Received: 28 February 2024 | Revised: 25 April 2024 | Accepted: 30 May 2024

DOI: 10.1002/aic.18509

RESEARCH ARTICLE

Process Systems Engineering

AIChE JOURNAL

Integrating dynamic economic optimization and encrypted control for cyber-resilient operation of nonlinear processes

Yash A. Kadakia[1] | Fahim Abdullah[1] | Aisha Alnajdi[2] | Panagiotis D. Christofides[1,2]

[1]Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, California

[2]Department of Electrical and Computer Engineering, University of California, Los Angeles, California

Correspondence
Panagiotis D. Christofides, Department of Chemical and Biomolecular Engineering, University of California, Los Angeles, CA 90095, USA.
Email: pdc@seas.ucla.edu

Funding information
National Science Foundation, Grant/Award Number: CBET-2227241

Abstract

This article proposes a two-layer framework to maximize economic performance through dynamic process economics optimization while addressing fluctuating real-world economics and enhancing cyberattack resilience via encryption in the feedback control layer for nonlinear processes. The upper layer employs a Lyapunov-based economic model predictive control scheme, receiving updated economic information for each operating period, while the lower layer utilizes an encrypted linear feedback control system. Encrypted state information is decrypted in the upper layer to determine the economically optimal dynamic operating trajectory through nonlinear optimization. Conversely, the lower layer securely tracks this trajectory in an encrypted space without decryption. To mitigate the cyber vulnerability of the upper layer, we integrate a cyberattack detector that utilizes sensor-derived data for attack detection. We quantify the errors stemming from quantization, disturbances, and sample-and-hold controller implementation. Simulation results of a nonlinear chemical process highlight the robustness and economic benefits of this new control architecture.

KEYWORDS
cyber-security, cyberattack detection, economic model predictive control, encrypted control, semi-homomorphic encryption

1 | INTRODUCTION

Networked control systems have emerged as a transformative paradigm in industrial operations, offering numerous advantages.[1] By harnessing networked communication protocols, these systems significantly reduce the need for extensive wiring and hardware, leading to cost savings and streamlined operations. Additionally, they modernize plant infrastructure by enabling real-time monitoring and control, thereby enhancing operational efficiency and responsiveness. With fewer physical components, maintenance issues are minimized, contributing to improved system reliability and reduced downtime. Further, the ease of implementation and scalability make networked control systems accessible to a wide range of applications, from small-scale operations to large industrial complexes. Given these benefits, networked control systems have become the standard for control systems, offering unparalleled flexibility, efficiency, and reliability in managing industrial processes. As technology continues to evolve, embracing networked control systems remains imperative for organizations aiming to maintain competitiveness and adaptability in an ever-changing industrial landscape.

While networked communication facilitates seamless and rapid data transfer, it also introduces vulnerabilities to cyberthreats. Breaches or compromises in these systems can have severe consequences such as disruptions of essential services or physical harm, which are threats to public safety. Recent advances in cyberattack techniques support the imperative of establishing robust cybersecurity protocols.[2] Real-world incidents reaffirm the critical need of cybersecurity in networked cyber-physical systems. For example, the

2015 BlackEnergy malware attack on SCADA controls overseeing Ukraine's power grid resulted in widespread power outages.[3] Similarly, Colonial Pipeline suffered a ransomware attack by DarkSide hackers in 2021, when its networked communication was encrypted and a ransom was demanded for the decryption keys. Subsequently, Colonial Pipeline had to shut down its fuel distribution operations, resulting in significant financial losses.[4] As cyber threats continue to evolve, cybersecurity concerns loom over process control systems. Modern control systems must be designed with robust security measures to mitigate the impact of cyberattacks. Some measures include implementing secure communication protocols, regularly updating software and firmware, and employing cyberattack detection systems with reconfiguration protocols in the event of an attack.

In traditional process control frameworks, model predictive control (MPC) is combined with a real-time optimizer, the latter of which is tasked with determining economically optimal steady states to be tracked by the MPC through a comprehensive plant model. However, as energy consumption and operational efficiency concerns escalate in industries like chemical and petrochemicals, economic model predictive control (EMPC) has emerged. EMPC enables dynamic optimization of economic cost functions while maintaining stability constraints. Extensive research in chemical process control literature indicates that several industrial processes can attain greater profits through time-varying operation compared to steady-state operation.[5,6] Also, today's dynamic economic landscape is characterized by rapid globalization, technological advancements, and unforeseen disruptions. Fluctuations in energy costs, commodity prices, currency values, interest rates, logistics costs, and market trends can significantly impact businesses and industries worldwide. By incorporating fluctuating real-world economics, EMPC systems can yield superior results, emphasizing the importance of dynamic optimization techniques for maximizing economic benefits and maintaining competitiveness in volatile environments.

Previous studies have explored topics like implementing secure communication in networked control systems through encryption,[7,8] developing cyberattack detectors,[9,10] creating cyberattack-resilient controllers,[11] and developing economic MPCs with time-varying objective functions.[6,12] However, these efforts have not yet resulted in control systems resilient to cyber threats that seamlessly integrate secure communication, cyberattack detection, nonlinear dynamic economic optimization, and real-time fluctuations in economics. Establishing such capabilities is critical for contemporary control systems to navigate economic challenges and cyber vulnerabilities in dynamic environments. This gap motivates our proposal for a new control framework aimed at effectively addressing this challenge.

Specifically, we introduce an encrypted two-layer control framework comprising a nonlinear Lyapunov-based economic model predictive control (LEMPC) scheme in the upper layer and an encrypted linear feedback control system in the lower layer. As we cannot perform nonlinear computations in an encrypted space, we decrypt state information in the upper layer to determine the economically optimal dynamic set point trajectory via nonlinear optimization. Conversely, the lower layer securely tracks these set points in an encrypted space without decryption, utilizing the additive homomorphic property of the Paillier cryptosystem for secure, private communication. To address the cyber vulnerability of the upper layer, we integrate a logic-based cyberattack detector. In the event of an attack, the encrypted lower layer autonomously continues operation, disregarding compromised signals from the upper layer, thus ensuring cyber-resilient operation. In Reference 6, a two-level EMPC system was implemented, consisting of an EMPC in the upper level computing the operating trajectory for the lower-level LMPC to track through closed-loop feedback. In our framework, the objective is to facilitate encrypted operating trajectory tracking without decryption using encrypted feedback at the lower-layer, by employing proportional-integral (PI) controllers which allow linear mathematical operations to be performed in an encrypted space without decryption. Unlike the previous approach which lacked encryption, this method ensures secure communication. While utilizing LMPC in the lower layer would enhance control input computation optimization, it would not fortify against cyberattacks as the computations would occur without encryption.

The subsequent sections of the article are structured as follows: in Section 2, we cover preliminaries, including notation, the class of systems under consideration, system stability assumptions, the cryptosystem employed for encryption, and the effects of quantization. In Section 3, we discuss the encrypted two-layer control framework, formulate the LEMPC, and present the stability analysis of the proposed control system. Section 4 presents and analyzes various closed-loop simulations of a nonlinear chemical process within the encrypted two-layer control framework.

2 | PRELIMINARIES

2.1 | Notation

The notation $x^\top$ represents the transpose of a vector x. The sets of real numbers, integers, and natural numbers are represented by $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{N}$, respectively. Additionally, $\mathbb{Z}_M$ refers to the additive group of integers modulo M. Set subtraction is indicated by "\", where $A\backslash B$ denotes the set of elements in A but not in B. A function denoted by $f(\cdot)$ belongs to the class $\mathcal{C}^1$ if it is continuously differentiable within its domain. Furthermore, a continuous function $\alpha:[0,a)\to[0,\infty)$ is classified as class $\mathcal{K}$ if $\alpha(0)=0$, and it is strictly increasing. The terms $\mathrm{lcm}(i,j)$ and $\gcd(i,j)$ represent the least common multiple and greatest common divisor of integers i and j, respectively.

2.2 | Class of systems

In this research, we focus on multi-input multi-output (MIMO) nonlinear systems, which are described by a set of ordinary differential equations (ODEs) in the following manner:

$$\begin{aligned} \dot{x} &= f(x(t),u(t),w(t)) \\ y &= x+v. \end{aligned} \tag{1}$$

The state vector is represented by $x \in \mathbb{R}^n$, and $y \in \mathbb{R}^n$ denotes the vector of continuously sampled state measurements. The control input vector, denoted by $u \in \mathbb{R}^m$, is subject to bounds defined by the set $U \subset \mathbb{R}^m$. Specifically, U is defined as $U = \{u \in \mathbb{R}^m | u_i^{\min} \le u_i \le u_i^{\max}, i = 1,\ldots,m\}$, where $u_i^{\min}$ and $u_i^{\max}$ represent the lower and upper bounds, respectively, of the ith control input in the vector u. Additionally, the disturbance vector is denoted by $w \in \mathbb{R}^w$, and the noise vector is denoted by $v \in \mathbb{R}^n$. Similarly, the disturbance and noise vectors are bounded by $|W(t)| \le \theta$ and the set $\overline{V} \in \mathbb{R}^n$, respectively. The function $f(\cdot)$ is locally Lipschitz and evaluates to zero at the origin $f(0,0,0) = 0$, establishing it as an equilibrium of Equation (1). We set the initial time as zero ($t_0 = 0$). Further, $S(\Delta)$ is defined as the set of piece-wise constant functions with a period of Δ.

We introduce a dynamic economic optimization and encrypted feedback control framework to guide the system of Equation (1) in tracking the reference trajectory representing time-varying operating set points, $x_E(t) \in \Omega_\rho$, where Ω_ρ is defined in the subsequent subsection. The rate of change of the reference trajectory is bounded by:

$$|\dot{x}_E(t)| \le \gamma_E. \tag{2}$$

To capture the deviation between the actual state trajectory $x(t)$ and the time-varying reference trajectory $x_E(t)$, we introduce,

$$e(t) = x(t) - x_E(t), \tag{3}$$

and we can characterize its dynamics by

$$\begin{aligned} \dot{e} &= \dot{x}(t) - \dot{x}_E(t) \\ &= f(x(t),u(t),w(t)) - \dot{x}_E(t) \\ &= f(e(t)+x_E(t),u(t),w(t)) - \dot{x}_E(t) \\ &= g(e(t),x_E(t),\dot{x}_E(t),u(t),w(t)). \end{aligned} \tag{4}$$

We assume that Equation (4) is continuously differentiable and possesses a unique equilibrium point for each fixed $x_E \in \Omega_\rho$. In other words, for every x_E there exists a corresponding u_E, resulting in $e = 0$ being an equilibrium of Equation (4). This condition can be expressed mathematically as

$$g(0,x_E,0,u_E,0) = 0. \tag{5}$$

Remark 1. Assuming that the system described by Equation (1) has an equilibrium for each fixed $x_E \in \Omega_\rho$ is crucial for enabling the tracking of the reference trajectory. With an EMPC in place, the economically optimal dynamic state trajectory can be determined for any initial condition $x_E(t_0) \in \Omega_\rho$, where $t_0 = 0$. Consequently, the generated reference state trajectory contains set points that can be effectively tracked for any $x_E \in \Omega_\rho$.

2.3 | Stabilizability assumptions

We assume the existence of an explicit stabilizing feedback control law, $u(t) = h(e(t),x_E(t)) \in U$, that renders the origin of the system of Equation (1) with $w \equiv 0$ and $v \equiv 0$ asymptotically stable, for each $x_E \in \Omega_\rho$. This assumption guarantees that the time-varying state trajectory $x_E(t)$ can be tracked and signifies the existence of a $\mathcal{C}^1$ control Lyapunov function $V(e,x_E)$ that satisfies the following inequalities:

$$\alpha_1(|e|) \le V(e,x_E) \le \alpha_2(|e|), \tag{6a}$$

$$\frac{\partial V(e,x_E)}{\partial e} g(e,x_E,0,h(e,x_E),0) \le -\alpha_3(|e|), \tag{6b}$$

$$\left|\frac{\partial V}{\partial e}\right| \le \alpha_4(|e|), \tag{6c}$$

$$\left|\frac{\partial V}{\partial x_E}\right| \le \alpha_5(|e|), \tag{6d}$$

$\forall e, x_E \in \mathbb{R}^n$ in an open region D surrounding the origin. The functions $\alpha_1,\alpha_2,\alpha_3,\alpha_4$, and α_5 belong to the class $\mathcal{K}$. For the system of Equation (1), the region of closed-loop stability can be defined as a level set denoted by Ω_ρ of the control Lyapunov function V. This set is described as $\Omega_\rho := \{x \in D | V(e,x_E) \le \rho\}$, where $\rho > 0$. Therefore, starting from any initial condition inside Ω_ρ, the control input $h(e,x_E)$ ensures that the closed-loop state trajectory remains within Ω_ρ.

Further, considering the local Lipschitz property to the vector field f and that the manipulated input vector u is bounded within nonempty convex sets, a positive constant exists such that

$$|f(x,u,w)| \le M_F, \tag{7}$$

$\forall x \in \Omega_\rho$, $u \in U$, and $w \in W$. Extending this to the system of Equation (4), considering that the rate of change of $x_E(t)$ is bounded by γ_E,

$$|g(e,x_E,\dot{x}_E,u,w)| \le M, \tag{8}$$

$\forall (x - x_E) \in \Omega_{\rho^*}$, $x_E \in \Omega_\rho$, $u \in U$, and $w \in W$. Further, due to the continuous differentiability of the control Lyapunov function $V(e,x_E)$ and the Lipschitz property of f, there exist positive constants $L_w, L'_w, L_e, L'_e, L'_E, L''_E, L'_u$ such that

$$\begin{aligned} &|g(e,x_E,\dot{x}_E,u,w)| - |g(e',x'_E,\dot{x}_E,u,0)| \\ &\quad \le L_e|e-e'| + L_E|x_E - x'_E| + L_w|w|, \end{aligned} \tag{9}$$

$$\begin{aligned} &\left|\frac{\partial V(e,x_E)}{\partial e} g(e,x_E,\dot{x}_E,u,w) - \frac{\partial V(e',x'_E)}{\partial e} g(e',x'_E,\dot{x}'_E,u',0)\right| \\ &\quad \le L'_e|e-e'| + L'_E|x_E - x'_E| \\ &\quad\quad + L''_E|\dot{x}_E - \dot{x}'_E| + L'_w|w| \\ &\quad\quad + L'_u|u-u'|, \end{aligned} \tag{10}$$

$\forall x_E, x'_E \in \Omega_\rho$, $e, e' \in \Omega_{\rho^*}$, $|\dot{x}_E| \le \gamma_E$, $|\dot{x}'_E| \le \gamma_E$, $u \in U$, and $w \in W$.

Remark 2. In various nonlinear systems commonly encountered in chemical process control systems, Lyapunov functions have often been formulated using state variables $V(x) = \bar{f}(x(t))$. In our study, leveraging the previous definitions of e and x_E, we can also represent the state vector as $x(t) = x_E(t) - e(t)$. Consequently, we broaden the Lyapunov function to take the form $V(e, x_E)$, as we proceed to examine the stability of the system within the proposed control framework in the following section.

2.4 | Paillier cryptosystem

In this article, we utilize the Paillier cryptosystem[13] to encrypt various signals, including state measurements (y), reference trajectory set points (x_E), and manipulated inputs (u), which are transmitted to and from the controllers. A key aspect of our approach is utilizing the semi-homomorphic property of additive homomorphism inherent in the Paillier cryptosystem. This property enables us to perform linear additive operations in an encrypted space, particularly within the lower encrypted feedback control layer. The encryption process begins with the generation of both public and private keys. As the Paillier cryptosystem is an asymmetric encryption scheme, it utilizes two different keys for encryption and decryption: a public key for encrypting plaintext and a private key for decrypting ciphertext. The procedure for generating these keys is:

1. Select two large prime integers (p and q) based on the desired key bit length, such that, $\gcd(pq, (p-1)(q-1)) = 1$.
2. Calculate, $M = pq$.
3. Search for an arbitrary integer $\bar{g}$ such that $\bar{g} \in \mathbb{Z}_{M^2}$, that is, the multiplicative group of integers modulo M^2.
4. Calculate $\lambda = \mathrm{lcm}(q-1, p-1)$.
5. Define $\bar{L}(x) = (x-1)/M$.
6. Verify the existence of the subsequent modular multiplicative inverse: $u = (\bar{L}(\bar{g}^{\lambda} \mathrm{mod} M^2))^{-1} \mathrm{mod} M$.
7. If the inverse does not exist, go back to step 3. If the inverse exists, $(M, \bar{g})$ is the public key and (λ, u) is the private key.

After obtaining the keys, authorized recipients receive the public and private keys for encryption and decryption, respectively. The message m is encrypted as follows:

$$E_M(m, r) = c = \bar{g}^m r^M \mathrm{mod} M^2, \tag{11}$$

where r is a random integer from the set $\mathbb{Z}_M$, and c is the resulting ciphertext obtained by encrypting m. Decryption is performed as follows to obtain m:

$$D_M(c) = m = \bar{L}(c^{\lambda} \mathrm{mod} M^2) u \mathrm{mod} M. \tag{12}$$

2.5 | Quantization

Prior to encrypting data using the Paillier cryptosystem, it must be processed to natural numbers in $\mathbb{Z}_M$. However, signal values are typically in floating-point format before encryption. As a result, a process known as quantization is employed to convert the floating-point numbers into $\mathbb{Z}_M$.[8] This involves creating a set, denoted as $\mathbb{Q}_{l_1,d}$, which is characterized by two parameters: l_1, representing the total bit count (combining integer and fractional bits), and d, indicating the number of fractional bits. The set, $\mathbb{Q}_{l_1,d}$, comprises rational numbers ranging from -2^{l_1-d-1} to $2^{l_1-d-1} - 2^{-d}$, with intervals of 2^{-d}. A rational number q within $\mathbb{Q}_{l_1,d}$ can be expressed as $q \in \mathbb{Q}_{l_1,d}$, where $\exists \beta \in \{0,1\}^{l_1}$, and $q = -2^{l_1-d-1}\beta_{l_1} + \sum_{i=1}^{l_1-1} 2^{i-d-1}\beta_i$. The function, $g_{l_1,d}$ maps a real number data point a to $q \in \mathbb{Q}_{l_1,d}$ as follows:

$$\begin{aligned} g_{l_1,d} &: \mathbb{R} \rightarrow \mathbb{Q}_{l_1,d} \\ g_{l_1,d}(a) &:= \arg \min_{q \in \mathbb{Q}_{l_1,d}} |a - q|. \end{aligned} \tag{13}$$

Subsequently, we convert the quantized data to a set of positive integers using a one-to-one (bijective) mapping referred to as $f_{l_2,d}$, as described in.[8] This mapping is structured to ensure that the quantized data is translated into a subset of the message space, $\mathbb{Z}_M$, and is performed as follows:

$$\begin{aligned} f_{l_2,d} &: \mathbb{Q}_{l_1,d} \rightarrow \mathbb{Z}_{2^{l_2}} \\ f_{l_2,d}(q) &:= 2^d q \mathrm{mod} 2^{l_2}. \end{aligned} \tag{14}$$

In the encryption process, plaintext messages from the set $Z_{2^{l_2}}$ are transformed to ciphertexts, which can subsequently be decrypted back into the original set $Z_{2^{l_2}}$. Next, to retrieve the original data from the set $\mathbb{Q}_{l_1,d}$, an inverse mapping, labeled as $f^{-1}_{l_2,d}$, is performed as follows:

$$f^{-1}_{l_2,d} : \mathbb{Z}_{2^{l_2}} \rightarrow \mathbb{Q}_{l_1,d}. \tag{15}$$

$$f^{-1}_{l_2,d}(m) := \frac{1}{2^d} \begin{cases} m - 2^{l_2} & \text{if } m \geq 2^{l_2-1} \\ m & \text{otherwise} \end{cases}. \tag{16}$$

To illustrate the process of encryption and decryption, we can refer to the example shown in Figure 1. For this specific instance, the selected quantization parameters are as follows: $d = 3$, $l_1 = 18$, and $l_2 = 30$. Let us consider the rational number $a = -1.31752$. The impact of quantization is demonstrated in Figure 1, where the quantization error, $|a - q| = 0.05748$, is evident.

Remark 3. Quantization-related errors tend to accumulate in multiplicatively homomorphic encryption schemes like ElGamal, due to the compounding nature of multiplication and associated scaling operations. In contrast, additive homomorphism, like in the Paillier

scheme employed in this article, is generally less prone to quantization error accumulation, as addition does not involve scaling or compounding of errors through multiplication. To mitigate this effect, one can select a higher quantization parameter.

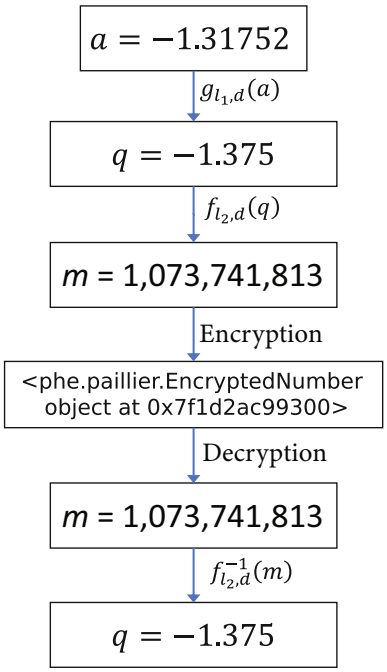

FIGURE 1 Visualization of the encryption-decryption process and effect of quantization when applied to a floating-point real number.

3 | DEVELOPMENT OF THE ENCRYPTED TWO-LAYER CONTROL FRAMEWORK

In this section, we describe the design of the proposed encrypted two-layer control framework, formulate the LEMPC and encrypted feedback controller, and perform a stability analysis of the encrypted control system.

3.1 | Design and implementation

In the encrypted control framework illustrated in Figure 2, at time t_k, sensor signals $x(t_k)$ undergo encryption to form ciphertext c_1 using a public key. These encrypted signals are then transmitted to a cloud hardware security module (HSM), a dedicated hardware device utilized for managing cryptographic keys and securely performing cryptographic operations within a cloud computing environment. After decryption using the private key, the quantized sensor signals $\hat{x}(t_k)$ are sent to the cloud server responsible for nonlinear EMPC computations, aimed at determining economically optimal dynamic set points $x_E(t)$ for $t = [t_k, t_k + t')$, where t' represents the EMPC operating period. Following this, the set points $x_E(t)$ are encrypted into ciphertext c_1' using the public key within another cloud HSM. Subsequently, these encrypted set points are transmitted to a set of PI (proportional-integral) controllers in the encrypted lower feedback control layer. Operating with a sampling period Δ significantly smaller than the operating period t', this lower layer computes control inputs to track the set point trajectory using encrypted sensor signals c_2, sampled at intervals of Δ. These control input computations take place within an encrypted space without decryption, leveraging the additive

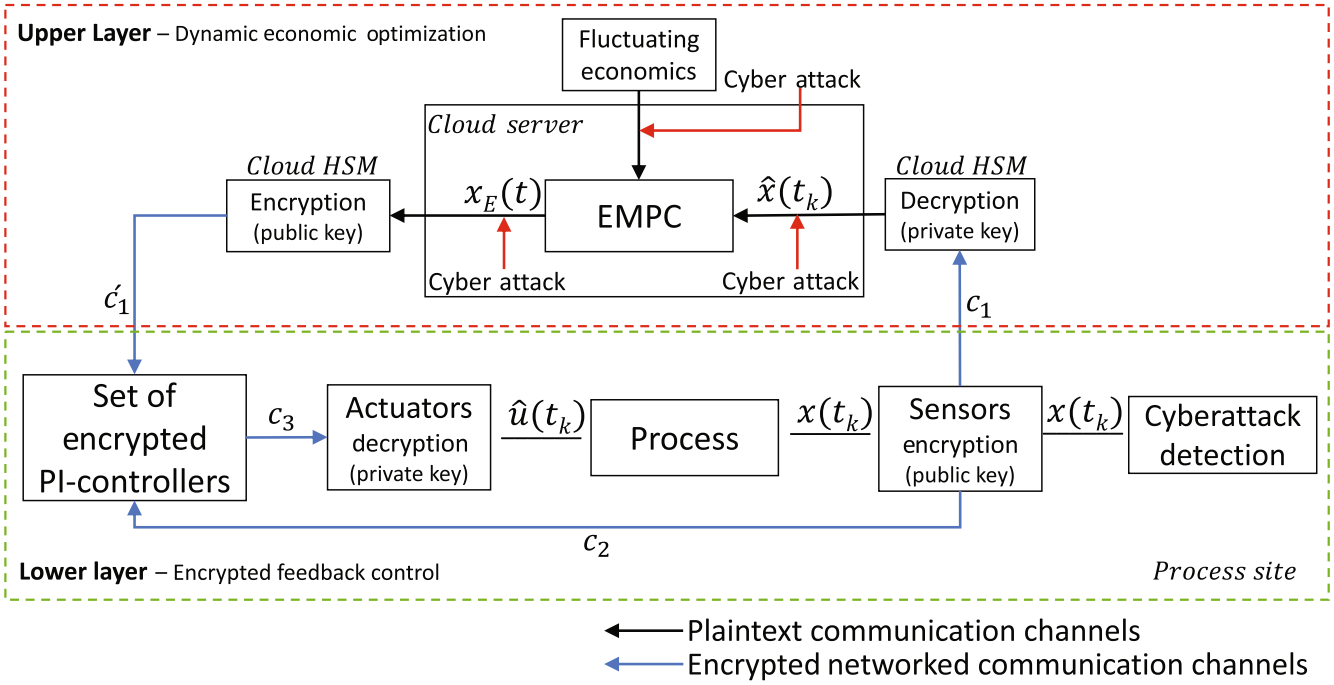

FIGURE 2 A block diagram of the proposed encrypted two-layer control framework.

homomorphic property of the Paillier cryptosystem. At the actuator, encrypted control inputs c_3 are decrypted to obtain the quantized input $\hat{u}(t_k)$, which is then applied to the process. This cycle within the lower layer continues until it receives a new encrypted state trajectory from the EMPC in the upper layer at the end of the operating period.

The closed-loop design depicted in Figure 2 has three potential points vulnerable to cyberattacks for data manipulation: the updated economic information containing the weights of the EMPC objective function, the decrypted sensor signal received from the cloud HSM, and the computed set points of the EMPC before transmission to the cloud HSM. To detect potential threats initiated against the vulnerable upper layer, a logic-based cyberattack detector is integrated into the lower layer, which utilizes sensor-derived data for attack detection. Upon detection, the control system logic reconfigures, disregarding signals received from the compromised upper layer, and operates independently. Detailed information of the cyberattack detector and reconfiguration mechanism is provided in Section 4.

Further, this design introduces three sources of error: one stemming from state quantization in the sensor-to-upper layer EMPC link, another arising from set point quantization in the upper layer EMPC-to-lower layer feedback controller link, and a third originating from control input quantization in the lower layer feedback controller-to-actuator link. These errors are bounded by:

$$|x(t_k) - \hat{x}(t_k)| \leq 2^{-d-1}. \tag{17a}$$

$$|x_E(t_k) - \hat{x}_E(t_k)| \leq 2^{-d-1}. \tag{17b}$$

$$|u(t_k) - \hat{u}(t_k)| \leq 2^{-d-1}. \tag{17c}$$

The bounds of the quantization error, as detailed in Equation (17), are derived in Remark 5. Further, an additional error is introduced in the applied control input. This stems from the lower layer feedback controller, $h(e,x_E)$, that uses the quantized error $\hat{e} = \hat{x} - \hat{x}_E$ to compute control inputs in an encrypted space. This error will be bounded by:

$$\begin{aligned} |e - \hat{e}| &= |(x - x_E) - (\hat{x} - \hat{x}_E)| \\ &= |(x - \hat{x}) + (\hat{x}_E - x_E)| \\ &\leq 2^{-d-1} + 2^{-d-1} \\ &\leq 2^{-d}. \end{aligned} \tag{18}$$

Remark 4. The two-layer encrypted dynamic optimization and control framework outlined in our work is adaptable and can be applied when other dynamic optimization strategies are used in the upper-layer to calculate the set points (current values of the operating trajectory) of the lower-layer control system, not just the economic MPC scheme employed in this article. The key objective of this structure is to facilitate nonlinear control and optimization within an encrypted system. In this framework, the upper layer computes set points through nonlinear dynamic optimization (which cannot be performed in an encrypted space), then encrypts these set points and transmits them to the lower layer. The lower layer, without decrypting the set points, utilizes encrypted measurement feedback to track these set points, integrating encryption with nonlinear dynamic optimization and control.

Remark 5. Quantization error occurs when a value intended for quantization does not precisely match any value in the set $\mathbb{Q}_{l_1,d}$, which is spaced apart by 2^{-d}. Suppose the value to be quantized is denoted as a, which is positioned between b and $b+2^{-d}$. If the absolute difference between a and b is smaller than that between a and $b+2^{-d}$, then a is assigned to b; otherwise, it is assigned to $b+2^{-d}$. As a result, the maximum potential difference between the actual and quantized values is half the resolution, or 2^{-d-1}. Therefore, increasing the value of d reduces the quantization error.

Remark 6. We operate the proposed closed-loop design under a few assumptions. Firstly, we assume that plaintext data is vulnerable to cyberattacks, wherein it can be manipulated or subjected to denial-of-service (DOS) attacks. However, we do not consider attacks on encrypted data due to its inherent privacy. Each encryption process generates a unique ciphertext due to the random number generated, making manipulation easily detectable. In case of an attack on encrypted data, the only recourse is to transfer control to a secure backup system isolated from any network. Secondly, we assume that the cloud server where nonlinear computations occur in plaintext is vulnerable to cyber threats. Lastly, we assume that the cloud HSMs responsible for housing cryptographic keys and performing cryptographic operations are fully secure. Cloud HSMs, offered by leading providers such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP), adhere to stringent security standards like FIPS 140-2/3.[14] They are chosen precisely because they are impervious to cyberattacks, validating this assumption.

Remark 7. While the proposed closed-loop design of the encrypted two-layer control framework is vulnerable to cyberattacks, it enhances cybersecurity by integrating a cyberattack detection and subsequent reconfiguration mechanism. Furthermore, it improves the robustness of the control system by transmitting data only once during each operating period between the lower and upper control layers, reducing the potential for attacks due to less-frequent data transmission. Additionally, in this design, the cloud server does not have access to either key, and no component has access

to both the public and private keys; they only have access to one or the other. Also, following the prevailing standard recommended by NIST, it is recommended to use cryptographic keys with a bit-length greater than 2048 to assure robustness.[15]

Remark 8. For large-scale processes with numerous states and inputs, employing a centralized MPC in the cloud server would entail significant computational expenses. Alternatively, decentralized and distributed MPCs could be integrated into the same framework to alleviate the computational burden associated with the centralized approach, as demonstrated in prior works.[16,17] In these works, encrypted data was decrypted at each sampling instance within the nonlinear MPC to compute control inputs. However, in our approach, decryption only occurs within the LEMPC of the upper layer at the start of each operating period, rather than at every sampling period. Control inputs for tracking the reference trajectory are then computed without decryption. As a result, the frequency of encryption-decryption operations at the controllers is substantially reduced in our proposed framework. This reduction enhances security by minimizing the opportunities for manipulating decrypted data.

Remark 9. The duration of the operating period t' is established by considering the lowest frequency required for updating economic data, including energy prices, raw material costs, product demand, or product selling prices. Within the EMPC objective function, this economic information remains constant throughout the operating period. Additionally, the chosen period can be shorter than the interval between updates of economic information. In this scenario, economic data would remain constant between operating periods. However, it should still be long enough to compute state trajectories optimized over a period significantly larger than the sampling period of the lower feedback layer, where these trajectories are tracked.

3.2 | Dynamic economic optimization

The optimization problem for the LEMPC in the upper layer of the proposed control framework is represented as:

$$\mathcal{J} = \max_{u_E \in S(\Delta_E)} \int_{t_k}^{t_{k+N_E}} L(\tilde{x}_E(t), u_E(t))\mathrm{d}t, \tag{19a}$$

$$\text{s.t.} \quad \dot{\tilde{x}}_E(t) = f(\tilde{x}_E(t), u_E(t)), \tag{19b}$$

$$u_E \in U, \ \forall\, t \in [t_k, t_{k+N_E}), \tag{19c}$$

$$|\dot{x}_E(t)| \le \gamma_E, \ \forall\, t \in [t_k, t_{k+N_E}), \tag{19d}$$

$$\tilde{x}_E(t_k) = \hat{x}(t_k), \tag{19e}$$

$$V(\tilde{x}_E(t_k)) \le \rho_{\text{secure}}, \ \forall\, t \in [t_k, t_{k+N_E}), \ \text{if } \tilde{x}_E(t_k) \in \Omega_{\rho_{\text{secure}}} \tag{19f}$$

$$\dot{V}(\tilde{x}_E(t_k), u_E) \le \dot{V}(\tilde{x}_E(t_k), \Phi(\tilde{x}_E(t_k))), \ \text{if } \tilde{x}_E(t_k) \in \Omega_\rho \backslash \Omega_{\rho_{\text{secure}}} \tag{19g}$$

where Δ_E is the LEMPC sampling period. Equation (19e) uses the quantized state, $\hat{x}(t_k)$, after decryption, to initialize the LEMPC plant model of Equation (19b). k represents the sampling instance, and N_E represents the number of sampling periods within the LEMPC prediction horizon. $\tilde{x}_E(t)$ is the predicted state trajectory of the LEMPC model of Equation (19b). This model is utilized to integrate the economic objective function of Equation (19a) to calculate the optimized LEMPC control inputs, $u_E(t)$, where $t \in [t_k, t_k + N_E)$. The LEMPC's goal is to maximize this objective function over the prediction horizon such that it satisfies the constraints of Equations (19c)–(19g). Equation (19c) represents the constraints imposed on the control inputs. The constraint of Equation (19d) ensures that the lower layer can track the reference trajectory $x_E(t)$ by limiting its rate of change, $\dot{x}_E(t)$. From the Lyapunov constraint of Equation (19f), the LEMPC ensures that, if the state $\bar{x}(t_k) \in \Omega_{\rho_{\text{secure}}}$ at time t_k, then it lies within this region for $t \in [t_k, t_k + N_E)$, where ρ_{secure} is a level set of the control Lyapunov function $V(\tilde{x}_E)$ such that $V(\tilde{x}_E) \le \rho_{\text{secure}}$. If $\tilde{x}_E(t_k)$ lies within the set $\Omega_\rho \backslash \Omega_{\rho_{\text{secure}}}$, the Lyapunov constraint of Equation (19g), ensures that LEMPC drives the predicted state trajectory $\tilde{x}_E(t)$ to the origin at a rate faster than or at least equal to the stabilizing controller $\Phi(\tilde{x}_E(t_k))$ (the existence of $\Phi(\cdot)$ follows from the stabilizability assumption on the process made in Section 2.3). Following the computation of optimized control inputs u_E by LEMPC, the reference trajectory $x_E(t)$ is derived by recursively solving the model described in Equation (19b), where u_E is implemented in a sample-and-hold fashion. The x_E values are logged at intervals of Δ, denoting the lower layer's sampling period, and subsequently relayed to the cloud HSM for encryption prior to transmission to the encrypted lower-layer control system for tracking.

Remark 10. The proposed LEMPC operates on feedback, as it starts with actual state measurements. However, in case of an event like a denial-of-service (DOS) attack where the threat actor blocks the decrypted sensor measurements from reaching the upper layer, we can initialize the LEMPC using the final value of the predicted state trajectory from the previous operating period. This assumes that at the end of the previous operating period, the deviation between the actual state trajectory and the reference trajectory is within the bounds as derived in Section 3.4.

3.3 | Encrypted feedback control

In the encrypted space, only linear mathematical operations are permissible. Consequently, we utilize the recursive rule to approximate integral terms within the set of proportional-integral controllers of the encrypted lower layer feedback control system, ensuring strictly linear mathematical operations, as illustrated below:

$$\begin{aligned} u_i(t_k) &= K_{c_i}\left(e_i(t_k)+\frac{1}{\tau_i}\int_0^{t_k} e_i(\tau)\mathrm{d}\tau\right) \\ &= K_{c_i}e_i(t_k)+I_{t_k} \\ &= K_{c_i}e_i(t_k)+K'_{c_i}e_i(t_k)+I_{t_{k-1}}, \end{aligned} \tag{20}$$

where $u_i(t_k)$ is the ith control input of the lower layer. The error of the ith state at time t_k is described by $e_i(t_k)=x_{E_i}(t_k)-x_i(t_k)$, with $x_{E_i}(t_k)$ and $x_i(t_k)$ denoting the set point (value of the economically optimal trajectory at t_k as calculated by the upper-layer EMPC) and state measurement of the ith state, at time t_k, respectively. t_k and t_{k-1} denote the sampling instances k and $k-1$, respectively. K_{c_i} and K'_{c_i} represent the proportional and integral gains, while I_{t_k} denotes the integral control action at t_k. At $k=0$, I_{t_0} is assumed to be 0. The lower layer has a sampling period of Δ, and applies the computed control inputs in a sample-and-hold manner for the time $t=[t_k,t_k+\Delta)$, and then recomputes the control input with the updated set point and state feedback at time $t=t_{k+1}$.

3.4 | Stability analysis

In this subsection, we examine the closed-loop stability of the proposed two-layer encrypted control framework, with the LEMPC at the upper layer and the encrypted feedback controller at the lower layer.

Theorem 1. *Considering the nonlinear system described in Equation (1), we analyze its stability under the encrypted lower layer feedback controller $\hat{h}(\hat{e},\hat{x}_E)$, under the influence of bounded disturbances. The lower layer feedback controller $h(e,x)$, operating without encryption, satisfies the inequalities specified in Equation (6). Additionally, we assume that the initial error $\hat{e}(t_0)=\hat{x}(t_0)-\hat{x}_E(t_0)$ lies within the region Ω_{ρ^*}. For the closed-loop system of Equation (1) under the encrypted lower layer feedback controller, we can determine positive real numbers $\epsilon_{\text{error}},\epsilon_w$, for which there exist Δ,Δ_E,γ_E, and d, that satisfy the following conditions:*

$$|\dot{x}_E(t)| \le \gamma_E < \frac{\hat{\theta}\alpha_3(\epsilon_{\text{error}})}{2L''_E+\alpha_4(\alpha_1^{-1}(\rho^*))+\alpha_5(\alpha_1^{-1}(\rho^*)+M\Delta)}, \tag{21}$$

$$\mu=\alpha_3^{-1}\left[\frac{(2L''_E+\alpha_4(\alpha_1^{-1}(\rho^*))+\alpha_5(\alpha_1^{-1}(\rho^*)+M\Delta))\gamma_E}{\hat{\theta}}\right], \tag{22}$$

$$-(1-\hat{\theta})\alpha_3(\mu)+L'_w\theta+L'_eM\Delta+L'_E\gamma_E\Delta_E+e_q \le -\epsilon_w/\Delta, \tag{23}$$

for some $\hat{\theta}$ with $0<\hat{\theta}<1$. If $(\hat{x}(t_0)-\hat{x}_E(t_0))\in\Omega_{\rho^*}$, then the deviation $\hat{e}(t)$ remains bounded in Ω_{ρ^*} under the encrypted stabilizing controller and the actual closed-loop state trajectory x is always bounded in Ω_ρ. Furthermore, given a sufficiently large time T, the deviation between the actual system of Equation (1) and the economically optimal trajectory is ultimately bounded by $|e(t)|\le\epsilon_{\text{error}}$ for $t\in[t_k,t_k+t')$.

Proof. We prove that the deviation between the actual system evolution and economically optimal set point trajectory under the lower layer encrypted feedback controller (i.e., $\hat{e}(t)$) is always bounded in Ω_{ρ^*} and, after a sufficiently large time $T<t'$, where t' is the operating period of the LEMPC from t_0 to t_0+t', the deviation is bounded in $B_{\epsilon_{\text{error}}}$. Also, based on the bound derived in Equation (18), we can say $e(t)$ is also bounded in Ω_{ρ^*} as $\hat{e}(t)\in\Omega_{\rho^*}$.

We assume that, at sampling time $t_k\in[t_0,t_0+t')$, $\hat{e}(t_k)\in\Omega_{\rho^*}\backslash B_\mu$. At t_0, the LEMPC recomputes a new optimal trajectory $x_E(t)$ for the encrypted lower feedback layer to track from t_0 to t_0+t'. We define two sets $B_{\epsilon_{\text{error}}}=\{|e(t)|\le\epsilon_{\text{error}}\}$ and $B_\mu=\{|e(t)|\le\mu\}$, where μ is defined in Equation (22) and $B_\mu\subset B_{\epsilon_{\text{error}}}$. If the deviation $\hat{e}(t)$ is bounded in the set $\Omega_{\rho^*}\backslash B_\mu$ and the conditions of Equations (21) and (22) are met, the deviation will decrease along the closed-loop state trajectory, and after a sufficiently large time T, the deviation will converge to the set B_μ. Furthermore, the deviation $e(t)$ is ultimately bounded in the ball $B_{\epsilon_{\text{error}}}$.

The time derivative of the control Lyapunov function along the deviation of system trajectory of Equation (3) is, without disturbances or encryption:

$$\dot{V}(e(t_k),x(t_k))=\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{e}(t_k)+\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k). \tag{24}$$

Using the Lipschitz property of Equation (6b), after substituting $\dot{e}(t_k)=\dot{x}(t_k)-\dot{x}_E(t_k)$, we get

$$\begin{aligned} \dot{V}(e(t_k),x(t_k)) &= \frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{x}(t_k) \\ &\quad -\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{x}_E(t_k) \\ &\quad +\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k) \\ &\le \frac{\partial V(e(t_k),x_E(t_k))}{\partial e}g(e(t_k),x_E(t_k),0,h(e(t_k),x_e(t_k)),0) \\ &\quad -\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{x}_E(t_k) \\ &\quad +\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k) \\ &\le -\alpha_3(|e(t_k)|)-\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{x}_E(t_k) \\ &\quad +\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k). \end{aligned} \tag{25}$$

The time derivative of the control Lyapunov function along the deviation and economically optimal state trajectory for $\tau \in [t_k, t_k+\Delta)$, under the encrypted feedback controller, with disturbances is

$$\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) = \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial e}\dot{e}(\tau) + \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial x_E}\dot{x}_E(\tau). \tag{26}$$

Adding and subtracting Equation (24) to and from Equation (26), we get

$$\begin{aligned}\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le\ & \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial e}\dot{e}(\tau) - \frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{e}(t_k)\\ &+\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{e}(t_k) + \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial x_E}\dot{x}_E(\tau)\\ &-\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k))\\ &+\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k)).\end{aligned} \tag{27}$$

Substituting Equation (25) in Equation (27), using the bound of Equation (2), and using the Lipschitz property of Equation (10), we get

$$\begin{aligned}\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le\ & -\alpha_3(|e(t_k)|) - \frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{x}_E(t_k)\\ &+\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k) - \frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{e}(t_k)\\ &-\frac{\partial V(e(t_k),x_E(t_k))}{\partial x_E}\dot{x}_E(t_k) + \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial e}\dot{e}(\tau)\\ &+\frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial x_E}\dot{x}_E(\tau)\\ \le\ & -\alpha_3(|e(t_k)|) + \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial e}\dot{e}(\tau)\\ &-\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{e}(t_k) + \frac{\partial V(\hat{e}(\tau),\hat{x}_E(\tau))}{\partial x_E}\dot{x}_E(\tau)\\ &-\frac{\partial V(e(t_k),x_E(t_k))}{\partial e}\dot{x}_E(t_k)\\ \le\ & -\alpha_3(|e(t_k)|) + L'_w|w(\tau)| + L'_e|\hat{e}(\tau)-e(t_k)|\\ &+L'_E|\hat{x}_E(\tau)-x_E(t_k)| + L''_E|\dot{x}_E(\tau)-\dot{x}_E(t_k)| + L'_u|\hat{u}-u|\\ &+\alpha_5(|\hat{e}(\tau)|)\gamma_E + \alpha_4(|e(t_k)|)\gamma_E.\end{aligned} \tag{28}$$

Using the quantization error bounds of Equations (17) and (18), in Equation (28), we get

$$\begin{aligned}\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le\ & -\alpha_3(|e(t_k)|) + L'_w|w(\tau)| + L'_e|\hat{e}(\tau)-e(\tau)| + L'_e|e(\tau)-e(t_k)|\\ &+L'_E|\hat{x}_E(\tau)-x_E(\tau)| + L'_E|x_E(\tau)-x_E(t_k)|\\ &+2L''_E\gamma_E + L'_u 2^{-d-1} + \alpha_5(|\hat{e}(\tau)|)\gamma_E + \alpha_4(|e(t_k)|)\gamma_E\\ \le\ & -\alpha_3(|e(t_k)|) + L'_w|w(\tau)| + L'_e 2^{-d} + L'_E 2^{-d-1}\\ &+L'_e|e(\tau)-e(t_k)| + L'_E|x_E(\tau)-x_E(t_k)|\\ &+2L''_E\gamma_E + L'_u 2^{-d-1} + \alpha_5(|\hat{e}(\tau)|)\gamma_E + \alpha_4(|e(t_k)|)\gamma_E.\end{aligned} \tag{29}$$

Due to the continuity of $e(t)$ and $x_E(t) \forall\, t \in [t_k, t_k+\Delta)$, and from Equation (8), we can write that $|e(\tau)-e(t_k)| \le M\Delta$, and $|x_E(\tau)-x_E(t_k)| \le \gamma_E\Delta_E \quad \forall t \in [t_k, t_k+\Delta)$. Using these bounds, and the inequalities of Equation (6), it follows from Equation (29):

$$\begin{aligned}\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le\ & -\alpha_3(|e(t_k)|) + L'_w|w(\tau)|\\ &+L'_e 2^{-d} + L'_E 2^{-d-1} + 2L''_E\gamma_E + L'_u 2^{-d-1}\\ &+L'_E\gamma_E\Delta_E + L'_e M\Delta + \alpha_5(|\hat{e}(\tau)|)\gamma_E + \alpha_4(|e(t_k)|)\gamma_E.\end{aligned} \tag{30}$$

As $e(t_k) \in \Omega_{\rho^*} \setminus B_\mu$, Equation (30) can be written as,

$$\begin{aligned}\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le\ & -\alpha_3(\mu) + L'_w\theta + L'_e M\Delta + L'_E\gamma_E\Delta_E + e_q\\ &+(\alpha_4(\alpha_1^{-1}(\rho^*)) + \alpha_5(\alpha_1^{-1}(\rho^*) + M\Delta) + 2L''_E)\gamma_E,\end{aligned} \tag{31}$$

with $e_q = L'_e 2^{-d} + L'_E 2^{-d-1} + L'_u 2^{-d-1}$ representing the error due to quantization (for performing encryption). If Equation (21) is satisfied, then there exists a γ_E such that the following equation holds:

$$\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le -(1-\hat{\theta})\alpha_3(\mu) + L'_w\theta + L'_e M\Delta + L'_E\gamma_E\Delta_E + e_q, \tag{32}$$

for some positive $\hat{\theta} < 1$. If the condition of Equation (23) is satisfied, then there exists $\epsilon_w > 0$ such that the following inequality holds for $\hat{e}(t_k) \in \Omega_{\rho^*} \setminus B_\mu$:

$$\dot{V}(\hat{e}(\tau),\hat{x}(\tau)) \le -\epsilon_w/\Delta,\ \forall \tau \in [t, t_{k+1}). \tag{33}$$

Integrating this bound over $t \in [t_k, t_{k+1})$, we get

$$V(\hat{e}(t_{k+1}),\hat{x}(t_{k+1})) \le V(\hat{e}(t_k),\hat{x}(t_k)) - \epsilon_w,\ \forall t \in [t_k, t_{k+1}), \tag{34}$$

$\forall \hat{e}(t_k) \in \Omega_{\rho^*} \setminus B_\mu$. Using the above inequalities recursively, if $e(t_k) \in \Omega_{\rho^*} \setminus B_\mu$, the deviation between the actual state trajectory and the economically optimal reference trajectory will converge to B_μ, within time T, without exiting the set Ω_{ρ^*}. Further, there exists a sufficiently large $\epsilon_{\text{error}} > 0$, such that if the deviation exits the ball B_μ, it is still maintained within $B_{\epsilon_{\text{error}}}$ as the increase in deviation would be bounded over one sampling period. From the Lyapunov constraints of the LEMPC in Equation (19f), and Equation (19g), the reference trajectory $x_E(t)$ will be bounded in $\Omega_{\rho_{\text{secure}}}$ within time T. As $e(t)$ is always bounded in the set Ω_{ρ^*}, from Theorem 1, and $x(t) = x_E(t) + e(t)$, the closed-loop state trajectory of the system will converge to the set Ω_{ρ_e} in time T, where $\Omega_\rho < \Omega_{\rho_e} < \Omega_{\rho_{\text{secure}}}$, and will remain there. ■

Remark 11. From Equation (31), we can identify five factors affecting the rate of change of the control Lyapunov function when $\hat{e}(t_k) \in \Omega_{\rho^*} \setminus B_\mu$: the lower layer control system and LEMPC sampling periods (Δ and Δ_E), disturbance bound (θ), rate of change of the reference state trajectory ($\dot{x}_E$), and the quantization parameter (d). While disturbance is inherent to the system, adjust-

ments to the other factors can be made to restrict the deviation between the state trajectory and reference state trajectory, thus achieving the desired tracking performance. In essence, decreasing the sampling times and the rate of change of the reference state trajectory while increasing the quantization parameter can help reduce the deviation between the actual state trajectories and reference trajectories.

4 | APPLICATION TO A NONLINEAR CHEMICAL PROCESS

In this section, we apply the proposed encrypted two-layer control framework on a nonlinear chemical process with disturbance and sensor noise, operating at an unstable steady state. Multiple simulation cases are presented and compared to demonstrate the economic benefits and cyber-resilience of the proposed control framework.

4.1 | Process description and model development

Specifically, the process considered is the conversion of reactant A to product B in a nonisothermal, well-mixed continuous stirred tank reactor (CSTR). This involves an irreversible second-order exothermic reaction, denoted as $A \rightarrow B$, with a reaction rate given by $r_B = k_0 e^{-\frac{E}{RT}} C_A^2$. The CSTR is equipped with a heating jacket that can either supply or remove heat at a rate Q. Using material and energy balance equations, we define the dynamic model of this process as follows:

$$\frac{dC_A}{dt} = \frac{F}{V}(C_{A0} - C_A) - k_0 e^{\frac{-E}{RT}} C_A^2. \tag{35a}$$

$$\frac{dT}{dt} = \frac{F}{V}(T_0 - T) + \frac{-\Delta H}{\rho_L C_p} k_0 e^{\frac{-E}{RT}} C_A^2 + \frac{Q}{\rho_L C_p V}. \tag{35b}$$

denotes the concentration of reactant A, and T represents the reactor temperature. The reactant A is introduced by the feed with a volumetric flow rate F, concentration C_{A0}, and a temperature of T_0. The liquid in the reactor maintains a constant heat capacity C_p and density ρ_L. Parameters such as ΔH, k_0, R, and E correspond to the enthalpy of reaction, pre-exponential constant, ideal gas constant, and activation energy, respectively. The values of these parameters are given in Table 1. The state variables, expressed in deviation terms, consist of the reactant concentration and the reactor temperature, denoted as $x^\top = [C_A - C_{As}, T - T_s]$, where the subscript "s" denotes the steady-state value. Initially, the CSTR operates at an unstable steady-state characterized by $[C_{As}, T_s] = [1.9537\ \text{kmol/m}^3, 401.87\ \text{K}]$, with inlet feed concentration and heat input rate denoted as $[C_{A0s}, Q_s] = [4\ \text{kmol/m}^3, 0\ \text{kJ/hr}]$. The control inputs are: $C_{A0} - C_{A0_s}$ and $Q - Q_s$, representing deviations from the steady-state inlet concentration and heat input rate, respectively. These inputs are constrained within the closed sets $[-3.5, 3.5]\ \text{kmol/m}^3$ and $[-5 \times 10^5, 5 \times 10^5]\ \text{kJ/h}$, respectively. At the initial time $t = t_0 = 0$, the system begins at equilibrium ($x_0 = [0,0]^\top$). Process noise, w_k, is introduced to the inlet flow rate, F, such that $|w_k| \le 0.1 \times F$. Here, k denotes the sampling period, and w_k is a normally distributed random variable with zero mean and a SD of 3.5% of the inlet flow rate of $5\ \text{m}^3/\text{h}$. Additionally, non-Gaussian measurement noise, extracted from industrial data as described in Reference 18, is added to all measured states. This noise is normalized and scaled by 1% before being applied to the concentration state, while it is applied to the temperature state without scaling.

TABLE 1 Parameter values for the chemical process example.

$F = 5\ \text{m}^3/\text{h}$	$V = 1\ \text{m}^3$
$k_0 = 8.46 \times 10^6\ \text{m}^3/(\text{kmol hr})$	$E = 5 \times 10^4\ \text{kJ/kmol}$
$R = 8.314\ \text{kJ/(kmol K)}$	$\rho_L = 1000\ \text{kg/m}^3$
$\Delta H = -1.15 \times 10^4\ \text{kJ/kmol}$	$T_0 = 300\ \text{K}$
$Q_s = 0\ \text{kJ/h}$	$C_{A0_s} = 4\ \text{kmol/m}^3$
$C_{As} = 1.9537\ \text{kmol/m}^3$	$T_s = 401.87\ \text{K}$
$C_p = 0.231\ \text{kJ/(kg K)}$	

The control objective is to increase the economic profit of the process described in Equation (35) by manipulating the inlet concentration and heat input rate, while ensuring that the state trajectories of the closed-loop system remain within the stability region Ω_ρ at all times using the two-layer control architecture. Ultimately, the system should converge to the economically viable region Ω_{ρ_e} and stay there. The objective function of the LEMPC optimizes the production rate of B, consumption of reactant A, and the heat input rate $Q - Q_s$ as follows:

$$L(x_E, u) = A_1 k_0 e^{-\frac{E}{RT}} C_A^2 - A_2(C_{A0} - C_{A0_s}) - A_3(Q - Q_s)^2, \tag{36}$$

where A_1,A_2, and A_3 are the potentially time-varying weighting factors that account for fluctuations in process economics, that is, product selling price, reactant cost, and energy cost, respectively. The control Lyapunov function $V(e, x_E) = x_E^\top P x_E$ is defined with the following positive definite P matrix:

$$P = \begin{bmatrix} 1060 & 22 \\ 22 & 0.52 \end{bmatrix}. \tag{37}$$

The time-varying weights chosen for the example considered are provided in Table 2.

The closed-loop stability region for the CSTR is defined as Ω_ρ, with $\rho = 320$, which is characterized as a level set of the Lyapunov function. The secure operating region $\Omega_{\rho_{\text{secure}}}$ for the LEMPC described in Equation (19) is defined with $\rho_{\text{secure}} = 85$. Further, the desired region of economic feasibility, Ω_{ρ_e}, within which the real state trajectory is to be bounded, is selected to have $\rho_e = 130$. The operating

TABLE 2 Time-varying Lyapunov-based economic model predictive control weights for chemical process example.

Time (t)	A_1	A_2	A_3
0 h $\le t <$ 1 h	1	17	1×10^{-8}
1 h $\le t <$ 2 h	0.99	14	0.8×10^{-8}
2 h $\le t <$ 3 h	1.01	5	0.84×10^{-8}
3 h $\le t <$ 4 h	0.98	7	0.9×10^{-8}
$t \ge$ 4 h	1.02	9	0.9×10^{-8}

period of the LEMPC is $t' = 1$ h. The lower layer encrypted control system operates with a sampling period of 1.8 s, whereas the LEMPC has a sampling period of 180 s. The prediction horizon for the LEMPC is set to $N_E = 20$ sampling periods. The integration step h_c chosen to integrate the LEMPC model using the explicit Euler method is 0.36 s. The positive definite matrix P in $V = x_E^\top P x_E$ and the stability region Ω_ρ are determined through simulations that search for the largest invariant set Ω_ρ in the state-space within which $\dot{V}$ is rendered negative, for all states in Ω_ρ under the stabilizing controller $h(e, x_E) \in U$. In the present example, $h(e, x_E)$ is a set of PI controllers, $[u_1, u_2]^\top$ of the form of Equation (20) with proportional gains $K_1 = 10^1$ and $K_2 = 10^4$, and integral time constants $\tau_1 = 10^{-3}$ and $\tau_2 = 10^{-6}$.

4.2 | Performing encryption in the two-layer control framework

Before encrypting and decrypting the data, parameters such as d, l_1, and l_2 are carefully selected. The integer bit count $l_1 - d$ is determined from extreme feasible states and control inputs. The upper limit of $\mathbb{Q}_{l_1,d}$ is calculated using from $2^{l_1-d-1} - 2^{-d}$, while the lower limit can be obtained from -2^{l_1-d-1}. The quantization parameter, d, is selected depending on the desired level of accuracy and operating range of state and control input values. Further, l_2 is chosen to exceed l_1. In the example presented in this section, $l_1 - d$ is calculated to be 16, determining l_1 and d. In the set $\mathbb{Q}_{l_1,d}$, numbers are separated by a resolution of 2^{-d}. In our simulations, we use $d = 8$ in all scenarios except when it is specifically changed and noted to be $d = 1$. For $d = 8$, $l_1 = 24$, and l_2 is selected as 30. Similarly, for $d = 1$, $l_1 = 16$, and l_2 is set to 20. Paillier Encryption is implemented using Python's "phe" module, PythonPaillier.[19] To solve the multiconstrained nonconvex optimization problem of the upper layer LEMPC in the two-layer encrypted control framework, we utilize the Python module of the IPOPT software.[20]

4.3 | Cyberattack detection and system reconfiguration

A logic-based cyberattack detector is integrated into the lower layer of the encrypted two-layer control framework. This detector receives sensor readings every three sampling instances of the lower control layer and utilizes this data to compute the control Lyapunov function $V(x)$. Importantly, this computation occurs prior to encryption or transmission to the cloud HSM, ensuring its security. In the event of a cyberattack, the objective of the attack is to divert the process from its operating trajectory while still maintaining it within the stability region, Ω_ρ. This may lead to a prolonged cyberattack that could go undetected, potentially being mistaken for a process disturbance. The upper layer LEMPC aims to maintain the operating trajectory within a more conservative region, $\Omega_{\rho_{\text{secure}}}$, and lacks information about the bounded region Ω_{ρ_e} as detailed in the earlier section. Therefore, if the detector records three consecutive instances where the control Lyapunov function has values $V(x) \ge \rho_e$, and its value increases compared to its last recorded value, it declares the process as being under attack. Subsequently, the control reconfiguration logic rejects the previously received economically optimal set points from the compromised upper layer. Subsequently, it utilizes the encrypted set points of the prior operating period when the system operated without attack detection.

Remark 12. In the proposed control architecture, the lower-layer control system receives encrypted set-points (values of the operating trajectory at the current time) that are maintained at different time intervals. The control actions implemented on the process by the lower-layer control system are calculated from encrypted feedback without decrypting the state information or the set points. Since the measured state data remains encrypted, it is very difficult to implement a cyberattack in the lower-layer control system; this is an important advantage of the proposed control architecture. On the other hand, cyberattacks can be launched in the upper-layer EMPC system that calculates the set-points for the lower-layer control system and this is where attack detection mechanisms are implemented to detect such attacks. With respect to cyberattacks that can influence encrypted communication, this is an issue that goes beyond the scope of the present work. It is important to note that given the linear nature of the lower-layer control system, alternative, perhaps more secure, encryption schemes can be used in the lower layer with similar properties being proved for the closed-loop system.

Remark 13. Since the lower layer solely receives encrypted set points from the upper layer and operates within the defined economically viable region, taking into account fluctuating economics, identifying cyberattacks that do not push the system outside this region becomes challenging. However, the absence of information in the compromised upper layer concerning the bounds of this region adds another layer of robustness to the proposed detection scheme. Detecting attacks

within this region would necessitate decrypted economic information from the upper layer, which could also be vulnerable to cyberattacks. Therefore, in this study, we only focus on cyberattacks capable of driving the system away from the economically viable operating region while maintaining it within the stable region.

Remark 14. As mentioned in Section 3.1, there are three potential points of cyberattack where plaintext data could be manipulated in the presented closed-loop design of Figure 2. For brevity, we only demonstrate results when a false-data injection cyberattack is initiated on the data received by the upper layer LEMPC after decryption, ensuring that the system does not exit the stability region. Detailed information on the launched cyberattack and similar classes of cyberattacks has been discussed in Reference 21. These attacks are designed to ensure that the system does not exit the stability region during the attack, making them difficult to detect.

4.4 | Simulation results of the encrypted two-layer control framework

The proposed encrypted two-layer control framework is applied to the nonlinear chemical process example with sensor noise and disturbances. Results depicted in Figures 3 and 4 illustrate the proposed two-layer framework's performance under an LEMPC objective function whose coefficients (weights) change for each operating period. Figures 5 and 6 display the closed-loop states and inputs and corresponding state-space trajectories under encrypted lower-layer control with set-points calculated at the upper layer using steady-state optimization with the same economic objective as in the LEMPC and with weights changing at each operating period. Furthermore, Figures 7 and 8 show the results under the encrypted two-layer control framework with an LEMPC objective function whose coefficients are set equal to the ones of the first operating period throughout the five-period operation. Finally, Figures 9 and 10 illustrate closed-loop states, inputs and state-space trajectories under encrypted lower-layer control with set-points calculated at the upper layer using steady-state optimization with the same economic objective as in the LEMPC and with weights set equal to the ones of the first operating period.

Analyzing these results in more detail, the closed-loop simulation results in Figures 3 and 4 illustrate time-varying operating trajectories for different operating periods. Initially, when raw material costs are high, a time-varying operation is preferred to maximize economic benefits. As raw material costs decrease over successive periods, steady-state operation becomes more favorable as determined by the upper-layer LEMPC. Figures 5 and 6 depict how different steady-states are maintained for each operating period with time-varying (changing every period and remaining constant within a single period) weights in the objective function of the steady-state optimizer. Figures 7 and 8 show that with time-invariant weights in the LEMPC objective function, similar dynamic trajectories are computed and

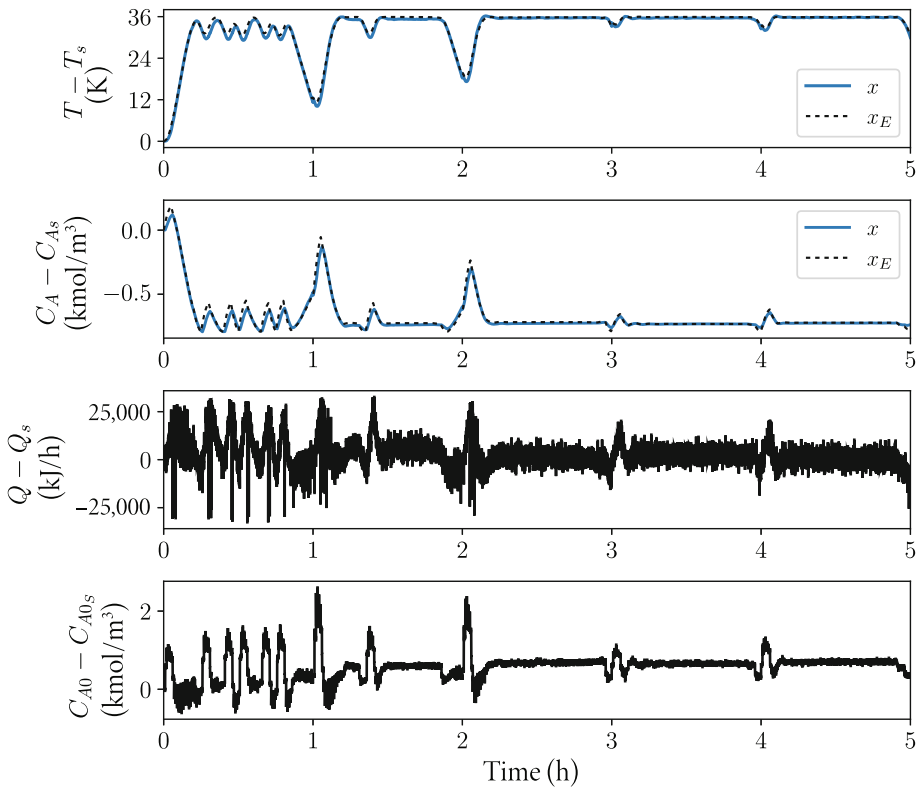

FIGURE 3 State and control input profiles under the encrypted two-layer control framework with an Lyapunov-based economic model predictive control objective function whose weights change for each operating period.

maintained across operating periods. Figures 9 and 10 demonstrate that steady-state operation is maintained when a time-invariant objective is used in the steady-sate optimizer for all operating periods. Comparing the performance of these scenarios justifies the application of EMPC through the encrypted two-layer framework to achieve economically optimal time-varying operation in certain periods over steady-state operation.

More specifically, Table 3 presents the total economic objective function values for the closed-loop simulations. These results demonstrate that the proposed framework, particularly with dynamic economic optimization, outperforms steady-state optimizers. Notably, the time-varying LEMPC objective function yields the highest economic objective function after 5 h of process time, followed by the LEMPC

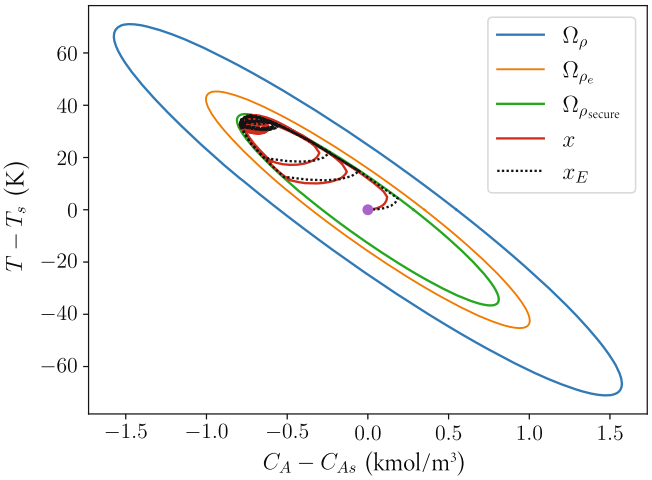

FIGURE 4 State-space plot for the evolution of the state and reference trajectories under the encrypted two-layer control framework with an Lyapunov-based economic model predictive control objective function whose weights change for each operating period.

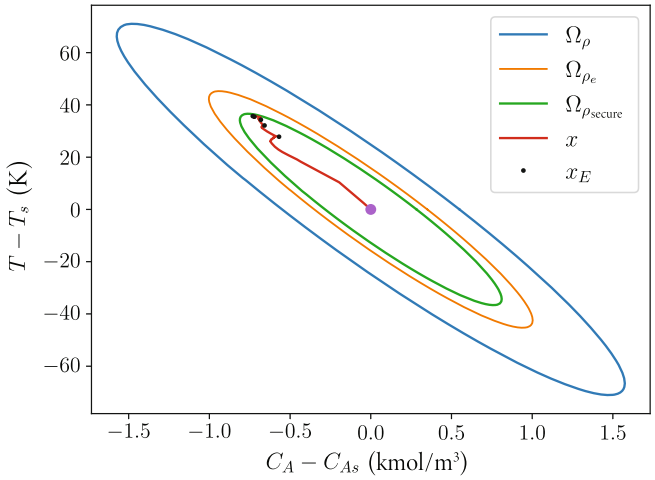

FIGURE 6 State-space plot for the evolution of the state and reference trajectories under encrypted lower-layer control with set-points calculated at the upper layer using steady-state optimization with the same economic objective as in the Lyapunov-based economic model predictive control and with weights changing at each operating period.

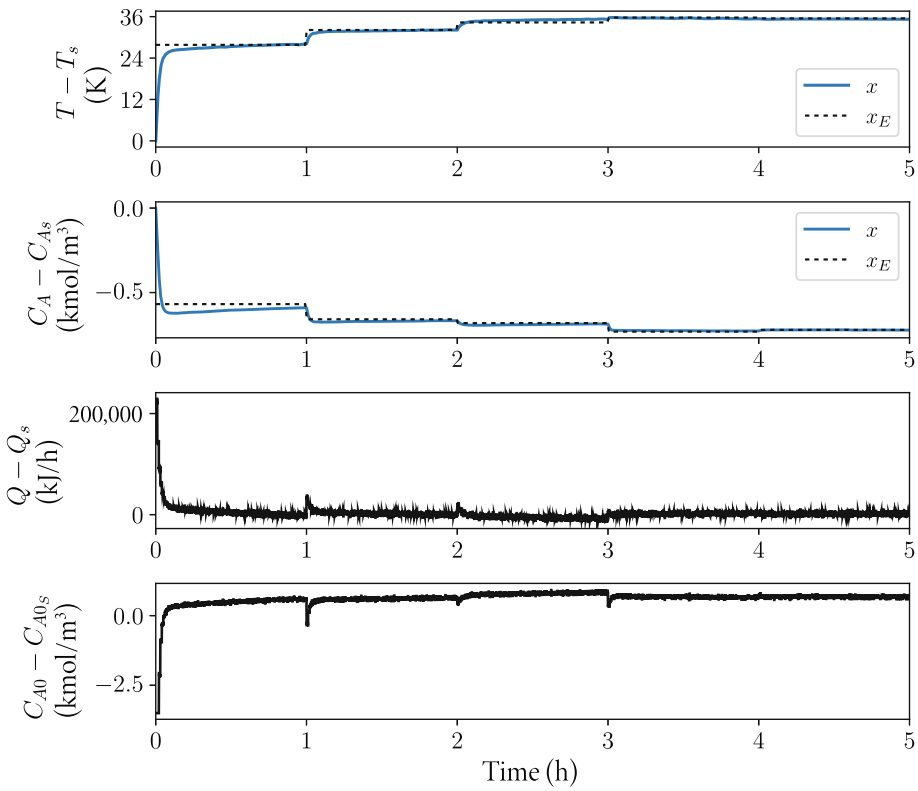

FIGURE 5 State and control input profiles under encrypted lower-layer control with set-points calculated at the upper layer using steady-state optimization with the same economic objective as in the Lyapunov-based economic model predictive control and with weights changing at each operating period.

with an objective function that uses time-invariant weights (i.e., the weights are kept the same for all operating periods). In all aforementioned cases, the lower layer encrypted feedback controllers track the state trajectory well, and it remains bounded in Ω_{ρ_e} at all times.

Figures 11 and 12 depict results under the encrypted two-layer control framework with a time-varying LEMPC objective function, without and with a cyberattack detection and reconfiguration mechanism, respectively. In both cases, a false-data injection attack is initiated at 4 h. With the detection and reconfiguration mechanism, the state trajectory is promptly returned within Ω_{ρ_e} upon exit as shown in Figure 12, while without it, the trajectory remains outside Ω_{ρ_e} for an extended period as depicted in Figure 11. After detection, the lower-layer controller follows the state trajectory from the previous operating period, during which no attack was detected, and the closed-loop state remained within Ω_{ρ_e} at all times. In all these simulations, the quantization parameter d is maintained at 8. Figure 13 illustrates results under the encrypted two-layer control framework with a time-varying LEMPC objective function for $d = 1$ (corresponding to increased quantization error), where the state trajectory exits Ω_{ρ_e} at certain points and struggles to track the operating trajectory effectively, unlike the other cases. All other parameters were maintained the same as the case presented in Figure 4, for comparison. This highlights the need for using a higher quantization parameter and validates the theoretical results.

Remark 15. As previously mentioned, we have employed both time-varying and time-invariant coefficients (weights) in the objective functions across different scenarios. However, the coefficients remain the same for the initial operating period in all cases. In conducting the economic performance comparison presented in Table 3, we utilized recorded state and control input trajectory data from the different closed-loop simulations spanning a process duration of 5 hours. This data was used to compute the total objective function value with time-varying (changing from period to period

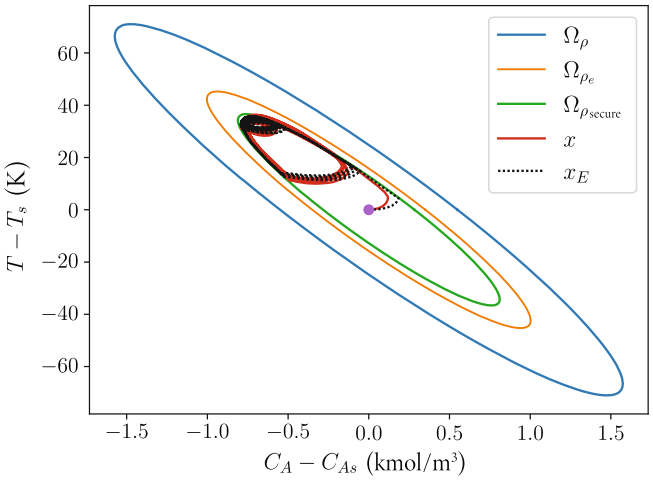

FIGURE 8 State-space plot for the evolution of the state and reference trajectories under the encrypted two-layer control framework with an Lyapunov-based economic model predictive control objective function that uses the same weights for each operating period.

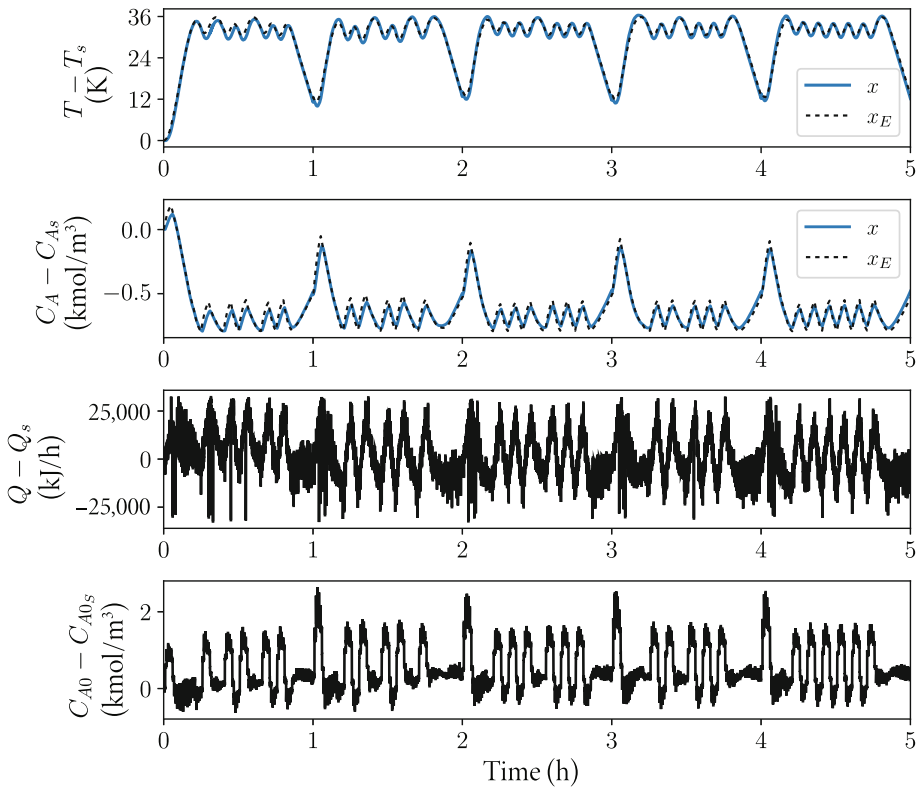

FIGURE 7 State and control input profiles under the encrypted two-layer control framework with an Lyapunov-based economic model predictive control objective function that uses the same weights for each operating period.

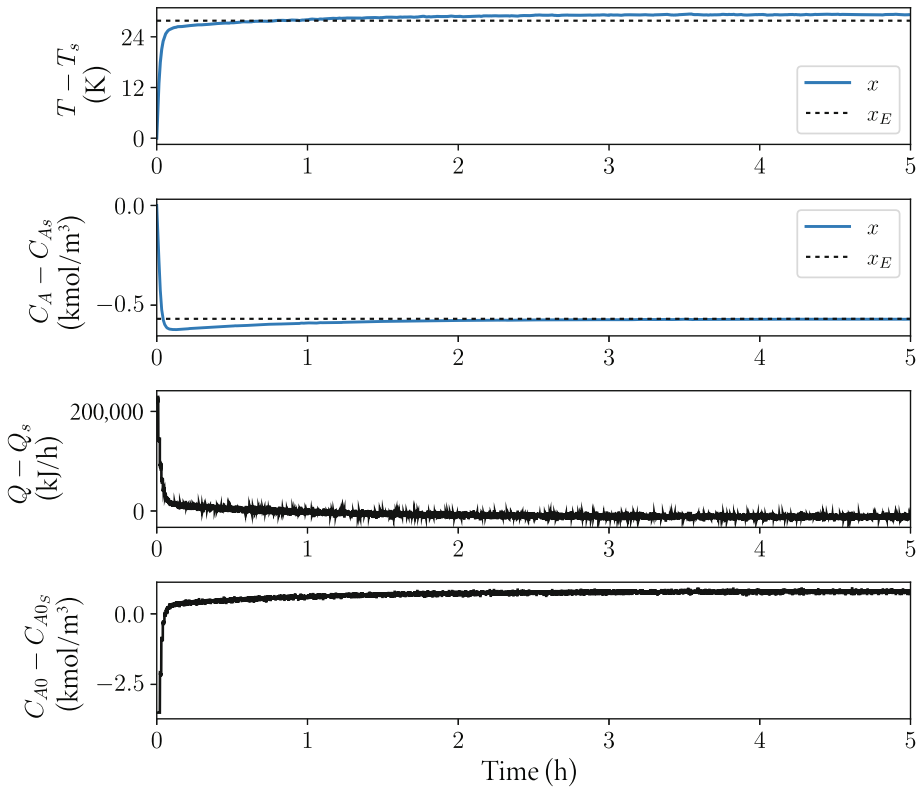

FIGURE 9 State and control input profiles under encrypted lower-layer control with set-points calculated at the upper layer using steady-state optimization with the same economic objective as in the Lyapunov-based economic model predictive control and with fixed weights.

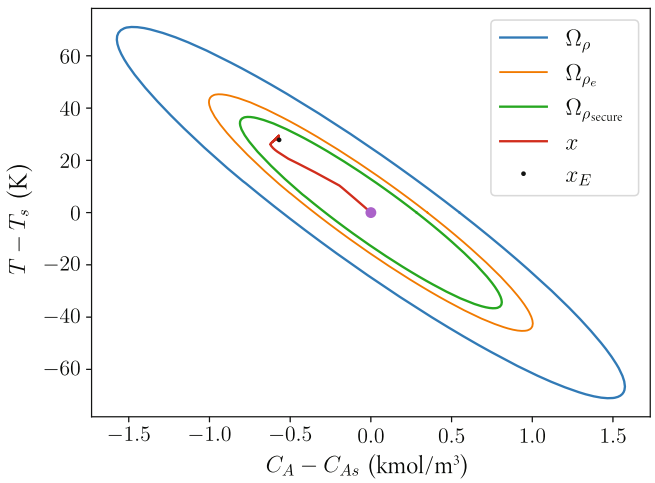

FIGURE 10 State-space plot for the evolution of the state and reference trajectories under encrypted lower-layer control with set-points calculated at the upper layer using steady-state optimization with the same economic objective as in the Lyapunov-based economic model predictive control and with fixed weights.

TABLE 3 Economic objective values for different simulations at the end of a 5-h process duration.

Operation type			
Objective function weights	Optimization	Total economic objective function	Increase (%)
Time-varying	LEMPC	70,569	47.66
	Steady state	56,541	18.30
Time-invariant	LEMPC	65,614	37.28
	Steady state	47,793	0

Abbreviation: LEMPC, Lyapunov-based economic model predictive control.

and staying constant within a single period) coefficients in all listed scenarios. This approach facilitates a quantitative comparison of the potential loss or gain resulting from the utilization or omission of time-varying coefficients in the objective function.

Remark 16. In Figure 13, the actual state trajectory exits the economically optimal operating region. This is attributed to the use of a different value for the quantization parameter, $d = 1$, as opposed to $d = 8$, resulting in a different bounded error and consequently, a distinct economically optimal region Ω_{ρ_e}. Despite this variation, we have depicted the same regions for comparison purposes, emphasizing that opting for a higher quantization parameter enables a stricter bounded error. Similarly, maintaining lower layer sampling times, and a lower rate of change of the state reference trajectory can lead to tighter bounds on the error.

Remark 17. With respect to comparing the proposed cybersecure, two-layer control architecture to other

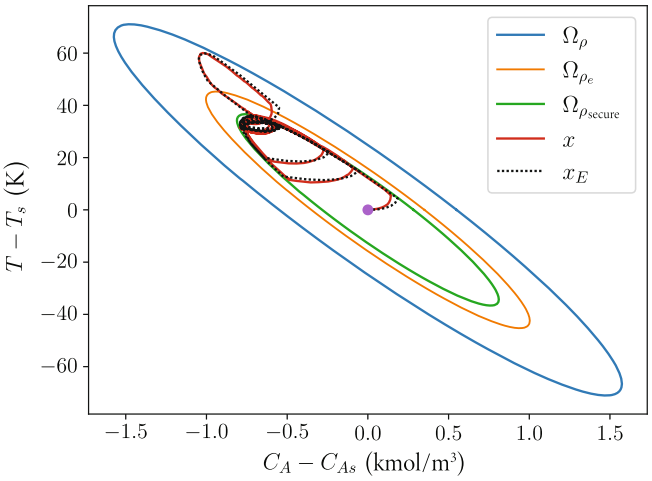

FIGURE 11 State-space plot for the evolution of the state and reference trajectories under the encrypted two-layer control framework using an Lyapunov-based economic model predictive control objective function whose weights change for each operating period, without cyberattack detection and reconfiguration, when a cyberattack is initiated at $t = 4$ h.

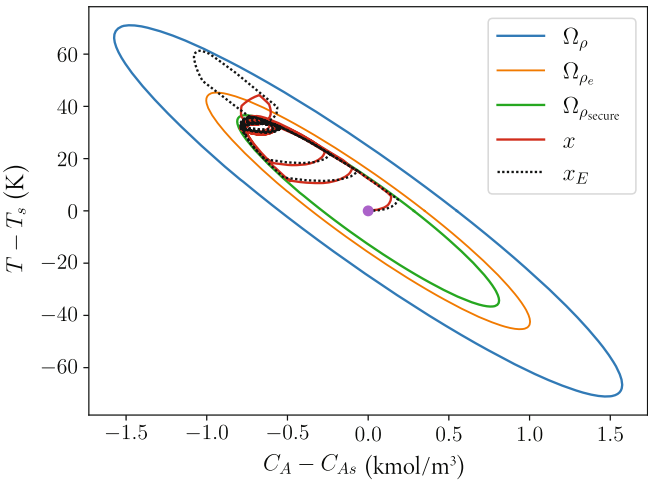

FIGURE 12 State-space plot for the evolution of the state and reference trajectories under the encrypted two-layer control framework using an Lyapunov-based economic model predictive control objective function whose weights change for each operating period, with cyberattack detection and reconfiguration, when a cyberattack is initiated at $t = 4$ h.

approaches, it is important to point out that it is not as optimal as the use of a single-layer EMPC system where there is no need to impose rate of change constraints in the operating trajectory calculated by the EMPC. However, such a single-layer EMPC system (in addition to requiring a significant computational load at the lower layer) is fully nonrobust to cyber-attacks as it requires decrypted signals to carry out calculations in the feedback control layer, rendering it vulnerable to cyber-attacks. If, on the other hand, one were to compare the two-layer control architecture with encryption at the lower layer to the same architecture without encryption, then the performance loss is relatively small when a sufficiently large d value is used as we have demonstrated above (see also Reference 22).

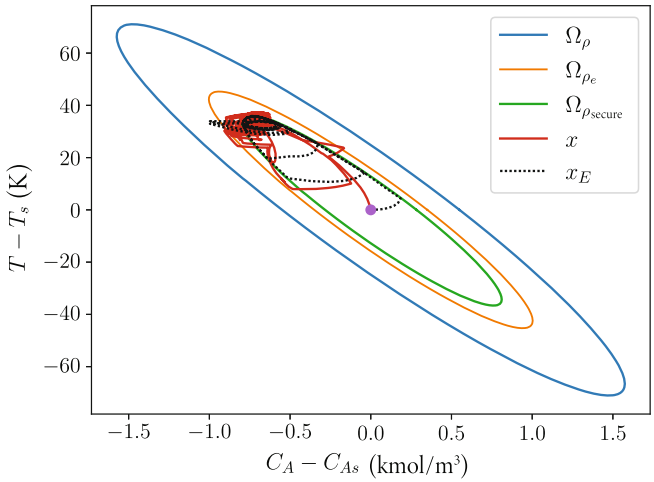

FIGURE 13 State-space plot for the evolution of the state and reference trajectories under the encrypted two-layer control framework using an Lyapunov-based economic model predictive control objective function whose weights change for each operating period, with $d = 1$.

5 | CONCLUSION

In this research, we introduced an encrypted two-layer framework to integrate dynamic economic optimization with encrypted control for nonlinear processes. At the upper layer, an LEMPC with a time-varying objective function computed the economically optimal state trajectories to be tracked by the encrypted lower-layer feedback control system. Through a comprehensive stability analysis, we established bounds on the deviation between the actual state trajectory and reference trajectory, and determined tunable parameters to achieve the desired bounded error. Theoretical results were demonstrated and validated using a chemical process example, and the economic benefits of the encrypted two-layer control framework were showcased. Moreover, we demonstrated the cyber-resilience of the proposed control framework through cyberattack detection and reconfiguration mechanisms when the process was subjected to a cyberattack.

AUTHOR CONTRIBUTIONS

Yash A. Kadakia: conceptualization; methodology; software; writing – review and editing; investigation; formal analysis. **Fahim Abdullah:** conceptualization; methodology; investigation; formal analysis; writing – review and editing. **Aisha Alnajdi:** investigation. **Panagiotis D. Christofides:** conceptualization; methodology; investigation; supervision; funding acquisition; writing – review and editing.

ACKNOWLEDGEMENT

Financial support from the National Science Foundation, CBET-2227241, is gratefully acknowledged.

DATA AVAILABILITY STATEMENT

The data that supports the findings of this study are available in Appendix S1.

ORCID

Yash A. Kadakia https://orcid.org/0009-0006-2266-8214
Panagiotis D. Christofides https://orcid.org/0000-0002-8772-4348

REFERENCES

1. Zhang XM, Han QL, Ge X, et al. Networked control systems: a survey of trends and techniques. *IEEE/CAA J Automat Sin*. 2019;7(1):1-17.
2. Gandhi R, Sharma A, Mahoney W, Sousan W, Zhu Q, Laplante P. Dimensions of cyber-attacks: cultural, social, economic, and political. *IEEE Technol Soc Mag*. 2011;30:28-38.
3. Khan R, Maynard P, McLaughlin K, Laverty D, Sezer S. Threat analysis of BlackEnergy malware for Synchrophasor based real-time control and monitoring in smart grid. *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research*. ACM; 2016:1-11.
4. Tsvetanov T, Slaria S. The effect of the colonial pipeline shutdown on gasoline prices. *Econ Lett*. 2021;209:110122.
5. Amrit R, Rawlings JB, Angeli D. Economic optimization using model predictive control with a terminal cost. *Annu Rev Control*. 2011;35(2):178-186.
6. Ellis M, Christofides PD. Integrating dynamic economic optimization and model predictive control for optimal operation of nonlinear process systems. *Control Eng Pract*. 2014;22:242-251.
7. Darup MS, Redder A, Quevedo DE. Encrypted cloud-based MPC for linear systems with input constraints. *IFAC-PapersOnLine*. 2018;51:535-542.
8. Darup MS, Redder A, Shames I, Farokhi F, Quevedo D. Towards encrypted MPC for linear constrained systems. *IEEE Control Syst Lett*. 2017;2:195-200.
9. Al-Abassi A, Karimipour H, Dehghantanha A, Parizi RM. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*. 2020;8:83965-83973.
10. Dutta V, Choraś M, Pawlicki M, Kozik R. A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors*. 2020;20:4583.
11. Paridari K, O'Mahony N, Mady AED, Chabukswar R, Boubekeur M, Sandberg H. A framework for attack-resilient industrial control systems: attack detection and controller reconfiguration. *Proc IEEE*. 2017;106(1):113-128.
12. Ellis M, Christofides PD. Economic model predictive control with time-varying objective function for nonlinear process systems. *AIChE J*. 2014;60(2):507-519.
13. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*. Springer; 1999:223-238.
14. Carvalho D, Morais J, Almeida J, Martins P, Quental C, Caldeira F. A technical overview on the usage of cloud encryption services. *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited; 2019:733-XI.
15. Barrett MP. *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST Cybersecurity Framework*; 2018.
16. Kadakia YA, Alnajdi A, Abdullah F, Christofides PD. Encrypted decentralized model predictive control of nonlinear processes with delays. *Chem Eng Res Des*. 2023;200:312-324.
17. Kadakia YA, Alnajdi A, Abdullah F, Christofides PD. Encrypted distributed model predictive control with state estimation for nonlinear processes. *Digit Chem Eng*. 2023;9:100133.
18. Luo J. *Machine Learning Modeling for Process Control and Electrochemical Reactor Operation*, Ph.D. Thesis. University of California. 2023.
19. Data61 C. Python Paillier Library. 2013 https://github.com/data61/python-paillier Accessed January 10, 2024.
20. Wächter A, Biegler LT. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Math Program*. 2006;106:25-57.
21. Kadakia YA, Suryavanshi A, Alnajdi A, Abdullah F, Christofides PD. Integrating machine learning detection and encrypted control for enhanced cybersecurity of nonlinear processes. *Comput Chem Eng*. 2024;180:108498.
22. Suryavanshi A, Alnajdi A, Alhajeri M, Abdullah F, Christofides PD. Encrypted model predictive control design for security to cyberattacks. *AIChE J*. 2023;69:e18104.

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: Kadakia YA, Abdullah F, Alnajdi A, Christofides PD. Integrating dynamic economic optimization and encrypted control for cyber-resilient operation of nonlinear processes. *AIChE J*. 2024;70(9):e18509. doi:10.1002/aic.18509