https://doi.org/10.5281/zenodo.12726563

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

DEVELOPMENT AND EXAMINATION OF FOG COMPUTINGBASED ENCRYPTED CONTROL SYSTEM

G BALA RENUKA, C SOUNDARYA, K BALAJI SUNIL CHANDRA
Assistant Professor [1,2,3]
GOLLA.BALARENUKA@GMAIL.COM, soundarya.chittepu@gmail.com, hod.cse@svitatp.ac.in
Department of CSE, Sri Venkateswara Institute of Technology,
N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Keywords:

ABSTRACT

An encrypted control system that use fog computing and is implemented in a real-world industrial context is the subject of this letter. The system that was created uses multiplicative homomorphic encryption to hide controller gains and signals via communication lines, protecting them from eavesdropping assaults. The designed system is confirmed to be feasible for position servo control of the motor-driven stage by experimental validation, which examined processing time, parameter variation, and performance deterioration.

Whether or not the plant parameters change, the created system retains its stability even after encrypting the controller gains and signals. Increasing the length of an encryption key really improves control performance, even if it increases processing time.

A ES
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726563

INTRODUCTION

CLOUD-BASED control systems [1] are becoming more prevalent; these systems allow controlled devices to be monitored and managed via a communication network in the cloud. A cloud-based control idea called Control as a Service (CaaS) was developed for use in automobiles in [2]. Introduced by the writers of [3], Robot Control as a Service follows. This idea also makes possible higher-level control for industrial robots, such as motion planning. Platform as a Service (PaaS) for cloud robotics applications is Rapyuta [4] working with RoboEarth [5]. The key benefit of these designs is that they are more efficient, flexible, and scalable than traditional networked systems [6]. Latencies between controlled devices linked to the cloud make cloud architectures unsuitable for lower-layer control, which still requires local execution (e.g., servo control of actuators) [7], [8]. As a decentralised computer system with an intermediary layer called fog, fog computing [9] may resolve this problem. Control systems built on fog computing minimise communication latency while preserving the benefits of cloud-based control systems, such as remote plant status monitoring and easy control law changes, and the elimination of the need to install the controller on-site. Fog also helps with cloud analytics by collecting and cleaning out filthy data [10].

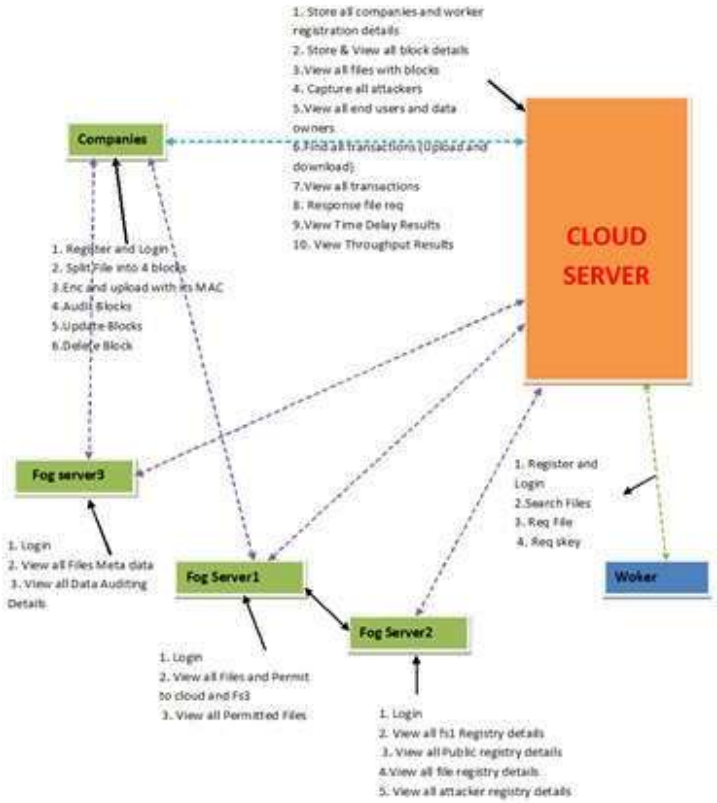
Although there are still security and privacy concerns with fog computing, just as there are with cloud computing, there are numerous possible advantages to fog computing, particularly for real-time applications [11]-[13]. Networked control systems and other cyber-physical systems are more vulnerable to assaults than information systems because of the direct impact that physical systems may have on actual surroundings [14], [15]. Inadequate security measures allow adversaries to spy, infiltrate, and deceive the system.The dangers of manipulators were confirmed by the authors of [16] via real assaults that interfere with controller gains. Essentially, you must conceal controller gains and to conceal signals from the attacks.An intriguing approach to enhancing the safety of control systems and decreasing the likelihood of eavesdropping attacks is encrypted control [17], which combines cryptography with control theory. The purpose of an eavesdropping assault is to get control system information for use in future, more damaging attacks such zero dynamics attacks [15]. An encrypted reference, encrypted sensor data, and encrypted controller parameters are used to compute control inputs in ciphertext in encrypted control systems that use ElGamal encryption [18], a kind of multiplicative homomorphic encryption, without decryption. Replay attacks, as well as controller or signal fabrication assaults, may be detected using encrypted control [19].
The encrypted control system was suggested in [21], [22] using Paillier encryption [20], which is additive homomorphic encryption. Using completely homomorphic encryption, the signal hiding approach was given by the authors of [23].Similar in structure encryption is used in control systems as a security mechanism, as mentioned before. Since ciphertext cannot perform multiplication between two data, obfuscating the controller parameters using additive homomorphic encryption is not a simple task. In addition, a great deal of computing power is needed for homomorphic operation of additive and completely homomorphic encryptions. Because of this, various encryption techniques aren't good for controlling mechanical systems at a lower layer.

In [24], an alternative method for improving the safety of control systems that rely on fog computing was presented up. A controller in the fog calculates the control input needed to reach mean square asymptotic stability in this approach, which involves adding artificial noise to sensor data. In contrast to the approach used in [17], however, the parameters and inputs to the controller are not hidden.
With the goal of realising safe contemporary control systems, such as Fig. 1, this letter focuses on the construction of an encrypted control system that is based on fog computing. In order to regulate the position of a linear stage, the created system employs an ElGamal encrypted basic PID controller. While earlier research has examined the practicality and characteristics of encrypted control systems by implementing them on Raspberry Pi, there has been no investigation of their validity in more realistic contexts, such as an industrial setting with networks and equipment. The first encrypted control system implementation, more typical of actual factory settings, is shown in this letter. There is confirmation that the impacts of load fluctuation and real-time properties are genuine. The created system encrypts a reference signal, stage location, PID gains, and other relevant data. Use of the appropriate ciphertext, without fog decryption, also determines control inputs in ciphertext. Even after implementing the controller encryption approach, the experimental

A ES
ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021
https://doi.org/10.5281/zenodo.12726563

findings show that the suggested control system maintains the stability and control performance of the original, unencrypted system.

I. SYSTEM ARCHITECTURE



EXISTINGSYSTEM

Medical costs have risen in tandem with the global population's ageing and the prevalence of chronic illnesses. As a result, medical professionals have embraced the use of technology solutions to enhance patients' health. The data produced by these systems has been stored and processed using methods rooted in Cloud Computing. However, delays that are unbearable for medical applications might be caused by utilising the cloud. To get around this issue, a new paradigm called "Fog Computing" arose, which moves processing and storage closer to the data sources. Still, it's not easy to manage patient records kept in Fog.

In addition, methods that attempt to investigate this issue should take availability, performance, interoperability, and privacy into account. In order to make medical record administration easier, this article demonstrates a software architecture that is based on Fog Computing. For the required privacy characteristics and to enable distributed authorization via Fog Nodes, this design employs Block chain ideas. Lastly, the current setup explains a case study that compares the suggested architecture's needs in terms of privacy, interoperability, and performance in a home-centered healthcare setting.

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; CEdoes not provide semantic security for data with lowentropy.
- The existing system, problem of Homomorphic encryption which is utilized as a security measure in control systems.

PROPOSED SYSTEM

To achieve mean-square asymptotic stability, the suggested solution involves adding noise to sensor data and

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726563

having a controller in the fog calculate the control input. In contrast to the approach used in [17], however, the parameters and inputs to the controller are not hidden. With the goal of realising safe contemporary control systems, such as Fig. 1, this letter focuses on the construction of an encrypted control system that is based on fog computing. In order to regulate the position of a linear stage, the created system employs an ElGamal encrypted basic PID controller. While earlier research has examined the practicality and characteristics of encrypted control systems by implementing them on Raspberry Pi, there has been no investigation of their validity in more realistic contexts, such as an industrial setting with networks and equipment. The first encrypted control system implementation, more typical of actual factory settings, is shown in this letter. There is confirmation that the impacts of load fluctuation and real-time properties are genuine. The created system encrypts a reference signal, stage location, PID gains, and other relevant data. In addition, The appropriate ciphertext is used without decryption in the fog to derive the control inputs in ciphertext. Results from experiments show that the suggested control system is just as stable and effective as the original, unencrypted system, even after using the controller encryption technique.

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 fullyhomomorphic encryption.

II. IMPLEMENTATION

Data belongs to the user, not the worker. The end purpose of this article is to address user data privacy, disaster recoverability, and alteration detection. E1,$2, and $3 Users have faith in the fog server. The user's data is entrusted to the fog server. Users may trust fog servers because of their close proximity to the user, strong physical protection, correct authentication, secure connection, and intrusion detection. The term "cloud server" is used to describe an online resource. This indicates that the cloud server is legally compliant with the SLA, but it plans to exploit user data for analysis. On the other side, a cloud server may seem to be helpful while really being an enemy. The cloud server may then alter the data and pass it off as the original. In a similar vein, data loss might be irreversible if the cloud server erases or conceals user files. In addition,

III. CONCLUSIONS

As the first encrypted control system to be deployed in a real industrial context, the control system developed in this letter is based on fog computing and is designed to be secure. To prevent attackers from gaining access, the controller's gain and signals are hidden. Both eavesdropping and zero dynamics assaults are thwarted by the created mechanism. Consequently, industrial control systems may benefit from including the controller encryption approach into their defense-in-depth strategies. The experimental findings show a correlation between key length and processing time and validate the practicability of tracking management under fluctuating loads. The controller encryption approach seems to be sufficiently practical, according on the findings in Section IV-A and IV-B. A long key length is preferable from the perspectives of control performance degradation and security level. Key length is limited by processing time, particularly encryption and decryption times, according to Section IV-C findings. Hardware implementations of encryption and decryption, such as a field programmable gate array, are necessary for the practical application of encrypted control systems in environments with restricted resources.A cloud-based control system based on fog computing will be considered for future development. We will also avoid gain falsifications, replay assaults, and denial of service attacks by implementing an attack detection technique [19].

REFERENCES

ISSN: 2096-3246
Volume 53, Issue 04, Nov 2021

https://doi.org/10.5281/zenodo.12726563

“Cloud control systems,” IEEE/CAA, [1] Y. Xia. Automatica JournalSinica, April 2015, volume 2, issue 2, pages 134–142.In the 2015 International Workshop on Swarm Edge Cloud in Seattle, Washington, USA, H. Esen, M. Adachi, D. Bernardini, A. Bemporad, D. Rost, and J. Knodel presented "Control as a service (CaaS): Cloud-based software architecture for automotive control applications" (pp. 13–18). "Robot control as a service towards cloud-based motion planning and control for industrial robots" was published in 2015 in the proceedings of the International Workshop on Robot Motion Control in Poznan, Poland, and was co-authored by A. Vick, V. Vonásek, R. Pˇeniˇcka, and J. Krüger. The paper "Rapyuta: A cloud robotics platform" was published in the IEEE Transactions on Automotive Science and Engineering in April 2015 and was written by G. Mohanarajah, R. D'Andrea, and M. Waibel. [5] In their article "Roboearth," published in the June 2011 issue of the IEEE Robot. Autom. Magazine, M. Waibe et al. [6] "A survey of research on cloud robotics and automation," published in the IEEE Transactions on Automation Science and Engineering, volume 12, issue 2, pages 398-409, April 2015, by B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg.

[7] "Integration of cloud computing and Internet of Things:Asurvey" by A. Botta, W. de Donato, V. Persico, and A. Pescape was published in 2016 in Future Gener. Comp. Syst., vol. 56, pp. 684-700. This sentence is paraphrased from an article published in the IEEE/CAA Journal of Automotive Systems, volume 5, number 5, pages 902-922, written by M. S. Mahmoud and M. M. Hamdan in 2018. In the proceedings of the first edition of the Mobile Cloud Computing Workshop, which took place in Helsinki, Finland in 2012, F. Bonomi, R. Milito, J. Zhu, and S. Addepalli discussed "fog computing and its role in the Internet of Things" (pp. 13-16).

[10]Presented in December 2016 by M. Chiang and T. Zhang in the IEEE Internet Things Journal, "Fog and IoT: An overview of research opportunities," volume 3, issue 6, pages 854-864. "Fog computing for the Internet of Things" [11] by Alrawais, Alhothaily, Hu, and Cheng Issues with security and privacy published in March/April 2017 by IEEE Computer Society, volume 21, issue 2, pages 34–42.

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