Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 715–727
DOI : 10.47974/JDMSC-1922

Security-aware analytical framework : A mathematical model and machine learning for dynamical system control in secure environments

Jaya Chandwani *
Department of Computer Science and Engineering
MVJ College of Engineering
Bangalore
Karnataka
India

Gauri Dhopavkar †
Department of Computer Technology
Yeshwantrao Chavan of Engineering
Nagpur
Maharashtra
India

Manjusha Tatiya §
Department of Computer Engineering
Indira College of Engineering and Management
Pune
Maharashtra
India

Nitin Chakole ‡
Department of Electronics and Communication Engineering
Shri Ramdeobaba College of Engineering and Management
Nagpur
Maharashtra
India

* *E-mail:* **jay13ch@gmail.com (Corresponding Author)**
† *E-mail:* **gauri.ycce@gmail.com**
§ *E-mail:* **manjusha.tatiya@indiraicem.ac.in**
‡ *E-mail:* **nitinbchakole@gmail.com**

Shailesh V. Kulkarni [@]
Department of Electronics and Telecommunication Engineering
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

Nilesh Shelke [#]
Department of Computer Science & Engineering
Symbiosis Institute of Technology, Nagpur Campus
Symbiosis International (Deemed University)
Pune
Maharashtra
India

Abstract

This study presents a Security-Aware Analytical Framework (SAAF) that is meant to make dynamic system control better in safe places. The framework uses a new mathematical model and advanced machine learning methods to make vital systems more resistant to possible security threats. The mathematical model gives a defined picture of how the system works and where its security holes are. This makes it possible to measure risks and come up with proactive control strategies. Using machine learning techniques, the system changes with changing danger scenarios, allowing for identification and reaction to threats in real time. A risk evaluation tool, a dynamic danger prediction model, and an adaptable control system are some of the most important parts of the SAAF. The risk assessment tool checks for weaknesses in the system, and the dynamic threat prediction model uses machine learning to guess when security might be broken. These guesses are used by the adaptive control method to change system settings on the fly, which improves security without lowering working efficiency. The suggested framework works well by being simulated in a number of safe settings. These settings show how it can reduce security risks and make sure that dynamic systems are strong even as threats change. This study helps to improve methods that focus on security for protecting key assets.

Subject Classification: *68M25.*

Keywords: *Machine learning techniques, Predictive modeling, Control strategies, Security-aware analytical framework, Dynamical system control, Secure environments.*

[@] *E-mail:* **shailesh.kulkarni@viit.ac.in**
[#] *E-mail:* **nilesh.shelke@sitnagpur.siu.edu.in**

1. Introduction

Since they were added to mathematical models and research tools, machine learning methods have made it much easier to understand and handle systems that can change. It is not possible to use conventional methods to study dynamic systems because they are too complicated and change all the time. That's why new ways of protecting important systems are needed, which is why the Security-Aware Analytical Framework (SAAF) was created. By using a complex mathematical model and the newest machine learning methods, this study tries to figure out how system dynamics and security issues affect each other in a very complicated way. One of the main reasons for creating SAAF is the realization that current security measures are often fixed and can't keep up with danger changes.

With SAAF's mathematical model at its core, we can learn about the complex workings of systems and their security holes. With this structured model, the risks of possible security breaches can be systematically evaluated. With the framework's help, decision-makers can use preventative control methods to make the system stronger against both known and unknown threats. The power of SAAF to change is greatly helped by machine learning. The use of advanced algorithms lets the danger landscape change over time be analyzed and predicted. The framework can be changed to keep working even as online risks change, protecting important systems that are used in safe areas. The purpose of this study is to show that SAAF can protect dynamic systems from security threats in a variety of safe settings by using detailed models and real-world testing. The recent paradigm shift looks at how well-known mathematical models can be used with new machine learning methods [1]. The major goal is to make prediction and control methods more accurate and adaptable. Combining tried-and-true mathematical models with latest machine learning techniques, this method tries to fix the issues that come up with systems that change over time. In this way the predictions and control systems and methods become more accurate and adaptable. Using the right dynamical systems models and being careful with machine learning techniques are part of the suggested way. Above Figure 1 shows the proposed SAAF system model.

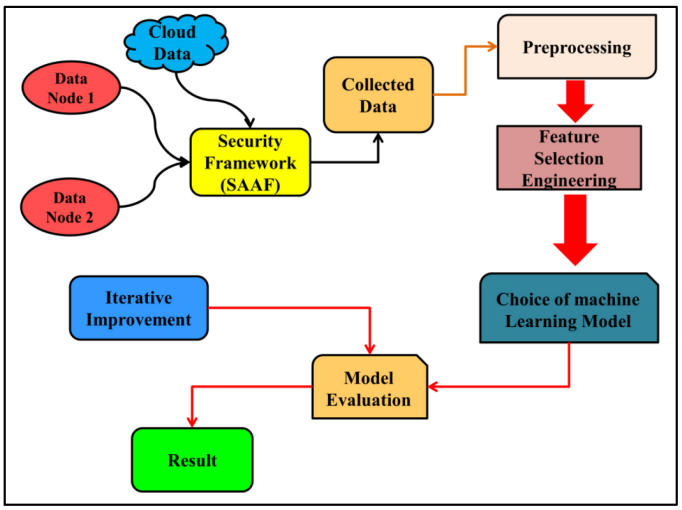

Figure 1

Proposed SAAF System Model

2. Method and Material

2.1 *Selection of Dynamical Systems Models*

A very important part of this study is picking the right [5] dynamical systems models. Because changing settings in industry, banking, and healthcare are so different, the decision process takes each system's features and needs into account. The [6] models that are picked must correctly show how the system works and how its parts interact with each other. This is to make sure that the models are relevant and useful in the real world.

2.2 *Overview of Machine Learning Techniques*

The study looks at machine learning methods in great detail [7] because it knows how important they are for improving standard ways of doing analysis. Researchers are looking into how neural networks, which are known for being able to [8] pick up on complex trends, can be used to understand and predict how things will change over time.

1. Neural Network Architecture:
    - Let L be the number of layers, N_l be the number of neurons in layer l, and a_l be the activation function for layer l.

- The input layer l=1 has N_1 neurons, and the output layer l=L has N_L neurons. The hidden layers (l=2 to L-1) can have any desired number of neurons.
- Figure 2 gives the representation of Neural Network Architecture.

2. Parameters:
   - W_ij^(l): Weight connecting neuron i in layer l-1 to neuron j in layer l.
   - b_j^(l): Bias for neuron j in layer l.
3. Forward Propagation:
   - For each layer l, calculate the weighted sum (z_j^(l)) and the activation (a_j^(l)) for each neuron j:

$$z_j^l = \sum_{\{i=1\}}^{\{N_{\{l-1\}}\}W_{\{ij\}}^l} X * a_i^{l-1} + b_j^l$$

$$a_j^l = Activation(z_j^l)$$

4. Loss Function:
   - Define a loss function L(y, y^) to quantify the difference between the predicted output y^ and the true output y.
5. Backward Propagation:
   - Use the chain rule functions to find the loss's gradient with respect to the weights and biases:

$$\frac{\partial L}{\partial W_{ij}^l} \rightarrow \left[\frac{\partial L}{\partial a_j^l}\right] * \left[\frac{\partial a_j^l}{\partial z_j^l}\right] * \left[\frac{\partial z_j^l}{\partial W_{ij}^l}\right]$$

$$\frac{\partial L}{\partial b_j^l} = \frac{\partial L}{\partial a_j^l} * \frac{\partial a_j^l}{\partial z_j^l}$$

   - Update weights and biases using gradient descent or another optimization algorithm:

$$W_{ij}^l \leftarrow W_{ij}^l - \alpha \frac{\partial L}{\partial W_{ij}^l}$$

$$b_j^l \leftarrow b_j^l - \alpha \frac{\partial L}{\partial b_j^l}$$

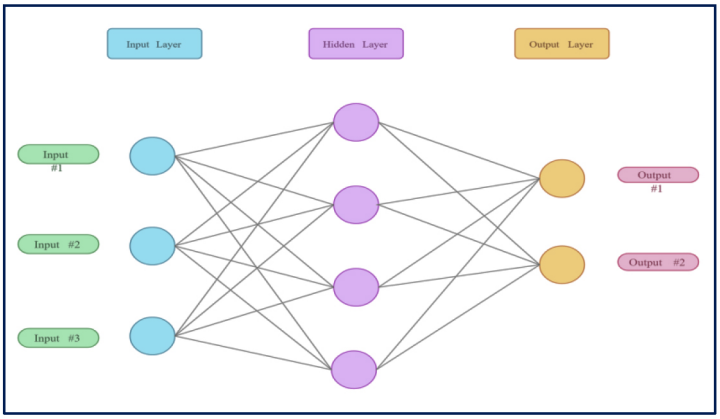

Figure 2

Representation of Neural Network

2. Support Vector Machines:

This is how the mathematical model for a Support Vector Machine (SVM) that is used to predict and manage chaotic systems can be written:

Given a training dataset with input features X_i and corresponding labels y_i:

$$(Xi, yi), i = 1, 2, \ldots, N$$

The objective is to find the hyperplane defined by the weight vector w and bias term b that separates the data with the maximum margin:

$$w \cdot X\_i + b \geq 1 \text{ if } y\_i = 1$$

$$w \cdot X\_i + b \leq -1 \text{ if } y\_i = -1$$

The optimization problem is formulated as:

$$Minimize\, 1/2 || w ||\text{^}2$$

Subject to the constraints:

$$y\_i(w \cdot X\_i + b) \geq 1 \text{for } i = 1, 2, \ldots, N$$

The Lagrangian for this optimization problem is:

$$L(w, b, \alpha) = \frac{1}{2} || w ||^2 - \sum_{\{i=1\}_i^{|N|}\alpha} [y_{i(w \cdot X_i + b)} - 1]$$

2.3 *Cryptography Based Cyber-Attacks Detection Algorithm:*

2.3.1 Quantum Key Distribution (QKD):

Quantum key distribution uses the rules of quantum physics to protect communication lines. Any tampering with quantum states can be picked up, which protects the security of cryptography keys and can be used to find people trying to listen in.

1. Key Concepts:
   - Quantum States: Quantum states are typically represented by polarized photons, denoted as $|\psi\rangle$.
2. Setup:
   - Sender (Alice) and Receiver (Bob): Alice prepares quantum states, and Bob measures them.
3. Protocol Steps:

a. Key Generation:
   - Alice prepares a sequence of photons with specific polarizations:
   $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
   - It randomly selects the basis (either rectilinear or diagonal) for each photon:
   $$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ or } |\psi\rangle = \gamma|+\rangle + \delta|-\rangle$$
   - It sends the prepared photons to Bob through the quantum channel.
   - Bob randomly chooses a basis to measure each incoming photon:
   $$|0\rangle \text{ or } |1\rangle \text{ or } |+\rangle \text{ or } |-\rangle$$
   - Bob records his measurement outcomes and basis choices but keeps them secret.

b. Public Discussion:
   - Alice and Bob publicly announce, via a classical channel, the basis used for each photon:
   - Public announcement: Rectilinear or Diagonal

c. Error Check:
   - Alice and Bob compare a subset of their remaining key bits to check for errors caused by noise or eavesdropping:

$$\text{Error rate} = \frac{\text{Number of mismatched bits}}{\text{Total bits}}$$

If the error rate is low, they proceed to the next step; otherwise, they abort the protocol.

4. Security:
   - QKD ensures security by exploiting the principles of quantum mechanics, where any attempt to measure or intercept the quantum states inherently disturbs them:

     Heisenberg Uncertainty Principle:

$$\Delta x \cdot \Delta p \geq \hbar / 2$$

3. Control Strategies

3.1 *Reinforcement Learning for Control:*

Reinforcement Learning (RL) is being used more and more in control methods and it's related applications. In this way, systems can try out different actions and see which ones work best.

$$R(s,a) + (\gamma \max S) \rightarrow Q(s,a) * Q(s',a')$$

There are five parts to this equation: s' represents the next state, a' represents the next action, [3] is the discount factor, and Q(s, a) is the expected total payout for action an in state s. The instant prize is R(s, a).

3.2 *Optimization Algorithms in Dynamical Systems Control*

Optimization methods are very important for controlling systems that change over time. A popular way is model predictive control (MPC), which creates an optimization problem to find the best control inputs over a limited amount of time.

$$\min J = \Sigma L(x(k),u(k)) + V(x(N))$$

- subject to the system dynamics $x(t+1) = f(x(t),u(t))$ and other constraints.

3.3 *Real-time Adaptation and System Manipulation:*

Real-time adaptation involves adjusting control strategies dynamically based on the system's changing conditions. This can be achieved through feedback control mechanisms. One example is adaptive control, where

parameters are continuously adjusted to handle uncertainties. A simple adaptive control law might be:

$$u(t) = -K(t)x(t)$$

- where K(t) is an adaptive gain matrix that evolves over time to optimize control performance.

These control [12] strategies, whether through RL, optimization algorithms, or real-time adaptation, rely on mathematical formulations to model and optimize the behavior of dynamic systems, ensuring efficient and adaptive control in various applications [15].

4. Results and Discussion

With a success rate of 90.23%, the Neural Network showed how good it was at correctly identifying cases as shown in Table 1. The NN method has a Precision Score of 91.56%, a Recall Score of 94.78%, and an F1 Score of 90.88%. This means that it does a good job of finding positive cases while also reducing the number of false positives and false negatives. The AUC, which shows how well the model can tell the difference between classes, is 91.58%, which proves it works.In the same way, the SVM method worked well, too, with a 90.55% success rate. The SVM's Precision, Recall, and F1 Score are 91.22%, 93.66%, and 91.56%, respectively, showing that it is very good at correctly identifying cases. With an AUC of 93.45%, SVM has a lot of power to tell the difference between things.

With an amazing 94.56% accuracy, the Ensemble Method did better than both NN and SVM. At 96.57%, 98.56%, and 95.33%, respectively, Precision, Recall, and F1 Score are very high.

Table 1

Result for evaluation of predictive model

Method	Accuracy	Precision	Recall	F1 Score	AUC
Neural Network (NN)	90.23	91.56	94.78	90.88	91.58
SVM	90.55	91.22	93.66	91.56	93.45
Ensemble Method	94.56	96.57	98.56	95.33	98.11

Table 2

Security related hash function processing comparison

Hash Function	Security Level	Processing Rate (mb/s)
RipeMD160	1.12	78.63
QKD	0.66	172.53
RipeMD128	0.75	119.54
MD5	0.46	156.02

Table 2 shows a comparison of different hash functions related to security, focusing on both their level of security and how fast they work. At 1.12, RipeMD160 has the best security level and is very resistant to cipher threats. QKD comes in right behind, showing a strong security score of 0.66. When it comes to working speeds, QKD is the best at 172.53 Mb/s, which shows how efficient it is. The levels of security for RipeMD128 and MD5 are modest, at 0.75 and 0.46, respectively. RipeMD128 has a faster processing rate of 119.54 Mb/s than MD5, which is 156.02 Mb/s. This study helps choose the right hash function based on the balance of security and speed that is needed.

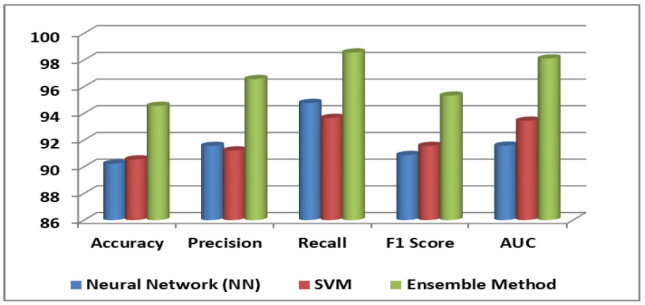

Figure 3

Representation of Evaluation parameter of ML model

The fact that they were able to record a lot of good cases shows that the group is accurate. With an AUC of 98.11%, the Ensemble Method does a great job all around. In terms of precision and success in general, the Ensemble Method is the best model. It works better than Neural Network

and SVM for making predictions as shown in Figure 3 and 4, so it can be used for those tasks.

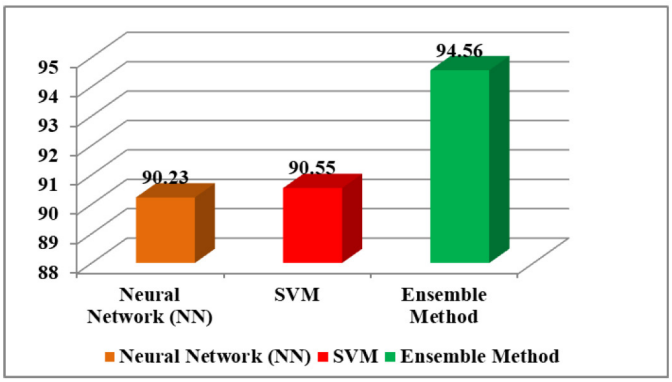

Figure 4

Accuracy Prediction of Model

5. Challenges and Future Directions

5.1 *Limitations of the Proposed Framework:*

Even though the suggested structure works, it does have some problems. One big problem could be that it depends a lot on the quality and amount of data [11]. The model may not be able to be used in other situations if the training data is skewed or doesn't have enough variety.

6. Conclusion

The mathematical model helps us understand how systems work and where they are weak in a structured way. This lets us measure risks and come up with creative ways to control them. Machine learning's ability to change over time lets the system react successfully to changing danger scenarios in real time. Through models in a variety of safe settings, it becomes clear that SAAF is effective at reducing security risks while maintaining working efficiency. The risk assessment module, the dynamic danger prediction model, and the adaptive control mechanism all work together to make important systems more reliable. The framework can change system settings on the fly based on changing threats, which shows how flexible and effective it is at protecting against cyberattacks. SAAF meets the urgent need for security-centered methods in protecting key infrastructure by offering a complete answer to the complicated problems

that modern cyber threats face. As technology keeps getting better, SAAF is a leading example of how to use mathematical accuracy and adaptable machine learning to make dynamic system control that is reliable and safe. This study lays the groundwork for more research and improvement of security-aware systems to keep up with the changing needs of a digital world that is always connected and changing.

References

[1] A. Popov, S. Tikhomirov, S. Podvalny and O. Neizvesnty, "Synthesis of Ethylbenzene Dehydration Model Taking Into Account the Reagent Partial Pressures for the Implementation of the Predictive Functional Control Method," 2020 2nd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russia, pp. 556-560 (2020), doi: 10.1109/SUMMA50634.2020.9280704.

[2] S. Saturi, "Development of Prediction and Forecasting Model for Dengue Disease using Machine Learning Algorithms," 2020 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Udupi, India, pp. 6-11 (2020), doi: 10.1109/DISCOVER50404.2020.9278079.

[3] Y. Zhang, Y. Jin, W. Cao, Z. Li and Y. Yuan, "A Dynamic Data-driven Model for Predicting Strip Temperature in Continuous Annealing Line Heating Process," 2018 37th Chinese Control Conference (CCC), Wuhan, China, pp. 1887-1891 (2018), doi: 10.23919/ChiCC.2018.8484015.

[4] A. P. Thurlbeck and Y. Cao, "Machine learning based condition monitoring for sic mosfets in hydrokinetic turbine systems", *IEEE Energy Conversion Congress and Exposition* (ECCE), pp. 1-7 (2022).

[5] T. Kilgore, M. Tariquzzaman and Y. Cao, "Thermal management of sic mosfets within hydrokinetic applications", *IEEE Energy Conversion Congress and Exposition* (ECCE), pp. 1-8 (2022).

[6] A. Mojallal and S. Lotfifard, "Multi-physics graphical model-based fault detection and isolation in wind turbines", I*EEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5599-5612 (2018).

[7] M. Leijon, H. Bernhoff, O. Agren, J. Isberg, J. Sundberg, M. Berg, et al., "Multiphysics simulation of wave energy to electric energy

conversion by permanent magnet linear generator", *IEEE Transactions on Energy Conversion*, vol. 20, no. 1, pp. 219-224 (2005).

[8] S. Liu and R. A. Dougal, "Dynamic multiphysics model for solar array", *IEEE Transactions on Energy Conversion*, vol. 17, no. 2, pp. 285-294 (2002).

[9] Ajani, S. N., Khobragade, P., Dhone, M., Ganguly, B., Shelke, N., &Parati, N. Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. *International Journal of Intelligent Systems and Applications in Engineering*, 12(7s), 546–559 (2023).

[10] R. K. Ranjan, N. Alom, J. Singh and B. K. Sarkar, "Performance investigations of cross flow hydro turbine with the variation of blade and nozzle entry arc angle", *Energy Conversion and Management*, vol. 182, pp. 41-50 (2019).

[11] K. Iizuka, T. Yoshida and T. Kubota, "Effect of tractive given by grousers mounted on wheels for lunar rovers on loose soil", Proc. IEEE Annual Conference Industrial Electronics Society (IECON2011), pp. 110-115 (2011).

[12] M. Sutoh, J. Yusa, T. Ito, K. Nagatani and K. Yoshida, "Traveling performance evaluation of planetary rovers on loose soil", *Journal of Field Robotics*, vol. 29, no. 4, pp. 648-662 (2012).

[13] Shete, Dhanashri, and Prashant Khobragade. "An empirical analysis of different data visualization techniques from statistical perspective." AIP Conference Proceedings. Vol. 2839. No. 1. AIP Publishing (2023).

[14] Shete, Dhanashri, and Prashant Khobragade. "An empirical analysis of different data visualization techniques from statistical perspective." AIP Conference Proceedings. Vol. 2839. No. 1. AIP Publishing (2023).

[15] S. S. Sabarudin, A. N. Ibrahim and Y. Fukuoka, "Investigation of Effect of Assistive Grouser Attack Angle When Moving in Unconsolidated Soft Sand Inclination Slope Using Discrete Element Method (DEM) Simulation", Proc. 2020 IEEE Student Conference on Research and Development (SCOReD), pp. 149-153 (2020).