Parallel	Quantum parallelism with interference-based amplitude manipulation
Example Task	Password cracking	Grover's algorithm; Shor's algorithm for factoring (breaking RSA (i.e., Rivest-Shamir-Adleman) encryption)
Limitations	Limited by Moore's Law	Sensitive to decoherence

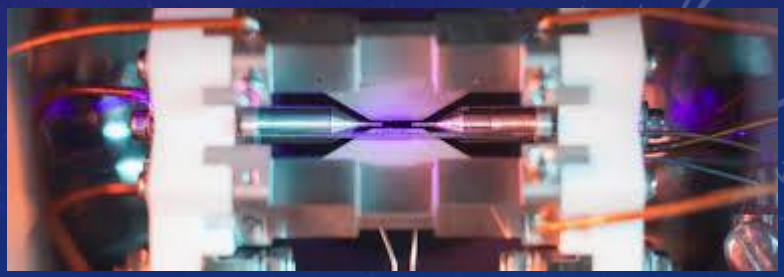
Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173. https://doi.org/10.3390/encyclopedia5040173

QC HARDWARE



- Superconducting circuits, which use supercooled electrical loops controlled by microwave pulses,

- Trapped ions: which use lasers to manipulate atoms suspended in electromagnetic fields.



Ion trap quantum computing | University of Oxford

Maintaining coherence and mitigating decoherence are primary challenges, motivating diverse physical implementations of qubits.

Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173

QC ALGOS

- **Shor’s Algorithm**

Developed by Peter Shor in 1994, Shor’s Algorithm is a quantum algorithm designed to efficiently factor large integers, a computationally infeasible task for classical computers. The security of widely used cryptographic systems like RSA relies on the difficulty of factoring large numbers.

- **Grover’s Algorithm**

Proposed by Lov Grover in 1996, Grover’s Algorithm enhances search capabilities in unsorted databases. It provides a quadratic speedup over classical search algorithms, allowing a quantum computer to find a specific item in a dataset in roughly the square root of the time required by a classical search.

KEY AREAS OF QUANTUM COMPUTING'S IMPACT

Area of Impact	Description	Potential Benefits	Challenges & Concerns
Cybersecurity & Post-Quantum Cryptography	Quantum computing threatens traditional encryption; PQC aims to resist quantum attacks using hard mathematical problems (e.g., lattice cryptography).	More secure systems in a post-quantum world.	Existing infrastructure is vulnerable; risk of cyberwarfare.
Information Retrieval	Quantum-enhanced algorithms (like Grover's) allow faster and more relevant data search and retrieval.	Rapid, precise access to information; supports complex queries.	May reduce role of libraries; risks of bias or over-reliance on "perfect" results.
Automation	Quantum optimization can drastically improve machine learning, logistics, and robotics.	Higher efficiency, fewer errors, optimized decision-making.	High costs, energy demands, risk of job displacement.
Knowledge-Based Industries	Quantum-AI systems could perform summarization, indexing, and analysis roles.	Frees humans to focus on ethics, strategy, and creativity.	Disruption of traditional professional roles.
Future of Work	Quantum computing boosts AI productivity across sectors.	Job creation in quantum tech; increased efficiency.	Threats to repetitive and cognitive jobs in both blue- and white-collar sectors.
Human Cognition & Society	Potential impact on mental engagement, purpose, and autonomy.	May liberate humans from routine tasks.	Risks of dependence, alienation, erosion of critical thinking.

Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173. https://doi.org/10.3390/encyclopedia5040173

THE QUANTUM THREAT TO CLASSICAL CRYPTOGRAPHY

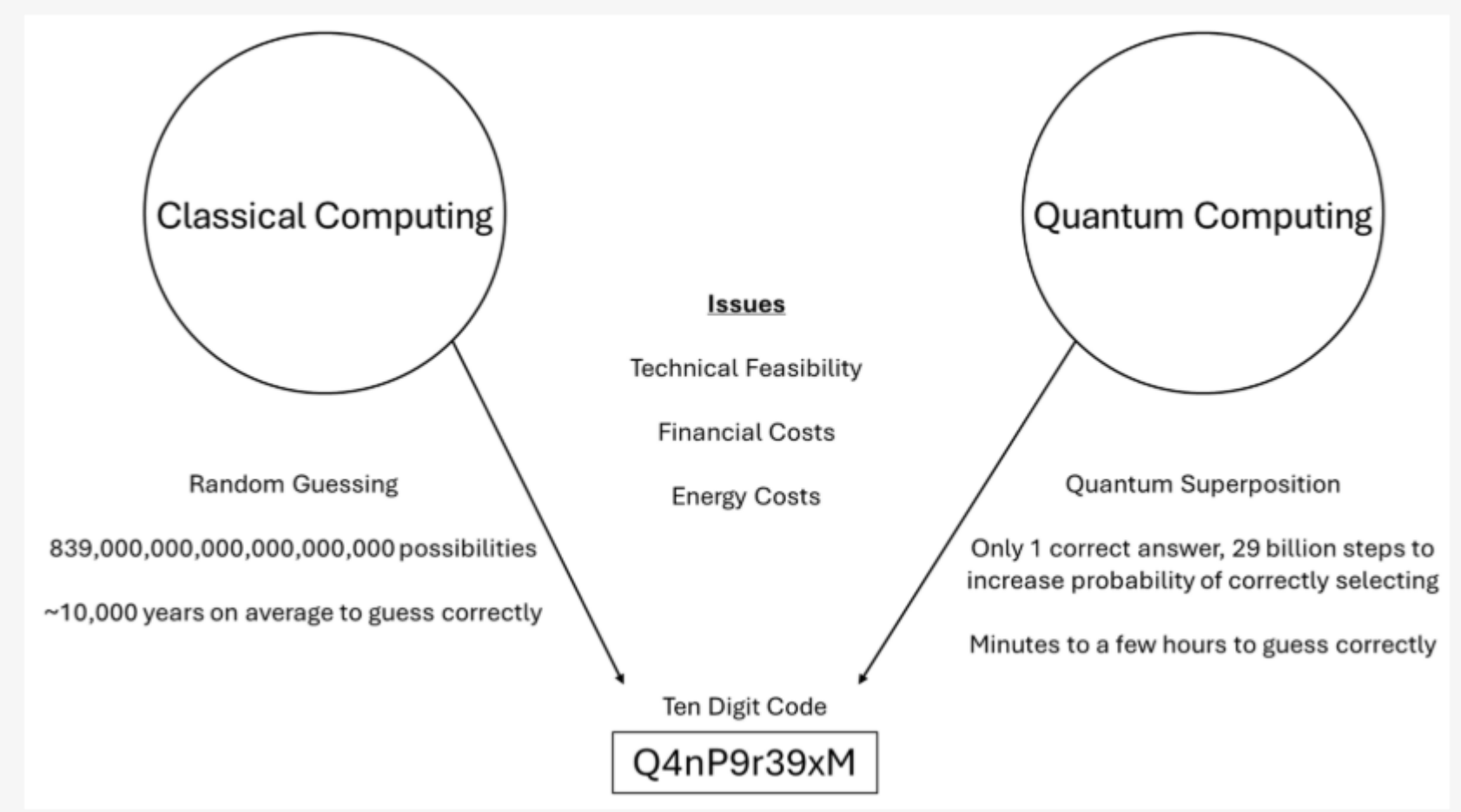
- Quantum computing represents a fundamental shift in computational paradigms, leveraging superposition and entanglement to process information exponentially faster than classical systems.

- Algorithms such as **Shor's algorithm** can factor large integers in polynomial time—rendering traditional cryptographic schemes like **RSA** and **ECC** insecure.

THE QUANTUM THREAT TO CLASSICAL CRYPTOGRAPHY

- With a classical computer, in order to try to crack a ten-character code, you would have to enter one combination at a time. If a code has
- 10 alphanumeric characters: 26 uppercase letters, 26 lowercase letters, and 10 numbers and ten characters in the password. There are 62^{10} potential combinations. This means there are 839 quintillion combinations of possibilities. Even an incredibly fast modern supercomputer, able to try 1 billion combinations per second, would take over 10,000 years on average to guess the right combination.
- Grover's algorithm provides a quadratic speedup for unstructured search problems by exploiting uniquely quantum phenomena such as superposition, phase inversion, and amplitude amplification through interference.
- This allows it to reduce the number of steps needed from 839 quintillion to about 29 billion, because Grover's algorithm provides a quadratic speedup, solving the problem in a number of steps roughly equal to the *square root* of 839 quintillion => 29 billion

THE QUANTUM THREAT TO CLASSICAL CRYPTOGRAPHY



Lund, B.D.; Shahriar, S. Quantum Computing: A Concise Introduction. Encyclopedia 2025, 5, 173. https://doi.org/10.3390/encyclopedia5040173

THE QUANTUM THREAT TO CLASSICAL CRYPTOGRAPHY

- Another QC algor that poses a major threat => Shor's algorithm.
- In modern encryption—such as RSA, which protects communications between systems—a key aspect to ensuring a message cannot be broken is ?
- The mathematical difficulty of factoring a very large number into its two original prime factors.
- The product of these two numbers—the modulus—is publicly known, but the identity of the two prime numbers is not.
- In RSA encryption, the number to be factored is hundreds of digits in length, and the correct pair of large prime numbers is incredibly difficult to identify using a classical computer, likely taking billions of years.
- However, Shor's algorithm, operating on a quantum computer, has the ability to factor these large numbers exponentially faster.
- Instead of checking the possibilities one by one, the algorithm uses quantum parallelism to find the factors within a few hours, which poses a significant threat to the security of RSA and similar encryption approaches.

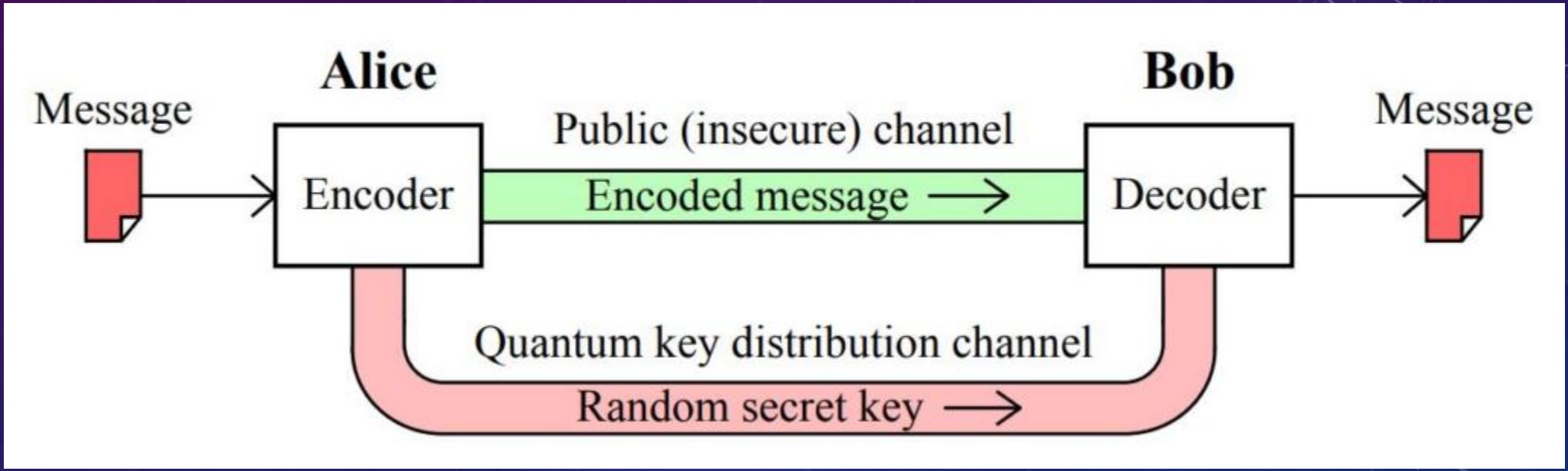
POST-QUANTUM CRYPTOGRAPHY (PQC): THE CLASSICAL DEFENSE

- Post-Quantum Cryptography (PQC) aims to develop **quantum-resistant algorithms** based on hard mathematical problems not efficiently solvable by quantum computers.
- Key algorithmic families include:
- **Lattice-based cryptography** (e.g., CRYSTALS-Kyber, Dilithium)
- **Hash-based cryptography** (e.g., SPHINCS+)
- **Code-based cryptography** (e.g., Classic McEliece)
- **Multivariate polynomial cryptography**

QUANTUM KEY DISTRIBUTION (QKD): PHYSICS-BASED SECURITY

- While PQC relies on computational hardness, **Quantum Key Distribution (QKD)** derives its security from **quantum physics**—specifically, the no-cloning theorem and measurement disturbance principle.
- Protocols such as **BB84** and **E91** use photon polarization to exchange secret keys, guaranteeing detection of any eavesdropping attempt.
  QKD networks are already operational in China's *Beijing–Shanghai backbone* and the *EU's Quantum Flagship program*.
- However, QKD's **hardware dependency and cost** limit immediate large-scale IoT deployment.

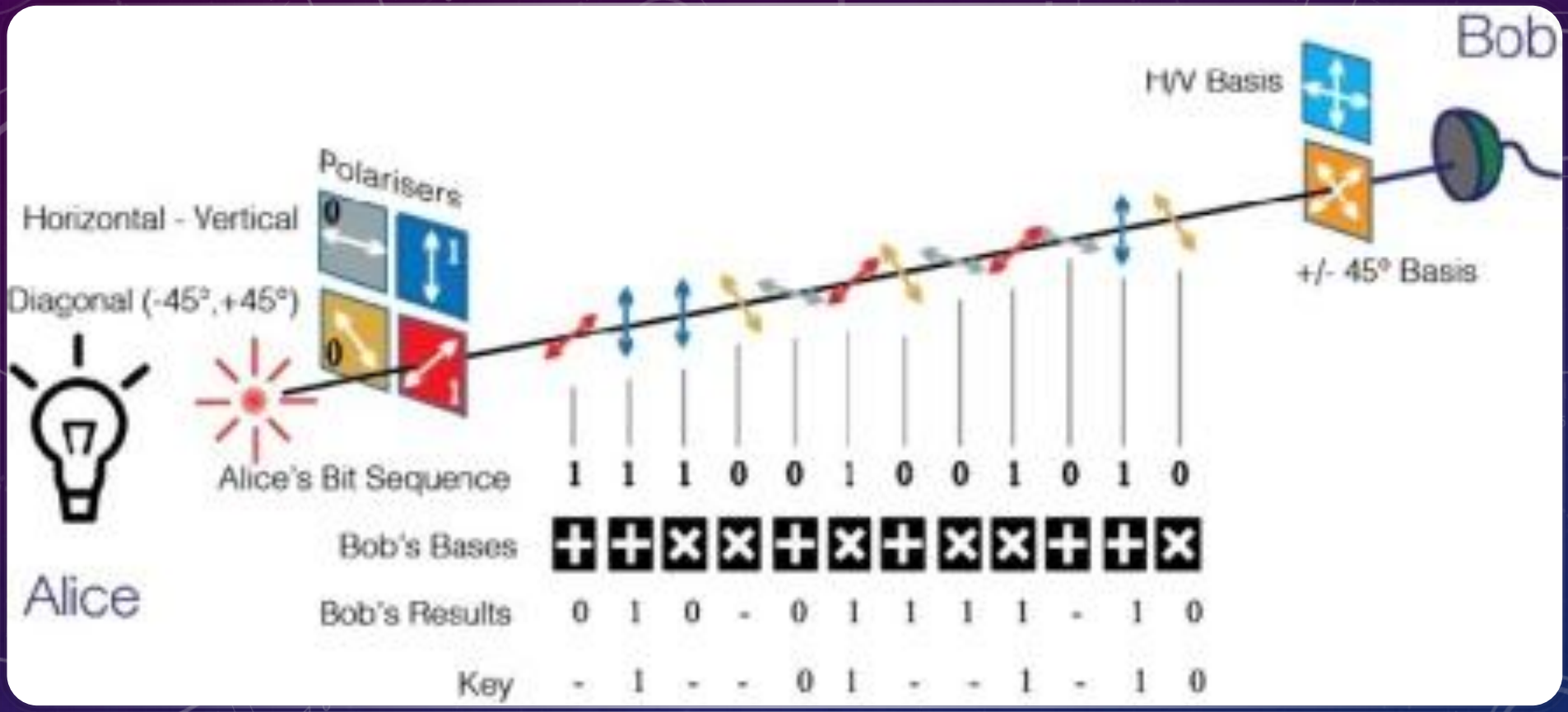
QUANTUM KEY DISTRIBUTION (QKD): PHYSICS-BASED SECURITY



qmunity.thequantuminsider.com/

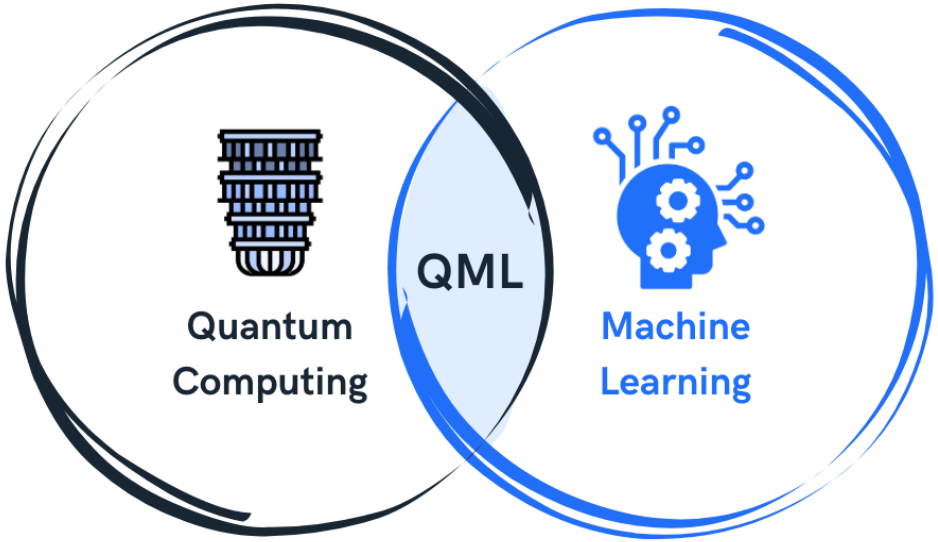
QUANTUM KEY DISTRIBUTION (QKD): PHYSICS-BASED SECURITY

- While PQC relies on computational hardness, **Quantum Key Distribution (QKD)** derives its security from **quantum physics**—specifically, the no-cloning theorem and measurement disturbance principle.
- Protocols such as **BB84** and **E91** use photon polarization to exchange secret keys, guaranteeing detection of any eavesdropping attempt.
  QKD networks are already operational in China's *Beijing–Shanghai backbone* and the *EU's Quantum Flagship program*.
- However, QKD's **hardware dependency and cost** limit immediate large-scale IoT deployment.



https://qt.eu/

QUANTUM KEY DISTRIBUTION (QKD): PHYSICS-BASED SECURITY



https://www.ingenii.io/

PART 3 – THE QUANTUM-AI NEXUS: QUANTUM MACHINE LEARNING (QML) FOR IOT SECURITY

Aparcana-Tasayco, Andres J., Xianjun Deng, and Jong Hyuk Park. "A systematic review of anomaly detection in IoT security: towards quantum machine learning approach." *EPJ Quantum Technology* 12.1 (2025): 1-39.

QUANTUM COMPUTING FOR ANOMALY DETECTION

- While classical ML methods like Random Forests, CNNs, and LSTMs remain effective for IoT intrusion detection, their scalability is challenged by the growing data volume, latency constraints, and dynamic threat patterns.

- Quantum Machine Learning (QML) leverages superposition and entanglement to explore multiple feature representations in parallel, offering exponential speed-ups in learning and anomaly classification.

QUANTUM COMPUTING FOR ANOMALY DETECTION

Recent surveys classify QML-based intrusion detection across **five dimensions**:

1. **Data Encoding** – Amplitude, angle, or hybrid embeddings.
2. **Model Architecture** – QSVM, QAE, VQC, QNN.
3. **Resource Utilization** – Low-qubit (NISQ) vs. large simulated circuits.
4. **Error Mitigation** – None, basic, or advanced quantum error correction.
5. **Deployment Strategy** – Simulation-only, NISQ hardware, or hybrid cloud–edge systems.

This taxonomy now serves as a **roadmap for practical QML deployment in edge-constrained IoT environments.**

STATE-OF-THE-ART QML APPROACHES

(1) Hybrid QSVM–IGWO IDS (Elsedimy EI, Elhadidy H, Abohashish SMM. A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. Clust Comput. 2024;27:9917–35**)**

- Combines **Quantum SVM** with **Improved Grey Wolf Optimizer (IGWO)** for high-performance intrusion detection.
- Uses feature selection (Information Gain) and BoT-IoT dataset.
- Outperforms classical KNN, RF, and LR baselines.

Limitation: lacks noise handling and real quantum hardware validation.

STATE-OF-THE-ART QML APPROACHES

(2) QAE–QkNN Quantum Deep Learning (. Hdaib M, Rajasegarar S, Pan L. Quantum deep learning-based anomaly detection for enhanced network security. Quantum Mach Intell. 2024;6:26.

- Integrates **Quantum Autoencoder (QAE)** with **Quantum kNN**, **QRF**, and **One-Class QSVM** for unsupervised anomaly detection.
- Tested on **KDD99, IoT-23, CIC IoT-23** datasets using **PennyLane** and **IBM Qiskit**.
- **Performance:** F1-score = **98.26%**; high precision and recall across attack classes.
- **Limitation:** limited scalability due to fidelity loss as circuit depth increases.

Conclusion: QML-based IDSs demonstrate *superior accuracy, faster convergence,* and *lower power consumption* compared to classical methods, though scalability and noise remain major constraints.

STATE-OF-THE-ART QML APPROACHES

Elsedimy et al. (2024) [136]	BoT-IoT	QSVM + IGWO	99.11	99.45	99.34	97.48	Not reported, Simulated (classical)	High accuracy; no noise/error mitigation; not executed on quantum hardware
Hdaib et al. (2024) [8]	KDD99, IoT-23, CIC IoT-23	QAE + QkNN	97.79	98.37	98.81	98.26	~120 ms per sample (IBM Q simulator),	Strong results on multiple datasets; limited scalability due to qubit constraints

OPEN CHALLENGES IN QML-BASED IOT SECURITY

Limited Generalization and Dataset Diversity

- Most QML studies rely on outdated datasets (KDDCup99, UNSW-NB15), lacking representation of *real-world, zero-day IoT attacks*.
  Future work must emphasize diverse, modern datasets reflecting 5G/6G-enabled IoT infrastructures.

Data and Concept Drift

- IoT environments evolve rapidly, causing **data distribution shifts** that degrade static model performance.
  Incorporate **continual and online learning** within QML frameworks to enable self-evolving anomaly detectors.

Scalability and Real-Time Constraints

- High circuit complexity, limited qubits, and energy budgets hinder large-scale QML deployment.
  Research into **TinyQML**, **quantum model compression**, and **edge–cloud hybridization** is critical.

Privacy and Federated Learning Security

- While federated learning (FL) protects data locality, it remains vulnerable to **poisoning and inversion attacks**.
  Integrate **quantum-secure aggregation** and **differential privacy-aware FL** to balance confidentiality and accuracy.

OPEN CHALLENGES IN QML-BASED IOT SECURITY

5G/6G-Enabled IoT Environments

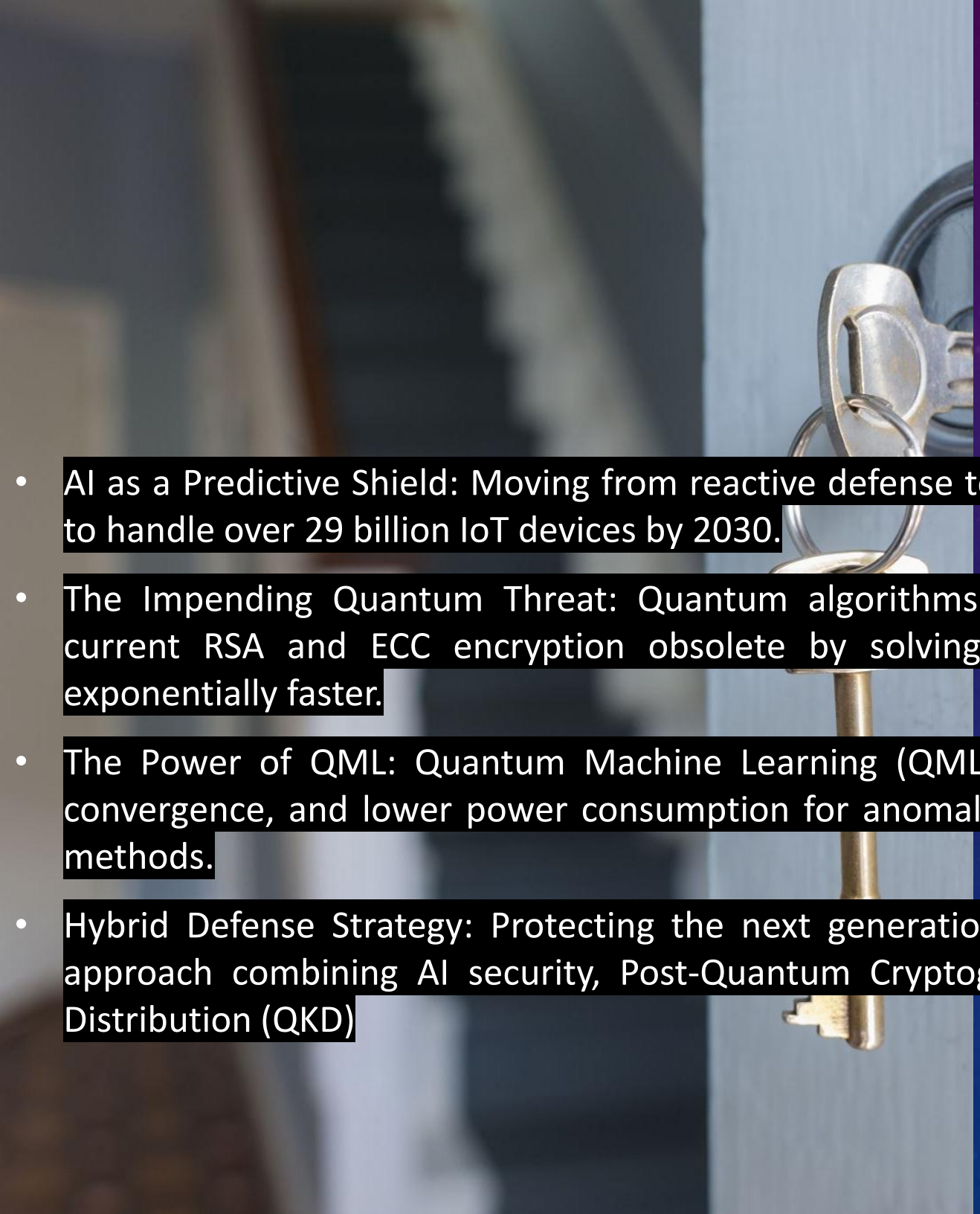
- Ultra-fast networks expand the attack surface.
  Develop **5G-aware QML** architectures capable of handling ultra-low latency data streams securely.

Lightweight and Multi-Class Models

- Most IDS models are binary and resource-heavy.
  Explore **quantum neural architecture search (Q-NAS)** and **quantum-pruned networks** for multi-class detection on edge devices.

Quantum Challenges in Critical Systems

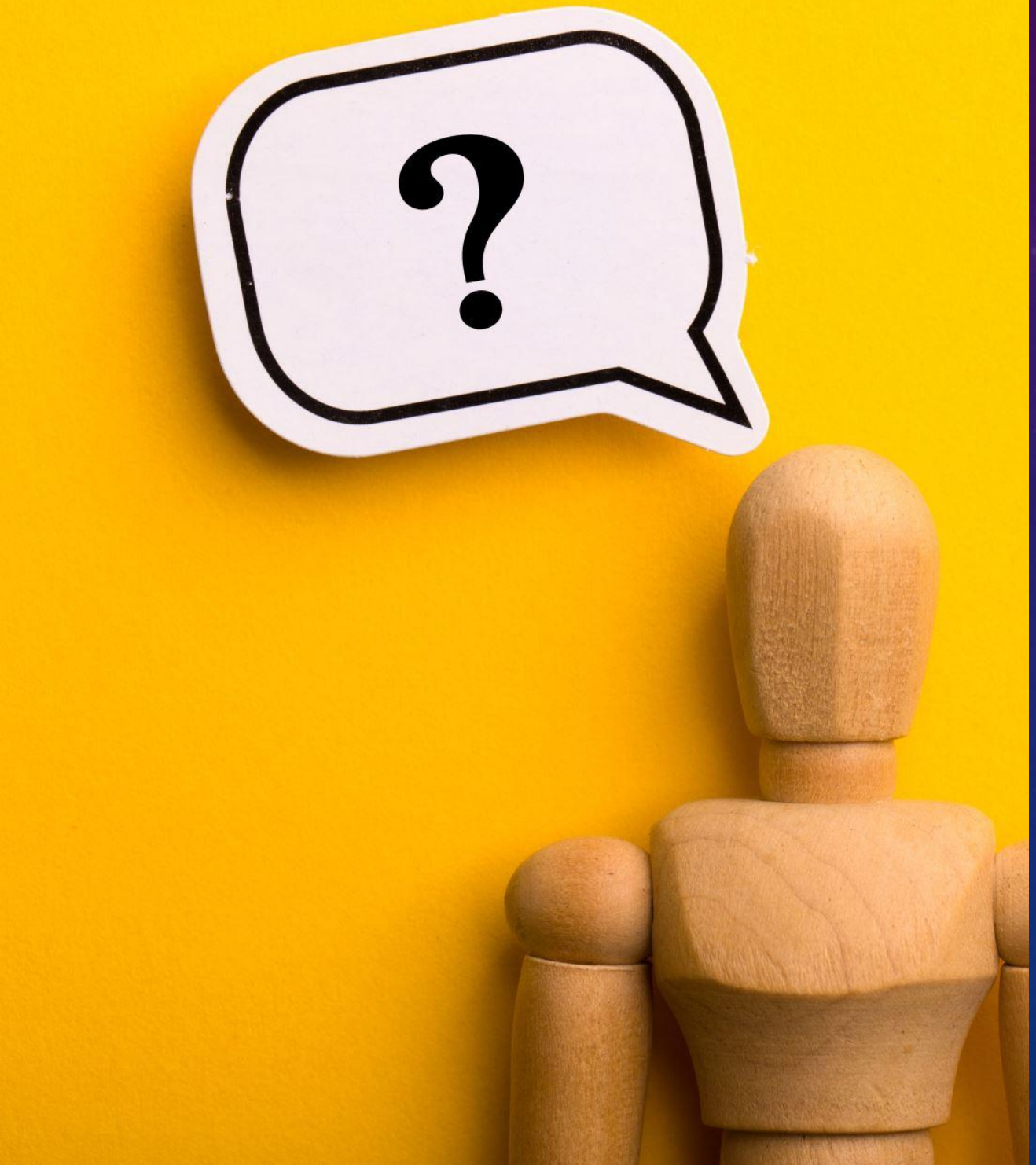
- Quantum hardware faces **noise, qubit decoherence, and interpretability issues**, limiting deployment in mission-critical contexts.
  Progress depends on **hybrid architectures**, **quantum feature engineering**, and **explainable QML**.



KEY TAKEAWAYS & SUMMARY

- AI as a Predictive Shield: Moving from reactive defense to predictive autonomy is essential to handle over 29 billion IoT devices by 2030.
- The Impending Quantum Threat: Quantum algorithms like Shor's and Grover's render current RSA and ECC encryption obsolete by solving factoring and search problems exponentially faster.
- The Power of QML: Quantum Machine Learning (QML) offers superior accuracy, faster convergence, and lower power consumption for anomaly detection compared to classical methods.
- Hybrid Defense Strategy: Protecting the next generation of IoT requires a multi-layered approach combining AI security, Post-Quantum Cryptography (PQC), and Quantum Key Distribution (QKD)

THANK YOU FOR YOUR ATTENTION



hsoubra@ece.fr