TAPShield: Securing Trigger-Action Platforms against Strong Attackers

Mojtaba Moazen Nicolae Paladi Adnan J.Ahsan Musard Balliu

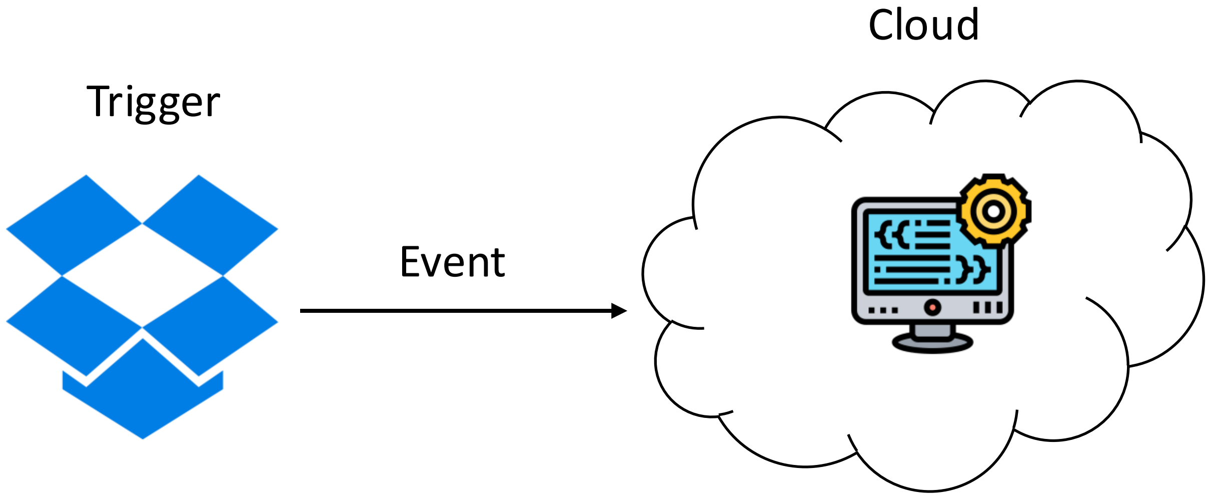
IEEE European Symposium on Security and Privacy (Euro S&P)

July 2025

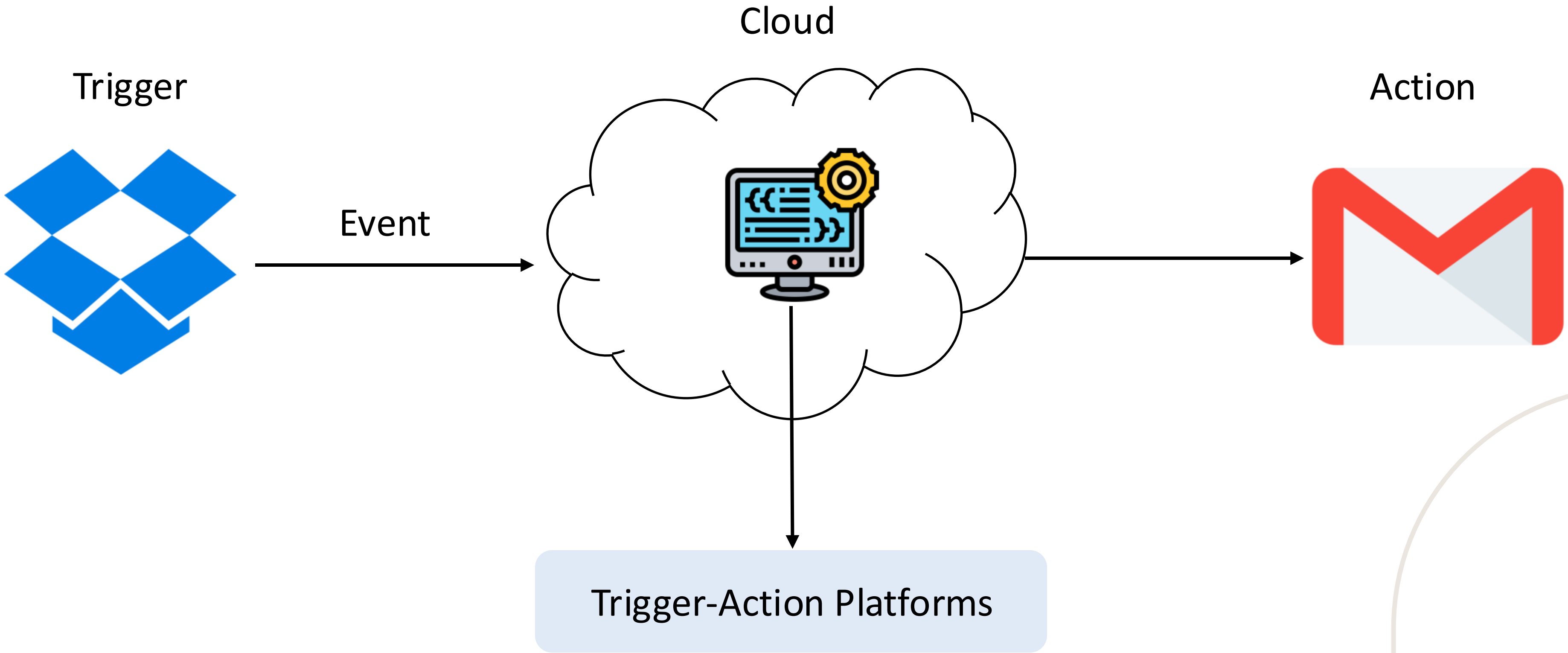
Trigger-Action Platforms

Trigger

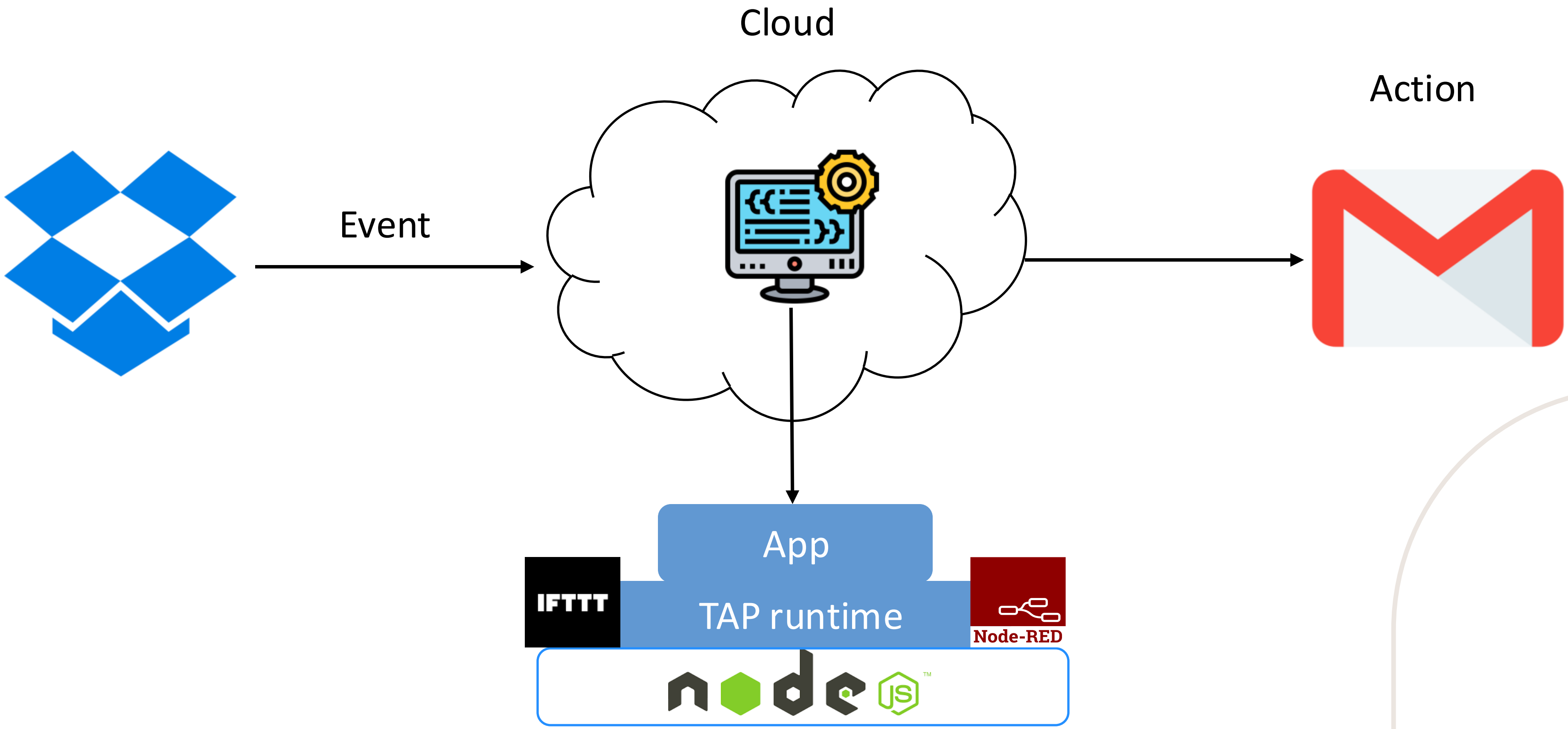
Trigger-Action Platforms



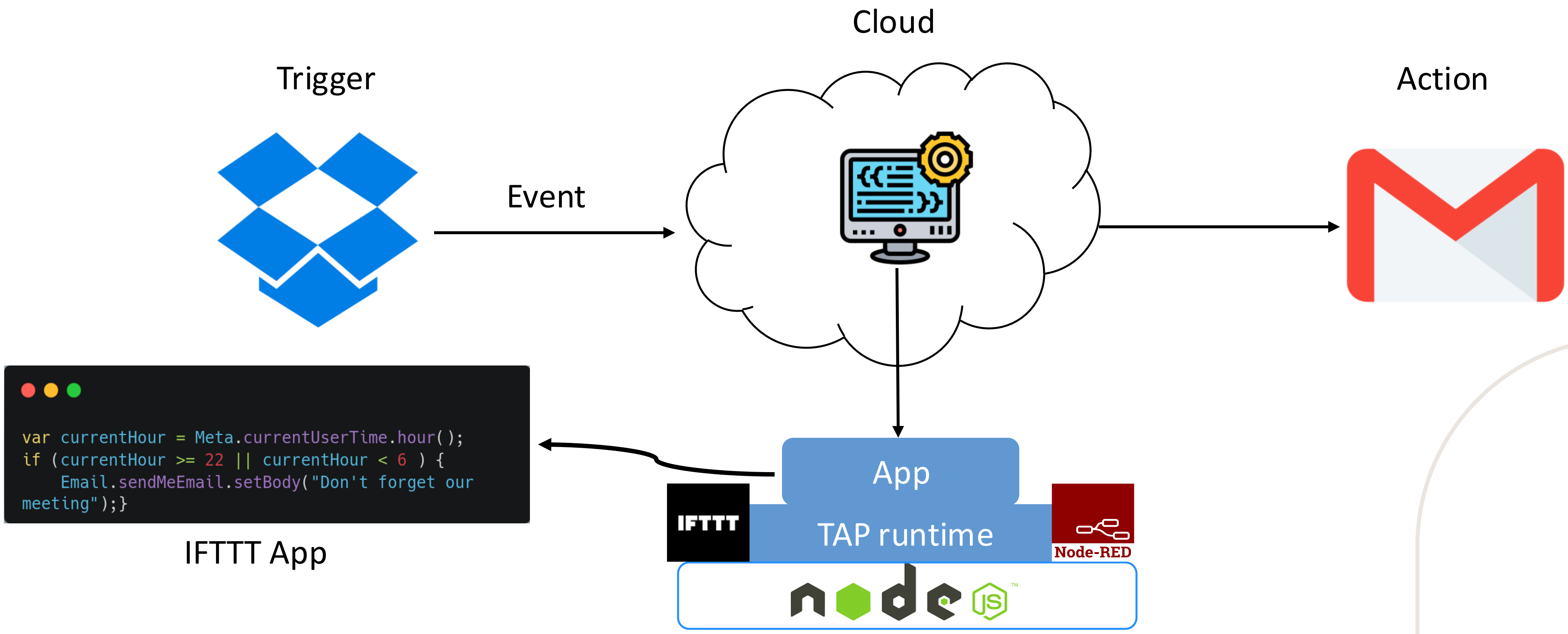
Trigger-Action Platforms



Trigger-Action Platforms



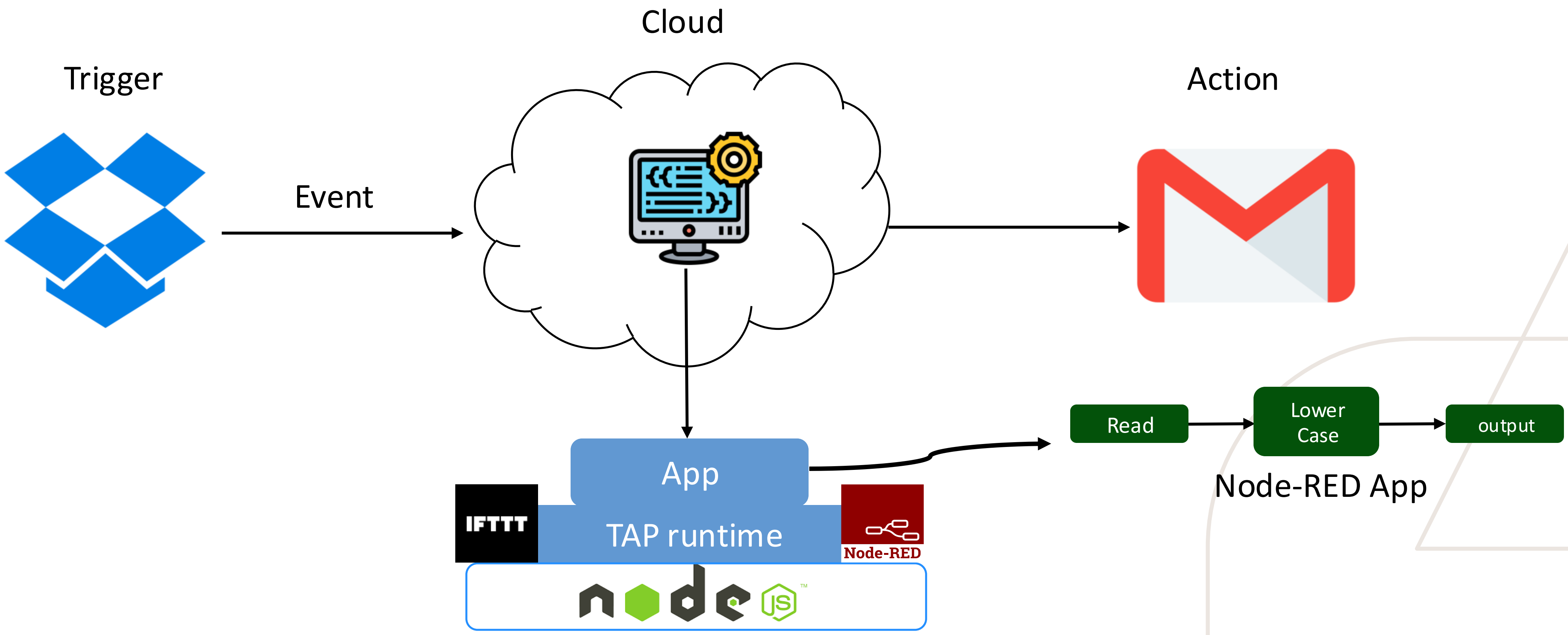
IFTTT App



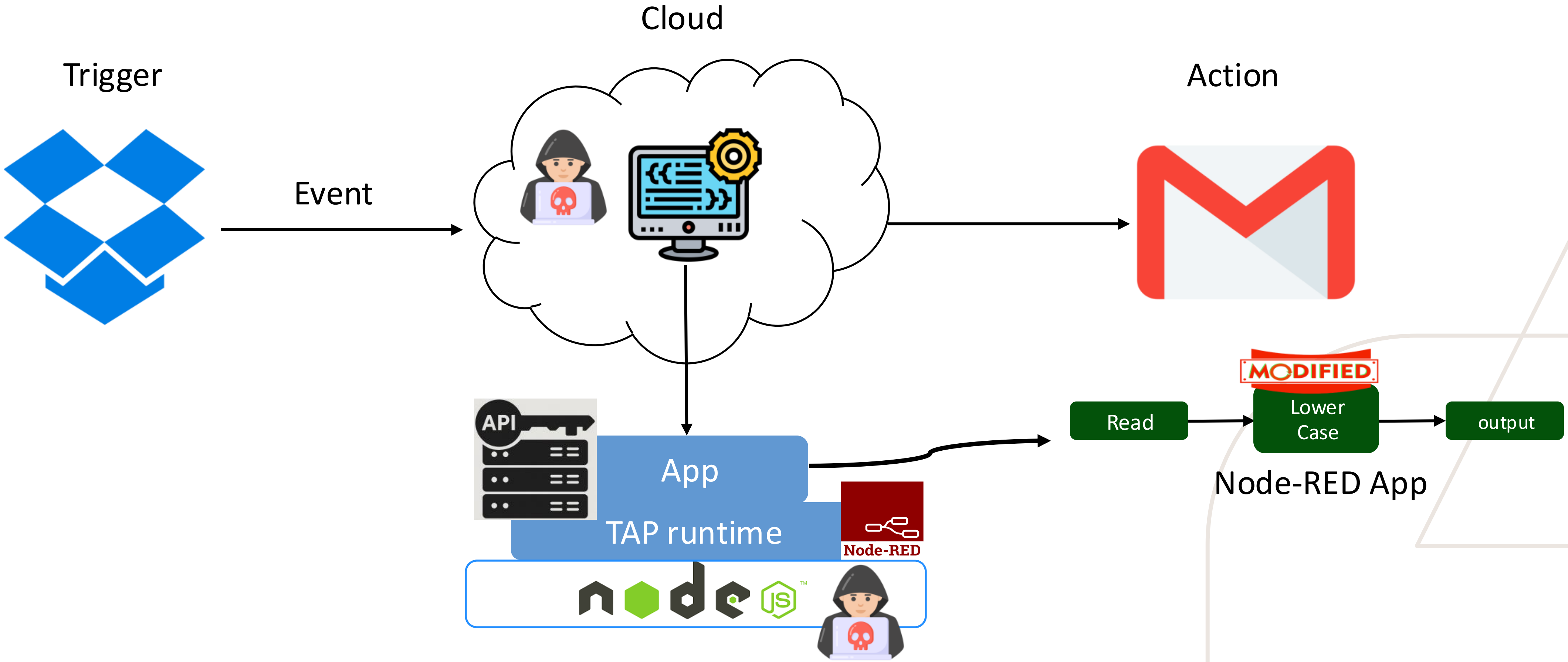
```
var currentHour = Meta.currentUserTime.hour();
if (currentHour >= 22 || currentHour < 6 ) {
    Email.sendMeEmail.setBody("Don't forget our
meeting");}
```

IFTTT App

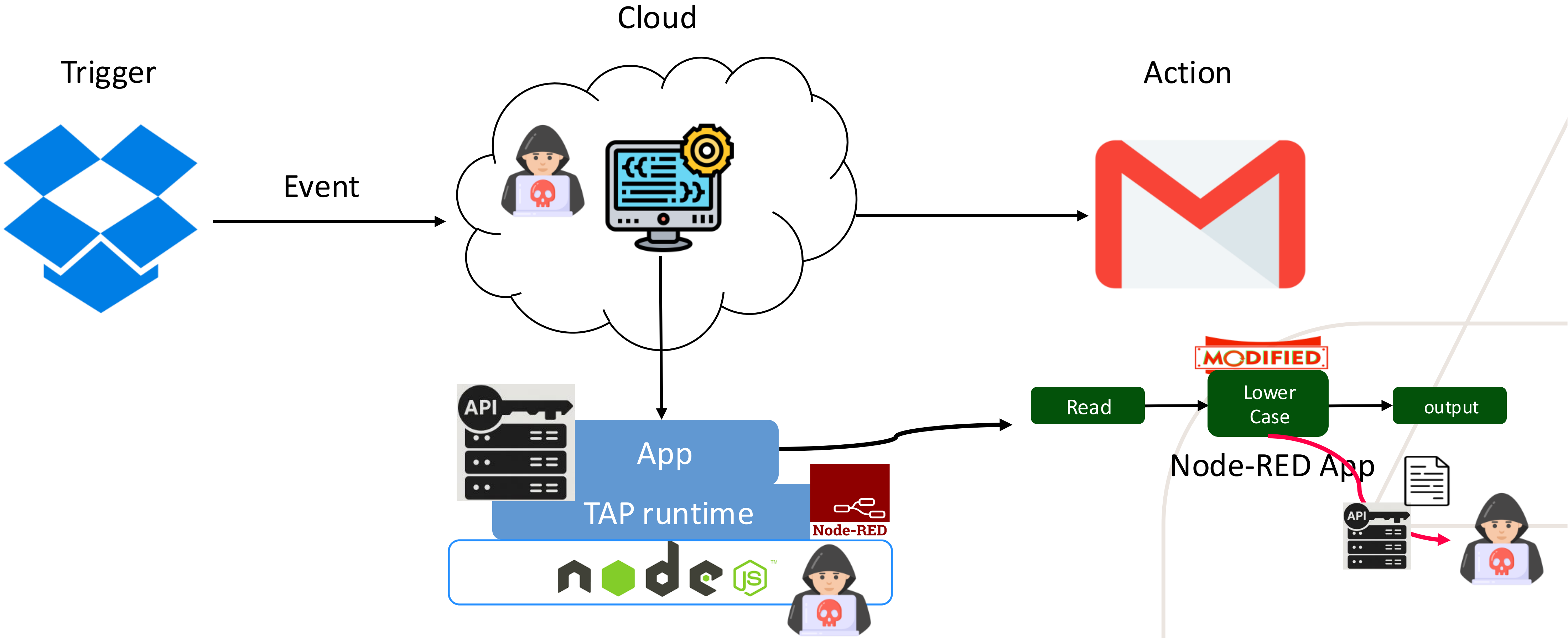
Node-RED App


Cloud
Trigger
Action
Event
App
IFTTT
TAP runtime
Node-RED
node
JS
Read
Lower Case
output
Node-RED App

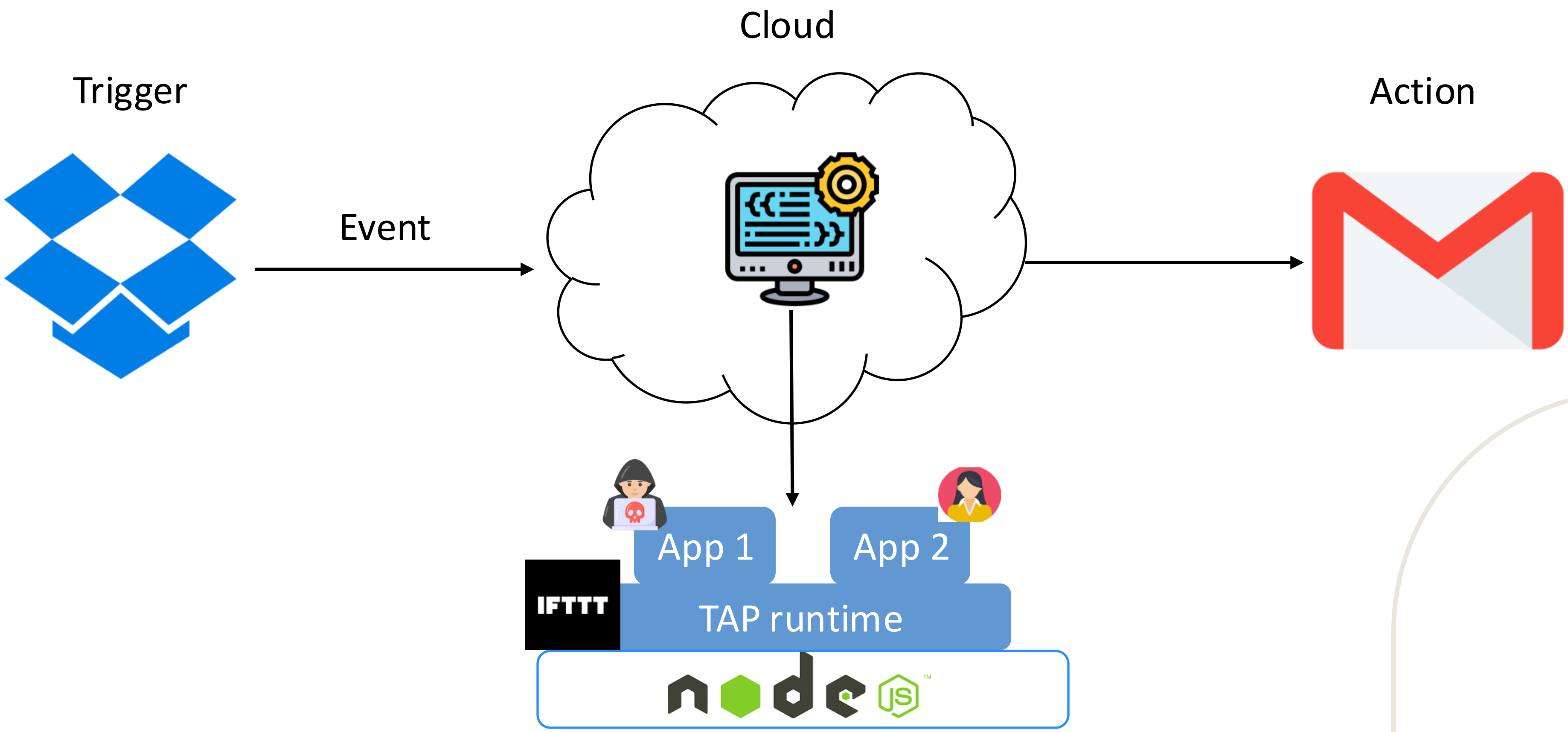
Attacker Models: Cloud-Level Attacker



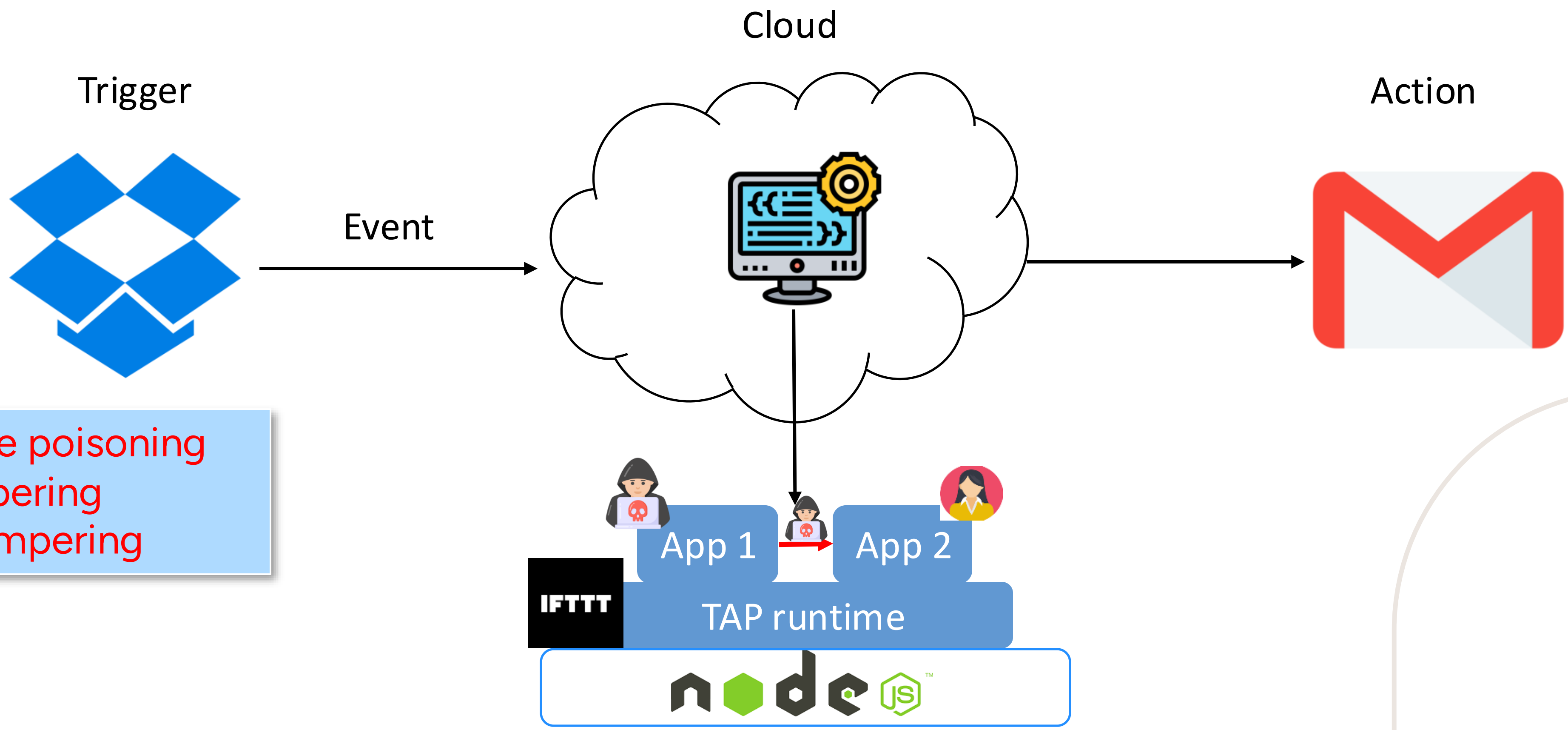
Attacker Models: Cloud-Level Attacker



Attacker Models: App-Level Attacker



Attacker Models: App-Level Attacker



- Prototype poisoning
- API Tampering
- Value Tampering

Research Questions

- **RQ1:**

How to secure TAPs from cloud and app-level attackers?

Cloud-level:

Isolation between host OS and app runtime

- Trusted Execution Environment (TEE)

Verify the runtime integrity:

- Remote Attestation

App-level:

Isolation between apps in TAP runtime

- JavaScript Sandboxing

- **RQ2:**

How to evaluate the solution's benefits in **security**, **performance**, and **compatibility**?

TAPShield Design

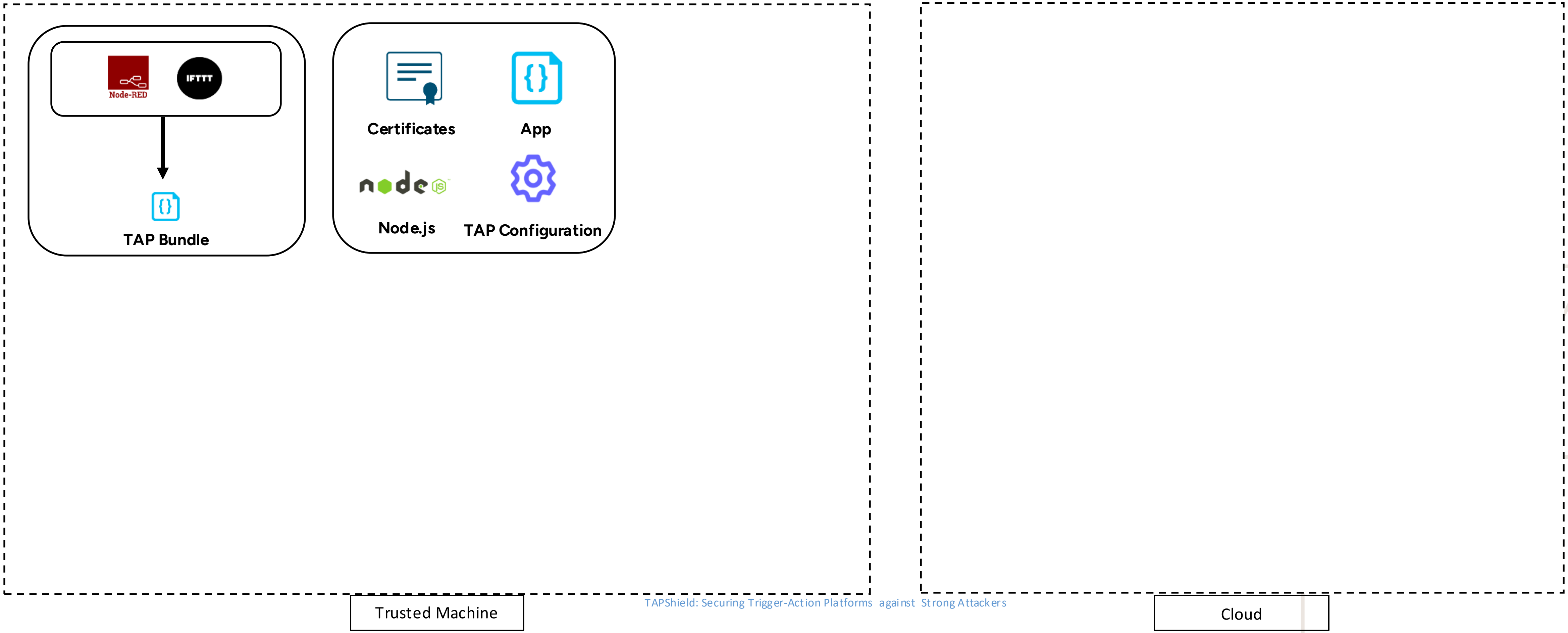
- Securing TAPs against both Cloud and App-level attacker model

Trusted Machine

Cloud

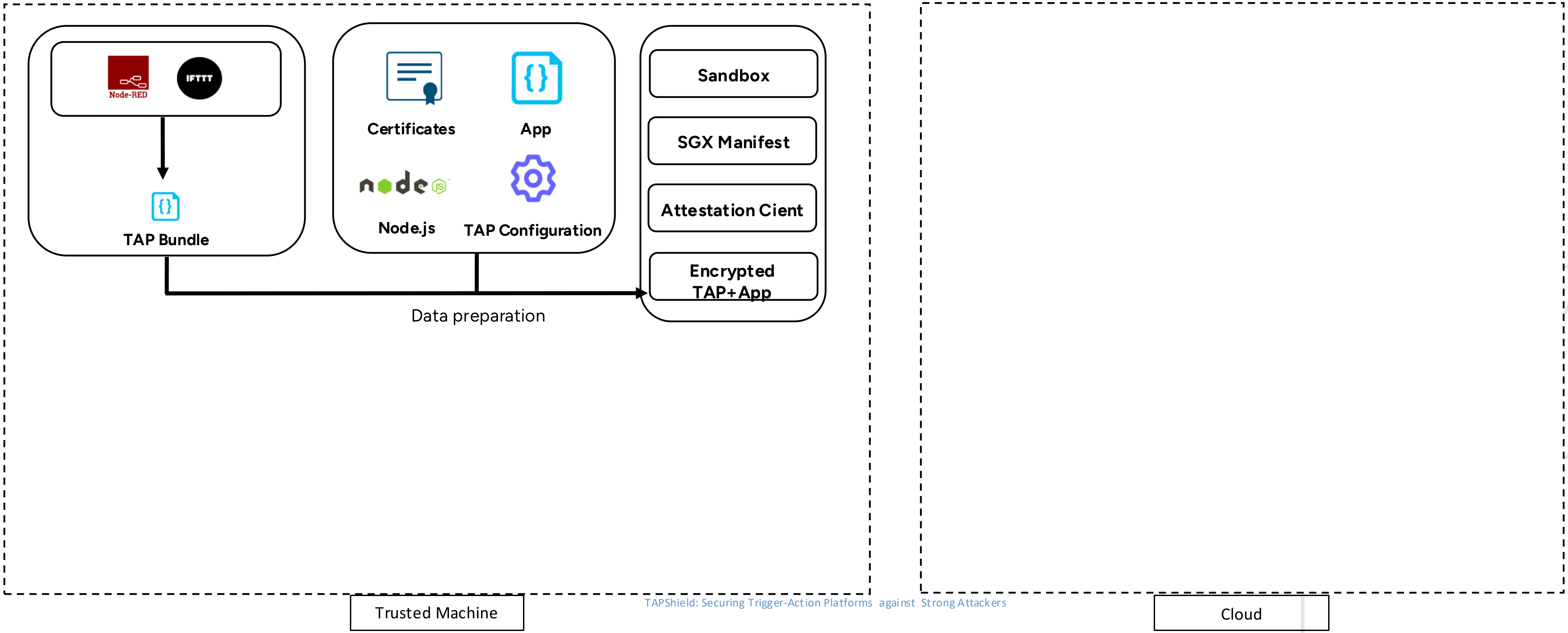
TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



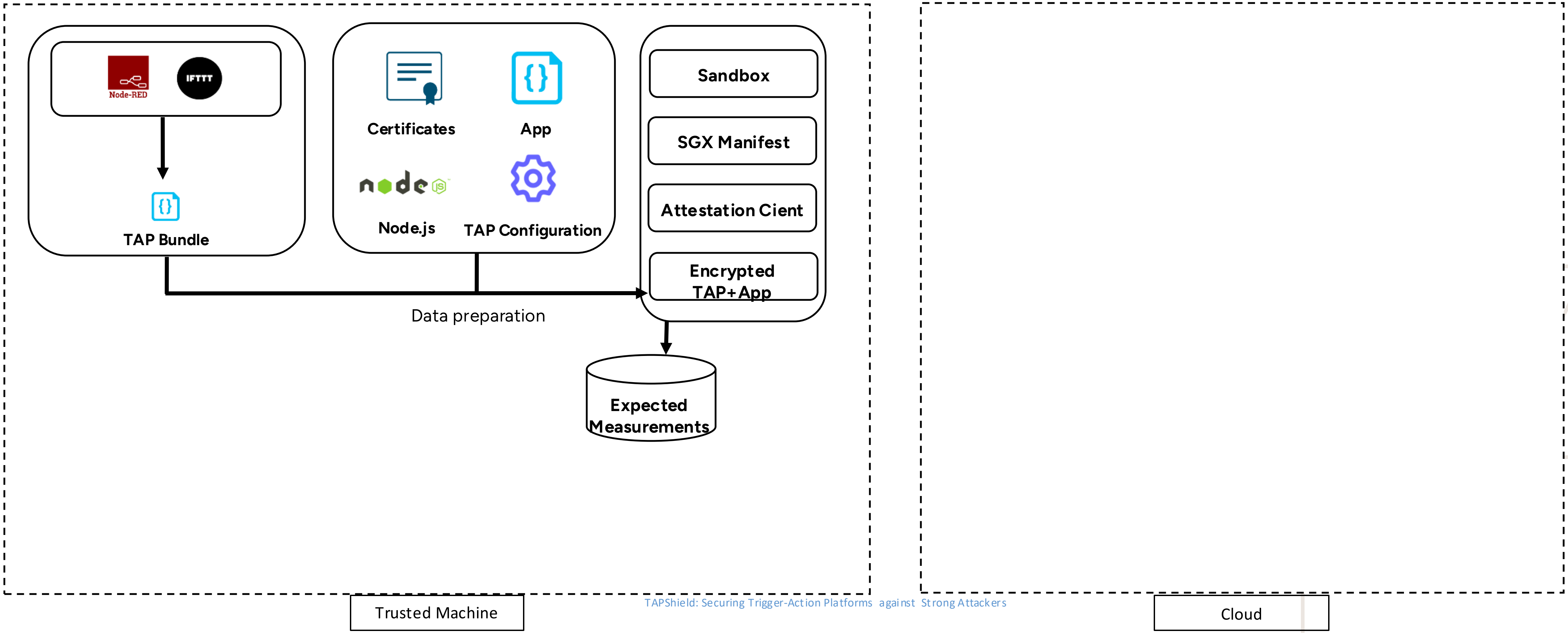
TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



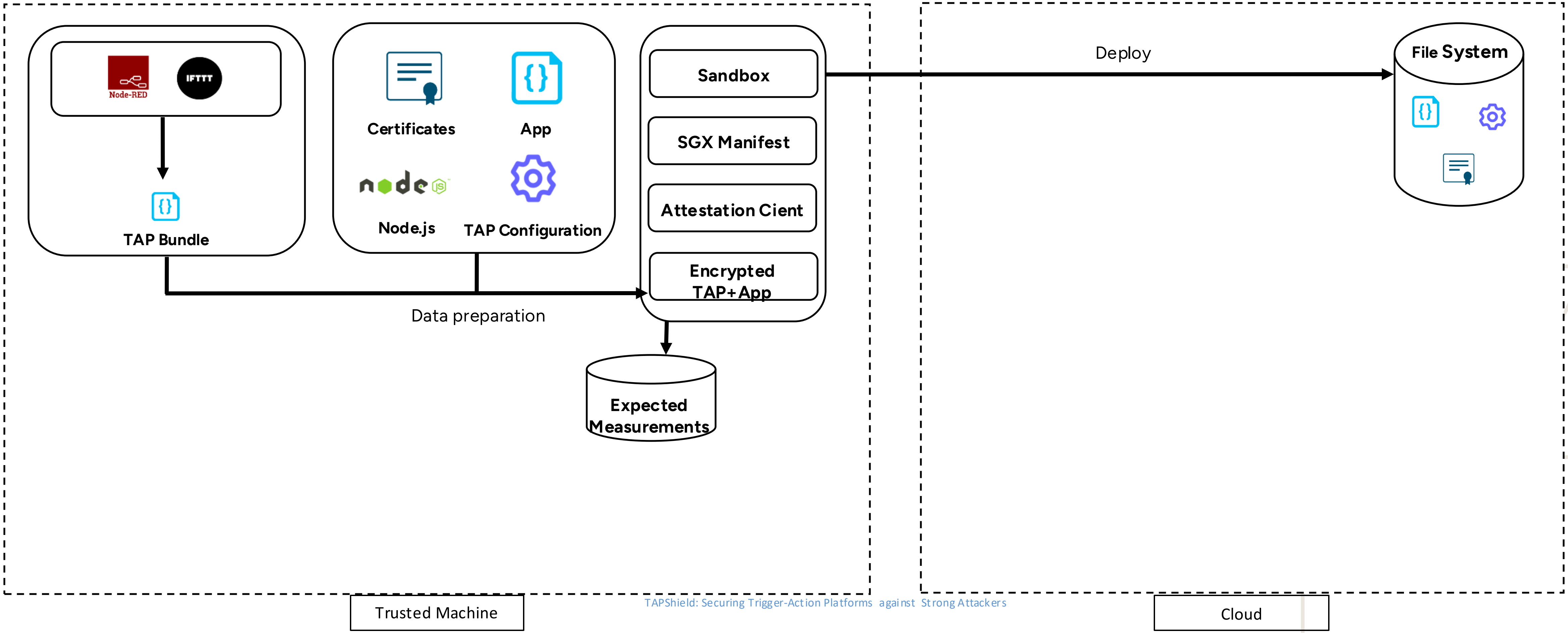
TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



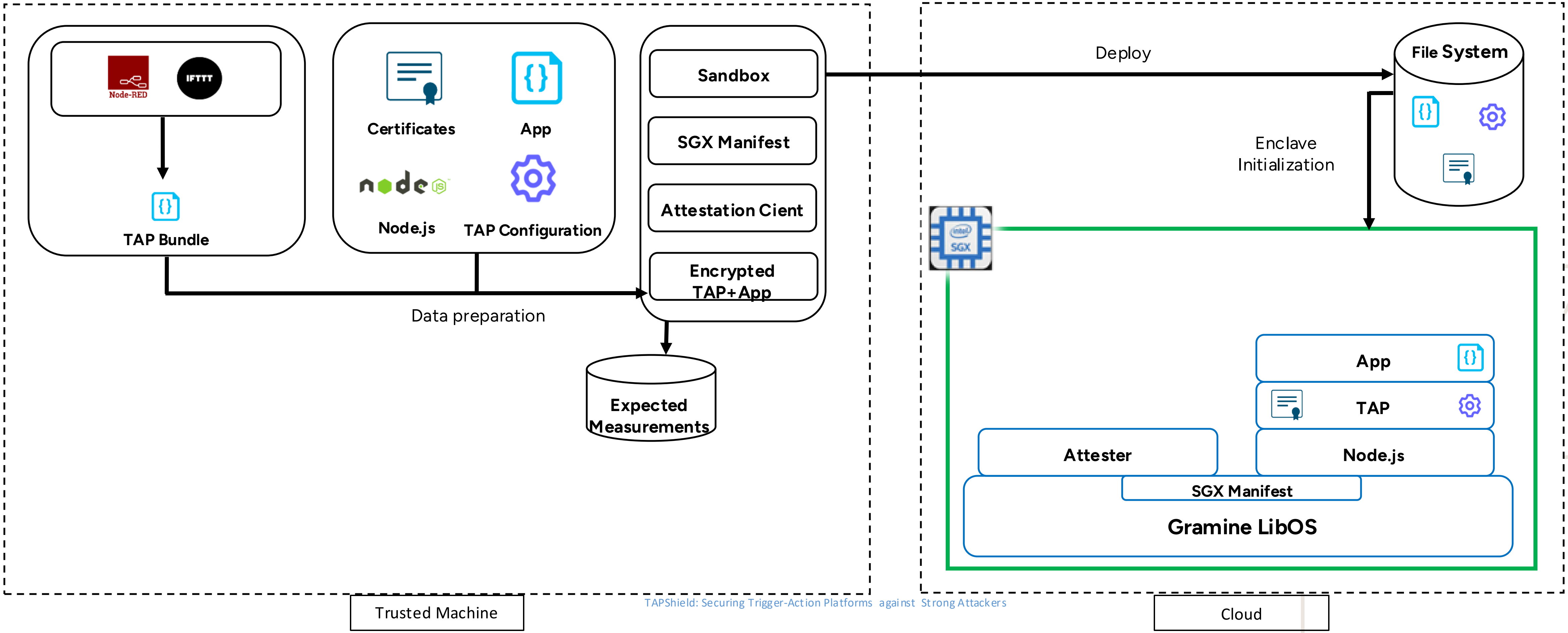
TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



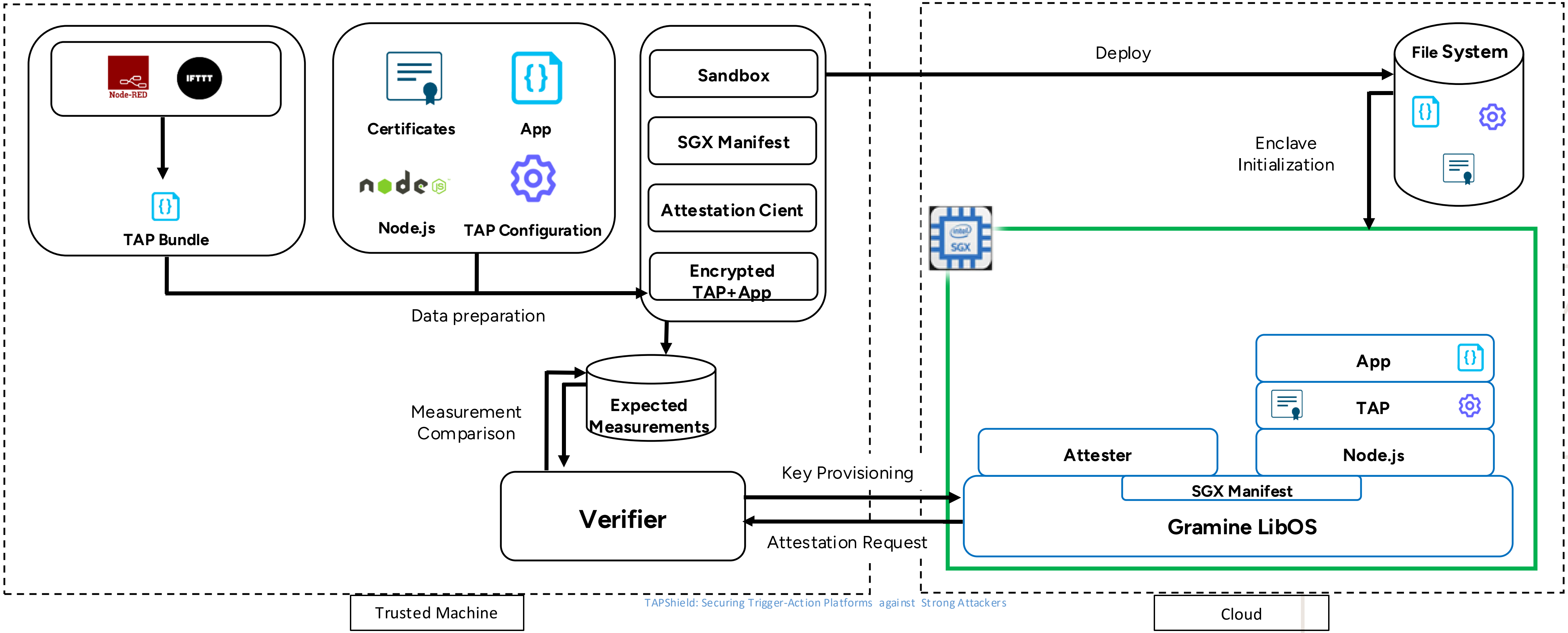
TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



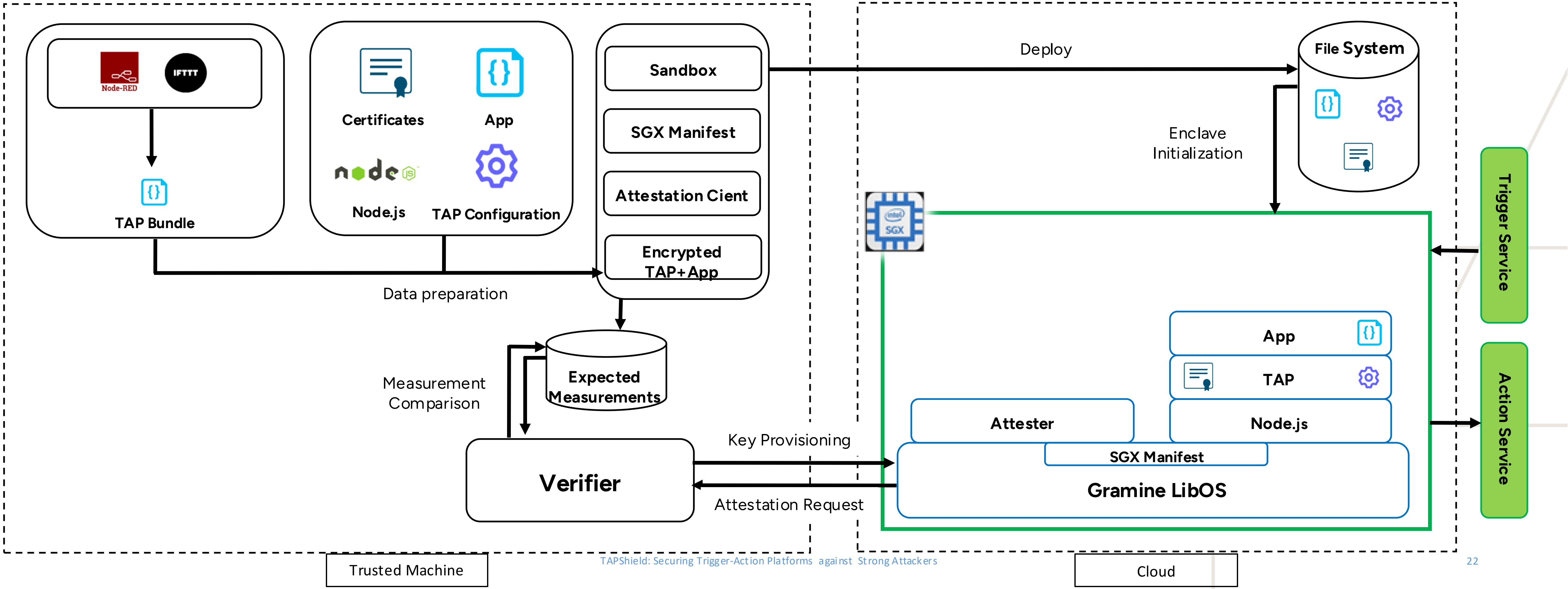
TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



TAPShield Design

- Securing TAPs against both Cloud and App-level attacker model



What are the Security and Privacy benefits ?

- **Node-RED**

- 10 Most popular flows in community are randomly selected
- We design two types of attacks as PoCs and verify the protection against those
  - **Leak sensitive information of app e.g. API Keys of Trigger and Action**
  - **Modify the functionality of apps after deployments**

- **IFTTT**

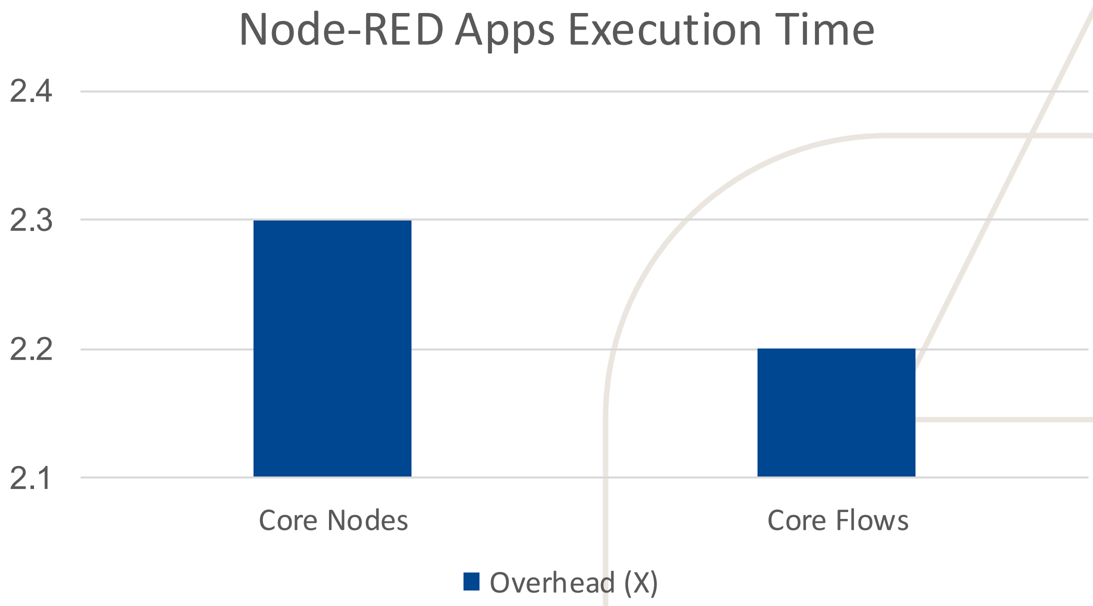
- We evaluated TAPShield **against 30 IFTTT apps including 20** most popular apps in 2024
- Attacks are designed based on **both attacker models w.r.t multi-tenant structure of IFTTT**

- TAPShiled effectively protects against both Cloud and App-level attacker for all attack scenarios

What is the performance overhead ?

- **Node-RED core flows**
- **114** flows are experimented in this evaluation
- **Node-RED core nodes**
- **12** most popular nodes in Node-RED

- Results show 2.2x overhead
- Average execution time: 1.8ms

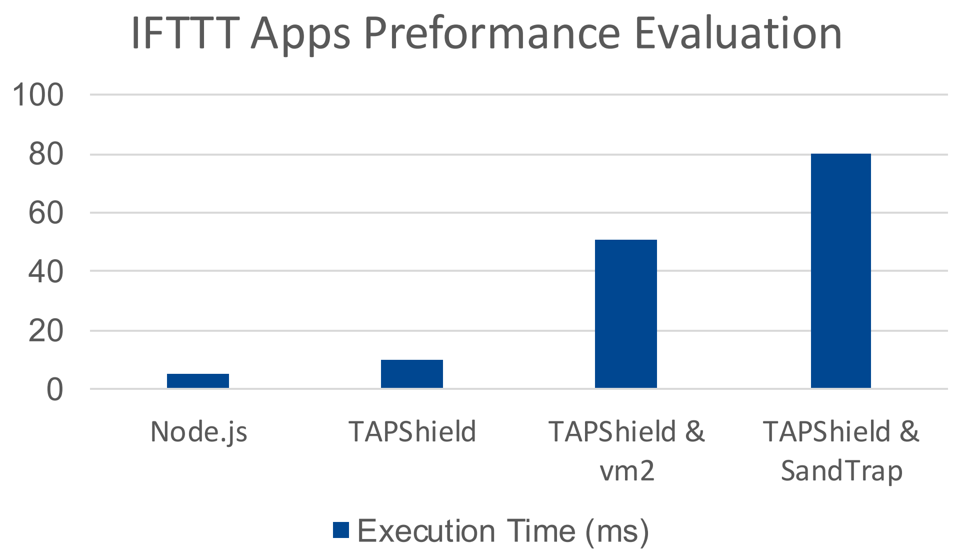


What is the **performance** overhead ?

- **IFTTT**

- We evaluated the execution time of **30 IFTTT apps** with TAPShield
- We evaluated with both **SandTrap and Vm2**

- Results shows a high overhead when we secure apps against both attacker model
- This overhead is **acceptable** given **IFTTT Pro/Pro+** users have a **5-minute** polling interval



To what extent is this approach **compatible** with real-world apps?

- **Node-RED**

- Identifying 5 Most-Dependent Upon flows in Node-RED Community
- Dependent Upon flow : **A flow which is dependent on more Nodes**
- **More nodes cause more computation at runtime and therefore more overhead**

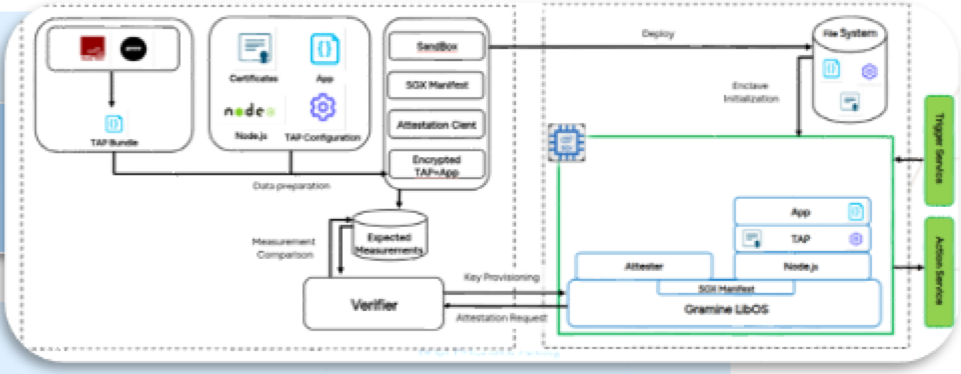
Flow Name	Specification	Number of Nodes	Number of Unique Nodes
Monitoring URL	Web app for testing URLs and endpoints	**206**	**23**
Weather Database	An app to store various weather utilities in MySQL	**100**	**10**

- **IFTTT**

- 50 random IFTTT apps are selected from **prior research and IFTTT website**

- TAPShiled is compatible with real world apps for Node-RED and IFTTT
- **Seamless execution** without any limitation

TAPShield Takeaways



- **Security**

- Securing Node-RED and IFTTT against two attacker model
- Seamless deployment for developers

- **Evaluation**

- Ensure **secure** application execution by protecting against **confidentiality** and **integrity** attacks
- Acceptable **performance** overhead
- **Compatible** with **real-world** applications developed by the community

Source Code

Contact