On Securing Cloud-Hosted Cyber-Physical Systems Using Trusted Execution Environments

A.M. Naseri, W. Lucia, M. Mannan, A. Youssef

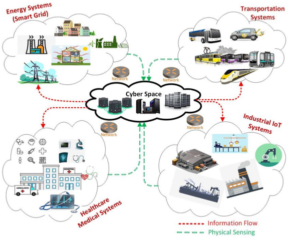
ICAS2021, Montreal, Canada

Outline

Cloud-Hosted CPSs

What is a Cyber-Physical System (CPS)?

- CPS is the term used to denote physical systems equipped with computation and communication capabilities.
- From a control point of view, CPSs can be modeled as networked control systems that can be compromised by cyber-attacks.

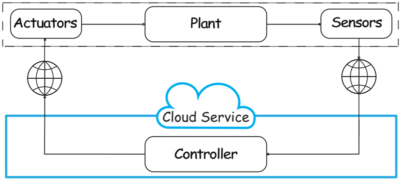


[1]

[1] Hassan, M.U., Rehmani, M.H. and Chen, J., 2019. Differential privacy techniques for cyber physical systems: a survey. IEEE Communications Surveys and Tutorials, 22(1), pp.746-789.

Cloud-Hosted CPSs

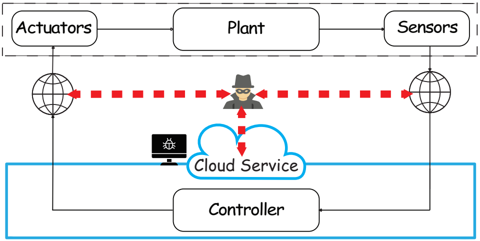
- **Setup:** The controller is implemented on a cloud service.
- **Advantages:**
  - High Computational Power
  - Wide Range of Availability
  - Setup and Maintenance Cost Reduction
- **Disadvantages:**
  - Security and Privacy of Cloud and Communication Channels



Problem Formulation

Cloud-Hosted CPSs - Vulnerabilities

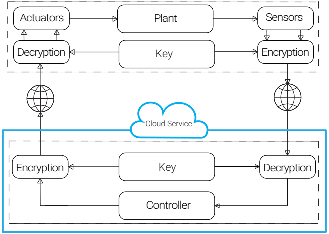
- Communication Channels Vulnerabilities
  - Eavesdropper on the Communication Channel
  - Modify Transmitted data on the channel
- Cloud Service Vulnerabilities
  - Insider/Outsider Attackers
  - Malware Infected Cloud



Existing Solutions

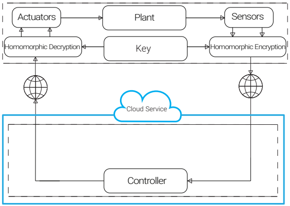
Encrypted Control Systems Using Conventional Cryptosystems

- Advantages:
  - Confidentiality of the channel is guaranteed.
- Disadvantages:
  - Cloud-service attack scenarios still feasible.
  - Key should be stored on the cloud.
  - Extra computational load for encryption/decryption.



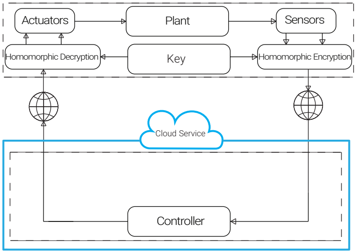
Encrypted Control Systems Using HE (1/2)

- Advantage:
  - Perform arithmetic operations on encrypted data.
  - Confidentiality of the channels is guaranteed.
  - There is no need to store the key on the cloud.
- Disadvantages:
  - Homomorphic Encryption Malleability.
  - Ciphertext expansion and extra communication load.
  - Confidentiality of the control logic can be violated.



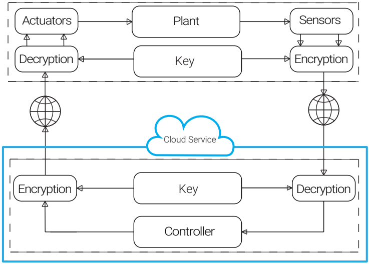
Encrypted Control Systems Using HE (2/2)

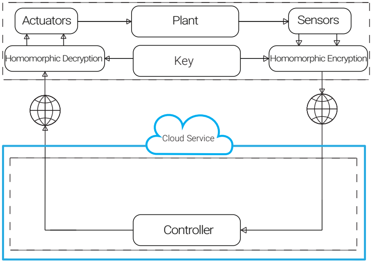
- Disadvantages (Cont.):
  - Control logic design is limited by the number and type of operations supported by the HE.
  - Advanced control strategies might require a re-design.



Effectiveness of Existing Solutions

- Limitations in terms of security/privacy/deployability.
- Still vulnerable against cloud-service attacks.





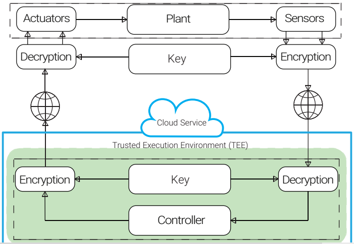
Proposed Security Solution based on TEE

Proposed Architecture

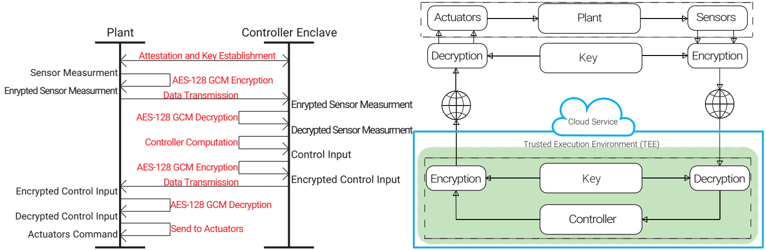
- The objectives of our proposal:
    - Secure the cloud-based CPSs against all the cyber-threat discussed.
    - Reduce the impact on the design and implementation of existing control strategies.
- For these purposes, we utilize: A Trusted Execution Environment (TEE).
    - A hardware-based solution, which provides an isolated environment to keep data and run code.
    - Any unauthorized access to the isolated environment is not possible, even by the operating system(OS).
    - It is assumed to be secure against any insider/outsider attacker, malware, or even a compromised OS.

Implementation

- TEE: Intel Software Guard Extension (SGX)
  - Provides a cryptographic attestation to ensure the integrity of control algorithm.
  - To keep code, data, and encryption key; SGX provides an isolated environment called "Enclave."
- AES-128 Galois/Counter Mode (GCM)
  - High throughput
  - Low latency



Closed-Loop Control System Flow with TEE



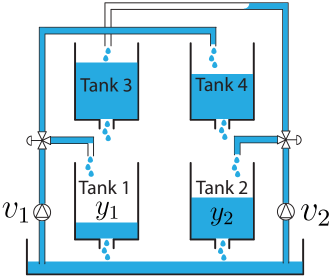
Security Analysis

- *Confidentiality*:
  - Encrypted data are sent over the channels.
  - The control algorithm, encryption/decryption operations are performed inside an enclave.
- *Integrity and Authentication*:
  - AES-128 GCM MAC tag ensures secure and authenticated communications.
  - Intel SGX attestation mechanism ensures control logic integrity

Experimental Results

Test Bed Setup

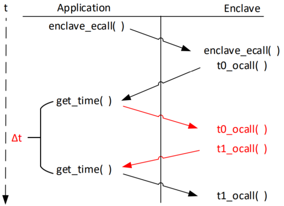
- Outside SGX:
  - Test Bed: Quadruple Tank Process.
- Inside SGX:
  - The LQG[1] controller implemented on the cloud and inside Intel SGX.



[1] Composed of a Kalman Filter + Linear Quadratic Controller

Measurements

- For simulation and time measurements we utilized an Intel Core i7-6700 CPU, which supports Intel SGX.
- Sampling time of the system is $T_s = 0.1sec$
- Measurements are an average time for 1000 times repeat of each operation.
- Δt is the additional introduced overhead.
- The average total CPU time required by both of the with SGX and without SGX implementations are $466.7+1.8+1.4+435.4 = 905.3\mu s$ and $466.7+1.8+1.4 = 469.9\mu s$



Operation	Time (μs)
Dynamic output feedback controller	466.7
AES-128 GCM encryption	1.8
AES-128 GCM decryption	1.4
Δt	435.4

Conclusion

Conclusion

- We proposed a solution to secure cloud-hosted/edge-hosted CPSs.
- The proposed networked control scheme is secure again different attacks against its security and privacy.
- The effectiveness of such a scheme is verified by means of numerical simulations.
- The obtained results show good promise in terms of real-time performance in CPSs applications.
- The proposed solution can also be implemented in a non cloud setting to help mitigating supply chain breaches.

Thank You!