UNVERISTÁ DEGLI STUDI
DI SALERNO

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Certifying IoT Data with Verifiable Credentials

22nd International Symposium on Network Computing and Applications

Carlo Mazzocca[1], Stefano Allevi[2], Rebecca Montanari[2]

[1]University of Salerno

[2]Univeristy of Bologna

Motivation: Trust External Data

IoT devices are among the **leading contributors** to data generation → **data gains value** only when utilized for insights, applications, and facilities

Companies and organizations are interested in **using data from various domains**

necessary infrastructure

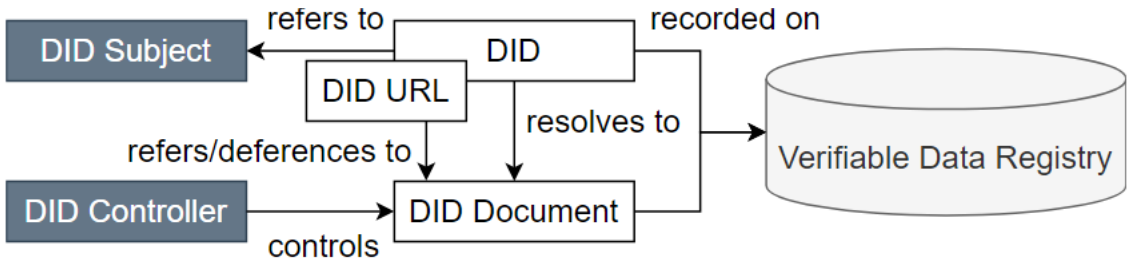
trust data

Identity of Things (IDoT)

We need to **identify trustworthy devices**

Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) hold the potential to **revolutionize digital identification**

- DID is a global identifier that **uniquely identify** entities → key pair (pk, sk)
- VC is an interoperable data structure capable of **representing claims** that are cryptographically verifiable



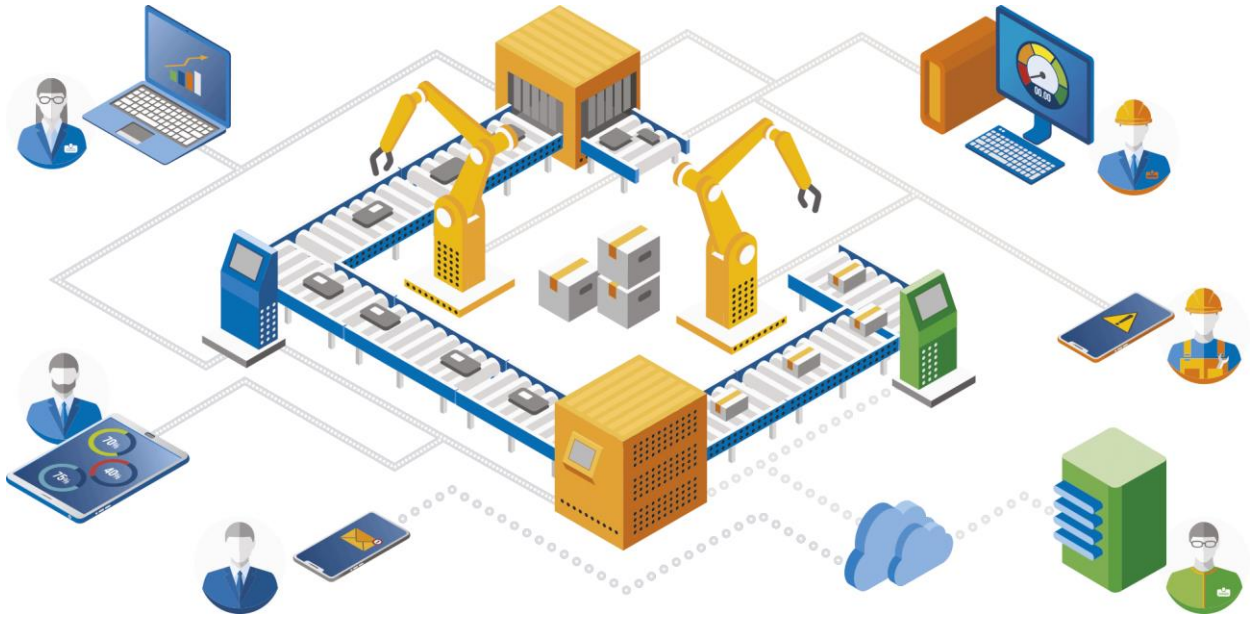
did:example:123456789abcdefghi

```
{
  "@context": [
   "https://www.w3.org/ns/did/v1",
   "https://w3id.org/security/suites/ed25519-2020/v1"
]
"id": "did:example:123456789abcdefghi",
"authentication": [{
  "id": "did:example:123456789abcdefghi#keys-1",
  "type": "Ed25519VerificationKey2020",
  "controller": "did:example:123456789abcdefghi",
  "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZp..."
  }]
}
```

VCs and IoT

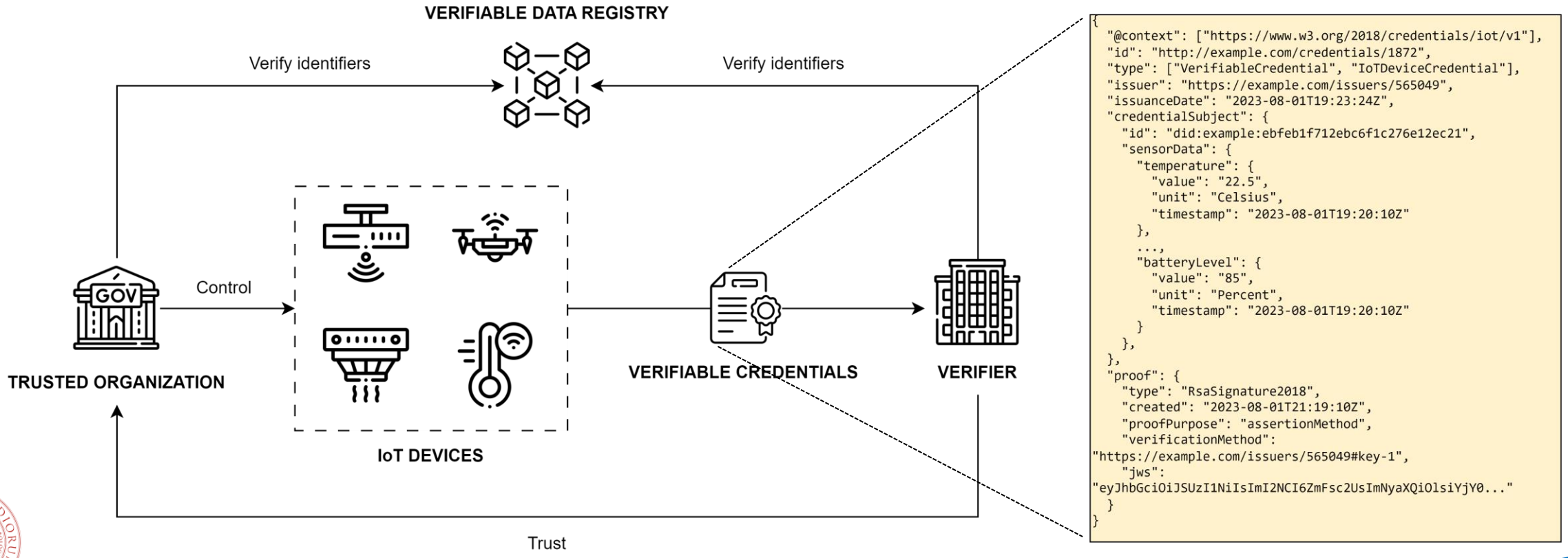
As VCs allow proving authenticity over certain attributes (e.g., device properties), they have mainly employed to establish mutual trust

However, they can be leveraged by IoT devices to **directly certify** their **data**



Data Certification

We assume that IoT devices are controlled by **trusted organizations** → provide devices with a DID and corresponding keys



Threat Model & Security Analysis

Unauthorized Data Modification: An adversary may intercept data and alter it to provide false information

Mitigation: VCs are signed with the sk of the issuing device. This also prevents *spoofing attacks*

Replay Attacks: Present outdated data

Mitigation: Include nonce or timestamps

Privacy Breaches: Expose sensitive data to unauthorized parties

Mitigation: Employ encryption mechanisms and selective disclosure techniques

Evaluation

We used two boards from FIT IoT-LAB[1]

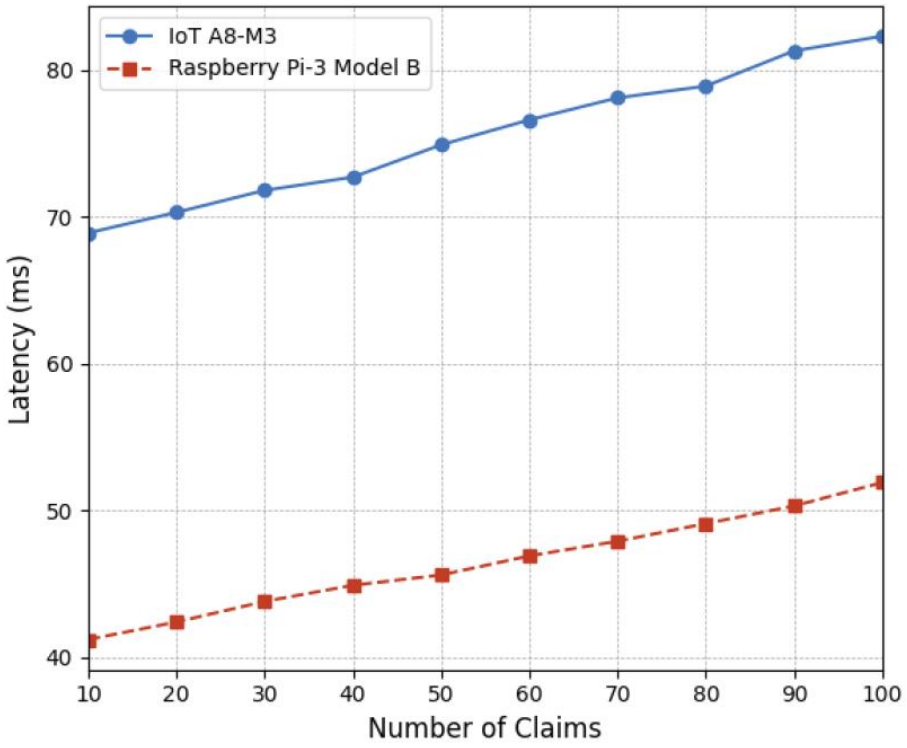
- **Raspberry Pi-3 Model B**: 4 ARM Cortex-A53 and 1GB of RAM
- **IoT Lab A8-M3**: 32-bit CPU and 256 MB of RAM

We varied the amount of data within VCs from 10 to 100 with step 10

[1]https://www.iot-lab.info/

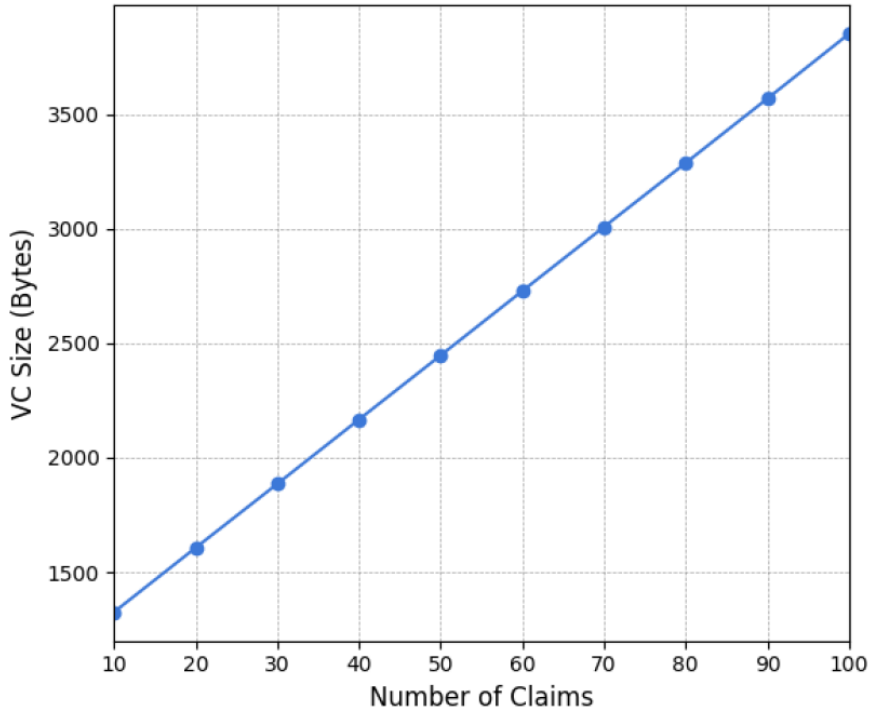
https://github.com/Allevs01/VCIoT.git

Some Results



MEMORY AND CPU USAGE VARYING THE NUMBER OF CLAIMS WITHIN VC.

Platform	Usage %	Number of Claims									
		10	20	30	40	50	60	70	80	90	100
Raspberry Pi-3 Model B	CPU	22.2	22.2	22.2	22.2	22.2	23.1	27.8	27.8	31.6	31.6
	MEM	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
IoT A8-M3	CPU	39.6	41.4	40.0	45.0	46.0	47.6	49.3	48.6	47.3	52.6
	MEM	4.1	4.1	4.1	4.1	4.1	4.2	4.2	4.3	4.2	4.3



constrained devices can directly certify data

limited storage and network overhead

Conclusion

- We evaluated the feasibility of IoT devices to **directly certify their data** through VCs

- We implemented a proof-of-concept and made it available to the research community

Future Work:

  - Extend our evaluation to a broader range of IoT platforms
  - Assess selective disclosure mechanisms
  - Evaluate the energy consumptions of VC-based data certification