DEVELOPMENT AND EXAMINATION OF FOG COMPUTING- BASED ENCRYPTED CONTROL SYSTEM

U.Guru Swamy, PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP
T.Anil Karuna Kumar, Assistant Professor, Dept. of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP

Abstract

This letter develops a fog computing-based encrypted control system in a practical industrial setting. The developed system conceals controller gains and signals over communication links using multiplicative homomorphic encryption to prevent eavesdropping attacks. Experimental validation confirms the feasibility of position servo control for the motor-driven stage with the developed system in terms of performance degradation, parameter variation, and processing time. The developed system inherits its stability regardless of whether plant parameters fluctuate or not even after the controller gains and signals are encrypted. Furthermore, although processing time becomes longer by increasing a key length of encryption, degradation of control performance is improved simultaneously.

Keywords: Networked Robots, Robot Safety, Motion Control, Encrypted Control, Fog Computing.

Introduction

Cloud-Based control systems, in which controlled devices are connected to a communication network to be monitored and controlled in the cloud, are gaining popularity. Control as a Service (CaaS) for automotive control, a cloud based control concept, was proposed in. The authors of introduced Robot Control as a Service. This concept also realizes higher-layer control (e.g., motion planning) for industrial robots. Rapyuta cooperating with Robo Earth is Platform as a Service (PaaS) for cloud robotics applications. The main advantage of these architectures lies in their improved flexibility, scalability, and efficiency over conventional networked systems. On the other hand, lower-layer control (e.g., servo control of actuators) still needs local execution, and a cloud architecture is not suitable for such control because of latencies between controlled devices connected to the cloud. This issue can be solved by fog computing, which a decentralized computing architecture with an intermediate layer is called fog. Fog computing-based control systems reduce communication delay and retain the advantages of cloud-based control systems, that is, the controller does not need to be installed locally, and operators can remotely monitor the plant condition and easily change the control law. Additionally, the fog aggregates and cleans dirty data to support analytics in the cloud. Fog computing offers many potential benefits, especially for real-time applications, although security and privacy issues in the fog persist similar to the case of the cloud . Attacks on cyber-physical systems, such as networked control systems, are more damaging than attacks on information systems because physical systems can directly affect real environments. Adversaries can eavesdrop, invade, and falsify the system if security measures have not been implemented sufficiently. The authors of verified the risks of manipulators by actual attacks, which tamper with controller gains. It is critical to obfuscate controller gains and to conceal signals from the attacks. Encrypted control, a fusion of cryptography and control theory, is a promising methodology to improve the security of control systems by reducing risks of eavesdropping attacks. Eavesdropping attacks aim to steal information of control systems in order to execute more severe attacks, such as zero dynamics attacks, in the future. In encrypted control systems using ElGamal encryption, which is multiplicative homomorphic encryption, control inputs are calculated in cipher text from encrypted controller parameters, encrypted sensor data, and an encrypted reference without decryption. Additionally, encrypted control can be applied for the detection of replay attacks and controller or signal falsification attacks .

The encrypted control system with Paillier encryption, which is additive homomorphic encryption was proposed . The authors of provided the signal concealment method with fully homomorphic encryption. Homomorphic encryption is utilized as a security measure in control systems, as noted above. However, it is not straightforward to obfuscate the controller parameters with additive homomorphic encryption because multiplication between two data cannot be executed in cipher text. Furthermore, additive and fully homomorphic encryptions require a large number of computational resources for homomorphic operation. Thus, these encryption schemes are not suitable for lower-layer control of mechanical systems.

Statement of the Problem

This concept also realizes higher-layer control (e.g., motion planning) for industrial robots. Rapyuta cooperating with Robo Earth is Platform as a Service (PaaS) for cloud robotics applications. The main advantage of these architectures lies in their improved flexibility, scalability, and efficiency over conventional networked systems.

On the other hand, lower-layer control (e.g., servo control of actuators) still needs local execution, and cloud architecture is not suitable for such control because of latencies between controlled devices connected to the cloud.

Encrypted control, a fusion of cryptography and control theory, is a promising methodology to improve the security of control systems by reducing risks of eavesdropping attacks.

The encrypted control system with Paillier encryption which is additive homomorphic encryption was proposed.

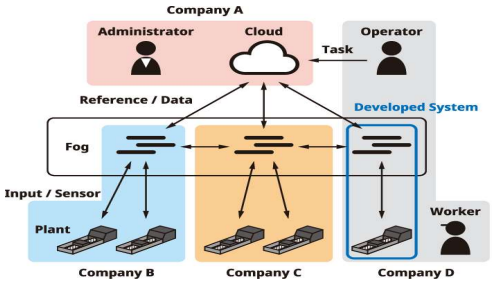
The authors of provided the signal concealment method with fully homomorphic encryption. Homomorphic encryption is utilized as a security measure in control systems.

Objectives of the study

- The developed system conceals controller gains and signals over communication links using multiplicative homomorphic encryption to prevent eavesdropping attacks.
- Experimental validation confirms the feasibility of position servo control for the motor-driven stage with the developed system in terms of performance degradation, parameter variation, and processing time.
- The developed system inherits its stability regardless of whether plant parameters fluctuate or not even after the controller gains and signals are encrypted.

Review of Literature

This letter focuses on developing the fog computing-based control system within the blue frame seen in illustrates the network architecture of the developed system. We use personal computers for a fog-computing environment and the interface between a controlled device and the network. The computers are connected to L2 switches, which in turn are connected to an L3 switch via an Ethernet cable. Additionally, as per the requirements of a logical network, both computers are installed in the same VLAN. The computers communicate with each other by TCP/IP socket communication, and the L3 switch addresses routing decisions. Scientific Linux, which is compatible with RedHat Enterprise Linux (RHEL), is used as the operating system for the computers. The computers are also equipped with the Advanced Robot Control System (ARCS) [30], a framework for real-time computation of the lower-layer control system.

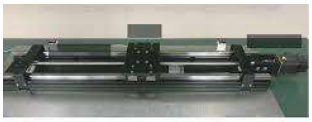


Research Methodology

This section introduces the architecture of the cloud and fog computing-based control system as well as its specifications. Furthermore, a C language library for the encrypted control is described.

Concept: illustrates a concept of the fog computing-based control system with a Public cloud. Company A administrates a cloud infrastructure and provides a platform to operate the higher-layer control. Company B, C, and D manage fog connected to the cloud and each other. Company B and C may be branches of Company D, and they aim to control devices, which include some actuators and are owned by each company. An operator sends tasks for the higher-layer control to an application in the cloud. The application generates reference signals to implement the tasks and transfers them to the fog. The fog decides the input signals from the reference signals and sensor data of the devices in real time. Additionally, the fog handles operating data and transfers them to the cloud. The cloud storages the data and visualizes them with a web interface for the operator.

Specifications: The developed system consists of a motor-driven stage, the plant-side computer, and the fog-side computer. Their specifications are described. Motor-driven stages or linear actuators are major components for factory automation. The stage is moved by an AC servo motor through a slide screw, and the AC motor and the slide screw are connected via a coupling. The AC motor with the attached rotary encoder is driven by the servo amplifier, and we use the servo amplifier as a current controller as it has sufficient control bandwidth. Note that although the developed system uses a slide screw, the security enhancement method in section II can also be applied to a system that uses a ball screw or other linear actuators.



(a) View of the whole plant.

(b) View of the whole plant with a 10 kg load.

C Language Library: This letter also develops a C language library to execute encrypted control. This library contains five functions, Gen, Enc, Dec+, Round and Mult. These functions operate based on BIGNUM library in OpenSSL to address multiple-precision integers. Gen searches a safe prime from a given key length, and then, it generates a public key pk and a secret key sk based on the safe prime. Enc encrypts each element of a matrix or vector by using pk, and Dec+ restores a plaintext vector from an encrypted matrix by using sk. The matrix or vector used in Enc is rounded into a plaintext space by Round; a function that corresponds to Q. Mult calculates the Hadamard product of an encrypted matrix and an encrypted vector. The process in the developed system using the developed C library. The plant-side computer obtains a current position from the rotary encoder through the counter board and the servo amplifier. Then, the plant-side computer converts the current position, reference input, and controller states, which are double-precision floating-point data, into multiple precision integers by using Round. The converted data are encrypted by Enc, and they are sent to the fog-side computer. The fog-side computer decides a control input in cipher text from the encrypted data and encrypted controller parameters by using Mult. Additionally, the fog-side computer returns the cipher text of the control input to the plant-side computer. The plant-side computer decrypts the cipher text by using Dec+, and then, inputs a command voltage into the servo amplifier through the D/A board. Note that Gen should be executed to obtain a key pair before the abovementioned periodic control process, and the encrypted controller parameters should be set in advance.

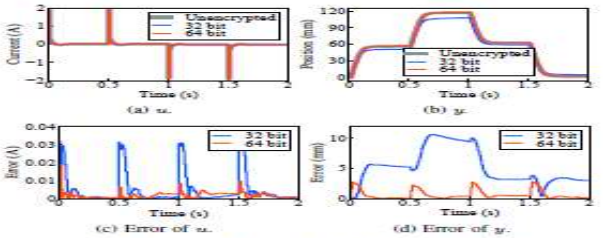
Results and Discussion

This section presents the results of some experiments for validating the developed system. Effect of load fluctuation and real-time computation in the proposed system are also indicated.

Performance Degradation and System Concealment: It is well known that the addition of a quantizer in a control loop decreases the performance of the control system. Thus, the control performance of the encrypted PID control system is expected to be worse than that of a normal PID control system because Q acts as a quantizer. This study includes investigation of the control performance deterioration caused by encryption in order to confirm the practicality of the proposed system. The validations of the gain and signal concealment are also included, and the conditions of this experiment are listed.

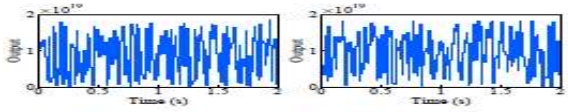
TABLE II
EXPERIMENTAL CONDITIONS FOR ENCRYPTION

Key length	λ	32 bit	64 bit
Scaling parameter for Φ	γ_c	10^3	10^3
Scaling parameter for ξ	γ_p	10^8	10^8



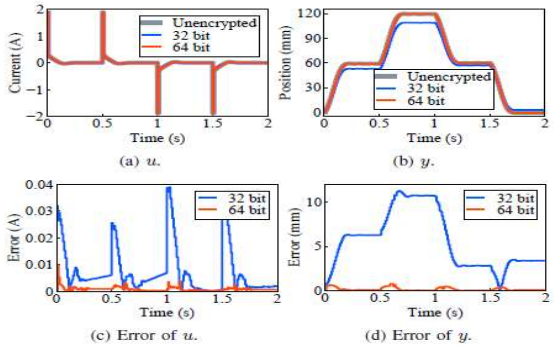
(a) u. (b) y. (c) Error of u. (d) Error of y.

Fig. 5. Comparison between the signals of the encrypted and unencrypted PID controllers.



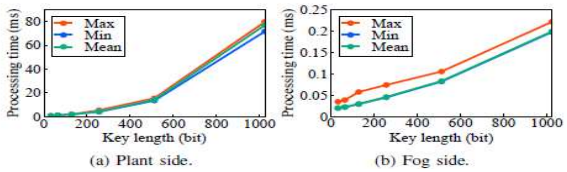
(a) First element of Enc (y). (b) Second element of Enc (y).

Effect of Load Fluctuation: Industrial robots process various tasks by changing their end effector according to the work content. Their model parameters depend on their posture and hand mass. This parameter fluctuation affects the performance of the tracking control and stability of the control systems. Therefore, in order to apply the controller encryption method to the control systems, it is necessary for the encrypted control system to maintain stability under uncertain conditions. This study examines the behavior of the developed system with a 10 kg load on the stage, as shown in Fig. 3(b), by conducting the same experiment as section IV-A. This load fluctuation affects the moment of inertia and the viscous friction of the stage, leading to a change in the time constant.



(a) u. (b) y. (c) Error of u. (d) Error of y.

Fig. 7. Comparison between the signals of the encrypted and unencrypted PID controllers with the load.



(a) Plant side. (b) Fog side.

Processing Time: A key of longer length makes the cipher text stronger. On the other hand, the encrypted controller increases processing time as the key length increases. Hence, the key length cannot be increased indiscriminately because real-time computation is critical for industrial control systems. This study measures the time taken to execute the encrypted control in the developed system with the library, and describes the relationship between the key length and processing time. The key length is changed from 32 bits to 1024 bits, and the processing time, excluding the communication time, is measured 100, 000 times for each key length. Then, the maximum processing time, minimum processing time, and mean processing time are obtained. TABLE III and TABLE IV list the results of the processing time, and Fig. 8 visualizes these results. The times for the plant side increase exponentially with the key length. In contrast, the times of fog side are almost proportional to it. These results indicate that the increase in processing time required for Enc and Dec+ is large compared to Mult. Note that the results cannot be compared with the processing time of other methods because the proposed system is the first implementation of an encrypted control system in the practical setting. Although we need more examination, the results are useful to choose the appropriate key length.

Conclusion

This letter develops a secure fog computing-based control system, which serves as the first implementation of an encrypted control system in an actual industrial setting. The controller gain and signals are concealed against adversaries. The developed system is resilient to eavesdropping attacks and prevents zero dynamics attacks. Thus, the controller encryption method can be employed as a new component of defense in depth for industrial control systems. The experiment results confirm the feasibility of tracking control under load fluctuation and indicate the relationship between the key length and processing time. The results in sections IV-A and IV-B suggest that the controller encryption method is sufficiently practical. From the viewpoint of security level and control performance degradation, the key length should be large. However, the results in section IV-C suggest that the key length is restricted by the processing time, especially the time of encryption and decryption. Therefore, the processes of encryption and decryption need to be implemented in the hardware (e.g., via a field programmable gate array) so that the encrypted control systems can be put to
practical use in a more resource-limited setting.
In future work, we will consider a fog computing-based control system with the cloud for higher-layer control. Additionally, we will implement an attack detection method to prevent DoS attacks, gain falsifications, and replay attacks.

References

1. Y. Xia, “Cloud control systems,” IEEE/CAA Journal of Automatica Sinica, vol. 2, no. 2, pp. 134–142, 2015.
2. H. Esen, M. Adachi, D. Bernardini, A. Bemporad, D. Rost, and J. Knodel,“Control as a service (CaaS): Cloud-based software architecture for automotive control applications,” in International Workshop on the Swarm at the Edge of the Cloud, Seattle, WA, USA, 2015, pp. 13–18.
3. A .Vick, V. Von´asek, R. P˘eni˘cka, and J. Kr¨uger, “Robot control as a service — Towards cloud-based motion planning and control for industrial robots,” in International Workshop on Robot Motion and Control, Poznan, Poland, 2015, pp. 33–39.
4. G. Mohanarajah, R. D’Andrea, and M. Waibel, “Rapyuta: A cloud robotics platform,” IEEE Transactions on Automation Science and Engineering, vol. 12, no. 2, pp. 481–493, 2015.
5. M. Waibel et al., “Roboearth,” IEEE Robotics & Automation Magazine, vol. 18, no. 2, pp. 69–82, 2011.
6. Penchalaiah, P., & Rajasekar, P. An Efficient Multi-User Hierarchical Authenticated Encryption Using Simultaneous Congruence for Highly Secure Data. International Journal of Future Generation Communication and Networking (WoS), ISSN, 2233-7857.
7. B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, “A survey of research on cloud robotics and automation,” IEEE Transactions on Automation Science and Engineering, vol. 12, no. 2, pp. 398–409, 2015.