DEVELOPMENT AND EXAMINATION OF FOG COMPUTING BASED ENCRYPTED CONTROL SYSTEM

Pokkuluri Sri Raja Lakshmi, Sri.G.Ramesh Kumar, Sri.V.Bhaskara Murthy,
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

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.

I. INTRODUCTION

CLOUD-BASED control systems [1], 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 [2]. The authors of [3] introduced Robot Control as a Service. This concept also realizes higher-layer control (e.g., motion planning) for industrial robots. Rapyuta [4] cooperating with RoboEarth [5] 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 [6].

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 [7], [8]. This issue can be solved by fog computing [9], which is a decentralized computing architecture with an intermediate layer 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 [10].

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 [11]–[13]. 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 [14], [15]. Adversaries can eavesdrop, invade, and falsify the system if security measures have not been implemented sufficiently.The authors of [16] 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.

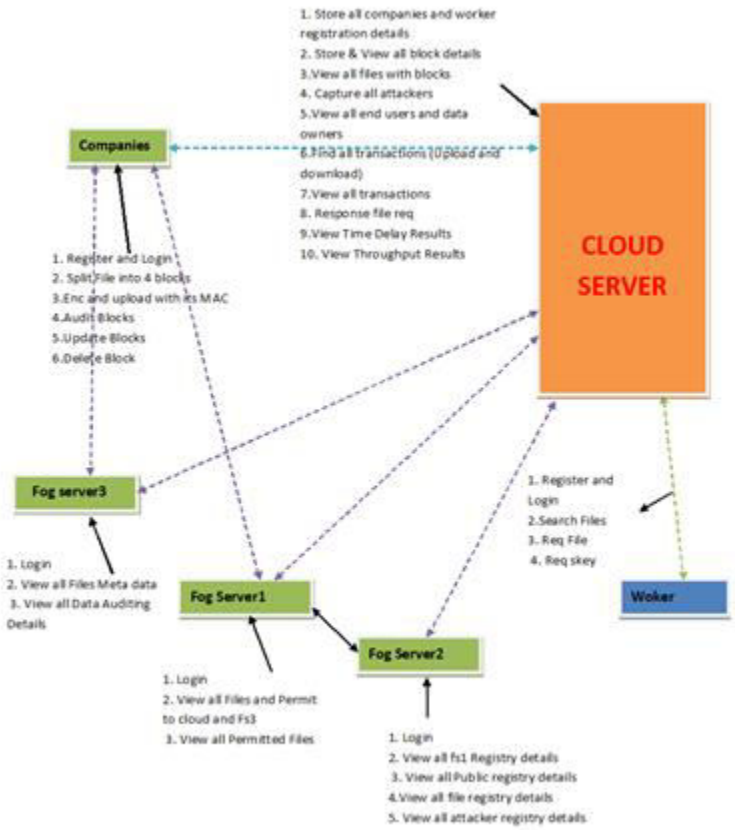
Encrypted control [17], a fusion of cryptography and control theory, is a promising methodology to improve the security of control systems by reducing risks of eavesdropping attacks. Eavesdropping attacks aim to steal information of control systems in order to execute more severe attacks, such as zero dynamics attacks, in the future [15]. In encrypted control systems using ElGamal encryption [18], which is multiplicative homomorphic encryption, control inputs are calculated in ciphertext 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 [19].

The encrypted control system with Paillier encryption [20], which is additive homomorphic encryption was proposed in [21], [22]. The authors of [23] 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 ciphertext. 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.
Another approach to security enhancement of fog computingbased control systems was proposed in [24]. In this method, an artificial noise is added to sensor data, and a controller in the fog determines the control input required to achieve mean square asymptotic stability. However, unlike the method of [17], the controller parameters and control inputs are not concealed.

This letter focuses on the development of a fog computing based encrypted control system with the aim to realize secure modern control systems, e.g., Fig. 1. The developed system uses a basic PID controller encrypted by ElGamal encryption for position control of a linear stage. In the previous studies [25], [26], although the feasibility and property of the encrypted control systems have been evaluated through implementations on Raspberry Pi, validity has not been investigated in realistic settings such as an environment using industrial equipment and networks. This letter demonstrates the first implementation of the encrypted control system that is more representative of a real environment in factories. The effects of the load fluctuation and real-time property are validated. The PID gains and stage position, as well as a

reference signal, are encrypted in the developed system. Additionally, control inputs in ciphertext are determined by using the relevant ciphertext without decryption in the fog. The experimental results confirm that the proposedcontrol system retains the stability and control performance of the original unencrypted control system even when the controller encryption method is applied.

II. SYSTEM ARCHITECTURE



III. EXISTING SYSTEM

The aging of the world's population and the growth in the number of people with chronic diseases have increased expenses with medical care. Thus, the use of technological solutions has been widely adopted in the medical field to improve the patients' health. In this context, approaches based on Cloud Computing have been used to store and process the information generated in these solutions. However, using Cloud can create delays that are intolerable for medical applications. Thus, the Fog Computing paradigm emerged as an alternative to overcome this problem, bringing computation and storage closer to the data sources. However, managing medical data stored in Fog is still a challenge.

Moreover, characteristics of availability, performance, interoperability, and privacy need to be considered in approaches that aim to explore this problem. So, this article shows a software architecture based on Fog Computing and designed to facilitate the management of medical records. This

architecture uses Block chain concepts to provide the necessary privacy features and to allow Fog Nodes to carry out the authorization process in a distributed way. Finally, the existing system describes a case study that evaluates the performance, privacy, and interoperability requirements of the proposed architecture in a home-centered healthcare scenario.

Disadvantages

- In the existing work, scheme is less effective due to this deterministic encryption scheme which allows identical data to be encrypted into the same cipher text. None the less; CE does not provide semantic security for data with low entropy.
- The existing system, problem of Homomorphic encryption which is utilized as a security measure in control systems.

IV. PROPOSED SYSTEM

In the proposed method, an artificial noise is added to sensor data, and a controller in the fog determines the control input required to achieve mean-square asymptotic stability. However, unlike the method of [17], the controller parameters and control inputs are not concealed.

This letter focuses on the development of a fog computing based encrypted control system with the aim to realize secure modern control systems, e.g., Fig. 1. The developed system uses a basic PID controller encrypted by ElGamal encryption for position control of a linear stage. In the previous studies [25], [26], although the feasibility and property of the encrypted control systems have been evaluated through implementations on Raspberry Pi, validity has not been investigated in realistic settings such as an environment using industrial equipment and networks.

This letter demonstrates the first implementation of the encrypted control system that is more representative of a real environment in factories. The effects of the load fluctuation and real-time property are validated. The PID gains and stage position, as well as a reference signal, are encrypted in the developed system. Additionally, control inputs in ciphertext are determined by using the relevant ciphertext without decryption in the fog. The experimental results confirm that the proposed control system retains the stability and control performance of the original unencrypted control system even when the controller encryption method is applied.

Advantages

- The system is more effective since the proposed system in which the encrypted control system with Paillier encryption, which is additive homomorphic encryption was proposed in the proposed secured system.
- The system is more secured since the system is implemented and provided the signal concealment method with fully homomorphic encryption.

V. IMPLEMENTATION

Worker: User is the owner of data. Privacy, disaster recoverability, modification detection of user's data is ultimate goal of this paper.

Fog Server1,2,3: Fog server is trusted to user. User relies on fog server with his data. Close proximity of fog devices to the user, robust physical security, proper authentication, secure communication, intrusion detection ensures fog server's reliability to the user.

Cloud Server: Cloud server is considered as *honest but curious*. This means that cloud server follows the Service Level Agreement (SLA) properly, but has an intention to analyze user's data. Conversely, cloud server may pretend to be good but acts as a potential adversary. In that case, cloud server may modify data in order to forge as original data. Similarly, cloud server may hide/loss the data resulting in permanent data loss of the user. Furthermore, hardware/software failure may result in data modification or permanent loss as well.

VI. CONCLUSIONS

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 Section 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 [19] to prevent DoS attacks, gain falsifications, and replay attacks.

REFERENCES

[1] Y. Xia, "Cloud control systems," IEEE/CAA J. Automatica Sinica, vol. 2, no. 2, pp. 134–142, Apr. 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 Proc. Int. Workshop Swarm Edge Cloud, Seattle, WA, USA, 2015, pp. 13–18.

[3] A. Vick, V. Vonásek, R. Pˇeniˇcka, and J.Krüger, "Robot control as a service

towards cloud-based motion planning and control for industrial robots," in Proc. Int. Workshop Robot Motion Control, Poznan, Poland, 2015, pp. 33–39.

[4] G.Mohanarajah, R.D'Andrea, andM.Waibel, "Rapyuta:Acloud robotics platform," IEEE Trans. Autom. Sci. Eng., vol. 12, no. 2, pp. 481–493, Apr. 2015.

[5] M. Waibel et al., "Roboearth," IEEE Robot. Autom. Mag., vol. 18, no. 2, pp. 69–82, Jun. 2011.

[6] B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, "A survey of research on cloud robotics and automation," IEEE Trans. Autom. Sci. Eng., vol. 12, no. 2, pp. 398–409, Apr. 2015.

[7] A. Botta,W. de Donato, V. Persico, and A. Pescape, "Integration of cloud computing and Internet of Things:Asurvey," Future Gener. Comput. Syst., vol. 56, pp. 684–700, 2016.

[8] M. S. Mahmoud and M. M. Hamdan, "Fundamental issues in networked control systems," IEEE/CAA J. Autom. Sinica, vol. 5, no. 5, pp. 902–922, 2018.

[9] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st Edition MCCWorkshop Mobile Cloud Comput., Helsinki, Finland, 2012, pp. 13–16.

[10] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet Things J., vol. 3, no. 6, pp. 854–864, Dec. 2016.

[11] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," IEEE Internet Comput., vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.

[12] M. Mukherjee et al., "Security and privacy in fog computing: Challenges," IEEE Access, vol. 5, pp. 19 293–19 304, 2017.