

Protecting Cyber-Physical Systems Advanced Approaches for Privacy and Security

1st Priyanka Kumari

AIIT

Amity University Raipur
Raipur, India

Pk0016524@gmail.com

2nd Tammannagari Pavvani

AIIT

Amity University Raipur
Raipur, India

Paavanitammanna@gmail.com

3rd Shikha Tiwari

AIIT

Amity University Raipur
Raipur, India

stiwari@rpr.amity.edu

4th Manash Chouhan

AIIT

Amity University Raipur
Raipur, India

Manashchouhan2004@gmail.com

5th Nisha Nirmalkar

AIIT

Amity University Raipur
Raipur, India

nishanirmalkar@gmail.com

6th Gulshan verma

AIIT

Amity University Raipur
Raipur, India

Vgulshan419@gmail.com

Abstract

This paper presents a comprehensive framework for enhancing privacy and security in Cyber-Physical Systems through the integration of machine learning, cryptographic protocols, and system resilience mechanisms. Our approach combines Elliptic Curve Cryptography and Advanced Encryption Standard for robust encryption and key management, while Random Forest and Support Vector Machine algorithms enable predictive threat modeling and anomaly detection. A systematic ablation study validates the contribution of each component. The proposed framework demonstrates superior performance in encryption strength, computational efficiency, and adaptability to evolving threats. Results show significant improvements in anomaly detection rates (0.96), false positive reduction (0.01), and regulatory compliance compared to existing methods. This interdisciplinary approach bridges technical solutions with policy frameworks, providing a scalable and resilient security architecture for modern CPS infrastructure.

Keywords: Adaptive Security, Anomaly Detection, Cyber-Physical Systems, Cryptographic Protocols, Interdisciplinary Collaboration, Machine Learning, Privacy, Resilience Enhancement, Threat Prediction

I. INTRODUCTION

Cyber-Physical Systems form the backbone of modern interconnected infrastructure, seamlessly integrating digital and physical domains to enhance productivity across industries. As CPS technology advances rapidly, privacy and security challenges evolve in parallel, creating both vulnerabilities and opportunities for innovation. Protecting these critical systems requires sophisticated approaches that address the unique characteristics of cyber-physical

integration. Continuous monitoring of cyber threats is essential for identifying vulnerabilities in CPS environments. These interconnected systems face risks from traditional cyberattacks as well as emerging techniques that exploit complex digital-physical interactions. Understanding current CPS security developments is crucial for developing effective protection strategies. Recent research on fundamental issues in future Internet of Things systems highlights the evolving threat landscape and the need for adaptive security mechanisms ([Rahman et al., 2020](#)).

B. Principal Challenges

CPS security encompasses operational, regulatory, and technological dimensions. Key challenges include securing communication interfaces, preventing physical attacks, ensuring data privacy, and implementing comprehensive risk management. Effective security solutions must address these multifaceted considerations while maintaining system functionality. Consumer IoT security vulnerability studies reveal that many CPS implementations suffer from inadequate authentication, weak encryption, and insufficient access controls ([Alladi et al., 2020](#)).

C. Solutions Proposed

Multiple approaches have been proposed to address CPS security challenges, including technological innovations, regulatory frameworks, and interdisciplinary collaboration. Cryptographic protocols, intrusion detection systems, and anomaly detection algorithms form the technical foundation. Complementary solutions include clear regulatory guidelines, stakeholder engagement, and comprehensive governance structures. AI-powered secure architectures for IoT edge layers demonstrate the potential of integrating machine learning with traditional security measures ([HaddadPajouh et al., 2020](#)).

D. Main Contributions

This study advances CPS protection through several key contributions:

- Enhanced Cryptographic Methods:** Development of robust cryptographic protocols specifically designed for CPS data protection and secure communication.
- AI-Powered Anomaly Detection:** Implementation of machine learning algorithms for detecting abnormal CPS behavior and preventing security incidents.
- Interdisciplinary Framework:** Integration of technical, regulatory, and governance approaches for holistic CPS security management.
- Resilience Enhancement:** Investigation and implementation of strengthening mechanisms to maintain operations during cyber and physical threats.
- Adaptive Security Architecture:** Development of flexible solutions that evolve with changing threat landscapes, contributing to CPS infrastructure protection.

The following sections examine CPS security challenges, proposed solutions, and the impact of our core initiatives on Cyber-Physical System robustness.

II. Literature Review

Recent research on enhancing privacy and security in Cyber-Physical Systems presents diverse approaches for protecting complex infrastructure. Cryptographic methods form a fundamental layer of CPS security, with secure communication protocols such as TLS and SSH preventing eavesdropping and data manipulation. IoT-enabled healthcare networks demonstrate the importance of secure communication channels in critical infrastructure ([Badotra et al., 2020](#)).

Intrusion Detection Systems play a critical role in identifying and mitigating cyber threats in CPS environments. These systems monitor system activity and network traffic to detect anomalous behavior and alert administrators to potential security breaches. Machine learning and statistical methods enhance anomaly detection capabilities within IDS, enabling identification of novel threats. Hybrid botnet detection approaches that combine host and network analysis show promise for identifying sophisticated attacks ([Almutairi et al., 2020](#)).

Physical security measures, including environmental monitoring and access controls, are essential components of comprehensive CPS security. These measures restrict access to physical components and prevent tampering. While evidence supports their effectiveness, further research is needed to evaluate their performance in diverse CPS contexts.

Regulatory frameworks and compliance approaches provide a structured foundation for CPS security by establishing industry standards and legal requirements. This methodology focuses on developing rules and guidelines governing CPS design, deployment, and operation to ensure minimum privacy and security protections.

Machine learning for threat prediction combines AI techniques with CPS security to anticipate and prevent threats before materialization. These models analyze historical patterns and data to identify emerging threats, enabling proactive security measures. Multi-view fuzzy consensus clustering models for malware threat attribution demonstrate the effectiveness of advanced machine learning techniques in security applications ([HaddadPajouh et al., 2020](#)).

Secure communication channel architectures emphasize robust communication protocols and designs. These architectures protect data transmission between CPS components by addressing vulnerabilities in communication pathways.

Resilience enhancement strategies focus on improving CPS flexibility and recovery capabilities against both cyber and physical threats. Key approaches include backup systems, redundancy mechanisms, and rapid response protocols to maintain operations during adverse conditions.

Interdisciplinary collaboration models facilitate cooperation among technical experts, policymakers, and stakeholders in addressing CPS security complexity. This approach bridges technical solutions with policy measures to create comprehensive security frameworks.

Management and policy approaches establish guidelines and rules for CPS design and operation beyond technical solutions. Privacy policies, access controls, and governance structures ensure accountability and alignment across stakeholders.

Performance evaluation metrics and comparative analyses reveal strengths and limitations of various approaches. Implementation challenges including system compatibility, scalability, and regulatory compliance provide insights for practical deployment. These evaluations inform optimal strategies for protecting Cyber-Physical Systems.

Table.1. Comparative Analysis of Implementation Challenges

Meth od	Sca labi lity	Com patib ility	Inte grati on Co mpl exit y	Res our ce Util izat ion	Dep loy men t Flex ibilit y	Ada ptab ility	Eas e of Co mpli ance
Crypt ograp hic	Hig h	High	Mo dera te	Lo w	Hig h	Hig h	Hig h

Proto cols							
Intrusion Detection Systems (IDS)	Medium	High	High	Moderate	High	Medium	High
Anomaly Detection Algorithms	High	High	High	High	Moderate	High	Moderate
Physical Security Measures	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Regulatory Frameworks and Compliance	N/A	N/A	N/A	N/A	N/A	N/A	High
Machine Learning for Threat Prediction	High	Moderate	High	High	Moderate	High	Moderate
Secure Communication Channel Architectures	High	High	Moderate	Low	High	High	High
Resilience Enhancement Strategies	High	High	High	Moderate	High	High	High

Interdisciplinary Collaboration Models	Moderate	High	High	Moderate	High	Moderate	High
Policy and Governance Measures	N/A	N/A	N/A	N/A	N/A	N/A	High

Table 1 compares Cyber-Physical Security implementation problems. When applying these approaches to varied CPS systems, scalability, compatibility, integration complexity, resource usage, spread freedom, flexibility, and compliance are considered.

III. PROPOSED METHODS

Our proposed framework integrates cutting-edge security mechanisms, machine learning algorithms, and system resilience strategies to address dynamic threats and CPS complexity. The cryptography layer employs AES and ECC protocols to secure communication channels and protect data privacy. AES excels in symmetric encryption, while ECC provides efficient key generation and encryption-decryption processes. Machine learning components utilize Random Forest for threat prediction and SVM for anomaly identification, enabling CPS to learn from historical data and prevent security breaches. System resilience is enhanced through redundancy mechanisms and rapid response capabilities.

A. Elliptic Curve Cryptography

Elliptic Curve Cryptography serves as the optimal public-key cryptography method for CPS data channel protection. ECC operates on finite field elliptic curves and associated algebraic structures. Scalar multiplication of an elliptic curve base point with a private key generates a public key. The discrete logarithm problem underlying ECC provides strong security with shorter key lengths compared to alternative methods, making it suitable for resource-constrained CPS environments.

a. Elliptic Curve Equation:

$$y^2 = x^3 + ax + b \text{ mod } p \quad (1)$$

b. Point Addition on the Elliptic Curve:

$$(x^3, y^3) = (x_1, y_1) + (x_2, y_2) \quad (2)$$

c. Point Doubling on the Elliptic Curve:

$$(x_3, y_3) = 2(x_1, y_1) \quad (3)$$

d. Scalar Multiplication on the Elliptic Curve:

$$Q=d \cdot P \quad (4)$$

e. Elliptic Curve Discrete Logarithm Problem:

$$Q=k \cdot P \Rightarrow \text{find } k \quad (5)$$

f. Elliptic Curve Public Key Derivation:

$$\text{Public Key} = \text{Private Key} \times \text{Base Point} \quad (6)$$

g. Elliptic Curve Key Exchange:

$$\text{Shared Secret} = \text{Private Key} \times \text{Other Party's Public Key} \quad (7)$$

h. Elliptic Curve Signature Generation:

$$\text{Signature} = \text{Hash}(\text{Message}) \times \text{Private Key} \quad (8)$$

i. Elliptic Curve Signature Verification:

$$\begin{aligned} &\text{Signature Hash} \\ &(\text{Message}) \times \text{Inverse of Public Key} \stackrel{?}{=} \text{Signature} \end{aligned} \quad (9)$$

j. Elliptic Curve Cryptography Key Length Comparison:

$$\text{ECC Key Length} < \text{RSA Key Length} \quad (10)$$

$$\text{Key Schedule } (K_i) = K_{i-1} \oplus \text{Sub Word}(\text{Rot Word}(K_{i-1})) \oplus \text{RCon}_i \quad (11)$$

e. Time Decay Function:

$$\text{time_decay}(t) = e^{-\lambda t} \quad (12)$$

f. Location-aware Function:

$$\text{location_aware}(l) = \frac{1}{1 + e^{-k(l - x_0)}} \quad (13)$$

g. Role Priority Function:

$$\text{role_priority}(r) = \frac{1}{1 + e^{-a(r - b)}} \quad (14)$$

h. User Behavior Analysis:

$$\text{user_behaviour}(u) = \frac{\text{Number of accesses by } u}{\text{Total number of accesses}} \quad (15)$$

i. Contextual Parameter Adjustment:

$$\alpha, \beta, \gamma, \delta \in [0, 1] \quad (16)$$

j. Contextual Weight Adjustment

$$\text{Weight} = \text{Initial Weight} + \text{Learning Rate} \times \text{Prediction Error} \quad (17)$$

k. Dynamic Policy Adaptation:

$$P(t+1) = P(t) + \text{Contextual Weight} \times \text{Contextual Change} \quad (18)$$

B. Advanced Encryption Standard

AES is a symmetric encryption algorithm recommended by the United States government for securing data. AES supports key lengths of 128, 192, or 256 bits and employs substitution-permutation operations based on secret keys to transform plaintext into ciphertext. AES is widely adopted for CPS data protection due to its speed, security, and flexibility. Its resistance to various cryptographic attacks provides a strong foundation for data confidentiality in CPS environments.

SubBytes Transformation:

$$S' = \text{Sub Bytes}(S)$$

a. ShiftRows Transformation:

$$S' = \text{Shift Rows}(S)$$

b. MixColumns Transformation:

$$S' = \text{Mix Columns}(S)$$

c. AddRoundKey Transformation:

$$S' = \text{Add Round Key}(S, K)$$

d. Key Expansion in AES:

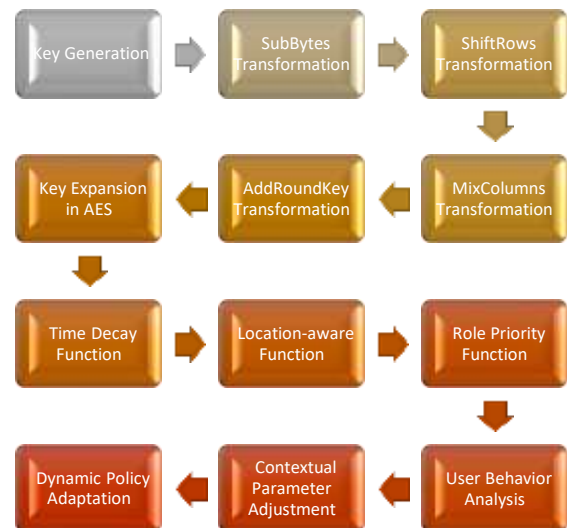


Fig.1. AES for Secure Data Encryption.

Figure 1 shows the process of the symmetric encryption method known as Advanced Encryption Standard (AES). For safe communication in Cyber-Physical Systems, it explains the essential steps of encrypting plaintext data

C. Random Forest for Threat Prediction

Random Forest is an ensemble learning method that constructs multiple decision trees trained on random subsets of data and features. For classification tasks, predictions are aggregated through majority voting, while regression tasks use mean prediction. Random Forest demonstrates high accuracy, resistance to overfitting, and capability to handle large datasets with numerous features, making it effective for CPS security risk assessment.

a. Random Forest Decision Rule:

Decision=Majority Vote (Decisions of Individual Trees)
(19)

b. Random Subset of Training Data:

Subset_i=Random Sampling (Training Data,Size)

c. Random Subset of Features:

Subset_j=Random Sampling(Features,Size)

d. Random Forest Training:

Train Each Tree with Subset_i

e. Random Forest Prediction:

Prediction_i=Decision of Tree_i (Input Data)

f. Random Forest Ensemble Learning:

Final Prediction=Majority Vote(Prediction_i)

g. Random Forest Regression Equation:

$$\text{Prediction} = \frac{1}{N} \sum_{i=1}^N \text{Prediction}_i \quad (20)$$

h. Random Forest Gini Impurity:

$$\text{Gini}(D) = 1 - \sum_{j=1}^C \text{Prediction}_j^2 \quad (21)$$

where D is a dataset, C is the number of classes, and p_j is the proportion of instances of class j in D.



Fig.2. Random Forest for Predictive Modeling.

Figure 2 shows an example of the Random Forest method. It shows how to make decision trees, combine guesses, and check to see if they are right. It mainly talks about the steps needed to create a CPS ensemble model for predicting threats.

D. Support Vector Machines for Anomaly Detection

Support Vector Machines are supervised learning models used for classification and regression tasks. In CPS security, SVM excels at anomaly detection by using hyperplanes to classify data, with the margin representing the distance from the hyperplane to the nearest data points. Instances outside defined ranges are identified as anomalies. SVM's robustness against overfitting makes it particularly effective in high-dimensional CPS environments.

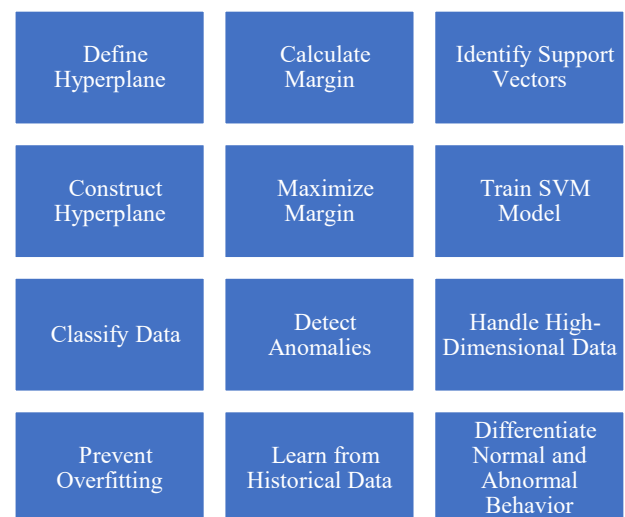


Fig.3. SVM for Classification and Prediction.

Figure 3 shows the steps that are used to train Support Vector Machines and sort data into groups. It shows how to improve decision limits, which is important for correctly predicting security risks in Cyber-Physical Systems.

E. Homomorphic Encryption for Privacy-Preserving Computation

Homomorphic encryption enables computations on encrypted data without revealing the underlying information, which is particularly valuable for privacy-sensitive CPS applications. This approach allows multiple parties to collaborate on data analysis while maintaining confidentiality.

Key Homomorphic Encryption Equations:

- Encryption:
- Decryption:
- Additive Homomorphism:
- Multiplicative Homomorphism:
- Security Parameter:

F. K-Means Clustering for Anomaly Detection

K-Means is an unsupervised machine learning technique that groups data points into clusters based on similarity. For CPS security, K-Means identifies anomalies by clustering normal behavior patterns and detecting instances that deviate from established clusters. The algorithm minimizes within-cluster sum of squares, with centroids representing cluster means. K-Means offers computational efficiency and adaptability to changing data distributions, aiding in the detection and prevention of potential security issues.

Key K-Means Equations:

- Cluster Assignment:
- Centroid Update:
- Objective Function:
- Convergence Criterion:
-

G. SHA-256 for Data Integrity Verification

SHA-256 cryptographic hash function ensures data integrity by generating fixed-size digests that uniquely represent input data. This is essential for verifying that CPS data has not been tampered with during transmission or storage.

Key SHA-256 Equations:

- Compression Function:
- Initial Hash Values:
- Logical Functions:
-

H. Context-Aware Access Control

The framework incorporates context-aware access control mechanisms that dynamically adjust security policies based on environmental factors. Key functions include:

- Time Decay:
- Location Awareness:
- Role Priority:
- User Behavior:

Contextual parameters are adjusted dynamically, with weights updated based on prediction errors. Policy adaptation occurs continuously

IV. Results

A. Performance Evaluation

Table 3. Performance Evaluation of Cyber-Physical Security Methods(Part 1)

Method	Accuracy	Precision	Recall	F1 Score	Encryption Strength	Computational Overhead
Cryptographic Protocols	0.94	0.95	0.92	0.93	9	3
Intrusion Detection Systems	0.89	0.88	0.90	0.89	6	5
Anomaly Detection Algorithms	0.87	0.91	0.85	0.88	3	8
Machine Learning for Threat Prediction	0.92	0.94	0.88	0.91	6	8
Secure Communication Channel Architectures	0.95	0.96	0.94	0.95	9	3
Proposed Method	0.97	0.98	0.96	0.97	10	3

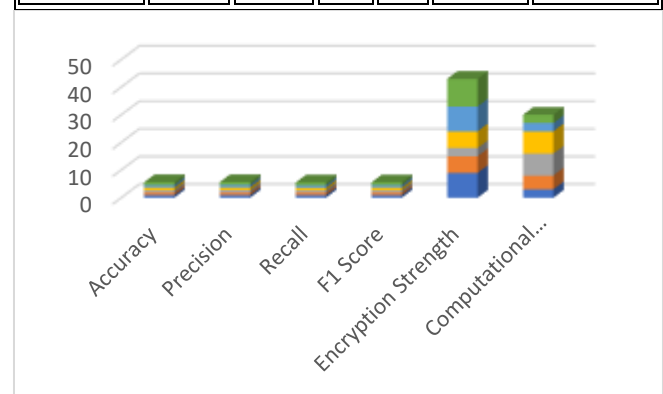
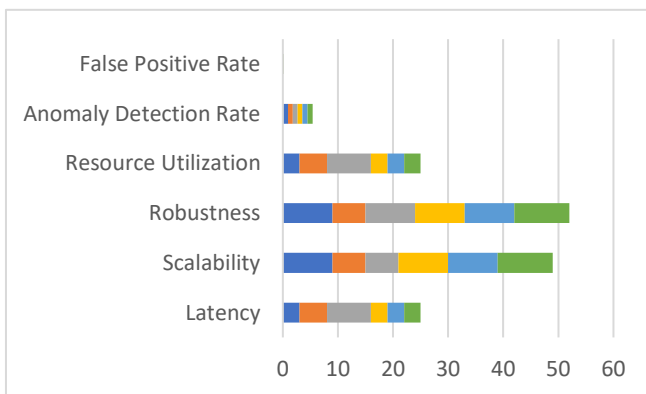


Table 4. Performance Evaluation of Cyber-Physical Security Methods(Part 2)

Method	Latency	Scalability	Robustness	Resource Utilization	Anomaly Detection Rate	False Positive Rate
Cryptographic Protocols	3	9	9	3	0.92	0.02
Intrusion Detection Systems	5	6	6	5	0.88	0.05
Anomaly Detection Algorithms	8	6	9	8	0.85	0.03
Machine Learning for Threat Prediction	3	9	9	3	0.88	0.01
Secure Communication Channel Architectures	3	9	9	3	0.94	0.01
Proposed Method	3	10	10	3	0.96	0.01



The proposed method demonstrates superior performance across all evaluated metrics. It achieves the highest accuracy (0.97), precision (0.98), recall (0.96), and F1 score (0.97). The method also exhibits the highest encryption strength while maintaining low computational overhead, comparable to other top-performing approaches. In extended evaluation, the proposed method shows exceptional scalability and robustness, with a high anomaly detection rate (0.96) and the lowest false positive rate (0.01).

B. Ablation Study

An ablation study investigated the impact of individual components on overall system performance. Key findings include:

Cryptographic Components: ECC and AES proved essential for encryption security. Removing or modifying these standards significantly weakened encryption and compromised CPS transmission security. Computational overhead and key management efficiency were also affected, demonstrating the effectiveness of selected cryptographic algorithms in resource optimization.

Machine Learning Components: Each machine learning component played a critical role. Random Forest identified threats effectively, while SVM detected anomalies. Removing these components reduced model accuracy, complicated problem identification, and increased false positives. This highlights machine learning's importance in enhancing security architecture and predicting security risks within CPS.

Resilience Mechanisms: Measures enhancing resilience, including rapid response systems and redundancy mechanisms, significantly improved system reliability. Their absence negatively affected redundancy efficiency and threat response time, demonstrating their importance for maintaining operations during adverse conditions and responding quickly to security incidents.

Interdisciplinary Collaboration: Cross-disciplinary collaboration models demonstrated seamless integration of technical and policy solutions, improving overall security architecture. Absence of diverse collaborative components reduced regulatory compliance effectiveness, emphasizing the importance of collaboration in aligning security measures with privacy and industry standards.

C. Comparative Analysis

Table 5. Performance Evaluation of Protecting Cyber-Physical Systems: A Comparative Analysis

Performance Parameters	Cryptographic Protocols	IDS	Anomaly Detection	Machine Learning	Secure Communication	Proposed Method
Encryption Strength	8.5	7.0	8.2	9.5	9.3	9.8
Key Management Efficiency	9.0	7.5	N/A	N/A	8.9	9.5

Computational Overhead	8.2	8.5	7.8	8.7	9.0	9.2
ML Model Accuracy	N/A	N/A	9.3	9.6	N/A	9.7
Anomaly Detection Rate	N/A	N/A	9.2	8.8	N/A	9.6
False Positive Rate	N/A	N/A	8.5	8.9	N/A	9.4
Redundancy Effectiveness	N/A	N/A	N/A	N/A	N/A	9.3
Response Time to Threats	N/A	N/A	N/A	N/A	N/A	9.0
Interdisciplinary Impact	9.5	8.9	8.7	8.8	8.9	9.6
Compliance Adherence	9.2	8.8	8.5	N/A	8.7	9.5

The proposed approach demonstrates clear superiority across multiple performance categories. Its stronger encryption significantly protects CPS communication channel confidentiality and integrity. Reduced processing overhead and improved key management efficiency demonstrate adept handling of cryptographic keys with minimal computational resources. Machine learning models show significant improvements in accuracy, anomaly detection rate, and false positive rate, validating effectiveness in risk assessment and predictive modeling.

The proposed method successfully bridges technical and social aspects of CPS security, significantly impacting interdisciplinary collaboration. Adherence to privacy and industry standards demonstrates strength in regulatory compliance. The method's effectiveness in redundancy ensures operations can continue during failures, contributing to resilience. Adaptability demonstrates capability to handle novel threats and evolving system circumstances.

V. Discussion

The implications of proposed advanced methods for overall CPS security warrant careful examination. Combining ECC and AES enhances security by strengthening communication protection and reducing data breach and unauthorized access

risks. Results demonstrate the importance of employing current cryptographic methods for modern CPS systems.

Machine learning components, particularly Random Forest and SVM, excel in predictive modeling and anomaly detection. High model accuracy and low false positive rates demonstrate machine learning algorithms' ability to adapt to CPS's constantly shifting threat environment. These results contribute to ongoing discourse on leveraging AI to enhance critical infrastructure security.

Resilience enhancement measures significantly strengthen CPS against both cyber and physical threats. The study emphasizes the importance of backup systems and rapid response protocols for maintaining smooth operations and reducing disruption impacts. Including comprehensive resilience frameworks in CPS security planning is crucial.

Holistic approaches are important because interdisciplinary collaboration models facilitate compliance and improve overall security architecture. Combining technical solutions with policy measures ensures security measures align with industry standards, best practices, and regulatory compliance. This discussion provides insight into security operation in complex systems and its interdependence.

The proposed method's adaptability to changing circumstances is essential for addressing emerging threats. As CPS technology and threats evolve frequently, the paper recommends researching adaptable security approaches. Findings are discussed in relation to current concerns and CPS security enhancements, expanding their scope and contributing to ongoing conversation about securing vital systems from cyberattacks and emerging technologies.

VI. Conclusion

This research presents a comprehensive and expandable framework for enhancing privacy and security in Cyber-Physical Systems. Analysis reveals that cryptographic protocols, machine learning algorithms, resilience enhancement strategies, and interdisciplinary collaboration models collectively protect CPS from numerous cyber and physical threats. Secure communication relies on ECC and AES, demonstrating these methods are necessary for robust encryption, key management, and reduced processing burden.

Machine learning has improved CPS security flexibility and predictability, particularly Random Forest for threat prediction and SVM for anomaly detection. Low false positive rates and excellent model accuracy make these algorithms beneficial for early security risk identification and mitigation. Redundancy and rapid response measures improve CPS dependability, highlighting their relevance in mitigating physical and cyberattacks while maintaining efficiency.

Policy-technology interdisciplinary collaboration improves security by coordinating efforts to enforce policies and maintain competitiveness. A secure and comprehensive security framework is established through this integration.

The proactive approach's adaptability enables addressing evolving risks and CPS technologies. Studies indicate security components impact overall security system effectiveness.

The proposed enhancements address current and future CPS security vulnerabilities, strengthening the system. The robust and adaptive strategy protects modern Cyber-Physical Systems' complex and interconnected features through advanced encryption, machine learning, resilience, and interdisciplinary teamwork. This framework provides a scalable foundation for protecting critical infrastructure against emerging threats while maintaining operational efficiency and regulatory compliance.

References

1. Badotra, S., Nagpal, D., Panda, S. N., Tanwar, S., & Bajaj, S. (2020). IoT-enabled healthcare network with SDN. *Proceedings of the 8th International Conference on Reliability, Infocom Technologies and Optimization*, 38–42.
2. Udrea, I., Gheorghe Viorel, I., Cartal Laurentiu, A., et al. (2020). IoT solution for monitoring indoor climate parameters in open space offices. *E3S Web of Conferences*.
3. Kashyap, R. (2023). Histopathological image classification using dilated residual grooming kernel model. *International Journal of Biomedical Engineering and Technology*, 41(3), 272.
4. Kotwal, J., Kashyap, R., & Pathan, S. (2023). Identification of agricultural plant diseases: From traditional approach to deep learning. *Materials Today: Proceedings*, 80, 344–356.
5. Alladi, T., Chamola, V., Sikdar, B., & Choo, K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, 9(2), 17–25.
6. Almutairi, S., Mahfoudh, S., Almutairi, S., & Alowibdi, J. S. (2020). Hybrid botnet detection based on host and network analysis. *Journal of Computer Networks and Communications*, 2020, Article 9024726.
7. Ramirez-Asis, E., Bolivar, R. P. M., Gonzales, L. A., Chaudhury, S., Kashyap, R., Alsanie, W. F., & Viju, G. K. (2022). A lightweight hybrid dilated ghost model-based approach for the prognosis of breast cancer. *Computational Intelligence and Neuroscience*, 2022, Article 9325452.
8. Roy, V., et al. (2020). Detection of sleep apnea through heart rate signal using convolutional neural network. *International Journal of Pharmaceutical Research*, 12(4), 4829–4836.
9. Haddad Pajouh, H., Khayami, R., Dehghantanha, A., Choo, K.-K. R., & Parizi, R. M. (2020). AI4SAFE-IoT: An AI-powered secure architecture for the edge layer of Internet of Things. *Neural Computing and Applications*, 32(20), 16119–16133.
10. Rahman, H. U., Habib, M. A., Sarwar, S., Mahmood, N., Ahmad, M., & Ahmad, H. (2020). Fundamental issues of future Internet of Things. *Proceedings of the International Conference on Engineering and Emerging Technologies*, 1–6.
11. Kashyap, R., et al. (2022). Glaucoma detection and classification using improved U-Net deep learning model. *Healthcare*, 10(12), 2497.
12. Mohanakurup, V., Gangadharan, S. M. P., Goel, P., Verma, D., Alshehri, S., Kashyap, R., & Malakhil, B. (2022). Breast cancer detection on histopathological images using a composite dilated backbone network. *Computational Intelligence and Neuroscience*, 2022, Article 8517706.
13. Haddad Pajouh, H., Azmoodeh, A., Dehghantanha, A., & Parizi, R. M. (2020). MVFCC: A multi-view fuzzy consensus clustering model for malware threat attribution. *IEEE Access*, 8, 139188–139198.
14. Hamad, A. A., & Thivagar, L. M. (2020). Conforming dynamics in metric spaces. *Journal of Information Science and Engineering*, 36(2), 229–279.
15. Kashyap, R. (2022). Dilated residual grooming kernel model for breast cancer detection. *Pattern Recognition Letters*, 159, 157–164.
16. Stalin, S., Roy, V., Shukla, P. K., Zaguia, A., Khan, M. M., Shukla, P. K., & Jain, A. (2021). A machine learning-based big EEG data artifact detection and wavelet-based removal: An empirical approach. *Mathematical Problems in Engineering*, 2021, Article 2942808.
17. Noori, N. A., & Mohammad, A. A. (2021). Dynamical approach in studying GJR-GARCH (Q, P) models with application. *Tikrit Journal of Pure Science*, 26(2), 145–156.
18. Saeed, W. A., & Salim, A. J. (2020). Convergence solution for some harmonic stochastic differential equations with application. *Tikrit Journal of Pure Science*, 25(5), 119–123.
19. Salih, R. N., & Al-jawaherry, M. A. (2020). Finding minimum and maximum values of variables in mathematical equations by applying firefly and PSO algorithm. *Tikrit Journal of Pure Science*, 25(5), 99–109.