THNIC bknix | 31-05-24

CYBLION.io

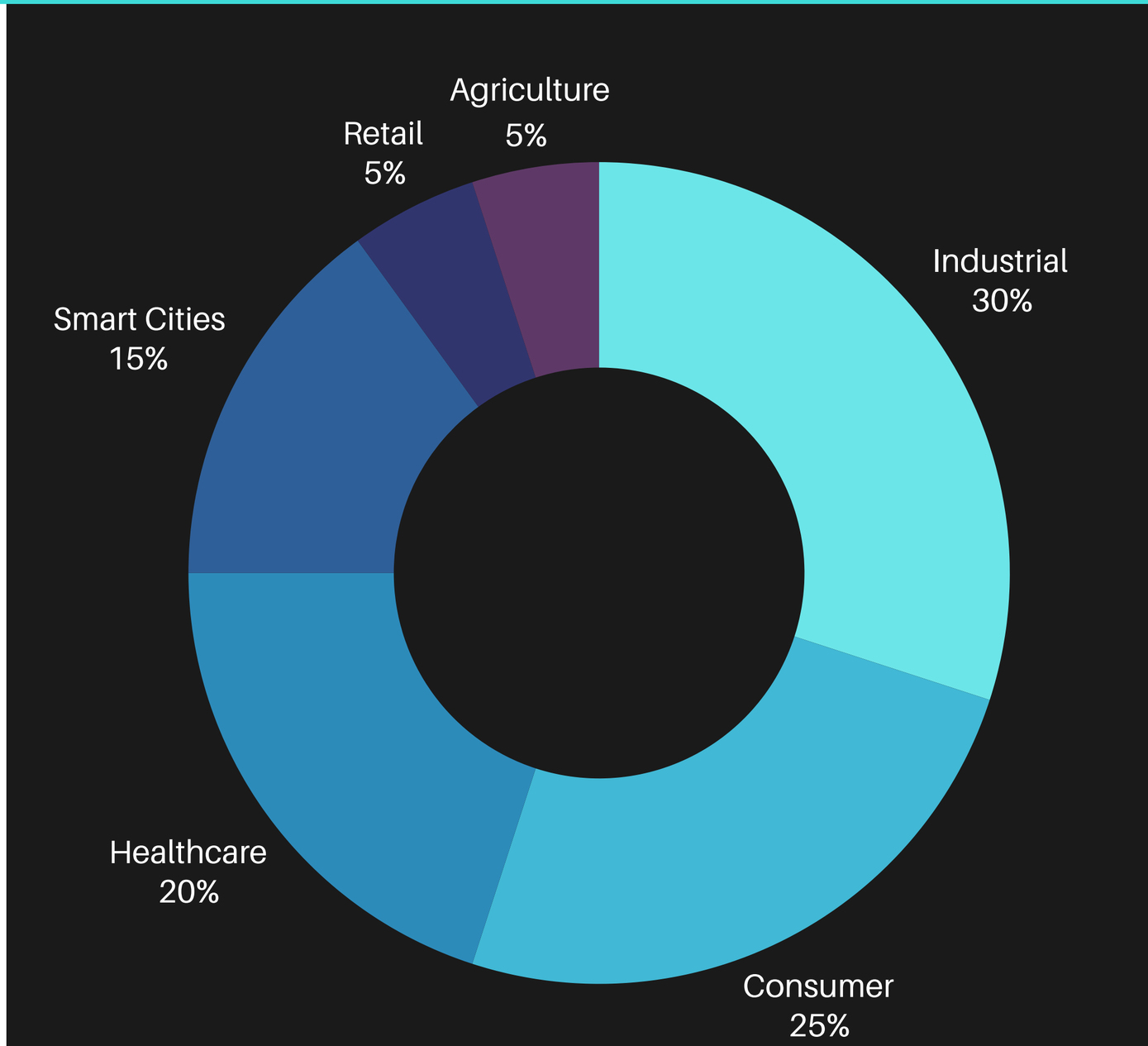
Privacy as a Service for IoT

DR. KALIKA SUKSOMBOON
SENIOR RESEARCHER, NECTEC

STATISTICS AND FACTS IN 2023

30%

of IoT usage is dedicated to industrial applications



Reference: Comparitech

IOT IS A KEY DRIVER IN MANUFACTURING

- Enhanced Operational Efficiency
- Improved Decision-Making
- Safety and Compliance
- Cost Reduction
- Competitive Advantage

Empower with IoT Cloud Platform

Key Benefits of IoT Cloud Platforms

- Using an IoT cloud platform empowers businesses by providing scalability, real-time insights, cost efficiency, enhanced security, and improved collaboration.
- It enables rapid innovation and seamless integration with existing systems, driving operational excellence and competitive advantage.

AWS leads with a 30-35% market share

Microsoft Azure holds about 25-30% of the market

Google Cloud IoT has a 15-20% market share

TRADITIONAL CLOUD PLATFORM

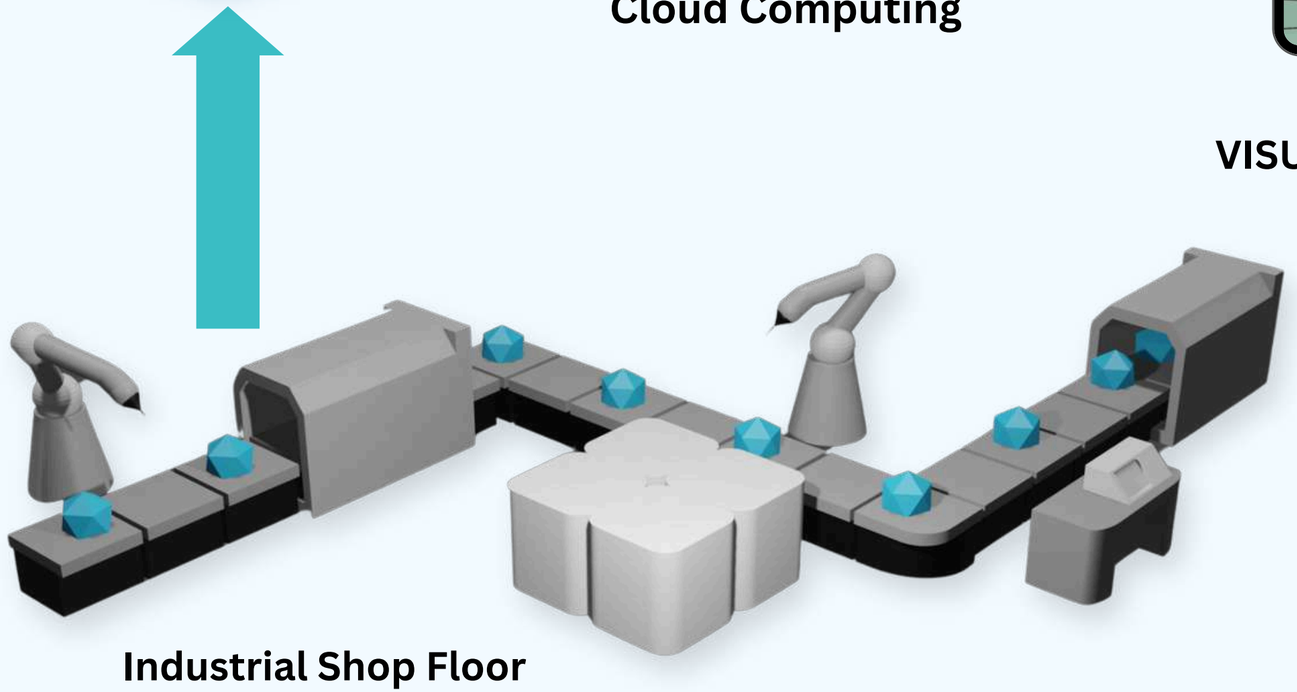
Edge Device

TLS

Cloud Computing

TLS

DATA VISUALIZATION



Industrial Shop Floor

Cybersecurity protection over the cloud and Internet

Offload data computation and data distribution by cloud computing

WHAT'S WRONG?

- Need a trust of the third party such as a Cloud Service Provider
- Not guarantee the cloud will not be attacked (i.e., Ransomeware, Data breach, ect.)
- The cloud can see your data while it is processing your data and distributing your data.

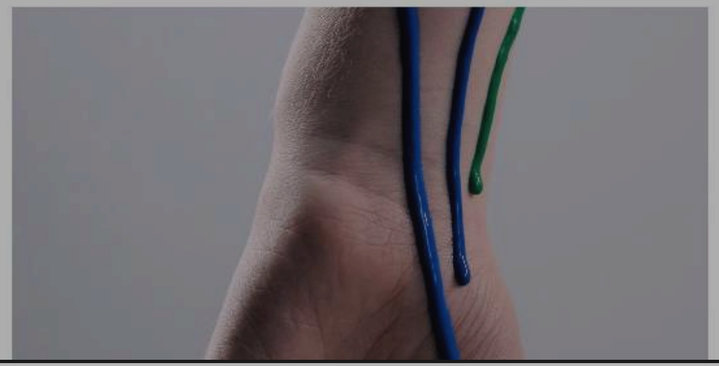
Cloud Data Breach

Microsoft data breach "BlueBleed" exposes 2.4TB of customer data

Customers being told GDPR disclosure unnecessary

ELIOT BEER

October 20, 2022 . 11:21 AM — 4 min read



A misconfigured Microsoft endpoint (an Azure storage bucket) exposed 2.4TB of Microsoft customer information, including emails and signed documents, the company has admitted. Strikingly the company's support staff appear to be telling customers that Microsoft has no GDPR obligations to report it to regulators.

Personal Data And Order Histories Of Amazon Japan Exposed - September 2019

Amazon Japan users encountered a strange thing in September 2019 when the order histories of other shoppers were viewable to them.

SHOULD WE CONCERN?

“ A recent cloud data leak made the factory owners rethink whether the move to Industry 4.0 might just be a trap. ”

“ How can we protect industrial individual data privacy while letting factories enjoy IoT benefits? ”

PRIVACY AS A SERVICE

1

SECURITY SERVICE

- Legacy privacy definition, called **"Privacy Tech 1.0"**
- Use security technologies to protect data leakage from untrusted or unauthorized parties.

PRIVACY AS A SERVICE

2

Privacy by Policy

- Privacy-by-policy is used to enforce compliance and accountability of privacy protection.
- To make privacy protection is a necessity for all service providers, I.e., GDPR, PDPA, HIPAA

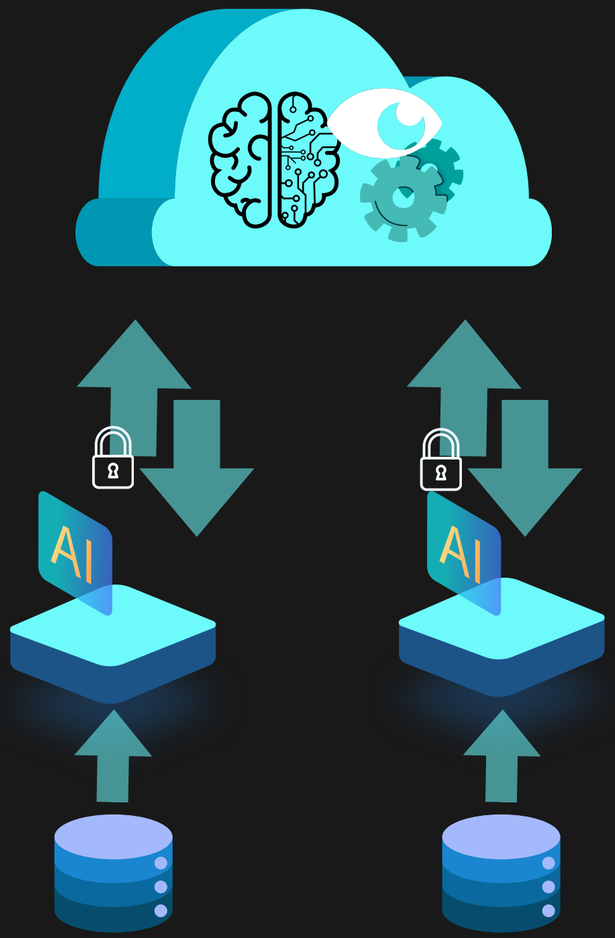
PRIVACY AS A SERVICE

3

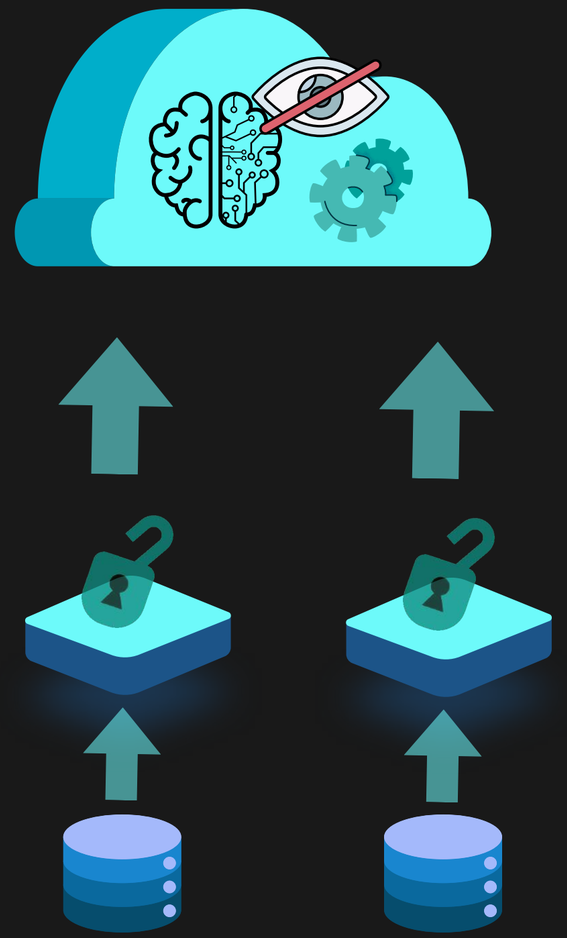
Privacy Enhancing Technologies (PETs)

- Enable privacy protection strategies to be implemented in engineering
- Use technologies such as
  - k-anonymous,
  - data marking,
  - TEE
  - SMPC,
  - ZKP,
  - differential privacy,
  - Federated Learning,
  - **Homomorphic Encryption (HE)**

Federated Learning



Homomorphic Encryption



PET as a Service Platforms

Using Homomorphic Encryption to Enhance Private Computing Services

EN|VIEL

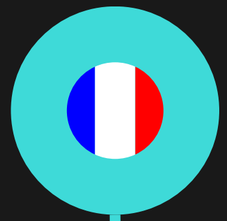
HE for financial and Healthcare has raised $4.1 million in funding

TRIPLEBLIND

Federated computing, HE and SMPC provide API for data scientists

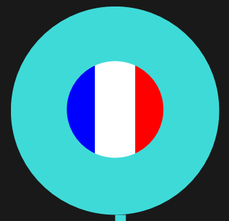
INPHER

XOR with MPC and secret computing with TFHE



ZAMA

TFHE for ML and enable Web2 and Web3



RAVEL

Ravel Homomorphic Encryption Provide Encrypted Financial Exchanges, GDPR, Large Scale Confidential Data Sharing & Analytics

HOMOMORPHIC ENCRYPTION

01 PHE

PHE provides good performance and protection, but limited utility. Support either "**Add**" **or** "**Multiply**" operations, not both.

02 SHE

SHE permits **fewer additions and multiplications** on encrypted data. Noise grows due to the number of operations. So, it requires bootstrapping to reduce the noise.

03 FHE

FHE allows you to compute additions and multiplications on encrypted data. However, the more complex the operation, the more resource and time may be required.

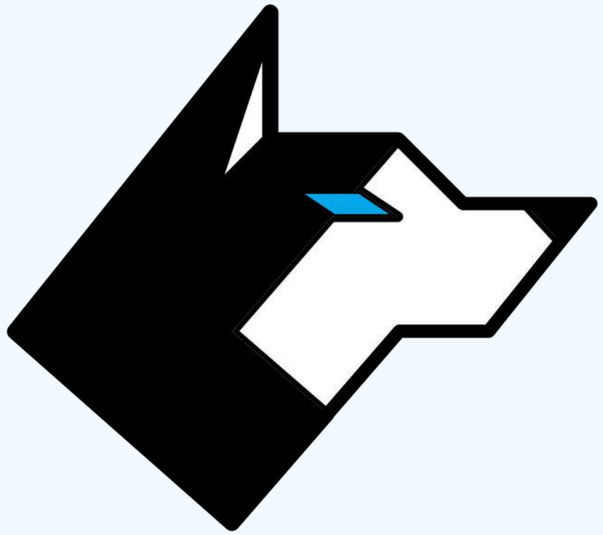
CHALENGES

- Most FHE schemes support only **positive integer**
- Most FHE supports only **Add** and Multiply operations on **positive integer**
- **No** scheme support "**Divider**" operation

HOW WE SLOVE IT

- Use the **RNS-CKKS scheme** to support Fixed-Point Number --> Real number
- Support "**Negative**" & "**Positive**" values
- Propose Our divider approximation algorithm for a Divider operation **without division!!!**

OUR PRIVACY AS A SERVICE PLATFORM FOR IOT



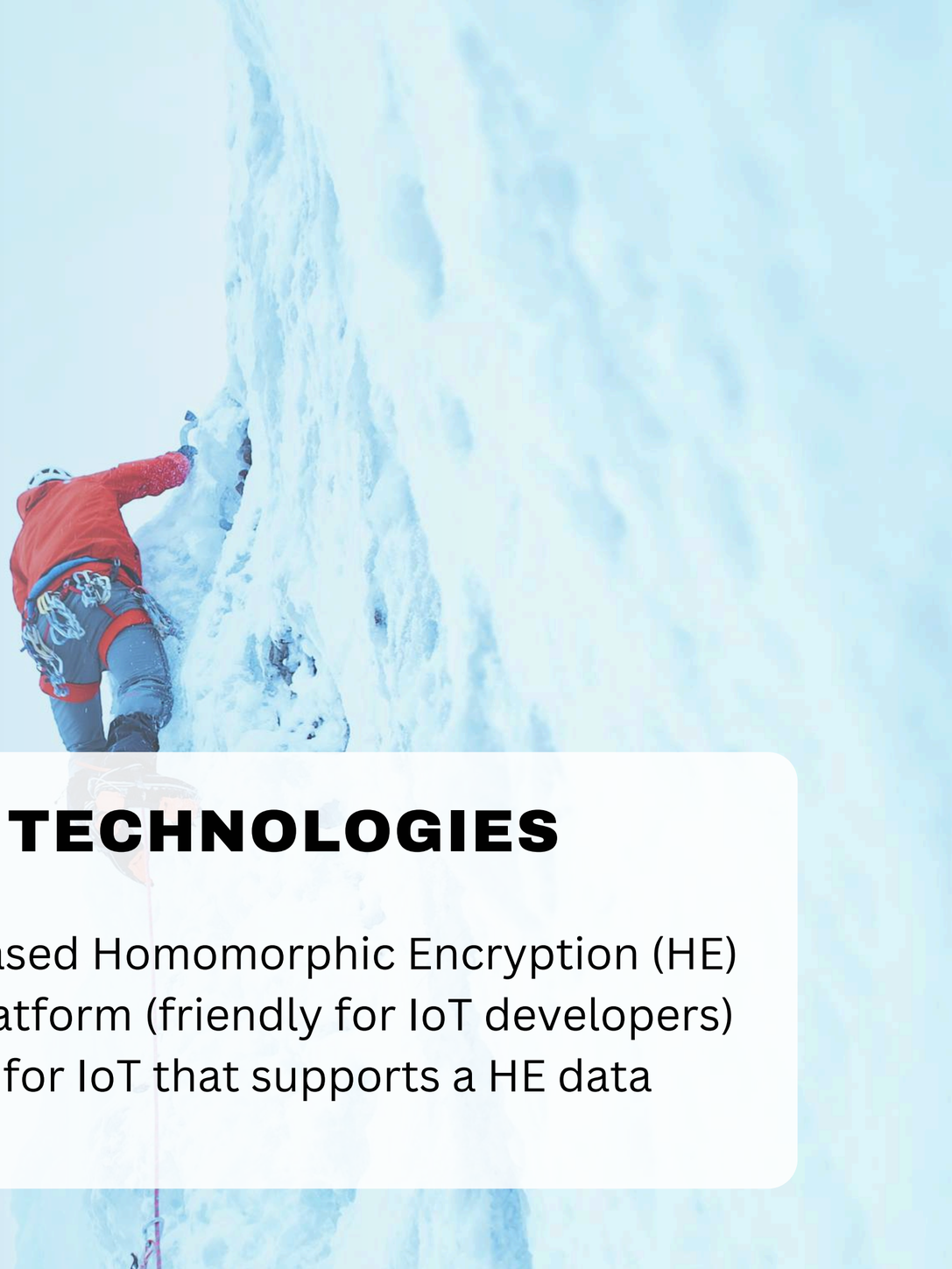
TRUSTED HUSKY

CYBLION aims for quality privacy enhancement as a service for users. The name is composed of “**Cyber“** and **"Brilliant,"** conjugated as **"CYBLION."**

Fortunately, the name sounds similar to the **Siberian husky** as the symbol of agility, trust, and power. The icon is simplified from a **Siberian husky** to convey a sense of modernity to fit the nature of the cybersecurity technology brand.

OUR GOAL

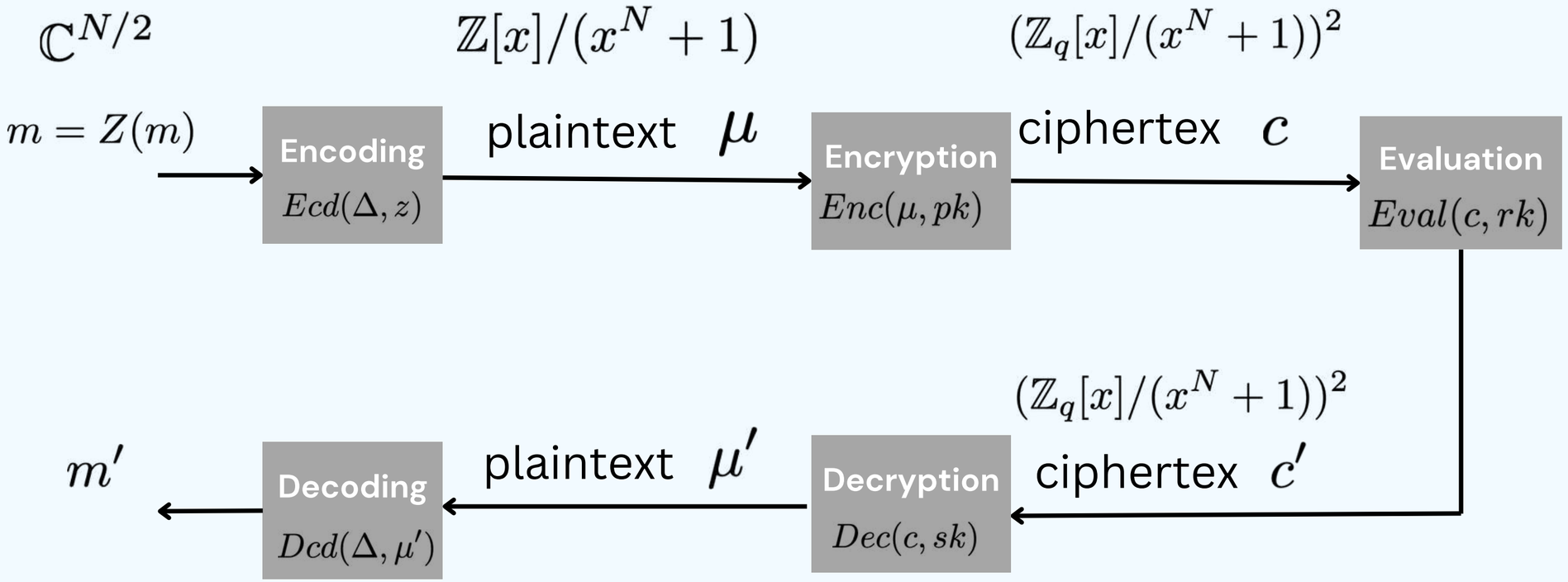
- To develop an IoT platform that allows IIoT/IoT developers to preserve and control data privacy via a mobile app while outsourcing computation to the cloud.



3 KEY TECHNOLOGIES

- RNS-CKKS-based Homomorphic Encryption (HE)
- Node-RED platform (friendly for IoT developers)
- MQTT broker for IoT that supports a HE data type

RNS-CKKS IN A NUTSHELL



CHALLENGE#1

A security parameter is a way of measuring of how "hard" it is for an adversary to break a cryptographic scheme.

PARAMETER SETTING

λ Define Security Level

Q Coefficient modulus $Q = \prod_{i=1}^{L} q_i$

n Polynomial modulus

Δ Scale Factor

$$P = (n, Q, \Delta)$$

$$p_L \rightarrow p_{L-1} \rightarrow p_{L-2} \rightarrow \cdots \rightarrow p_1$$

n	Bit-length of coefficient modulus Q		
	128-bit security	192-bit security	256-bit security
1024	27	19	14
2048	54	37	29
4096	109	75	58
8192	218	152	118
16384	438	300	237
32768	881	600	476

Step 1: Select security bit $\lambda = 128$

Step 2: Choose a scale factor Δ and coefficient modulus q_i

Step 3: Determine ***L***, the number of levels (no of operations)

Step 4: Determine polynomail modulus n

CHALLENGE#2

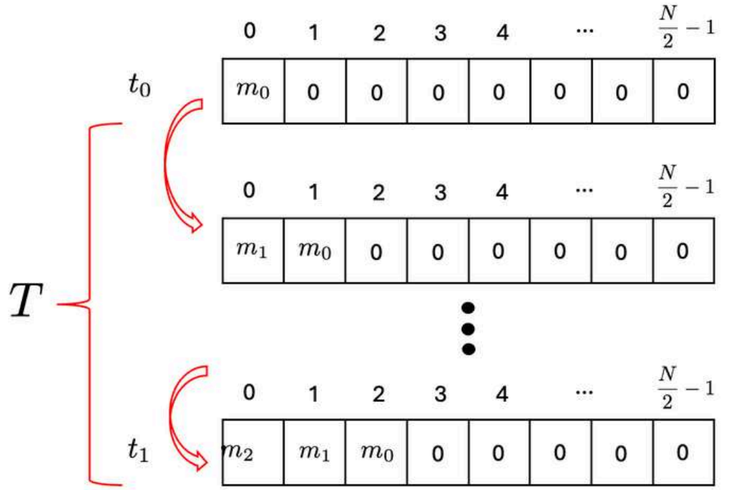
EXISTING IOT CLOUDS

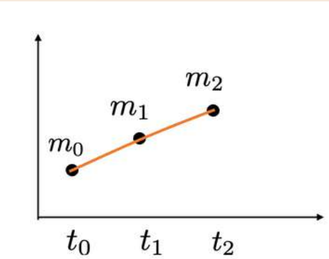
Not support HE

CHALLENGE#3

SINGLE INPUT MULTIPLE DATA (SIMD)

$$M = [m_1, m_2, \ldots, m_{n/2}] \Rightarrow Ecd(M; \Delta) \Rightarrow E_k(Ecd(M; \Delta)) \Rightarrow c$$





WAIT FOR

$$T = \sum_{i=1}^{n/2} t_i - t_{i-1}$$

- Need to wait for the updated data > 17 hr (n = 8192 IoT feed data every 15 mins)

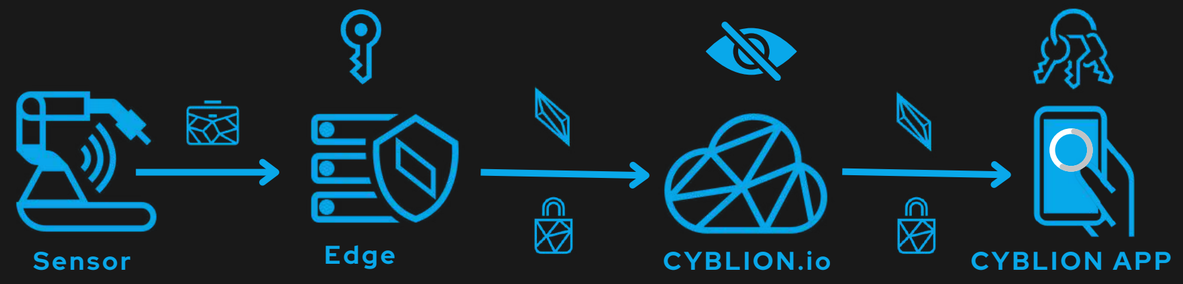
Design Principles

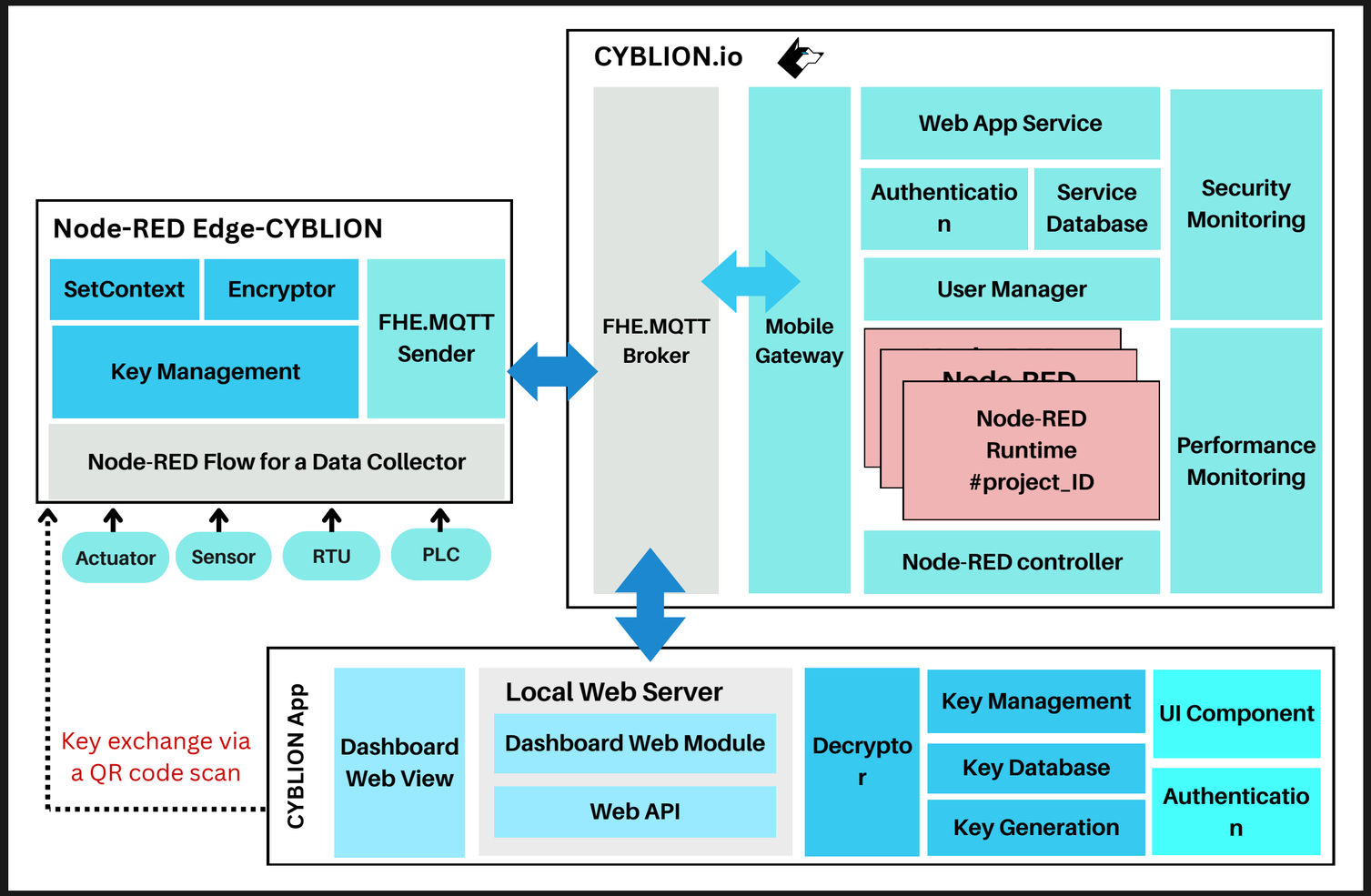
01 Make it simple for regular developers so that they not have to interact with complex HE parameter settings

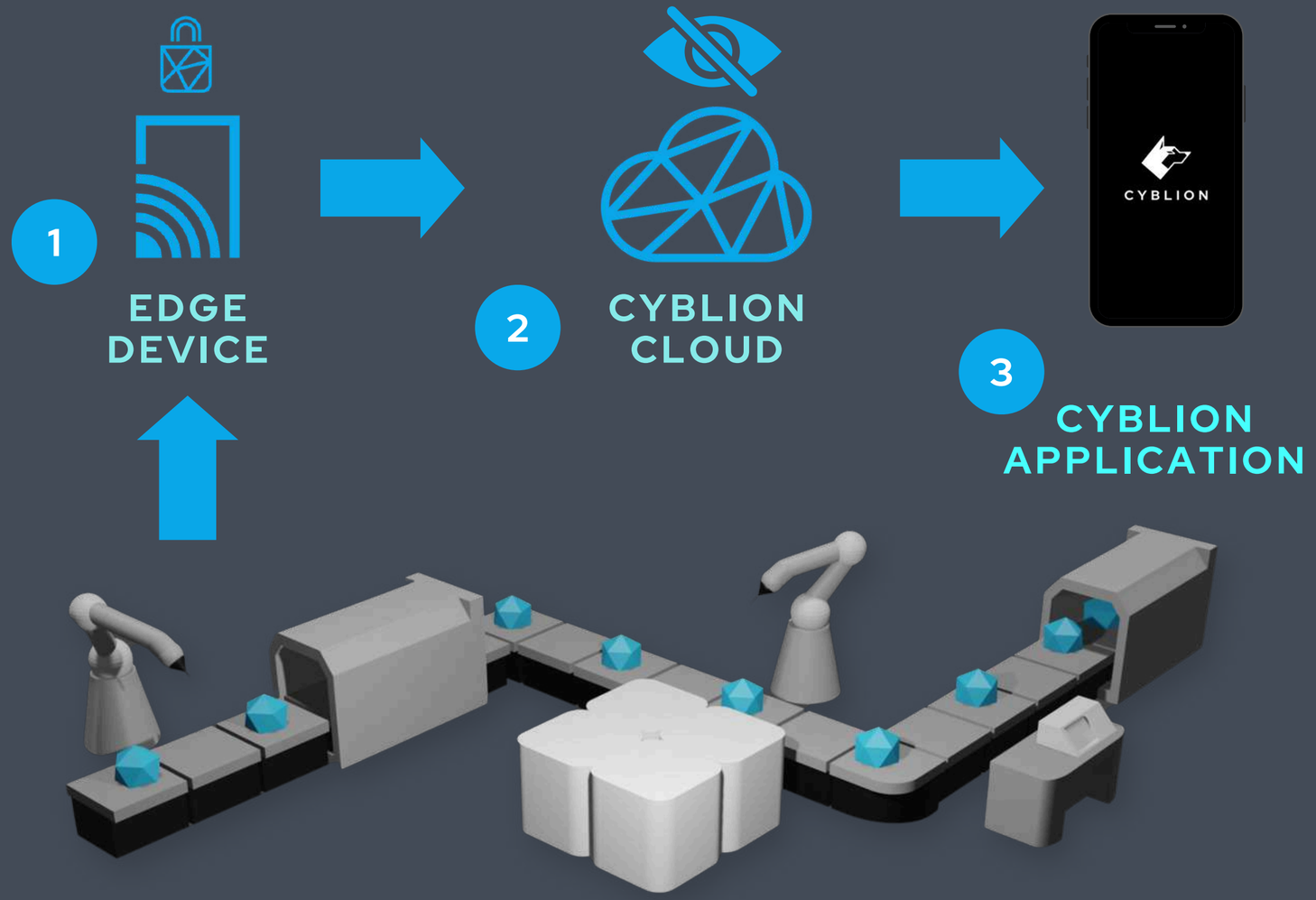
02 Sufficiently powerful to satisfy both security and privacy

03 Easy to use and flexibly compose IIoT computation functions without cryptographic expertise

04 Data packing in a single plaintext matching with IoT-like data







CYBLION SOLUTION

Preserve data privacy during computation

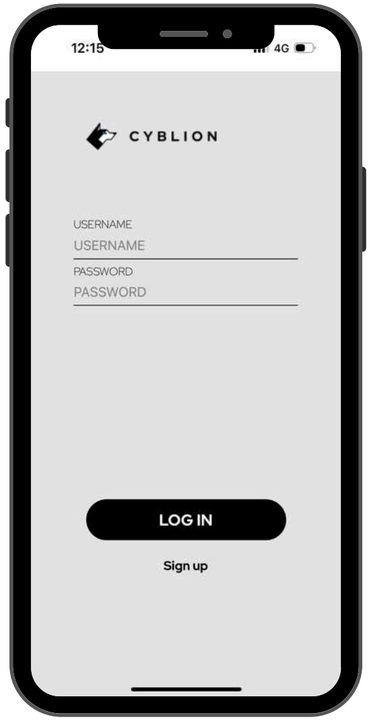
Cybersecurity protection over the cloud and Internet

Offload data computation and data distribution by cloud computing

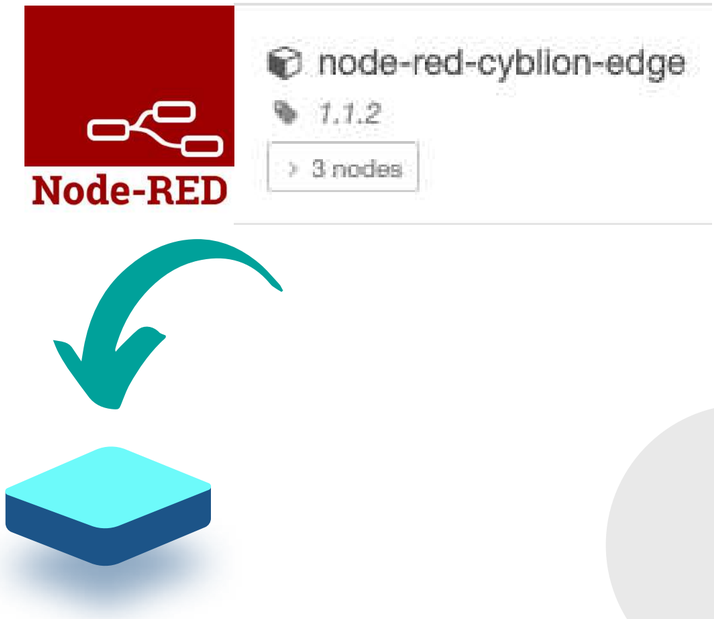
Prevent data breach to the third party

HOW DOSE IT WORK?

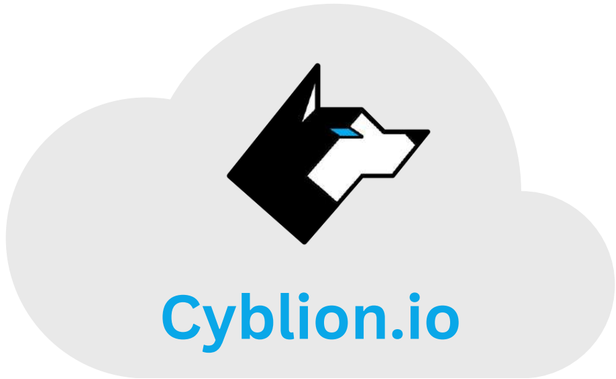
CYBLION REQUIREMENTS



Cyblion App in
iOS & Android

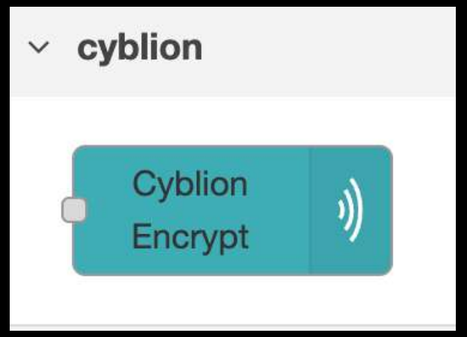


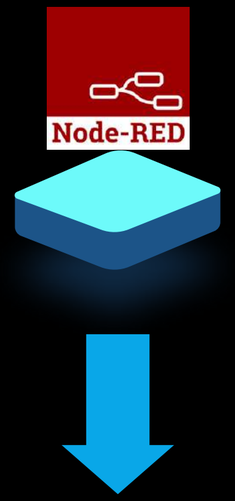
Node-RED installation
in the Edge computing

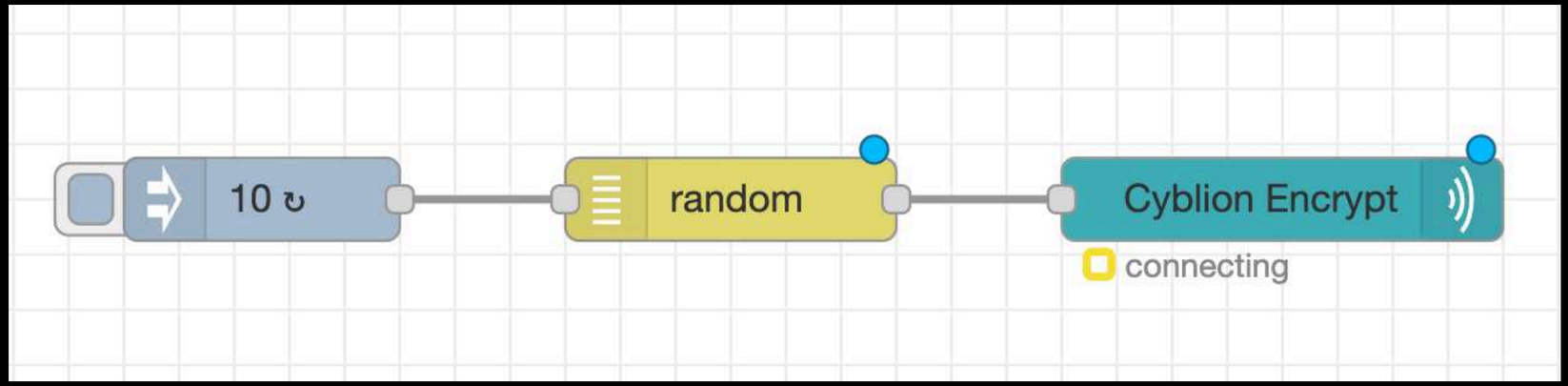


Cloud computing
with a NETPIE user account

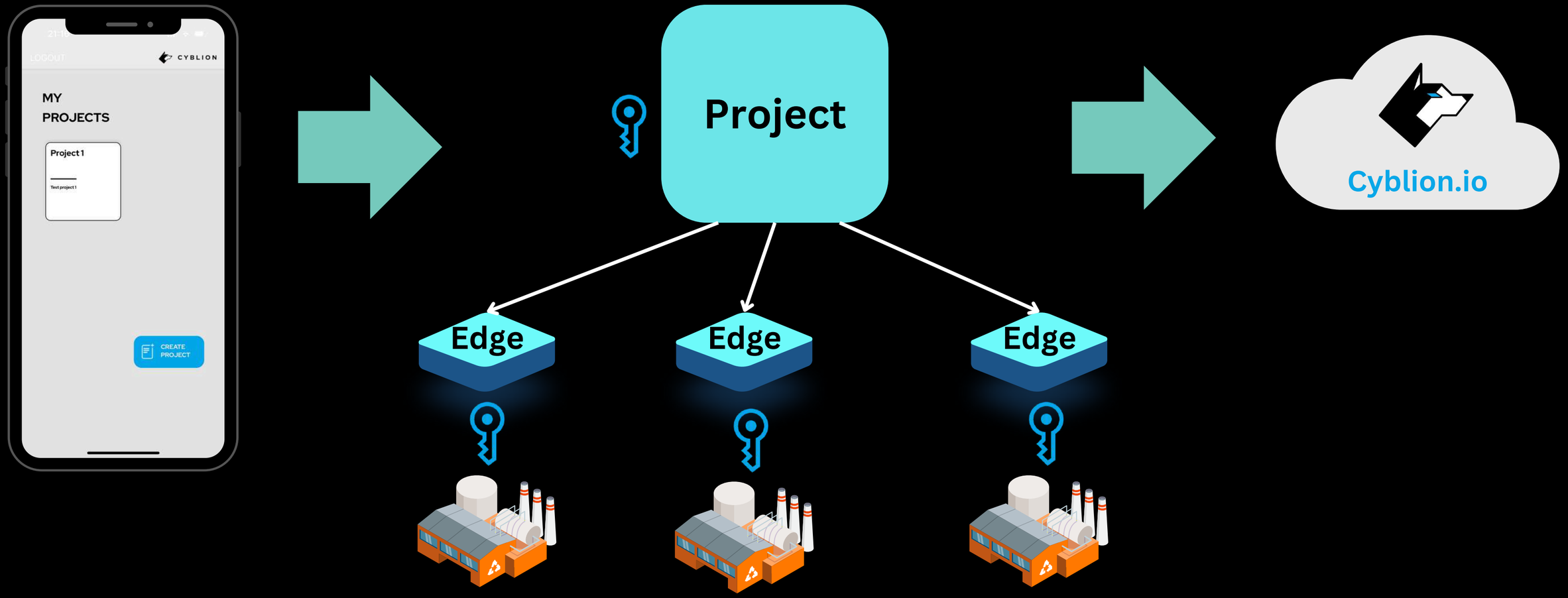
INSTALL CYBLION-EDGE

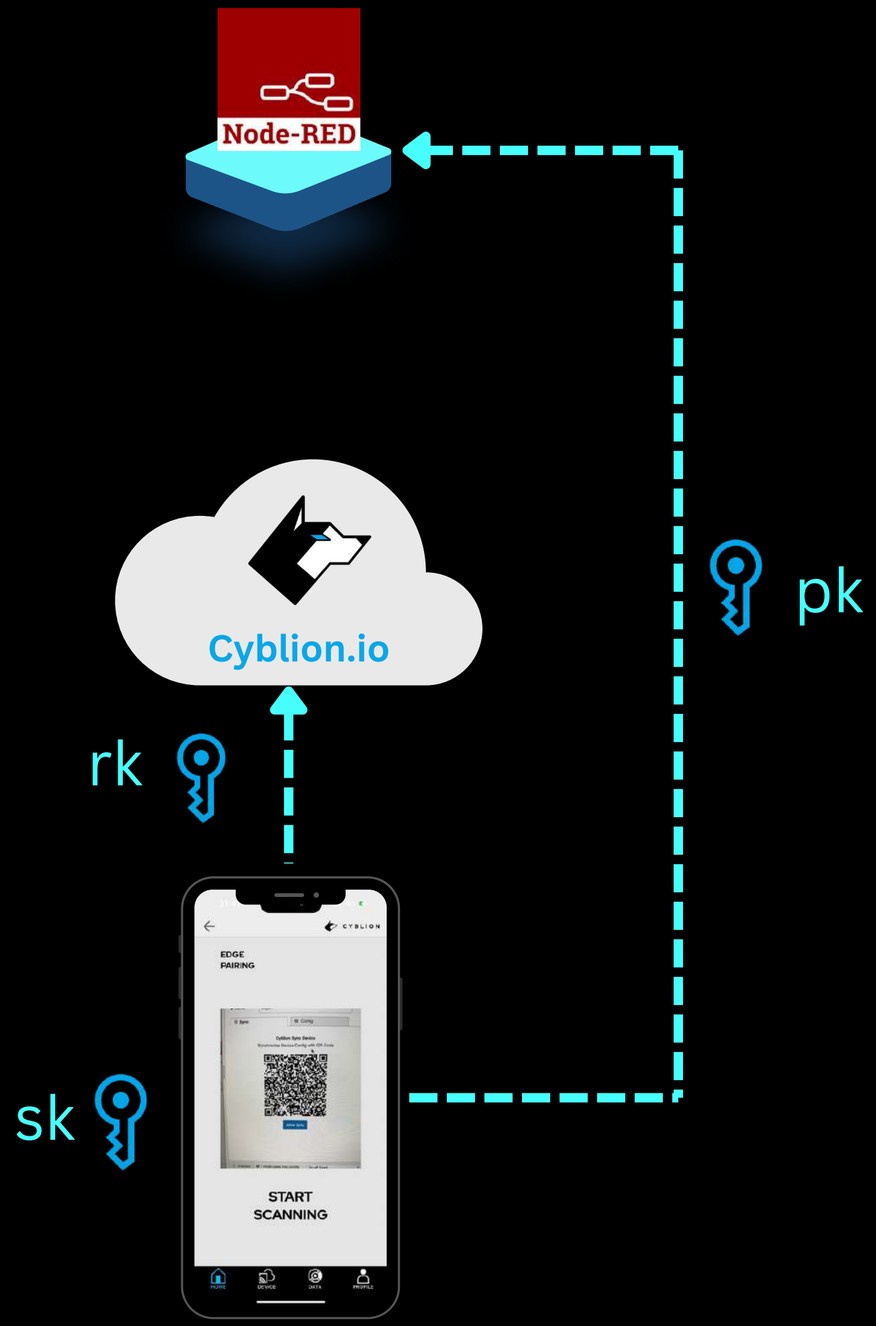




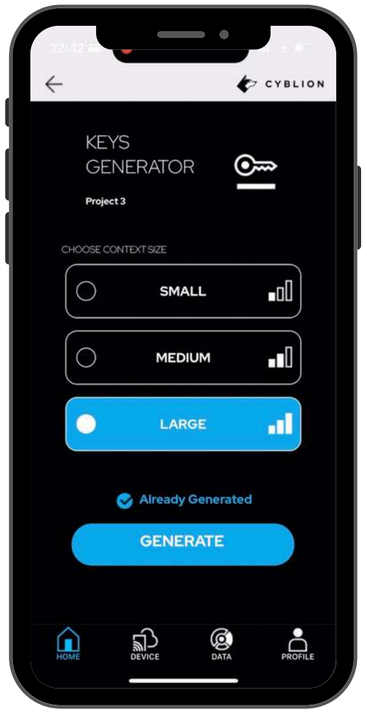


PROJECT AND EDGE DEVICES



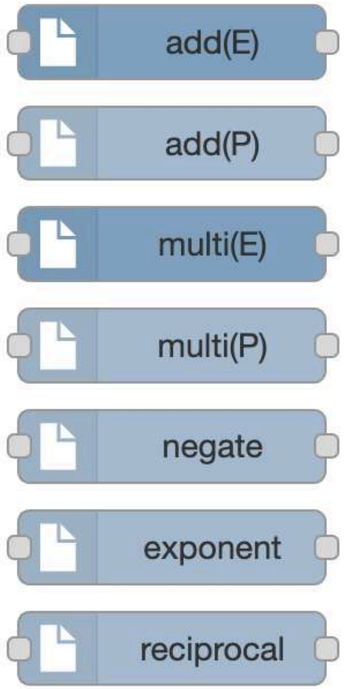


USERS SELECT THE KEY SIZE

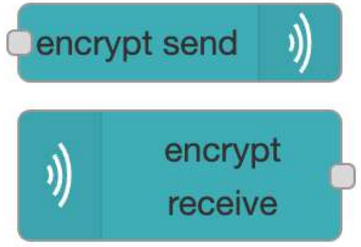


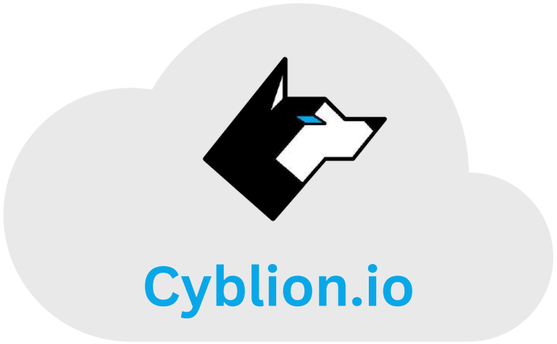
Parameter Size	Scale Factor	No. Operations
Small	2^{30}	3
Medium	2^{40}	3
Large	2^{40}	7

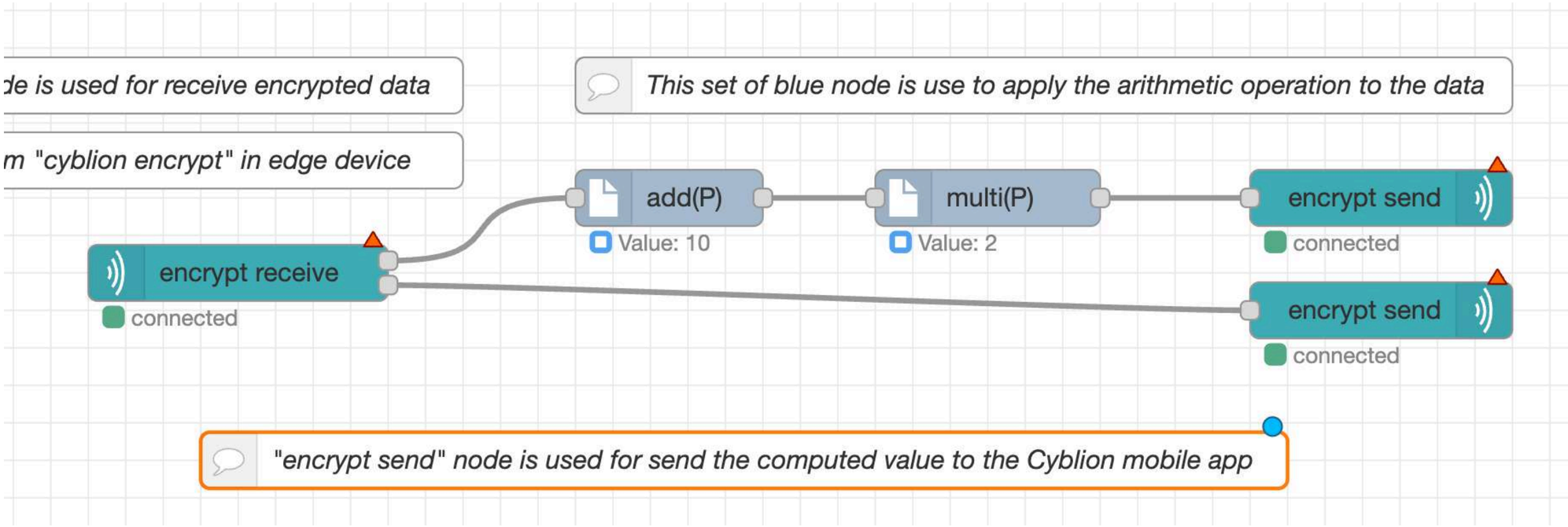
Arithmetic Operations

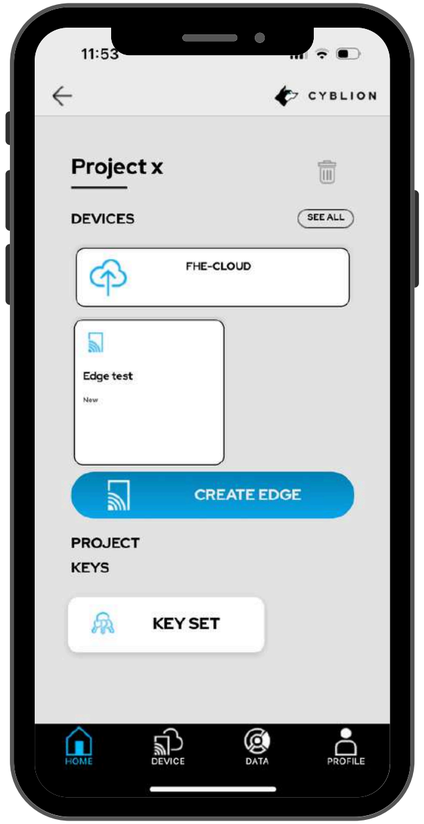


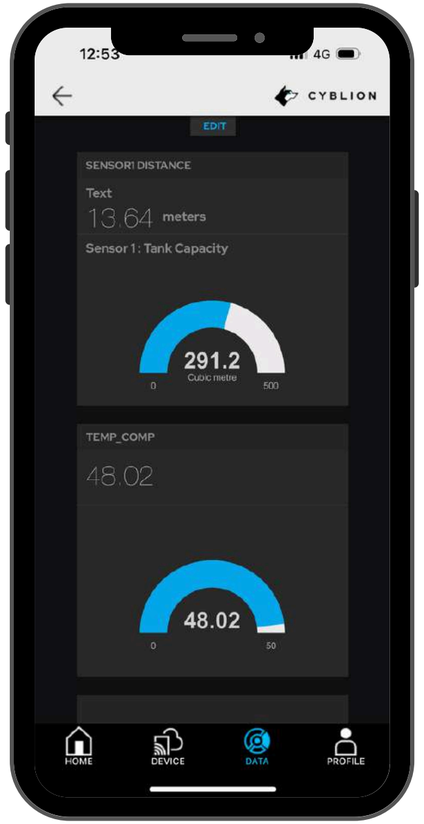
MQTT

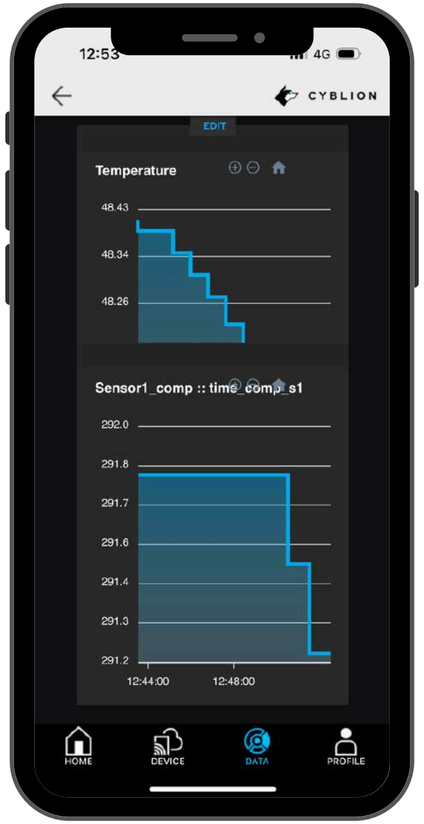







11:53
CYBLION
Project x
DEVICES
SEE ALL
FHE-CLOUD
Edge test
New
CREATE EDGE
PROJECT
KEYS
KEY SET
HOME
DEVICE
DATA
PROFILE


12:53
4G
CYBLION
EDIT
SENSOR1 DISTANCE
Text
13.64 meters
Sensor 1: Tank Capacity
291.2
Cubic metre
0
500
TEMP_COMP
48.02
48.02
0
50
HOME
DEVICE
DATA
PROFILE


12:53
4G
CYBLION
EDIT
Temperature
48.43
48.34
48.26
Sensor1_comp :: time_comp_s1
292.0
291.8
291.7
291.6
291.4
291.3
291.2
12:44:00
12:48:00
HOME
DEVICE
DATA
PROFILE

FACTORY USE CASE

DESIGN

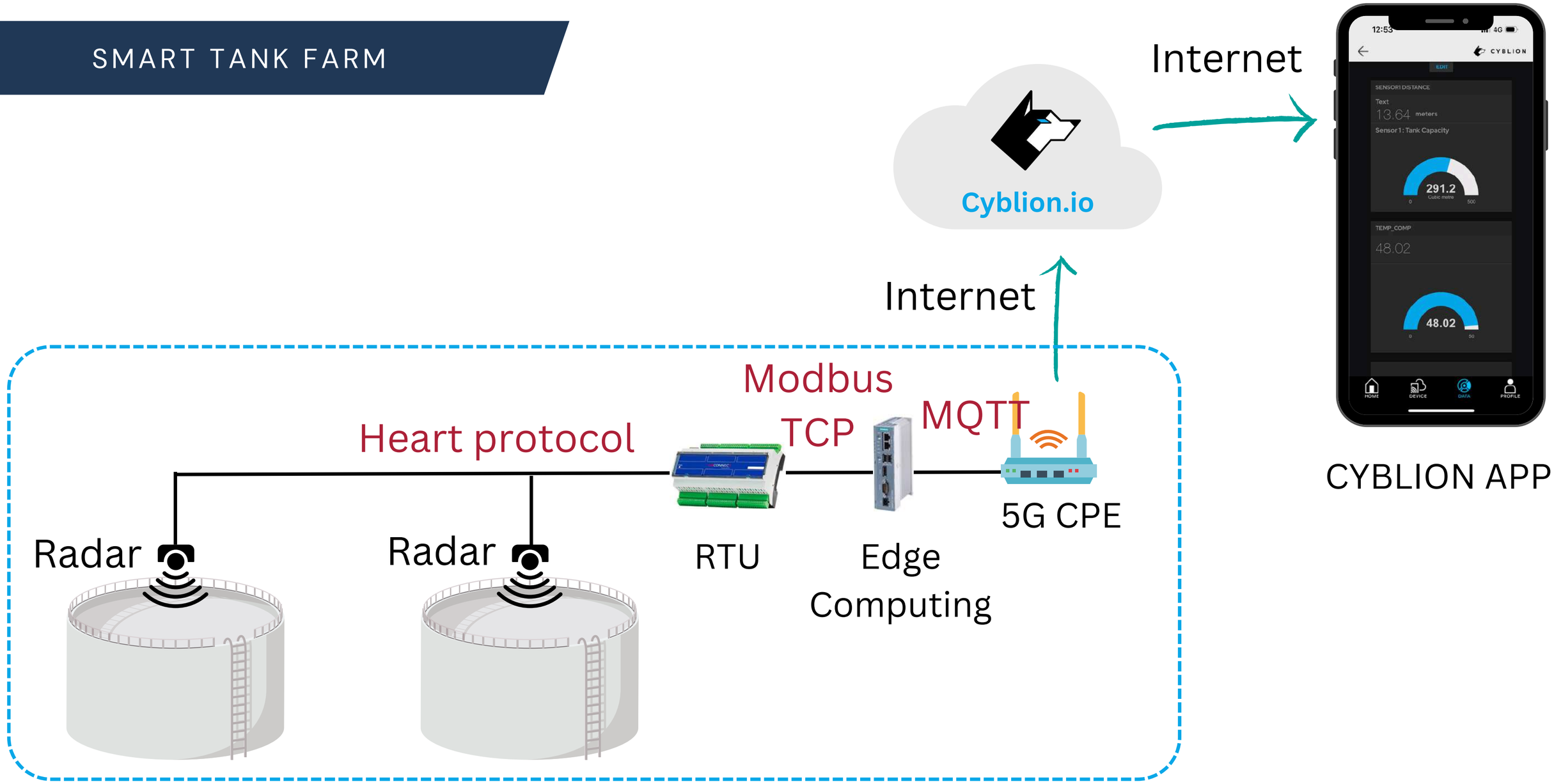
We design a solution to fit with the Factory's use case

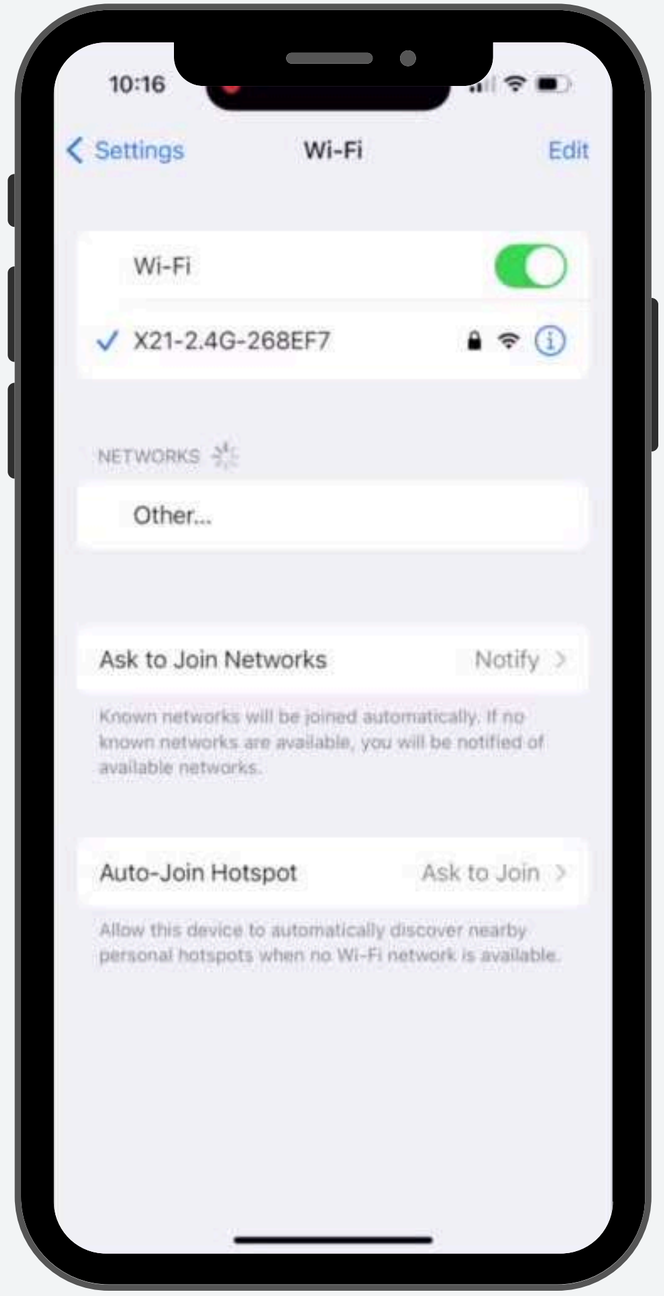
SMART TANK FARM MONITORING SYSTEM

PRIVATE DATA MONITORING

The factory's staff can monitor the level of oil in their tanks in real-time via mobile phone

SMART TANK FARM





CYBLION App

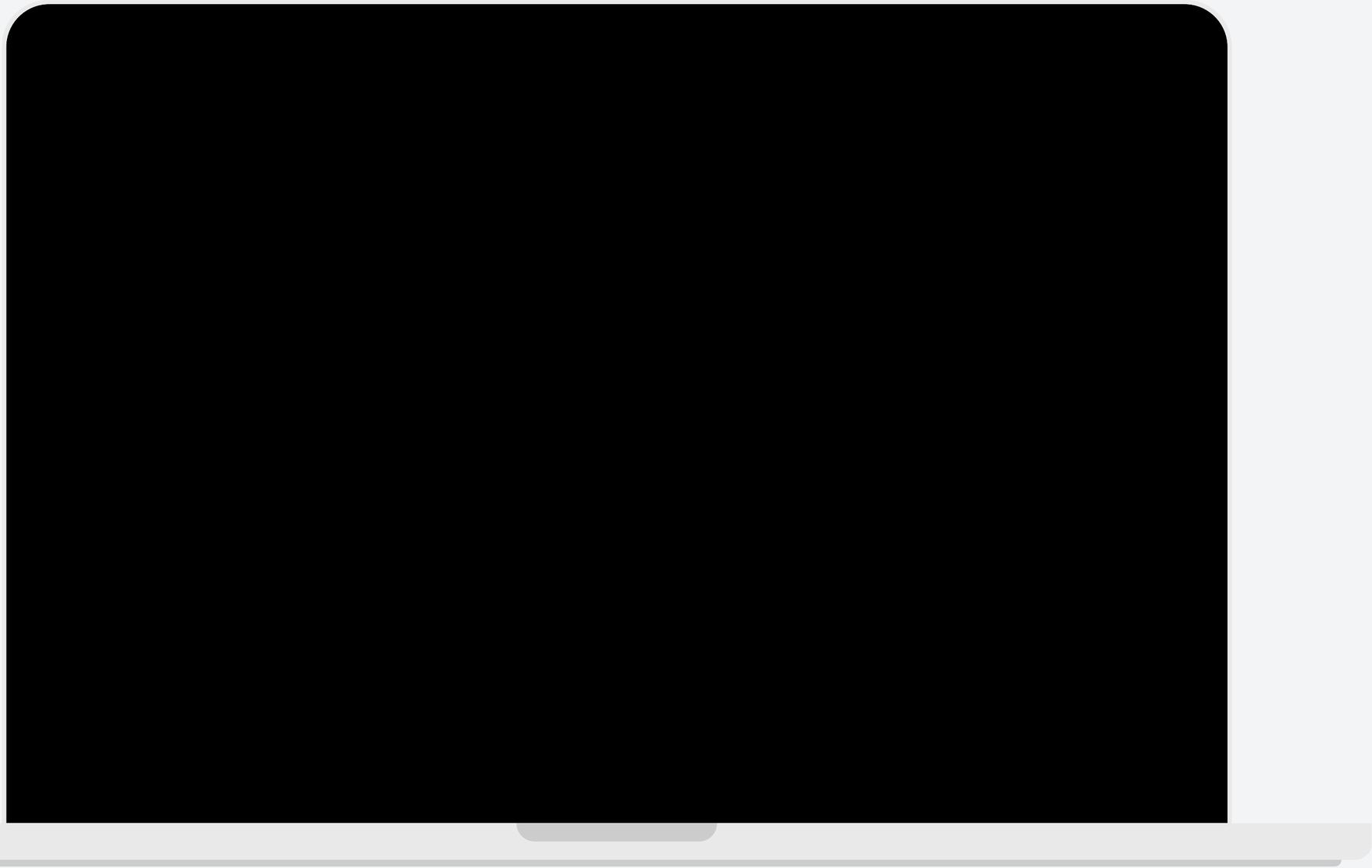
Edge Device

Router

PAIR A PUBLIC KEY

- During pairing a encryption key stage, a mobile and an edge device must connect to the same network
- Create keys by choosing the context size
- Pair the public key to the edge device via the QR code

SSH



IoT 2050
Edge Device

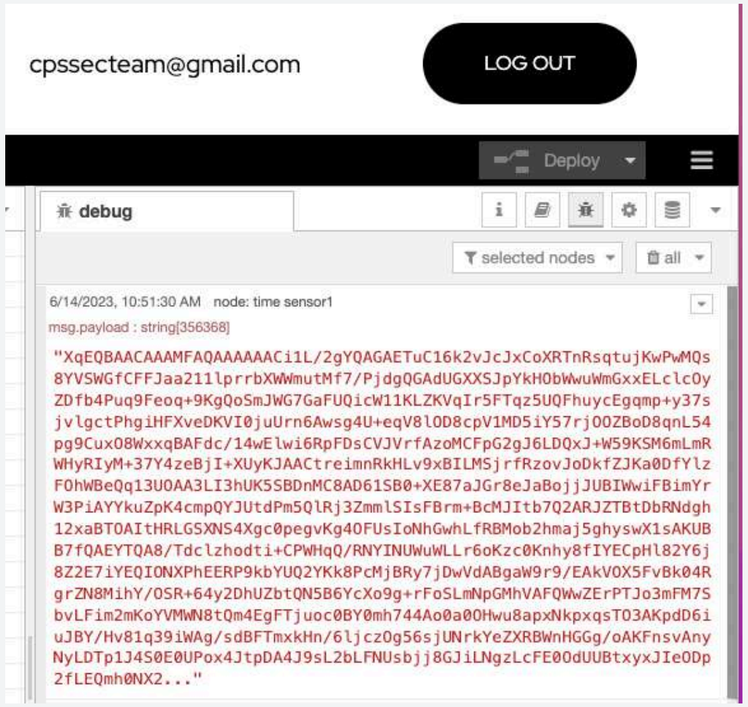
TVOP USE CASE

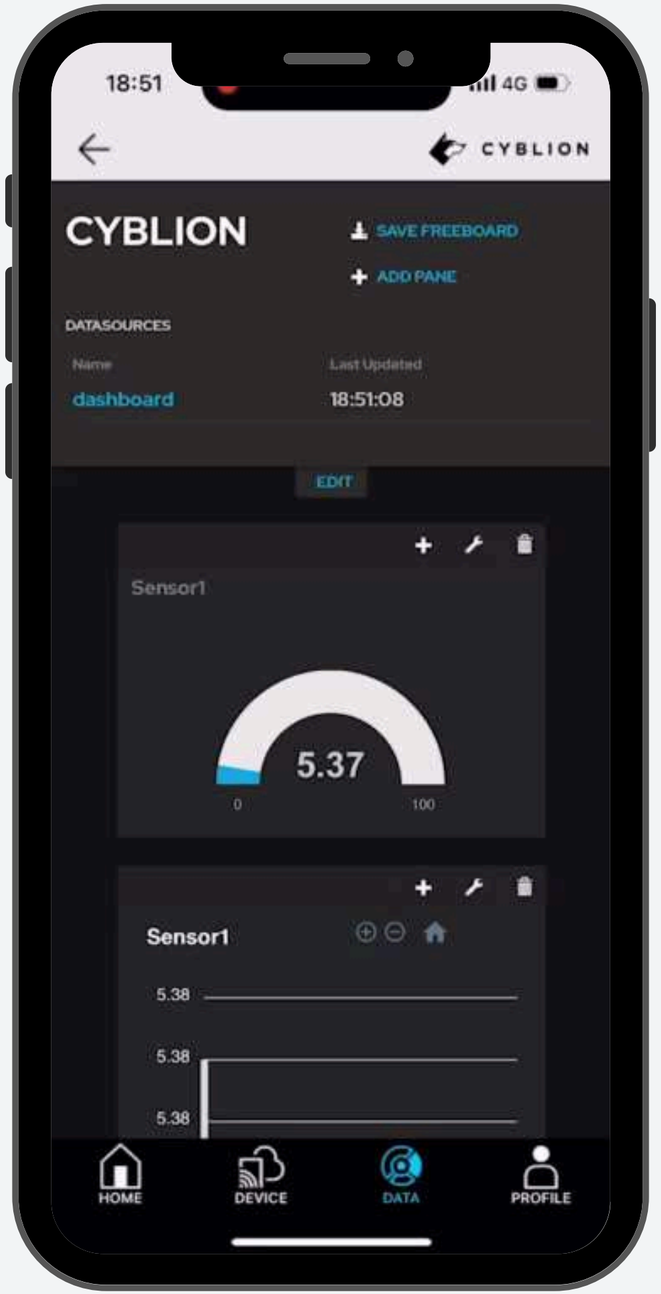
CYBLION CLOUD

Cloud Computing

Cyblion.io

Data in Cyblion.io





Mobile App

Edge Device

Router

- Select the icon **"DATA"** to see the dashboard
- User can create a graph and select the appropriate type of data for visualization
- Compare to the unencrypted data in NETPIE App

CONNECT THE DATA ANYWHERE ANYTIME

OPEN FOR RESEARCH COLLABORATION

RESEARCH & DEVELOPMENT

PERFORMANCE

We still need improvement on the computation complexity and ciphertext size

SCALABILITY

There is some rooms to improve the scalability of distributed edge computing

OUR BEST TEAM

Advisory Board

Panita Pongpaibool

ADVISOR

Sukumal kitisin

ADVISOR

Research Team

Kalika Suksomboon

CRYPTOGRAPHY/
PROJECT MANAGEMENT

Aimaschana Niruntasukrat

IOT EDGE COMPUTING/
RESEARCHER

Koonlachat Meesublak

IOT CLOUD PLATFORM/
RESEARCHER

Sophon Mongkolluksamee

CYBERSECURITY/ RESEARCHER

OUR BEST TEAM

Development Lead

Chavee Issariyapat

DEVOPS LEAD AND BACKEND CLOUD DEV

Development Team

Nattapon Tansangworn

NETPIE ARCHITECT

Nataset Tanabodee

EDGE & CLOUD DEVOPS SOFTWARE ENGINEER

Tawan Hohum

MOBILE APP DEVOPS

Eakarat Saktawornlerd

MOBILE APP DEVOPS, UX/UI SOFTWARE ENGINEER

THANK YOU

LEARN MORE ABOUT CYBLION

Welcome to talk to me!
&
I will give you a trial account.

Download

CYBLION

Download on the App Store

GET IT ON Google Play