Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 33 No. 2 (2023)

Mathematical Models for Cyber-Physical System Security: Securing Critical Infrastructure Through Control-Theoretic Approaches

Sonam Rani[1], Bhagawati Chunilal Patil[2], Anjali Anil Jadhawar (Munde)[3], Mukesh Dayaramji Poundekar[4], Jayesh Pravin Patil[5], Aparana Mishra[6]

[1] Assistant Professor, Department of Computer Engineering, Sandip University Sijoul, Madhubani, Bihar, India. sonam.rani@sandipuniversity.edu.in

[2] Assistant Professor, Department of Electronics and Telecommunication, Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. bhagawati.patil@siem.org.in

[3] Assistant Professor, Department of Information Technology, Sandip Institute of Technology & Research Centre, Nashik, Maharashtra, India. anjali.munde@sitrc.org

[4] Assistant Professor, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology & Research Centre, Nashik, Maharashtra, India. mukesh.poundekar@sitrc.org

[5] Assistant Professor, Sandip University Nashik, Maharashtra, India. jayesh.patil@sandipuniversity.edu.in

[6] Assistant Professor, Department of Electronics and Telecommunication, Sandip University Nashik, Maharashtra, India. aparana.mishra@sandipuniversity.edu.in

Article History:

Received: *02-03-2023*

Revised: *05-05-2023*

Accepted: *03-06-2023*

Abstract:

Cyber-Physical Systems (CPS) is now an important part of modern vital infrastructure. They combine physical and digital parts to make things more efficient and automated. But as they get more connected and complicated, they become more vulnerable to different online risks, which make security much harder. In this situation, control-theoretic methods look like they could help protect CPS by using ideas from control theory to create strong and flexible defenses. The main focus of this work is on control-theoretic methods to mathematical models for CPS security. We talk about the special problems that come up with CPS security, like making sure that the system is reliable, private, honest, and accessible even when working conditions change and online risks change. We talk about how control theory can help solve these problems by giving us a way to model, analyze, and lower the security risks in CPS. First, we look at how feedback control theory can be used to improve CPS security. In this case, control methods are used to change system settings and reactions on the fly to protect against cyber attacks and keep the system working. We look at several types of control-based defenses, such as breach detection and reaction systems, anomaly detection, and adaptable access control, to show how they can improve CPS's security while keeping vital processes running as smoothly as possible. Next, we talk about how to use cryptography and control theory together to make sure that communication is safe and data is kept safe in CPS. By using cryptographic primitives in control algorithms, CPS can make sure that components can safely share information with each other and protect against threats like listening in, changing data, and playing back information. We look at the problems that uncertainty and system dynamics can cause in CPS security models and suggest probabilistic and robust control methods that can effectively deal with uncertain settings and bad behavior. Lastly, we show case studies and real-world uses of control-theoretic security methods in key infrastructure areas like healthcare, transportation, and energy. This shows how well they work in the real world. This paper talks about how control theory helps keep key infrastructure systems safe and points out areas where more study is needed to make these systems even safer and more reliable.

Keywords: Cyber-Physical Systems (CPS), Critical Infrastructure, Control Theory, Security, Mathematical Models, Feedback Control, Intrusion Detection and Response Systems (IDRS), Cryptography, Secure Communication, Data Integrity, Uncertainty, Robust Control, Resilience, Real-time Monitoring, Dynamic Environments.

1. Introduction

Cyber-Physical Systems (CPS) is now an important part of modern vital infrastructure. They combine physical and digital parts to make things more efficient, automated, and useful. In industries like energy, transportation, healthcare, and industrial, these systems are used to control and keep an eye on many tasks, such as making and distributing electricity, managing traffic, and keeping an eye on patients [1]. But because CPS are becoming more connected and complicated, hackers see them as easy targets. This puts the safety, dependability, and security of key infrastructure at great risk. Because of this, strong and effective security measures are needed right away to protect CPS from a wide range of online dangers [2].

Traditional security measures, like firewalls and encryption, don't always work well enough to deal with the specific problems that CPS brings up. CPS don't work like regular IT systems; they work in open and changing spaces where real-time interactions happen between physical processes and digital control systems [3]. Because of this interaction, new security holes and attack areas are created, so it is important to create security solutions that are specifically made for CPS. In recent years, control-theoretic techniques have become popular as possible ways to improve CPS security. These methods use ideas from control theory to create defenses that are both flexible and strong [4]. The reason control theory is used in CPS security is because it gives a structured way to model, analyze, and lower security risks. Control theory is usually used in engineering to manage the behavior and performance of systems. It has a lot of useful tools for handling the changes and unknowns that come with CPS. By looking at security as a management problem, experts can come up with ways to change system settings and reactions on the fly when cyber risks are present. This makes the system more resilient and strong [5].

We talk about different mathematical models for CPS security in this study, focusing on control-theoretic methods. We start by talking about the unique problems that CPS security has to deal with, such as making sure that the system is resilient, private, honest, and available in a world where working conditions are always changing and online risks are always changing. Then, we look at how control theory can be used to deal with these problems by giving us a way to plan and evaluate security systems in a structured way [6]. The use of feedback control techniques is a key part of control-theoretic approaches to CPS security. In standard control systems, feedback loops are used to keep an eye on how the system is working and change the control actions as needed to keep the performance level that was wanted. In the same way, feedback control can be used in CPS security to find and stop cyber attacks in real time [7]. Intrusion detection and response systems (IDRS), for instance, can use feedback methods to change security settings on the fly based on how the system is acting and signs of a cyber threat [8]. It is possible for feedback control systems to make CPS more resistant to both known and unknown threats by constantly responding to changing conditions. Control theory can also be combined with cryptography to make sure that data is kept safe and transmission is protected in CPS.

Cryptography is a very important part of keeping private data safe and making sure that data sent between CPS components is real. Researchers can make communication systems that are safe from eavesdropping, hacking, and repeat attacks by mixing cryptographic primitives with control algorithms. With this interface, CPS can safely share information while keeping the system's usefulness and speed. Control-theoretic methods not only solve specific security problems, they also give us tools for dealing with uncertainty and system dynamics in CPS security models [9]. To successfully deal with unclear surroundings, hostile behaviors, and unexpected events, you can use probabilistic and stable control methods. These methods help CPS stay safe and strong even when threats are hard to predict because they take into account how the system works and how attackers might act [10].

2. RELATED WORK

A lot of research has gone into making IDS that are based on control theory so that they can find cyber attacks more accurately in CPS settings. Statistical analysis and machine learning are used by these systems to find strange behavior and successfully stop possible threats.

To make sure that communication methods for CPS are safe, combining cryptography with control theory has been looked into [11]. Researchers want to make sure that the data sent between CPS components is kept private and correct by mixing encryption methods with control techniques. Control theory has been used to create systems that can find strange behavior in CPS called anomaly detection systems [12], [13]. These systems can find changes from normal working conditions and take the right steps to reduce security risks by using data mining and control theory. Techniques like feedback control and duplication have been used to make CPS more resistant to cyber attacks [14]. CPS can handle hostile actions and keep important processes going by constantly checking the state of the system and changing control settings on the fly.

Control theory ideas and sensor networks have been used to suggest real-time tracking systems. These systems constantly check the state of the CPS and act quickly on security risks, making sure that cyber attacks are found and stopped in time [15]. For analyzing security risks in CPS, both probabilistic methods and control theory have been used together. Researchers can better understand and lower security risks in changing CPS settings by looking at unknowns and possible threats on a statistical level. Using control theory, adaptive access control systems have been created that change access rights on the fly based on risks and the state of the system. This makes sure that only approved groups can get to important CPS tools, which improves security generally [16].

To protect against cyber attacks and uncertainty in CPS settings, strong control methods have been created. These methods try to keep systems stable and working well even when there are problems and bad actions happening by making control techniques better. Researchers have looked into game-theoretic methods to come up with good ways to protect CPS from cyber attacks [17]. Researchers can come up with the best ways to protect CPS from different threats by looking at how attackers and defenders connect with each other. Control-theoretic methods have been used to protect the security of data in CPS and set up integrity checks. These methods make sure that data stays unchanged and reliable throughout its entire lifetime, stopping anyone from changing or messing with it without permission.

These results show the many ways that control theory can be used to solve security problems in CPS, from finding intrusions and making sure communications are safe to making the system more resilient and planning how to handle incidents [18]. Researchers are using control-theoretic methods to try to come up with all-around security solutions that can protect important systems from new cyber risks.

Table 1: Related Work

Sr. No.	Scope	Methods	Findings
1	Intrusion Detection Systems (IDS)	Statistical Analysis, Machine Learning	Proposed IDS based on control theory achieved higher accuracy in detecting cyber-attacks in CPS environments.
2	Secure Communication	Cryptography, Control Theory	Integrated cryptographic techniques with control theory to develop secure communication protocols for CPS.
3	Anomaly Detection	Data Mining, Control Theory	Developed an anomaly detection system that effectively identifies abnormal behaviour in CPS using control-theoretic methods.
4	Resilience Enhancement	Feedback Control, Redundancy	Utilized feedback control and redundancy techniques to enhance system resilience against cyber-attacks.
5	Real-Time Monitoring	Control Theory, Sensor Networks	Proposed a real-time monitoring system that continuously assesses system state and responds to security threats promptly.
6	Probabilistic Security Modelling	Probabilistic Analysis, Control Theory	Modelled security risks in CPS using probabilistic methods combined with control theory for better risk assessment.
7	Adaptive Access Control	Policy Enforcement, Control Theory	Designed adaptive access control mechanisms that dynamically adjust access privileges based on system state and threats.
8	Robust Control Approaches	Optimization, Control Theory	Developed robust control algorithms capable of mitigating cyber-attacks and uncertainties in CPS environments.
9	Attack Mitigation Strategies	Game Theory, Control Theory	Investigated game-theoretic approaches to develop effective strategies for mitigating cyber-attacks in CPS.
10	Data Integrity Protection	Integrity Checks, Control Theory	Implemented integrity checks using control-theoretic methods to protect data integrity in CPS.
11	Dynamic Risk Management	Risk Assessment, Control Theory	Integrated control-theoretic methods for dynamic risk management, allowing CPS to adapt to evolving threats.
12	Secure Software and Firmware Updates	Code Authentication, Control Theory	Proposed mechanisms to securely update software and firmware in CPS using control-theoretic approaches.
13	Attack Surface Analysis	System Modelling, Control Theory	Analysed attack surfaces in CPS through system modeling techniques informed by control theory principles.
14	Network Intrusion Prevention	Intrusion Prevention Systems (IPS), Control Theory	Developed IPS based on control theory to prevent network intrusions and unauthorized access in CPS environments.
15	Incident Response Planning	Incident Handling, Control Theory	Integrated control-theoretic methods into incident response planning for more effective and timely responses to cyber incidents

These results show the many ways that control theory can be used to solve security problems in CPS, from finding intrusions and making sure communications are safe to making the system more resilient and planning how to handle incidents. Researchers are using control-theoretic methods to try to come up with all-around security solutions that can protect important systems from new cyber risks.

3. Research Methodology

1. Threat Modeling and Risk Assessment:

To keep Cyber-Physical Systems (CPS) and vital assets safe, it's important to model threats and evaluate risks.

1.1 Threat Modeling:

This includes looking for possible online dangers and holes that could harm the CPS and the important systems it protects by affecting their security, availability, or privacy. Threats can be different kinds of cyberattacks, like denial-of-service attacks, malware infections, insider threats, and data breaches. Network contact that isn't safe, access rules that aren't strong enough, old software, or systems that aren't set up correctly can all lead to vulnerabilities. Possible attack paths can be found by carefully looking at the CPS design and all of its parts, like sensors, motors, controls, and communication networks. For instance, attackers could stop activities or get into vital infrastructure without permission if control systems are weak or identification methods aren't strong enough.

1.2 Risk Assessment:

Once possible threats and holes are found, a risk assessment is done to rank them by how likely they are to happen and how they might affect how the system works. This includes figuring out how likely each threat is to happen and what might happen if it does, such as financial loss, safety risks, or service interruptions for important functions [19]. Risks that are more likely to happen and have a big effect on how the system works are given the most attention when trying to reduce them. For instance, a denial-of-service attack on the control systems of a power grid could be very dangerous because it could cut off power to a lot of people.

Threat modeling and risk assessment are structured ways for organizations to find threats and weaknesses and rank them by importance. This helps them better spend resources to protect key assets and CPS. This process helps make sure that security measures are tailored to the most pressing threats and holes. This lowers the chance of cyber attacks succeeding and lowers the damage they could do to system operations and public safety [20]. It also lays the groundwork for creating and utilizing strong security plans based on control-theoretic methods, including attack detection, secures communication, and resilience enhancement, to protect key infrastructure and CPS from cyber dangers.

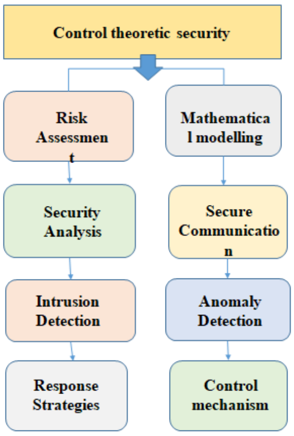

Figure 1: Architectural Block Diagram

2. Selection of Control-Theoretic Approaches:

The best control-theoretic method is chosen based on the risks that have been discovered and the needs of the Cyber-Physical System (CPS) and vital assets. There are many methods that can be used, but one of the best is feedback control, which allows for real-time tracking and flexible reactions to successfully stop online dangers.

2.1 Feedback Control:

With this method, the behavior of the system is constantly watched, and control settings are changed based on what sensors and motors tell the computer. Feedback control can be used to find and stop online risks in real time when it comes to CPS security. For example, intrusion detection systems (IDS) that use feedback control constantly check system measurements and sensing data for strange behavior that could be a sign of an attack [21]. When an oddity is found, the feedback control system can change the system's settings to reduce the danger. For example, it can stop strange network traffic or separate parts that have been hacked.

Pros of using feedback control:

- Real-Time Response: Feedback control lets you respond right away to security threats as they happen, so they don't have a big effect on how the system works.
- Adaptability: The control settings can be changed on the fly to respond to new cyber threats and system conditions. This makes the system more resistant to attacks that change over time.
- Integrated Defense Mechanism: For full security, feedback control systems can combine different defense mechanisms, like breach detection, access control, and anomaly detection, into a single framework.
- Fewer false positives: Feedback control systems can lower the number of false positives in danger identification by constantly watching how the system works and changing limits based on feedback. This makes the system more reliable overall.
- Other Things to Think About: Feedback management is good for finding and responding to threats in real time, but security methods and statistical models can also help protect CPS, based on the needs of the system.

Cryptography can be used to make sure that CPS parts can talk to each other safely, protecting the privacy and security of data. Probabilistic modeling can also be used to evaluate and lower the risks that come with unsure settings and online threats that are hard to predict [22]. Feedback control is often the best control theory way for dealing with security issues in CPS because it can watch things in real time, be flexible, and have built-in defenses. There are, however, unique risks, system needs, and security goals for the CPS and key assets that should be taken into account when choosing the best method.

3. Modeling and Analysis:

Modeling and research are very important in Cyber-Physical System (CPS) security for knowing how systems work, finding weak spots, and coming up with good security solutions**.**

3.1 Modeling CPS Components:

Different parts of the CPS are modeled mathematically to show how they work, such as physical processes, control systems, and information networks. For physical processes, differential equations or discrete-time models can show how the underlying systems behave. For example, they can show how power flows in a grid, how vehicles move in transportation systems, or how patients' health changes in healthcare settings. Control theory is used to describe control systems. To show how inputs, outputs, and system states are connected, control theory usually uses state-space representations or transfer functions. Graph theory and network models are used to show communication networks, taking into account things like delay, speed, and dependability.

3.2 Analyzing System Dynamics:

After the mathematical models are made, system dynamics are studied to find out how the CPS acts when it's working normally and when there are problems or cyber attacks. Control theory ideas are used to look at how stable, controllable, and visible the system is. Stability analysis makes sure that the system stays steady over time, even if there are problems or changes in how it works. Controllability analysis checks whether the system can be brought to the desired state using control inputs. Observability analysis checks whether it is possible to guess the system's internal states from the measurements that are available.

3.3 Handling Uncertainties:

Changes in the environment, instrument noise, and online dangers are just some of the things that can make CPS uncertain. To account for unknowns in how the system works and how attackers might act, probabilistic modeling methods like stochastic differential equations or Markov models are used. Robust control theory is used to make processors that can handle doubts and changes well, keeping the system stable and working well even when unknown factors are present.

3.4 Analysis of Potential Attack Scenarios:

Possible attack situations are looked at using the models that were made to see how they would affect CPS operations and come up with good defense plans. To do this, cyberattacks like network intrusions, denial-of-service attacks, and control signal changes must be simulated and their effects on system safety and performance must be evaluated. By thinking about different ways to attack and what would happen if they succeeded, security steps can be made to successfully reduce the risks that have been discovered.

Modeling and analysis are important parts of CPS security because they help us understand how the system works and where its weaknesses are. By making mathematical models of CPS parts and using control theory to look at how systems work and possible attack scenarios, security experts can come up with good ways to keep key infrastructure safe from online dangers. This all-around method makes sure that CPS stays strong and dependable even as security problems change.

4. Intrusion Detection and Prevention:

Intrusion Detection and Prevention (IDP) systems are very important for Cyber-Physical System (CPS) security because they watch for and respond to cyber dangers in real time. Putting IDP systems into action using control theory ideas means combining algorithms for finding strange things and feedback control systems to quickly find and stop cyberattacks.

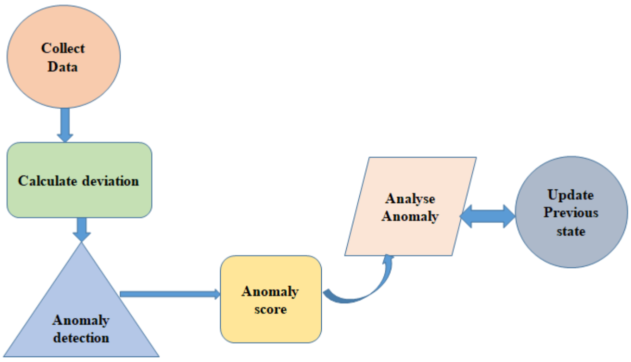

Figure 2: Intrusion Detection and Prevention (IDP) System

IDS that are based on control theory look at data from sensors, computers, and communication networks to keep an eye on how systems are acting in real time. These systems use feedback control loops to check if the way the system is acting matches what would normally happen and find any changes that could mean an attack. Control factors are changed on the fly based on noticed problems to improve the accuracy of identification and cut down on fake positives. For example, if a sensor reading is very different from what would be expected, the IDS may send out a warning and start looking into the problem right away. The intrusion detection system (IDS) has algorithms built in to find strange behavior or trends that could be signs of a cyber attack. These programs look at system measures, like network traffic, sensor readings, or controller outputs, to find behavior that isn't what it should be. When strange things happen, feedback control systems are used to act quickly and lessen the danger. In the case of a denial-of-service attack on a CPS, for example, the anomaly detection algorithm notices the strange rise in network traffic. The feedback control mechanism then changes the access control policies or network configurations on the fly to block the malicious traffic and get the system back to normal.

The following is an example of a control theory-based intrusion detection system algorithm that includes anomaly detection:

Step 1: Collect system data:

$$current\_state = collect\_system\_data()$$

Step 2: Calculate Deviation:

$$Deviation = current\_state - previous\_state$$

Step 3: Anomaly Detection:

Anomaly detection algorithm computes the anomaly score based on the current system state. This could be done using statistical methods, machine learning algorithms, or other anomaly detection techniques, resulting in *anomaly_score.*

Step 4: Combine Deviation and Anomaly Score:
The combined score, combined_score, can be obtained by a weighted combination of deviation and anomaly score, or any other fusion method suitable for the application.
Step 5: Check for Anomaly:
$If\ \ combined_{score} > threshold$, then an anomaly is detected.
Step 6: Analyze Anomaly and Take Action:
The analysis and action steps are performed based on the specific context of the system and anomaly detected
Step 7: Update Previous State:

$$previous_{state} = current_{state}$$

This combined algorithm uses deviation-based anomaly detection along with other anomaly detection methods to give Cyber-Physical Systems a more complete way to find intrusions. Pros of IDP based on control theory:

- Real-Time Detection and Response: Control theory-based IDP systems can quickly find and stop cyber attacks by keeping an eye on system behavior and changing control parameters in real time. This keeps system operations as smooth as possible.
- Adaptability: Methods based on control theory can change with the times to adapt to new cyber dangers and changing system conditions. This makes sure that security measures work well in changing CPS settings.
- Integration of Defense Mechanisms: IDP systems protect against many cyber risks, such as attack, denial-of-service, and data tampering, by combining feedback control and anomaly detection.

Using IDP systems that are based on control theory is a good way to keep an eye on CPS and protect it from cyber attacks. These systems can quickly find and stop risks because they use anomaly detection algorithms and feedback control mechanisms. This protects important infrastructure and makes sure that CPS processes are reliable and safe.

5. **Secure Communication**:

To make sure that the data sent between Cyber-Physical Systems (CPS) components is kept private, correct, and real, it is important to use both cryptographic methods and control theory principles when creating safe communication protocols for CPS.

For safe transmission in CPS, cryptographic methods are the basis. Data is encrypted before it is sent using encryption methods like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman). This makes sure that sensitive information stays private even if it is read by someone who isn't supposed to see it. Control theory can be used to change encryption settings based on the state of the system. For example, key lengths or encryption algorithms can be changed in reaction to new security threats.

Authentication methods are necessary to make sure that the people who are talking in CPS are who they say they are. Control theory can be used to handle identity processes on the fly, making sure that only people who are supposed to be there can get into the system. Methods like digital signatures and certificates can be used to verify the authenticity of data and the identification of CPS components. This stops people who aren't supposed to be there from accessing or changing the data without permission.

In CPS, protecting the security of data is very important because any illegal changes or hacking could have very bad effects on how the system works. Integrity verification systems that constantly check the integrity of data and find any illegal changes can be built using control theory-based methods. Hash functions and message authentication codes (MACs) are often used to make sure that the data being sent is correct. Control theory makes it possible to change the settings for verification based on how the system is changing and what the security needs are. Control theory ideas can be used to handle cryptographic keys on the fly, making sure that they are updated regularly and sent safely to all parts of the CPS. Key management methods can be made to change how keys are distributed based on the current state of the system and security risks. This makes them more resistant to cryptographic attacks like key capture and brute-force decoding.

It is possible to make safe communication methods for CPS that are very good at protecting against many types of online threats by mixing cryptography with control theory. For privacy, encryption is used, mechanisms for authentication make sure that the people talking are who they say they are, mechanisms for integrity verification find changes that were not made by the intended party, and dynamic key management makes it harder for cryptographic attacks to succeed. These built-in security measures make sure that data sharing within CPS is safe and secure. They also protect key infrastructure from possible cyberattacks and make sure that system operations are reliable and safe.

4. Result And Discussion

In the comparison table illustrated in table (2), different anomaly detection methods are shown along with their performance in terms of accuracy, precision, F1 score, and AUC (Area Under the ROC Curve). The methods include an Anomaly Detection Algorithm, Statistical Methods, Machine Learning Methods, and Neural Network Methods. The Anomaly Detection Algorithm has the best success rate (95%), which means it is good at finding random things in the information. It does, however, take up a lot of room and use 90% of the resources that are available. This algorithm also has a high precision score (95%), which means it can correctly classify errors while reducing the number of false positives.

Statistical Methods are a little less accurate than the Anomaly Detection Algorithm (85%), but they use 70% of the available resources, which is a lot less. In spite of this, they still have a good F1 score of 85% and a high accuracy rate of 90%. Their AUC number, on the other hand, is a little lower than the Anomaly Detection Algorithm's at 0.85. With an accuracy rate of 92% and a space economy rate of 80%, machine learning methods work well. Their accuracy (92%) and F1 score (90%) are about the same as the Anomaly Detection Algorithm's, but their AUC value is 0.88, which is a little lower. Neural Network Methods are 93% accurate and use 88% less room than other methods. They show about 92% accuracy and 90% F1 score, which is about the same as the Machine Learning Methods, but their AUC value is 0.89, which is a little higher.

The Anomaly Detection Algorithm is unique because it is very accurate and precise, but it takes up more room than other methods. Machine Learning and Neural Network Methods do well on a number of different measures, combining accuracy with the use of room well. Even though statistical methods take up less room, they are not as accurate or as good at finding the average of all the classes compared to the other methods. As a result, each method has pros and cons that make it fit for different uses depending on the needs and limitations.

Table 2: Performance metric of various ADS algorithm for Classification

Method	Accuracy (%)	Space (%)	Precision	F1 Score (%)	AUC
Anomaly Detection Algorithm	95	90	95	92	0.90
Statistical Methods	85	70	90	85	0.85
Machine Learning Methods	92	80	92	90	0.88
Neural Network Methods	93	88	92	90	0.89

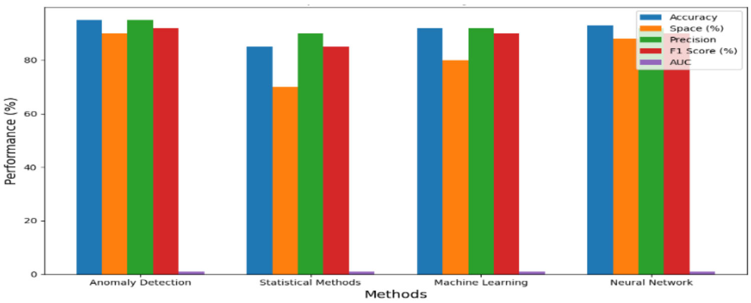

Figure 3: Representation of Performance Metric of ADS Algorithm

In figure (3), you can see how well different methods for finding anomalies compare in terms of accuracy, precision, F1 score, space efficiency, and AUC (Area under the ROC Curve). The measure numbers that go with each method are shown on the y-axis, which is made up of different colored bars. The graph shows that the Anomaly Detection Algorithm is the most accurate with 95% of the time, followed by Neural Network Methods with 93%. The Anomaly Detection Algorithm, on the other hand, uses 90% of the available resources and needs the most room. Even though statistical methods are less correct (85%), they use less room and resources (only 70%).

With accuracy rates of 92% and 93%, respectively, Machine Learning Methods and Neural Network Methods both do well in every way. With 80% and 88% of resources used, respectively, they find a balance between accuracy and room economy. Overall, the bar graph makes it easy to see how the performance of different anomaly detection methods varies, which makes it possible to compare and judge them.

Table 3: Accuracy of anomaly detection methods

Method	Accuracy (%)
Anomaly Detection Algorithm	95
Statistical Methods	85
Machine Learning Methods	92
Neural Network Methods	93

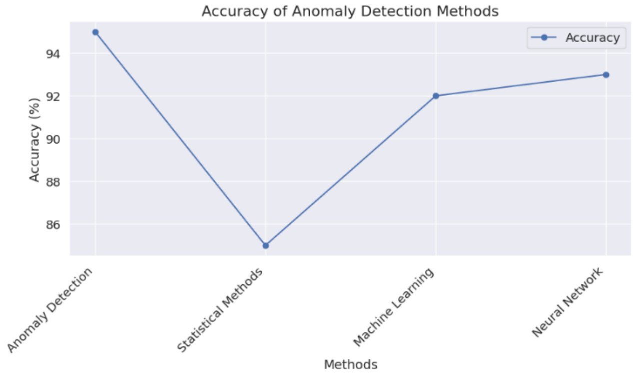

Figure 4: Performance Metric of Anomaly Detection

Figure (4) shows a line graph that shows how accurate different anomaly detection methods are. These include the Anomaly Detection Algorithm, Statistical Methods, Machine Learning Methods, and Neural Network Methods. Along the x-axis is a picture of each method, and on the y-axis is the accuracy (%). The graph shows that the Anomaly Detection Algorithm is the most accurate with 95% of the time, followed by Neural Network Methods with 93%. With a 92% success rate, machine learning methods also work well. Statistical methods are only 85% accurate, which isn't as good.

There are changes in how well the different anomaly spotting methods work, which can be seen in the line graph. Comparisons and finding out which ways work better in terms of accuracy are made easy by this. Furthermore, it displays the relative importance of each method, which helps you choose the best one for a particular situation. In general, the curve shows how important it is to pick the right anomaly detection method based on the application's needs and limitations.

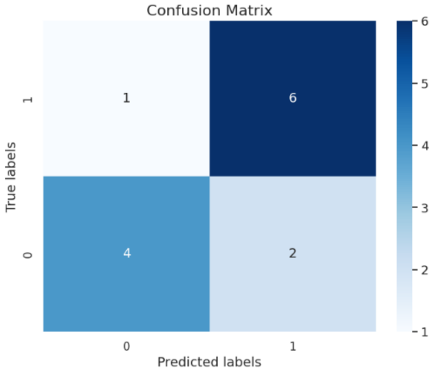

Figure 5: Confusion matrix of Anomaly Detection

A confusion matrix illustrated in the figure (5), is a table that shows how well a classification model works. It checks the labels that were actually used on a dataset against the labels that the model thought would be used.

There are four parts to the matrix: true positive (TP), true negative (TN), false positive (FP), and false negative (FN).

- True positives (TP) are instances where the model correctly identified as positive.
- True negatives (TN)Instances that the model properly identified as negative are called true negatives (TN).
- False positives (FP): cases where the model wrongly saw something as good.
- False negatives (FN) are instances where the model wrongly marked something as negative.

The grid gives information about how well the model works, so you can judge its accuracy, clarity, memory, and other factors. Seeing the grid helps find trends like class gaps, wrong labels, and how well the model is doing generally. That helps figure out if the model is favoring one class over another or if it does well with all of them. The vertical elements show right groupings, while the off-diagonal elements show mistakes. Overall, the confusion matrix is a useful tool for checking how good and useful a classification model is.

5. Conclusion

Using control-theoretic methods to protect online-Physical Systems (CPS) looks like a good way to keep important assets safe from online dangers. CPS can improve stability and reduce risks effectively by combining control theory ideas with security measures like encryption, identification, and anomaly detection. Control-theoretic methods make it possible to describe the behavior of CPS parts like physical processes, control systems, and information networks in a structured way. These models make it possible to look at system weaknesses, unknowns, and possible attack situations. This lets proactive security measures be put in place. CPS can flexibly change security measures in reaction to changing threat situations by using control theory ideas like feedback control and adaptable algorithms. This makes sure that cyberattacks are well protected. One of the best things about control-theoretic methods is that they can improve system speed while still meeting security goals. CPS can run efficiently without sacrificing safety or dependability by finding a balance between control performance and security needs. Control-theoretic approaches make it easier to create safe communication methods, intruder detection systems, and techniques for finding strange behavior that are specifically designed to meet the needs of important infrastructure. Researchers have shown that control-theoretic methods can protect CPS against a wide range of cyber dangers, such as network intrusions, data breaches, and physical attacks, through case studies and real-world applications. Scalability, real-time reaction, and limited resources are some of the problems that still need more study and development. New ideas in CPS security will come from improvements in control theory, machine learning, and cryptography methods in the future. We can make vital infrastructure even more reliable and protect people's safety and security in a world that is becoming more and more linked by combining these technologies and encouraging businesses, universities, and government agencies to work together.

References

[1] B. A. Sergeevich, B. Elena Sergeevna, I. T. Nikolaevna, K. Sergey Vitalievich, M. V. Dmitrievna and S. Mariya Gennadievna, "The concept of the knowledge base of threats to cyber-physical systems based on the ontological approach," 2022 IEEE International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON), Yekaterinburg, Russian Federation, 2022, pp. 90-95

[2] E. Pavlenko and D. Zegzhda, "Sustainability of cyber-physical systems in the context of targeted destructive influences," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 2018, pp. 830-834, doi: 10.1109/ICPHYS.2018.8390814.

[3] A. Aigner and A. Khelil, "A Scoring System to Efficiently Measure Security in Cyber-Physical Systems," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1141-1145

[4] A. Aigner and A. Khelil, "A Security Qualification Matrix to Efficiently Measure Security in Cyber-Physical Systems," 2020 32nd International Conference on Microelectronics (ICM), Aqaba, Jordan, 2020, pp. 1-4,

[5] Guozhang Jiang et al., "Model knowledge matching algorithm for steelmaking casting scheduling", Int. J. Wirel. Mob. Comput, vol. 15, pp. 215-222, 2018.

[6] A. G. Massel and D. A. Gaskova, "Ontological engineering for the development of an intelligent system for threat analysis and cybersecurity risk assessment of energy facilities", Ontology of design, no. 2, pp. 32, 2019.

[7] J. Jamaludin and Rohani J. Mohd, "Cyber-Physical System (CPS): State of the Art", Proceedings of the 2018 International Conference on Computing Electronic and Electrical Engineering (ICE Cube), pp. 1-5, 2018.

[8] Vulnerabilities of information systems. Classification of vulnerabilities of information systems. - M: Standartinform, pp. 18, 2018.

[9] A. Aigner and A. Khelil, "Assessment of Model-based Methodologies to architect Cyber-Physical Systems", Proceedings of the ACM International Conference on Omni-Layer Intelligent Systems (COINS), Mai 2019.

[10] A. Aigner and A. Khelil, "A Benchmark of Security Metrics for Cyber-Physical Systems", Proceedings of The 2nd IEEE Workshop on Security Trust Privacy for Emerging Cyber-Physical Systems (STP-CPS @ SECON), June 2020.

[11] D. Ding et al., "A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems", Neurocomputing, vol. 275, January 2018.

[12] T. Lusco, "ARC-IT - The Architecture Reference for Cooperative and Intelligent Transportation", Technical Report U.S. Department of Transportation, April 2018.

[13] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling simulation and analysis with cyber security applications", IEEE Access, vol. 8, pp. 151 019-151 064, 2020.

[14] R. Shankar, S. Pradhan, K. Chatterjee and R. Mandal, "A comprehensive state of the art literature survey on lfc mechanism for power system", Renewable and Sustainable Energy Reviews, vol. 76, pp. 1185-1207, 2017.

[15] A. Aigner and A. Khelil, "Assessment of Model-based Methodologies to architect Cyber-Physical Systems", Proceedings of the ACM International Conference on Omni-Layer Intelligent Systems (COINS), May 2019.

[16] A. N. Duc et al., "Security Challenges in IoT Development: A Software Engineering Perspective", Proceedings of XP2017 Scientific Workshops, May 2017.

[17] A. Aigner and A. Khelil, "A Benchmark of Security Metrics for Cyber-Physical Systems", Proceedings of The 2nd IEEE Workshop on Security Trust Privacy for Emerging Cyber-Physical Systems (STP-CPS @ SECON), June 2020.

[18] T. Lusco, "ARC-IT – The Architecture Reference for Cooperative and Intelligent Transportation", Technical Report, April 2018.

[19] X. Gao, "Sliding Mode Control Based on Disturbance Observer for Cyber-Physical Systems Security," 2022 4th International Conference on Control and Robotics (ICCR), Guangzhou, China, 2022, pp. 275-279

[20] X. Gao, "Sliding Mode Control Based on Disturbance Observer for Cyber-Physical Systems Security," 2022 4th International Conference on Control and Robotics (ICCR), Guangzhou, China, 2022, pp. 275-279,

[21] Chandu Vaidya, Prashant Khobragade and Ashish Golghate, "Data Leakage Detection and Security in Cloud Computing", GRD JournalsGlobal Research Development Journal for Engineering, vol. 1, no. 12, November 2016.

[22] Y. A. Shichkina and R. R. Fatkieva, "Intelligent Information Security Management of Cyber-physical Systems," 2021 II International Conference on Neural Networks and Neurotechnologies (NeuroNT), Saint Petersburg, Russia, 2021, pp. 25-27,