UQAC
Université du Québec
à Chicoutimi

IARIA

ON SECURING THE INTERNET OF THINGS: CHALLENGES AND PERSPECTIVES

FEHMI JAAFAR

07/27/2022

fehmi.jaafar@uqac.ca

Fehmi Jaafar, PhD

Background

- Bachelor's and Master's, Computer Engineering,(Tunisia University).
- PhD. in Computer Sciences (Montréal University, 2014)
- Postdoc at Queens University and Polytechnique Montreal (2014-2016)
- Full time Adjunct Assistant Professor, Concordia University of Edmonton (2016-2018)
- Researcher at **CRIM** (Computer Research Institute of Montreal (2018-2021)
- Associate Professor at Quebec University at Chicoutimi (2021)

Other affiliations

- Affiliate Professor at Laval University
- Consultant Expert - Auditor General of Quebec (Le Vérificateur Général du Québec)
- Vice Chair - The Internet of Things and Related Technologies Committee - Standards Council Canada
- Member of the Board of Directors of Internet Society Canada Chapter

2

PLAN

1. AN OVERVIEW OF RESEARCH ACTIVITIES
2. THE COMPUTER SECURITY IN THE INTERNET OF THINGS
3. EXAMPLES OF IOT SECURITY ISSUES
4. PROPOSED SOLUTIONS
5. ONGOING RESEARCH ACTIVITIES

3

4

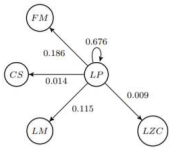
1: AN OVERVIEW OF RESEARCH ACTIVITIES

SOFTWARE ANALYTICS TO IMPROVE THE QUALITY AND THE SECURITY OF SOFTWARE SYSTEMS:

Analysis of the Impact of Software Anti-patterns

Fehmi Jaafar, Yann-Gaël Guéhéneuc, Sylvie Hamel, Foutse Khomh, and Mohammad Zulkernine, Evaluating the Impact of Design Pattern and Anti-pattern Dependencies on Faults and Changes:
Journal of Empirical Software Engineering EMSE, 2015.

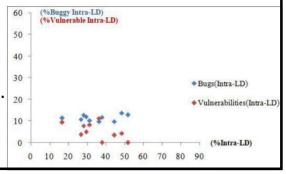
Anti-patterns Mutations



Zeinab Azadeh Kermansaravi, Md Saidur Rahman, Foutse Khomh,**Fehmi Jaafar**, and Yann-Gaël Guéhéneuc. "Investigating design anti-pattern and design pattern mutations and their change-and fault-proneness."

Journal of Empirical Software Engineering EMSE, 2021.

Software Security Comprehension



Manel Grichi, **Fehmi Jaafar**, E. E. Eghan and Bram Adams:
On the Impact of Interlanguage Dependencies in Multilanguage Systems.

IEEE Transactions on Reliability, 2021.

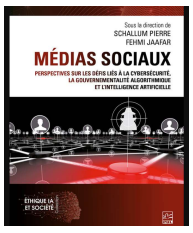
1: AN OVERVIEW OF RESEARCH ACTIVITIES

CLOUD SECURITY:

Ameyed, Darine, **Fehmi Jaafar**, and Jaouhar Fattahi. "A slow read attack using cloud." In 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. SSS-33. IEEE, 2015.

Singh, Gurjot Balraj, **Fehmi Jaafar**, and Sergey Butakov. "Analysis of overhead caused by security mechanisms in IaaS cloud." In *2018 5th International Conference on Control, Decision and Information Technologies (CoDIT)*, pp. 952-958. IEEE, 2018.

SOCIAL MEDIA SECURITY



(2021). Social Media: Perspectives on the Challenges of Cybersecurity, Algorithmic Governmentality and Artificial Intelligence.
Schallum Pierre and Fehmi Jaafar.
Laval University Press, Quebec, Canada
ISBN; paper 978-2-7637-5328-7; PDF: 9782763753294.

6

2: THE SECURITY IN THE INTERNET OF THINGS

7

2: THE SECURITY IN THE INTERNET OF THINGS

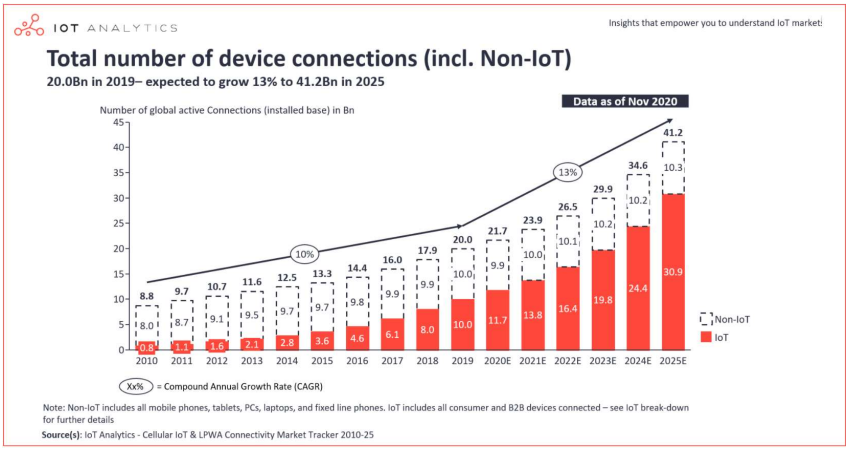
CONNECTED OBJECT

- Connected physical object that can exchange data to or from one location to another.
- These objects need to be uniquely identifiable and possess the ability to autonomously collect data about their environment.
- Embedded computation hardware and software as well as some form of network connectivity to an edge or remote computing resource.

8

2: THE SECURITY IN THE INTERNET OF THINGS

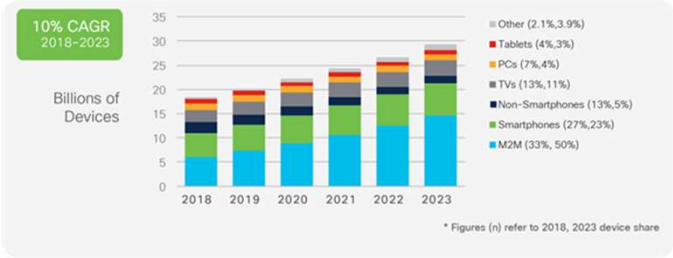
NUMBER OF CONNECTED OBJECTS



9

2: THE SECURITY IN THE INTERNET OF THINGS

RESOURCE LIMITATION



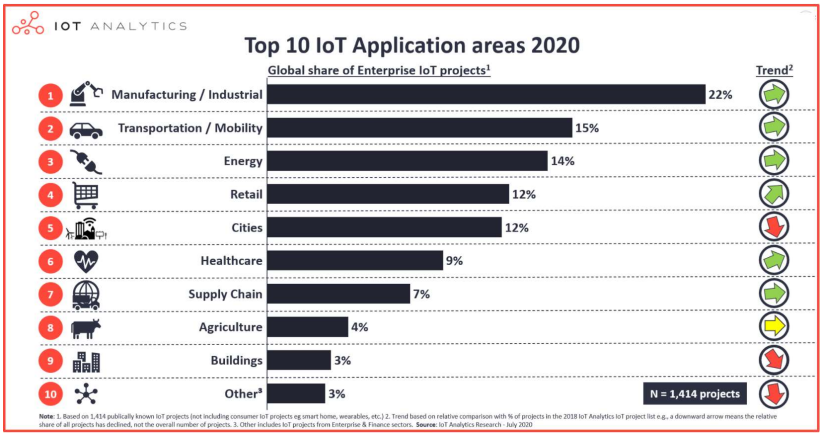
Source: Cisco Annual Internet Report, 2018–2023

By 2021, there will be more than 10 billions M2M connected devices (e.g., GPS in smart cars, asset tracking systems in shipping, manufacturing, and medical systems).

10

2: THE SECURITY IN THE INTERNET OF THINGS

THE INTERNET OF THINGS IS EVERYWHERE AND ANYWHERE



11

3: EXAMPLES OF IOT SECURITY ISSUES

12

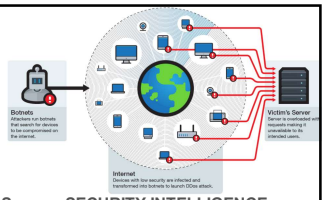
3: EXAMPLES : DDOS

THE FIRST IOT CYBERATTACK ? THE DDOS ATTACKS FROM 2016

- **Mirai botnet**: Less than 50,000 connected objects orchestrate DDoS attacks against DNS services: loss of GitHub, Twitter, Reddit, Netflix, Airbnb services.
- Internet search for IP addresses corresponding to connected objects (IoT).
- Mirai uses the default passwords to control the object.

13

3: EXAMPLES : DDOS



Source: SECURITY INTELLIGENCE

IOT CYBERATTACKS WITH HIGHER IMPACT?

- 15% of IoT Devices use default passwords (Source: Positive Technologies report).
- Just five sets of password to access 10% of all the connected IoT devices: support/support, admin/admin, admin/0000, user/user and root/12345
- Shodan, Censys, or ZoomEye, allow malware authors to identify millions of connected vulnerable devices.
- New Mirai variants are using exploits vulnerabilities in IoT devices.
- Currently, 60 percent of IoT devices contain such vulnerabilities (83% of medical imaging devices are running on unsupported operating systems). Source: the 2020 IoT Threat Report, Palo Alto Networks

14

3: EXAMPLES : CPD

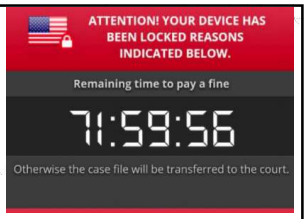
Source: Rein Kelly

PRIVACY AND CONFIDENTIALITY THREATS

- 98% of all IoT traffic is unencrypted, exposing personal and confidential data on the network (Source: the 2020 IoT Threat Report, Palo Alto Networks).
- IoT Toys, smart phones, fitness trackers, etc.
- Listen to unencrypted network traffic, collect personal or confidential information, then exploit that data for profit on the dark web.

15

3: EXAMPLES : RANSOMWARE



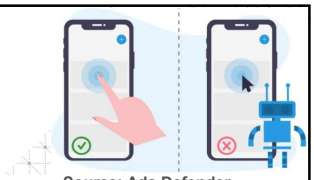
Source: Kaspersky

IOT RANSOMWARE THREAT

- Malware targeting Internet of Things (IoT) devices has risen to 20.2 million, up 50% in 2020 (Source: the 2020 SonicWall Cyber Threat Report).
- Target: IoT devices providing real-time management and control (Medical IoT, Hotels, etc.)
- Attackers are using infected devices as the entry point into the corporate network (Las Vegas casino).

16

3: EXAMPLES : CLICKFRAUD



Source: Ads Defender

ONLINE FRAUD

- IoT devices infected by Mirai were used as botnet to perform **clickfraud**, a form of online advertising fraud that costs advertisers billions of dollars each year.
- **Impression Fraud**: Bots can browse websites, visit links and even watch videos (opinion manipulation and influence activities).

17

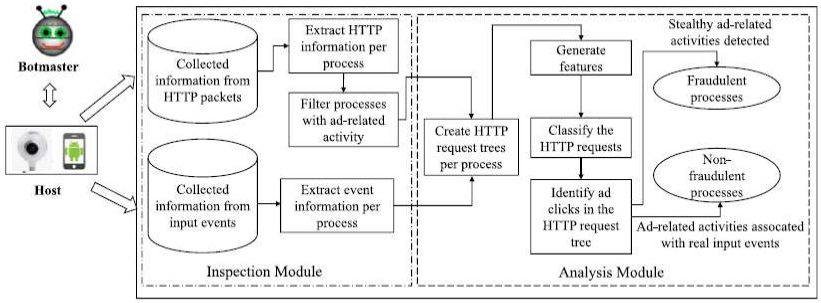
4: PROPOSED SOLUTIONS

18

4: PROPOSED SOLUTIONS

FCFRAUD

We implemented a cloud detection tool: the IoT devices send the data to the cloud in an encrypted manner.



Workflow of FCFraud

19

4: PROPOSED SOLUTIONS

FCFRAUD

- Web ad requests have some common characteristics: a large number of query parameters; their responses are normally images or JavaScript contents.
- FCFraud extracts features from the query parameters, the HTTP headers (both the request and the response), and the constructed HTTP request trees.
- FCFraud marks a HTTP request as fraudulent if it clicks on an ad using a software simulated click or an independent HTTP request (without a click) while executing in the background.

20

4: PROPOSED SOLUTIONS

FCFRAUD

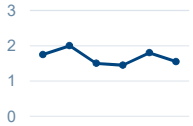
We test 5 classification algorithms: Naive Bayes, Support Vector Machines, K-Nearest Neighbors, C4.5, and Random Forest.

Classification Algorithm	Avg. Accuracy (%)	Precision (%)	FP Rate (%)
NaiveBayes	89.76 / 92.99	54.71 / 39.41	10.71 / 6.18
SVM	95.49 / 97.55	100.00 / 100	0.00 / 0.00
C4.5	99.32 / 97.21	96.21 / 80.65	0.54 / 0.72
2kNN	99.27 / 98.18	96.54 / 92.31	0.49 / 0.30
5kNN	99.33 / 99.29	96.72 / 87.14	0.46 / 0.54
RandomForest	99.61 / 98.23	98.05 / 90.00	0.27 / 0.42

The confirmation that a device is participating in ClickFraud criminal activities in less than 20 minutes.

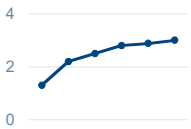
21

4: PROPOSED SOLUTIONS



IoT Normal behavior

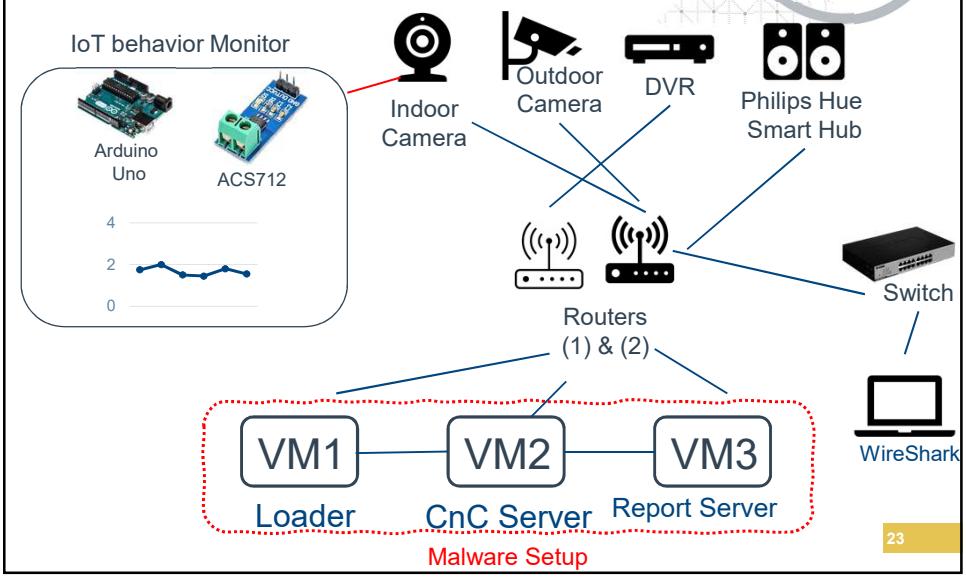
Empirical Study



Infected IoT behavior

22

4: PROPOSED SOLUTIONS

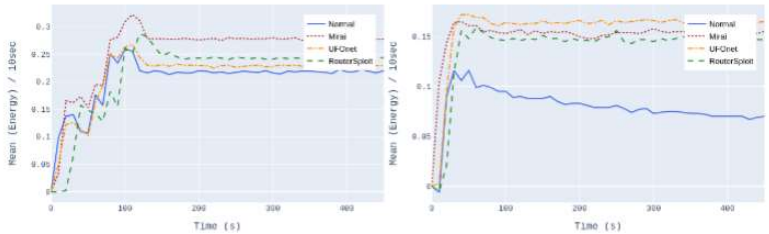


23

4: PROPOSED SOLUTIONS

EMPIRICAL OBSERVATIONS

- In terms of network behavior, the rate of exchange of packets per millisecond was higher in infected IoT devices while packets marked as “Data” were lower.
- The majority of malicious network traffic consisted of malformed packets compared to “clean” IoT devices.
- Abnormal energy consumption during and after the cyber attack.
- The ability to identify infected IoT devices in less than one minute.

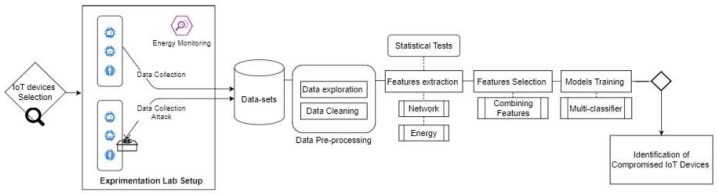


24

4: PROPOSED SOLUTIONS

EMPIRICAL OBSERVATIONS

- Energy consumption analysis is more effective than network traffic scanning for detecting infected objects (DT, RF, etc.).
- An increase of about 10% in the average value of the energy consumption of infected IoT devices (about 0.1 Watt per device per second).



Fehmi Jaafar, Darine Ameyed, Amine Barrak, and Mohamed Cheriet. **Identification of Compromised IoT Devices: A Combined Approach Based on Energy Consumption and Network Traffic Analysis**. The 21st IEEE International Conference on Software Quality, Reliability, and Security (QRS 2021).

25

4: PROPOSED SOLUTIONS

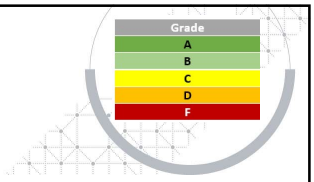
IOT DEVICES CLASSIFICATION

- We are using some criteria to determine the dangerousness of an IoT device.
- We are assigning scores for each criteria ranging from 1 to 3, where a higher value means more dangerousness. Depending of the criteria, the scale can be about frequency or range.
- Finally, we will associate a score with a grade.

Grade	+		-
A	6	7	8
B	9	10	11
C	12	13	14
D	15	16	17
F	18		

26

4: PROPOSED SOLUTIONS



IOT DEVICES CLASSIFICATION

- To grade our device, we are using 6 categories: device, hardware, resistance, firmware, system, and user authentication. In each category, we will have different criteria.

Device Firmware

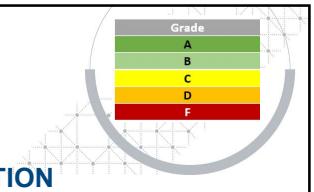
Criteria	1	2	3
Known vulnerability / Exploit	Unknown	Present	Very present
Updatability	Absent	Rare	Frequent

User Authentication

	1	2	3
Authentication	Absent	Basic	Secure
Account management	Absent	Basic	Full
Brute-force protection	Exist	Encrypted with obsolete encryption	Absent
Event logging	Access event logged	Partial logging	Absent
Passwords	Require change after setup with complexity requirements	Require change after setup	Default, common, easy to guess
Security Layer	Present	Partial	Absent

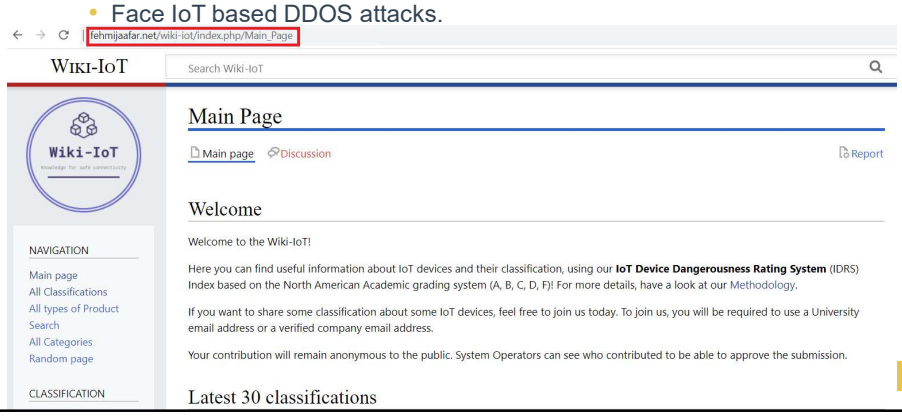
27

4: PROPOSED SOLUTIONS



HOW TO USE THE IOT DEVICES CLASSIFICATION

- Inform the consumer about how risky an IoT device may be.
- An online platform for IoT security assessment.
- Face IoT based DDOS attacks.



4: PROPOSED SOLUTIONS

TERMINATE OR DENY CONNECTION FROM RISKY CONNECTED DEVICES DURING DDOS ATTACKS

Car Kit Raspberry	
Classification	
Latest grade	D
Latest classification date	2021-07-27
Information	
Name	Car Kit Raspberry
Brand	Raspberry
Generation	3006
Model	B07KB8S6RP
Release date	2018-11-08
Type	
Website	[1]
Status	
More	
Dimensions	
Mass	
Operating system	Android
CPU	
Memory	
Storage	
Battery	
Charging	
Camera	
Sound	
Connectivity	

Grade
A
B
C
D
F

Device		
Criterion	**Value**	**Proof**
Known hardware tampering	Rare	[2]
Known vulnerabilities	Very common	[3]
Prior attacks	Rare	[4]
Updatability	Very common	[5]

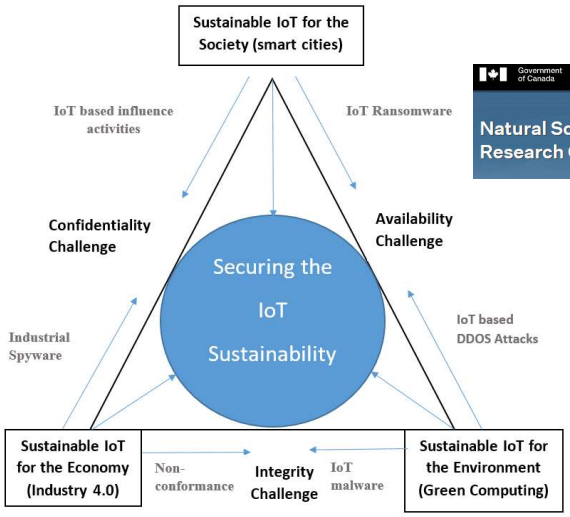
System		
Criterion	**Value**	**Proof**
Authentication with other systems	Partial	[6]
Communications	No encryption	[7]
Storage	No encryption	[8]

29

5: ONGOING RESEARCH ACTIVITIES

30

5: ONGOING RESEARCH ACTIVITIES



Government of Canada / Gouvernement du Canada
Discovery Grants program
Natural Sciences and Engineering Research Council of Canada

31

5: ONGOING RESEARCH ACTIVITIES

THE BLOCKCHAIN TO SECURE PRIVATE DATA IN IOT

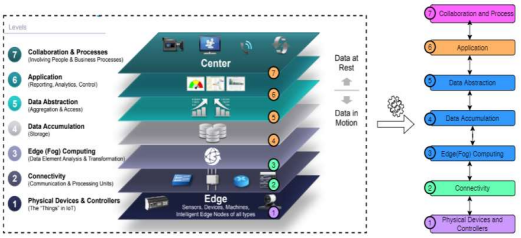
- A university/industrial collaboration (CRIM, Ericsson, etc.)
- Analysis of IoT software vulnerabilities.
- Exploring the application of the Blockchain to secure private data.

Mitacs Accelerate

ERICSSON

UQAC Université du Québec à Chicoutimi

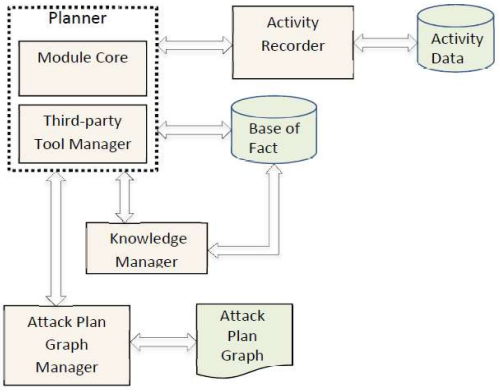
ENCQOR 5G



32

5: ONGOING RESEARCH ACTIVITIES

SPECIFICATION AND DEVELOPMENT OF INTELLIGENT SYSTEMS TO SECURE NATIONAL DEFENSE INFORMATION SYSTEMS



National Defence

33

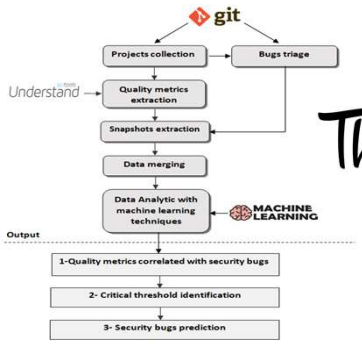
5: ONGOING RESEARCH ACTIVITIES

THE INTERNET OF THINGS AND THE CHALLENGE OF DIGITAL IDENTITY

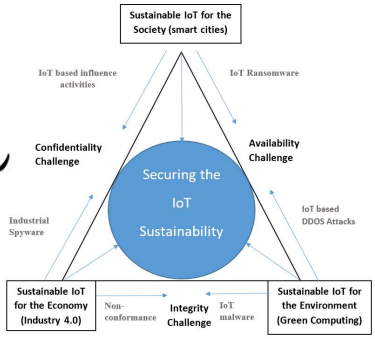
- The creation of a secure and trusted relationships between devices, systems, data, and people.
- Secure and Personalized services based on IoT and Digital Identity Management.

34

Conclusion



Thank You



POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

National Defence

CRIM

UNIVERSITÉ LAVAL

Université de Montréal

Économie et Innovation Québec

Public Safety Canada
publicsafety.gc.ca

UNIVERSITÉ Concordia UNIVERSITY

CONCORDIA UNIVERSITY OF EDMONTON