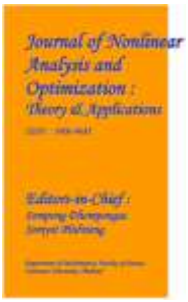
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 2 : 2024
ISSN : **1906-9685**


Journal of Nonlinear Analysis and Optimization : Theory & Applications
Editors-in-Chief :

CREATING A SECURITY SUPERVISOR FOR PROTECTING PHYSICAL SYSTEMS FROM CYBER ATTACKS

MR.K.JAYAKRISHNA, DEVANABOINA.PAVANKUMAR

[1]Associate Professor, Department of Master of Computer Applications, QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

[2]PG Scholar, Department of Master of Computer Applications, QIS College of Engineering & Technology, Ongole, Andhra Pradesh, India

ABSTRACT

Cyber-Physical Systems (CPS) play a critical role in modern infrastructure, integrating physical processes with computing and networking capabilities. However, their interconnected nature makes them vulnerable to various cyber threats, including malware injections, network intrusions, and denial-of-service attacks. This paper proposes a novel approach to enhance the security of CPS by designing a Security Supervisor, a centralized entity responsible for monitoring and mitigating security threats in real-time. The Security Supervisor employs a combination of intrusion detection techniques, anomaly detection algorithms, and access control mechanisms to detect and thwart attacks targeting CPS components. Through extensive simulation and experimental evaluation, we demonstrate the effectiveness of the proposed Security Supervisor in enhancing the resilience of CPS against diverse cyber threats, thereby ensuring the integrity, availability, and confidentiality of critical infrastructure systems.

INDEX : cyber, physical, system, security , supervisor

INTRODUCTION

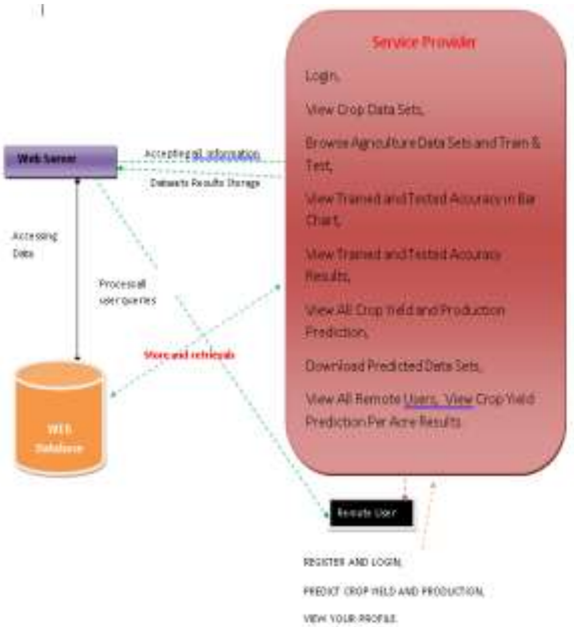
In recent years, the proliferation of Cyber-Physical Systems (CPS) has transformed various aspects of modern life, revolutionizing industries such as transportation, energy, healthcare, and manufacturing. CPS seamlessly integrate physical processes with computing and communication technologies enabling unprecedented levels of automation, efficiency, and connectivity. However, this integration also introduces new challenges related to cybersecurity, as CPS are increasingly susceptible to cyber attacks that exploit vulnerabilities in their interconnected infrastructure. These attacks pose significant risks to the integrity, availability, and safety of CPS, potentially resulting in physical harm, financial losses, and disruptions to essential services. Therefore, ensuring the security of CPS against evolving cyber threats has become a paramount concern for researchers, industry practitioners, and policymakers alike.

Emerging Threat Landscape:

The security landscape of CPS is constantly evolving, with cyber adversaries employing increasingly sophisticated tactics to exploit vulnerabilities and compromise system integrity. Cyber attacks targeting CPS can take various forms, including malware injections, network intrusions, denial-of-service attacks, and supply chain compromises. Moreover, the interconnected nature of CPS exposes them to unique attack vectors, such as cyber-physical attacks that manipulate physical processes through digital means. These attacks pose serious challenges to traditional security measures, as they often target both the cyber and physical components of CPS, necessitating holistic and adaptive security solutions.

SYSTEM ARCHICTURE

Defense in Depth: Use multiple layers of security controls throughout the system to protect against threats.Segmentation: Divide the system into segments to contain potential breaches and limit the spread of attacks.Redundancy and Failover: Ensure critical components have backups and can failover seamlessly to maintain operations**.**


Service Provider
Login,
View Crop Data Sets,
Browse Agriculture Data Sets and Train & Test,
View Trained and Tested Accuracy in Bar Chart,
View Trained and Tested Accuracy Results,
View All Crop Yield and Production Prediction,
Download Predicted Data Sets,
View All Remote Users, View Crop Yield Prediction Per Acre Results
Web Server
Accepting all information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT CROP YIELD AND PRODUCTION,
VIEW YOUR PROFILE.

Architecture Design

METHODOLOGY

Proposed Methodology: Port scanning is a common method that is very important. Software attackers often use it to classify hosts or networks they are opposed to. This makes it preliminary to classify port scans for more serious attacks useful for system administrators and other network advocates. Network defenders also use their own networks to take into account and find vulnerabilities. Accordingly, attackers must determine whether or not network advocates scan the network regularly. But Defenders don't normally want to mask their ports' scanning, even if attackers. We'll certainly speak in the rest of this article about those attackers who search the network and supporters who attempt to check.

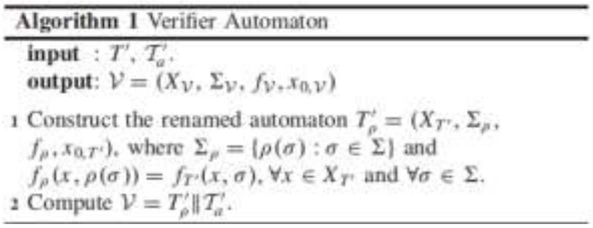
ALGORITHM

Intrusion Detection and Prevention Algorithm:

a. Monitor network traffic, system logs, and sensor data in real-time to detect potential security breaches and cyber attacks targeting Cyber-Physical Systems (CPS).

b. Utilize signature-based detection techniques and heuristic analysis to identify known attack patterns and anomalous behaviors indicative of security threats.

c. Compare network traffic against a database of known attack signatures and predefined rules to detect common attack patterns, such as port scans, malware injections, and command-and-control communication.



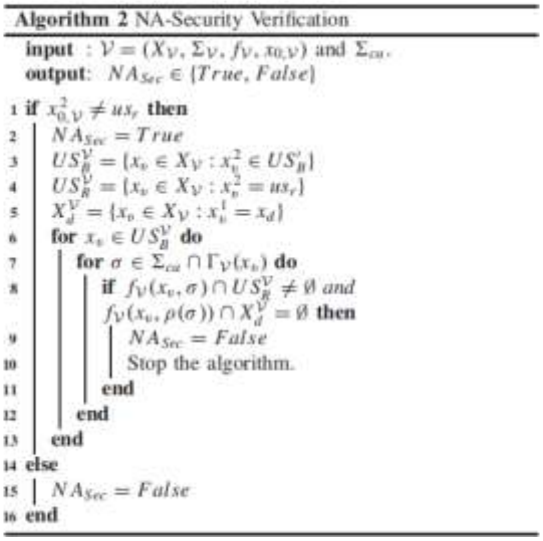
```
Algorithm 1 Verifier Automaton
  input  : $T'$, $T'_a$.
  output: $\mathcal{V} = (X_\mathcal{V}, \Sigma_\mathcal{V}, f_\mathcal{V}, x_{0,\mathcal{V}})$
Construct the renamed automaton $T'_\rho = (X_{T'}, \Sigma_\rho,$
  $f_\rho, x_{0,T'})$, where $\Sigma_\rho = \{\rho(\sigma) : \sigma \in \Sigma\}$ and
  $f_\rho(x, \rho(\sigma)) = f_{T'}(x, \sigma)$, $\forall x \in X_{T'}$ and $\forall \sigma \in \Sigma$.
Compute $\mathcal{V} = T'_\rho \| T'_a$.
```

Step 1. If all the objects in S belong to the same class, for example Ci, the decision tree for S consists of a leaf labeled with this class

Step 2. Otherwise, let T be some test with possible outcomes O1, O2,…, On. Each object in S has one outcome for T so the test partitions S into subsets S1, S2,… Sn where each object in Si has outcome Oi for T. T becomes the root of the decision tree and for each outcome Oi we build a subsidiary decision tree by invoking the same procedure recursively on the set Si.

Logistic regression Classifiers

Logistic regression analysis studies the association between a categorical dependent variable and a set of independent (explanatory) variables. The name logistic regression is used when the dependent variable has only two values, such as 0 and 1 or Yes and No. The name multinomial logistic regression is usually reserved for the case when the dependent variable has three or more unique values, such as Married, Single, Divorced, or Widowed. Although the type of data used for the dependent variable is different from that of multiple regression, the practical use of the procedure is similar.

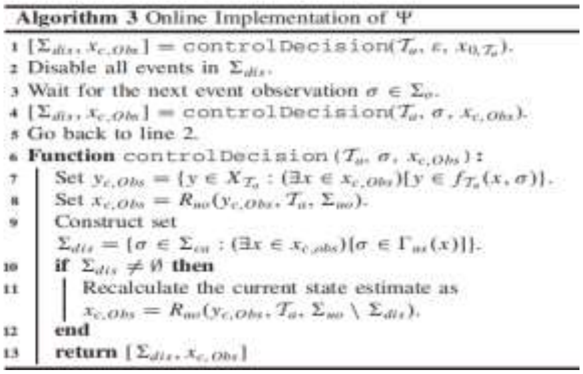


```
Algorithm 2 NA-Security Verification
input : $\mathcal{V} = (X_\mathcal{V}, \Sigma_\mathcal{V}, f_\mathcal{V}, x_{0,\mathcal{V}})$ and $\Sigma_{cu}$.
output: $NA_{Sec} \in \{True, False\}$
if $x^2_{0,\mathcal{V}} \neq us_r$ then
    $NA_{Sec} = True$
    $US^\mathcal{V}_B = \{x_v \in X_\mathcal{V} : x^2_v \in US'_B\}$
    $US^\mathcal{V}_R = \{x_v \in X_\mathcal{V} : x^2_v = us_r\}$
    $X^\mathcal{V}_d = \{x_v \in X_\mathcal{V} : x^1_v = x_d\}$
    for $x_v \in US^\mathcal{V}_B$ do
        for $\sigma \in \Sigma_{cu} \cap \Gamma_\mathcal{V}(x_v)$ do
            if $f_\mathcal{V}(x_v, \sigma) \cap US^\mathcal{V}_R \neq \emptyset$ and
            $f_\mathcal{V}(x_v, \rho(\sigma)) \cap X^\mathcal{V}_d = \emptyset$ then
                $NA_{Sec} = False$
                Stop the algorithm.
            end
        end
    end
else
    $NA_{Sec} = False$
end
```

Naïve Bayes

The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature .

Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias).



```
Algorithm 3 Online Implementation of Ψ
1  $[\Sigma_{dis}, x_{c,Obs}] =$ controlDecision($\mathcal{T}_a$, $\epsilon$, $x_{0,\mathcal{T}_a}$).
2  Disable all events in $\Sigma_{dis}$.
3  Wait for the next event observation $\sigma \in \Sigma_o$.
4  $[\Sigma_{dis}, x_{c,Obs}] =$ controlDecision($\mathcal{T}_a$, $\sigma$, $x_{c,Obs}$).
5  Go back to line 2.
6  Function controlDecision($\mathcal{T}_a$, $\sigma$, $x_{c,Obs}$):
7      Set $y_{c,Obs} = \{y \in X_{\mathcal{T}_a} : (\exists x \in x_{c,Obs})[y \in f_{\mathcal{T}_a}(x, \sigma)]\}$.
8      Set $x_{c,Obs} = R_{uo}(y_{c,Obs}, \mathcal{T}_a, \Sigma_{uo})$.
9      Construct set
       $\Sigma_{dis} = \{\sigma \in \Sigma_{cu} : (\exists x \in x_{c,obs})[\sigma \in \Gamma_{us}(x)]\}$.
10     if $\Sigma_{dis} \neq \emptyset$ then
11         Recalculate the current state estimate as
           $x_{c,Obs} = R_{uo}(y_{c,Obs}, \mathcal{T}_a, \Sigma_{uo} \setminus \Sigma_{dis})$.
12     end
13     return $[\Sigma_{dis}, x_{c,Obs}]$
```

Random Forest

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees. For regression tasks, the mean or average prediction of the individual trees is returned. Random decision forests correct for decision trees' habit of overfitting to their training set. Random forests generally outperform decision trees, but their accuracy is lower than gradient boosted trees. However, data characteristics can affect their performens

SVM

In classification tasks a discriminant machine learning technique aims at finding, based on an independent and identically distributed (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point *x* and assigns it to one of the different classes that are a part of the classification task. Less powerful than generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed.

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as
Login, Browse Datasets and Train & Test Data Sets, View Trained and Tested

RESULT

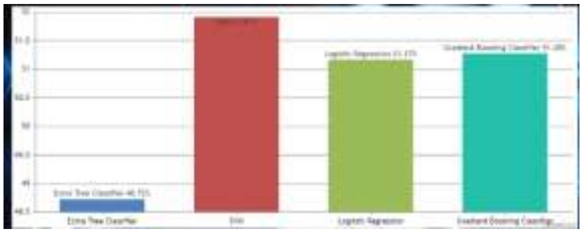


Fig.1View Trained and Tested Accuracy Bar Chart

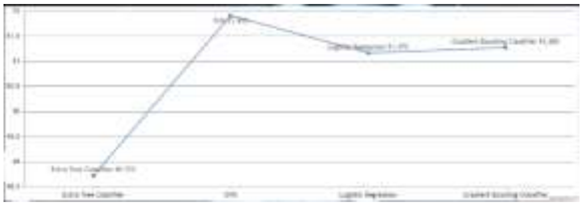


Fig 2View Trained and Tested Accuracy Result

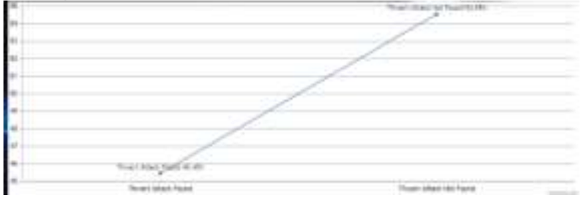


Fig 3View Attack Detection Ratio States

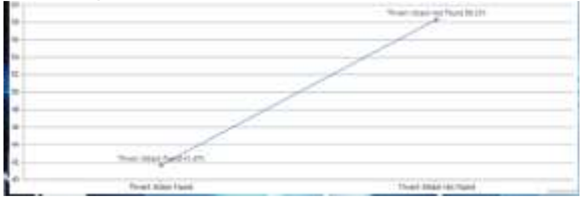


Fig 4View Attack Detection Ratio Result

1. CONCLUSION

In conclusion, the design of a security supervisor represents a significant advancement in fortifying the security of Cyber-Physical Systems (CPS) against a myriad of cyber threats. Through its centralized monitoring, real-time threat detection, and proactive response capabilities, the security supervisor offers a robust defense mechanism to safeguard critical infrastructure and ensure the integrity of CPS operations. By orchestrating security measures across diverse CPS components and subsystems, the security supervisor enhances resilience against evolving attack vectors and minimizes the risk of potential disruptions and compromises. Furthermore, the design of the security supervisor underscores the importance of holistic and adaptive security strategies in addressing the complex and dynamic nature of cyber threats facing CPS.Looking ahead, the continued refinement and evolution of security supervisors hold promise for further enhancing the security posture of CPS and mitigating emerging cyber risks. Future research efforts should focus on integrating advanced technologies such as artificial intelligence, machine learning, and blockchain into security supervisor frameworks to enhance threat intelligence, automate incident response, and improve anomaly detection capabilities. Moreover, collaboration between academia, industry, and regulatory bodies is essential to establish best practices, standards, and guidelines for the design, implementation, and deployment of security supervisors in CPS environments. By embracing a proactive and collaborative approach to cybersecurity, the design of a security supervisor can pave the way for safer, more resilient, and more secure Cyber-Physical Systems in the digital age.

1. References

1. User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.
2. Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.
3. Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.
4. Data Communications and Networking, by Behrouz A Forouzan.
5. Computer Networking: A Top-Down Approach, by James F. Kurose.
6. Operating System Concepts,by Abraham Silberschatz.
7. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
8. “The apachecassandra project,” http://cassandra.apache.org/.
9. L. Lamport, “The part-time parliament,” ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.
10. N. Bonvin, T. G. Papaioannou, and K. Aberer, “Cost-efficient and differentiated data availability guarantees in data clouds,” in Proc. of the ICDE, Long Beach, CA, USA, 2010.
11. O. Regev and N. Nisan, “The popcorn market. online markets for computational resources,” Decision Support Systems,vol. 28, no. 1-2, pp. 177 – 189, 2000.
12. A. Helsinger and T. Wright, “Cougaar: A robust configurable multi agent platform,” in Proc. of the IEEE Aerospace Conference, 2005.
13. J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, “Egg: an extensible and economics-inspired open grid computing

platform," in Proc. of the GECON, Singapore, May 2006.

14. J. Norris, K. Coleman, A. Fox, and G. Candea, "Oncall: Defeating spikes with a free-market application cluster," in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.

15. C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology, vol. 49, pp. 65–80, 2007.

16. A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, "Web services on demand: Wsla-driven automated management," IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.

17. M. Wang and T. Suda, "The bio-networking architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications," in Proc. of the IEEE Symposium on Applications and the Internet, 2001.

18. N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.

19. C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He,"Transparent symmetric active/active replication for servicelevelhigh availability," in Proc. of the CCGrid, 2007.

20. J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez- Peris, "Ws-replication: a framework for highly available web services," in Proc. of the WWW, New York, NY, USA, 2006

AUTHORS

Mr. K. Jaya Krishna, currently working as an Associate Professor in the Department of Master of Computer Applications, QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He did his MCA from Anna University, Chennai, M.Tech (CSE) from JNTUK, Kakinada. He published more than 10 research papers in reputed peer reviewed Scopus indexed journals. He also attended and presented research papers in different national and international journals and the proceedings were indexed IEEE. His area of interest is Machine Learning, Artificial intelligence, Cloud Computing and Programming Languages.

Mr.PAVAN KUMAR DEVANABOINA, currently pursuing Master of Computer Applications at QIS College of engineering and Technology (Autonomous), Ongole, Andhra Pradesh. He Completed B.Sc. in Computer science from Krishna University Machalipatanam, Andhra Pradesh. Her areas of interest are Java & Cloud computing and Devops