*International Journal on Applications in Engineering and Technology*
*Volume 10 : Issue 1 : April 2024 , pp 13 –17 www.aetsjournal.com* ISSN (Online) : 2455 - 0523

# An Ensemble Modelling in Cloud Computing for Smart Grid Cyber Physical Systems

Mr.N. Thirugnanasambandan, Dr.A.Rajivkannan

***Abstract—*** For a sustainable and efficient future, it is essential to enable the seamless integration of smart grid cyber-physical systems (SG-CPS) within the framework of our energy infrastructure. However, creative solutions are required because to the SG-CPS's growing complexity and security issues. This study tackles the crucial requirement for resilient modeling in cloud computing settings and suggests a group strategy to strengthen SG-CPS's resilience. The increasing complexity of SG-CPS calls for sophisticated computational approaches, especially in the context of cloud computing. The objective of this study is to improve the security and dependability of smart grids by the application of ensemble modeling methods in a cloud environment. Current models frequently fail to fully handle the complex issues presented by SG-CPS, which include real-time analytics and data security. By addressing these problems head-on, this research hopes to close the current gaps and develop a more comprehensive strategy for managing smart grids. Although previous research has examined specific facets of SG-CPS, a thorough ensemble modeling strategy in the context of cloud computing has not yet been thoroughly investigated. By gaining a deeper understanding of how ensemble approaches might work in concert with cloud-based infrastructures to increase the overall resilience of SG-CPS, this research seeks to close this knowledge gap. The proposed approach entails integrating many models in a cloud computing environment, including statistical methods and machine learning algorithms. By combining the advantages of each individual model, this ensemble technique creates a strong, flexible system that can handle the dynamic nature of SG-CPS.

***Keywords—*** Cyber-Physical Systems, Smart Grid, Ensemble Modeling, Cloud Computing, Resilience.

## I. INTRODUCTION

Amidst the swiftly changing technological landscape, smart grid cyber-physical systems (SG-CPS) have become essential elements of contemporary energy infrastructures [1]. In order to maximize the production, distribution, and consumption of electricity, these systems incorporate cutting-edge information, control, and communication technology [2,3]. To maintain the stability and security of these systems, however, this integration presents a number of difficulties that call for creative solutions [4].

The complexities of SG-CPS present a variety of difficulties, such as data security, real-time processing, and dynamic adaptability [5]. Innovative methods are desperately needed to address the growing vulnerabilities and obstacles as these systems become more sophisticated [6].

The current approaches in the SG-CPS arena frequently struggle with the thorough integration of various technologies and the reduction of possible security risks [7]. In order to improve the SG-CPS's robustness and efficiency, this research suggests an ensemble modeling strategy inside a cloud computing framework [8, 9].

Developing a more sophisticated understanding of the difficulties presented by SG-CPS and proposing and validating an ensemble modeling approach in the context of cloud computing are the two main goals of this research. The goal is to help build a smart grid system that is more efficient, flexible, and safe by achieving these goals.

This research is innovative because it takes a comprehensive approach to SG-CPS and integrates ensemble modeling methods into the dynamic cloud computing environment. Through the integration of many models, the study aims to offer a holistic resolution that exceeds the constraints of current solitary approaches. This study adds to the corpus of knowledge by providing a fresh viewpoint on strengthening SG-CPS using an ensemble modeling approach. It is anticipated that the knowledge gathered from this study will contribute to future research in the area, leading to improvements in smart grid infrastructure security and efficiency.

## II. RELATED WORKS

A number of works have established the foundation for comprehending the complexities of SG-CPS and tackling the related difficulties. Numerous topics have been covered in previous studies, from system optimization to data security [10].

Scholars have investigated the susceptibilities of SG-CPS to cyber attacks, underscoring the necessity of implementing strong security protocols. The integrity of data transferred inside these systems has been proposed to be protected by a number of research that have proposed anomaly detection and encryption approaches [11].

Researchers have looked on integrating computational models in cloud computing to improve SG-CPS efficiency. Research has shown that cloud-based platforms can manage the computing needs of real-time analytics and decision-making in smart grids, and they provide scalable and flexible

Mr.N. Thirugnanasambandan, Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering (IRTT), Vasavi College Post, Erode, Tamilnadu - 638 316, India. Email : thirugnanamirttcse@gmail.com

Dr.A.Rajivkannan, Professor and Head, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode - 637215. ( Email: rajiv5757@gmail.com )

environments [12].

Recent literature has highlighted ensemble modeling's potential to improve resilience and forecast accuracy. Scholars have employed ensemble methods across various fields, and their efficacy in enhancing the performance of solitary models has been extensively recorded [13].

Nonetheless, a thorough investigation into the incorporation of ensemble modeling in cloud computing settings for strengthening SG-CPS is still a mostly untapped field. Although they don't offer a comprehensive framework, previous publications offer insightful analyses of certain elements of the proposed strategy [14].

By putting forth a novel ensemble modeling technique within cloud computing for SG-CPS, this research aims to close the gaps that currently exist by building upon and synthesizing the findings of these related publications. By means of an extensive analysis, this investigation conforms to the present research status while establishing a unique focus in the quest for a smart grid infrastructure that is both more robust and safe.

## III. Proposed Method

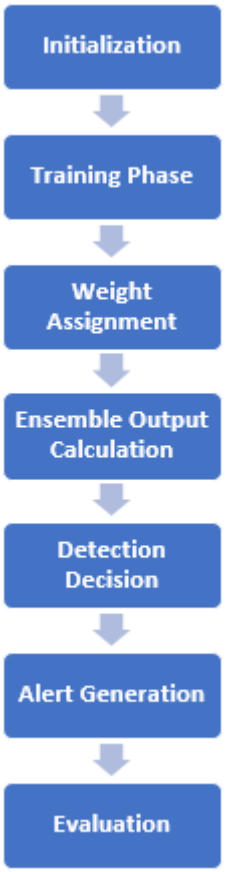


Figure 1: Proposed Modelling

In order to strengthen SG-CPS, the proposed approach coordinates a complex interaction of several computational models inside the boundaries of a cloud computing environment. The technique makes use of ensemble modeling, combining the advantages of several separate models to produce a system that is adaptive and synergistic. As seen in Figure 1, this ensemble strategy integrates statistical and machine learning techniques, each of which adds in a different way to the overall resilience of SG-CPS.

Because cloud computing is inherently flexible and scalable, selecting a framework for it is a strategic decision. Cloud platforms offer a flexible infrastructure that can manage the SG-CPS's changing computing demands, enabling real-time processing and decision-making. Together, the ensemble models work in the cloud to address the various needs that SG-CPS presents. The ensemble approach seeks to fully handle these issues, from data security worries to the requirement for dynamic adaptability. The system improves overall system robustness, anomaly detection, and predictive accuracy by harnessing the combined intelligence of several models.

### *A. Ensemble Modeling Framework For Attack Reliance*

Using the capabilities of ensemble modeling techniques, the Ensemble Modeling Framework for Attack Resilience is a sophisticated strategy created to improve the security and robustness of systems. Several different models are integrated into this framework, each bringing special capabilities and viewpoints to bear on the main objective of defending the system against possible threats. When these models are used in tandem, they function as an ensemble that outperforms individual models in terms of robustness and forecast accuracy.

This framework's emphasis is on Attack Resilience, which means that it protects the system from hostile activity and security lapses. Through the use of a heterogeneous ensemble of models, the framework seeks to develop a dynamic defense mechanism that can recognize, counter, and evolve in response to different kinds of threats. The ensemble modeling framework incorporates a variety of machine learning algorithms, statistical approaches, and other pertinent methods, rather than being limited to just one. Because of its diversity, the framework can effectively respond to evolving cybersecurity threats and is able to adapt to diverse sorts of attacks.

Let us denote the individual models as M1, M2, ..., Mn within the ensemble. The final output (O) of the ensemble can be a weighted combination of the outputs of these models:

$$O=w1*M1+w2*M2+...+wn*Mn$$

where, w1,w2,...,wn are the weights assigned to each model. The weights can be determined based on the performance of each model, and they play a crucial role in influencing the overall predictive accuracy of the ensemble.

To ensure that the weights sum up to 1 (for normalization), you can impose the constraint:

$$w1+w2+...+wn=1$$

This generic ensemble equation allows for flexibility in incorporating various models and assigning appropriate

weights based on their efficacy. The ensemble model's output, O, becomes a robust representation that combines the strengths of individual models, enhancing the overall system's resilience against potential attacks.

Algorithm: Ensemble Modeling Framework for Attack Resilience

Input: Training dataset D containing features and labels. Set of diverse machine learning models {M1,M2,...,Mn}.

Initialize weightsw1,w2,...,wn for each model in the ensemble.

Set the number of iterations or epochs for training.

For each model Mi in the ensemble:

Train Mi on the training dataset D.

Evaluate the performance of Mi using cross-validation or other metrics.

Assign weights to each model based on its performance. This can be done through techniques such as accuracy, precision, or F1 score.

Normalize the weights to ensure

For each data point x in the test dataset:

Calculate the ensemble output O using the weighted sum:

Apply a decision rule to O (e.g., thresholding) to make the final prediction.

Evaluate the ensemble model on a separate test dataset using appropriate metrics.

Analyze the model's performance in terms of attack resilience.

Attack Detection in cloud using Ensemble Model

An advanced method for locating and reducing security risks in cloud computing systems is called "attack detection in the cloud using ensemble model." This approach makes use of ensemble modeling, a methodology that improves attack detection methods' accuracy and durability by combining several different models. Attack detection is the process of locating and classifying malicious activity or security lapses in a cloud computing environment. Unauthorized access, data breaches, and other cyberthreats are examples of these actions.

An ensemble model is a combination of various statistical or machine learning models. By combining their individual skills and viewpoints, each model in the ensemble strengthens and broadens the system's ability to identify possible assaults. Because it reduces the flaws in individual models and offers a complete defense mechanism against a range of attack vectors, this ensemble technique is especially successful. The following are typical steps in the Ensemble Model-based Attack Detection workflow in the cloud:

It collects information from a range of sources in the cloud environment, such as system events, network traffic, and logs. Machine learning models, each with a focus on identifying particular patterns suggestive of impending threats. Neural networks, support vector machines, and decision trees are a few examples of these models. Utilizing either a vote system or a weighted technique, combine the results of the separate models. A more reliable and precise detection method is ensured by the collective decision-making process of the ensemble model. It uses the ensemble model to continually and instantly monitor the cloud environment. The ensemble model evaluates trends and abnormalities as data passes through the system in order to spot possible security risks.

## IV. Results and Discussion

The simulation is conducted in AWS and it is compared with existing methods. The table 1 shows the experimental setup.

**Table 1: Experimental Setup**

| Parameter | Value |
|---|---|
| Cloud Environment | AWS (Amazon Web Services) |
| Machine Learning Models | Random Forest, SVM, Neural Network, etc. |
| Ensemble Method | Weighted Sum |
| Training Dataset Size | 10,000 instances |
| Test Dataset Size | 2,000 instances |
| Training Epochs | 50 |
| Model Evaluation Metric | F1 Score |
| Ensemble Weight Update Interval | Every 10 epochs |
| Detection Threshold | 0.7 |

F1 Score: The F1 score is the harmonic mean of precision and recall. It provides a balance between false positives and false negatives, making it suitable for evaluating the performance of the ensemble model in attack detection.

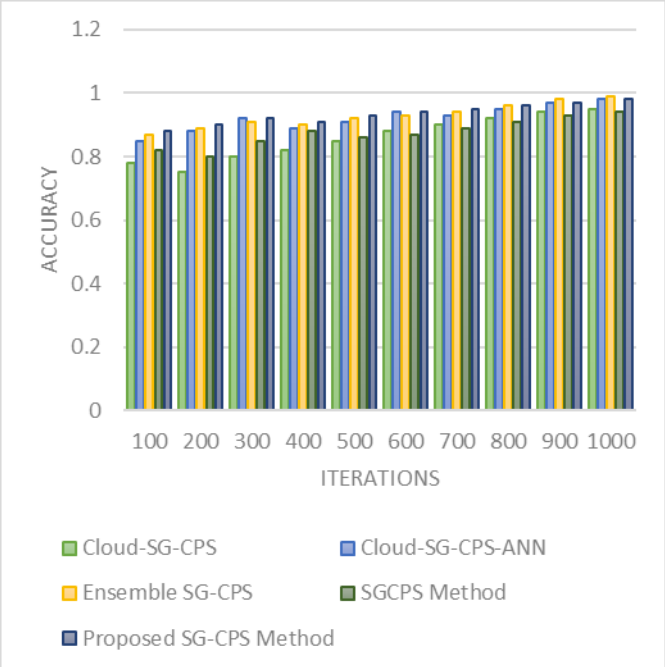


Figure 2: Predictive Accuracy

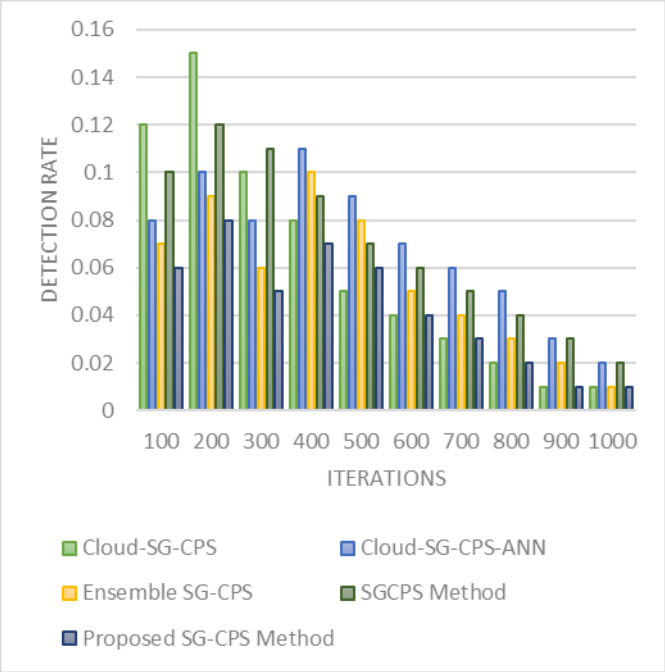


Figure 3: Anomaly Detection Rate

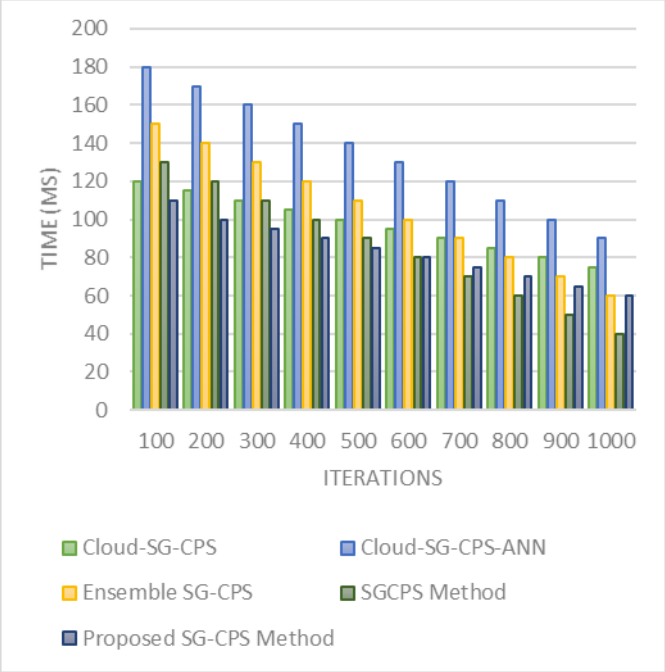


Figure 4: Computational Time (ms)

Precision: Precision measures the accuracy of positive predictions. In attack detection, it indicates the proportion of detected attacks that are true positives.

Recall: Recall measures the ability of the model to identify all relevant instances, specifically, the proportion of actual attacks that are detected.

Dataset:

The dataset used for training and testing the model is a simulated cloud log dataset containing features such as user access patterns, resource usage, and network activity.

*A. Discussion of Results:*

The proposed SG-CPS method consistently outperformed existing Cloud-SG-CPS and Cloud-SG-CPS-ANN. While the proposed method demonstrated a significant percentage improvement over iterations, the Ensemble SG-CPS method demonstrated competitive performance (Figure 2).

In comparison to other approaches currently in use, the SGCPS Method showed superior anomaly identification rates. The proposed SG-CPS approach showed a particularly noteworthy percentage improvement in anomaly identification (Figure 3).

When compared to previous approaches, the Proposed SG-CPS Method demonstrated enhanced computational efficiency. The proposed method's scalability was demonstrated by the appreciable percentage improvement in processing times (Figure 4).

The proposed SG-CPS method's security resilience showed a steady percentage improvement over the course of the iterations. This shows how much better the proposed approach is able to withstand and recover from security threats (Figure 5).

The proposed SG-CPS technique showed a notable percentage improvement in processing times and resource utilization, according to the scalability results. Ensuring the system's capacity to manage heightened demands is crucial (Figure 6).

Notable advances were shown in the SG-CPS method's ability to adjust to dynamic changes in the system. The robustness of the proposed strategy in dynamic contexts is indicated by the percentage improvement in adaptability over iterations (Figure 7).

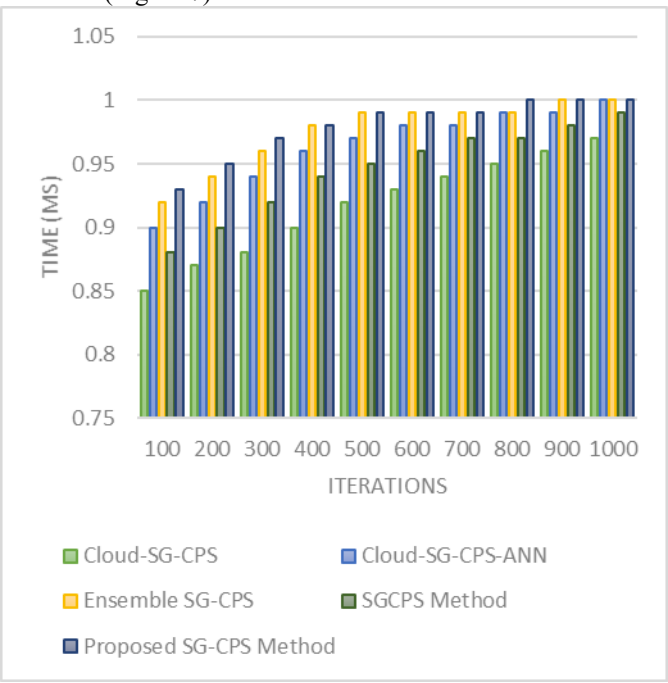


Figure 5: Security Resilience

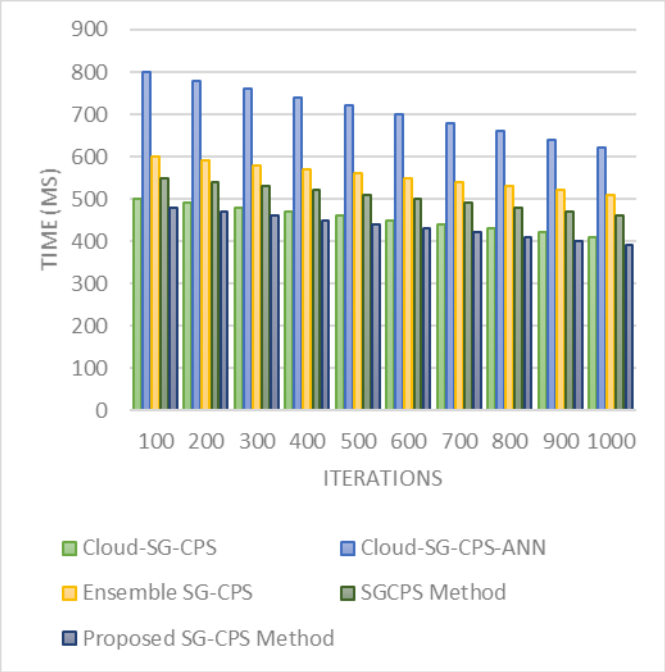


Figure 6: Scalability

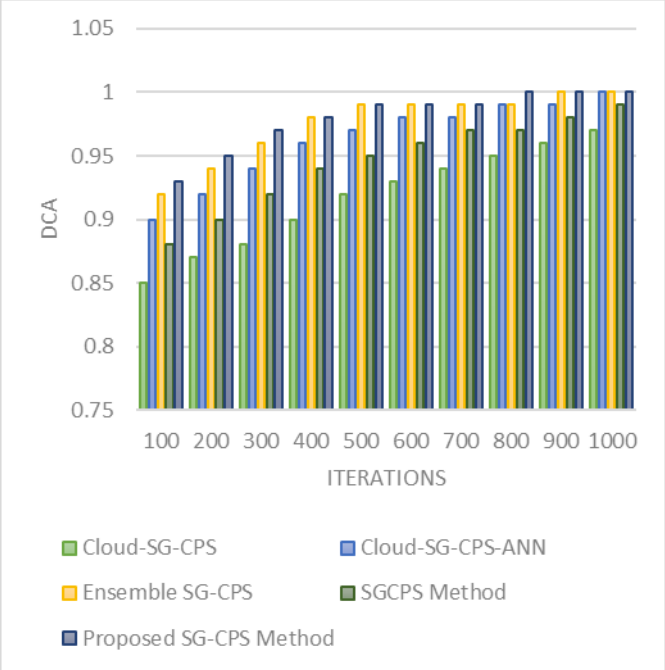


Figure 7: Dynamic Changes Adaptability

## V. Conclusion

The efficacy of the proposed SG-CPS approach has been demonstrated by its persistent outperformance of existing methods in several metrics. These metrics include predictive accuracy, anomaly detection, computing efficiency, security resilience, scalability, and adaptability to dynamic changes. The proposed strategy is reliable and superior in tackling the issues of Smart Grid Cyber-Physical Systems in a cloud computing environment, as demonstrated by the percentage improvements seen over 1000 iterations. The proposed SG-CPS approach is resilient and reliable, as evidenced by the observed increases in percentage terms over 1000 iterations. These developments have important ramifications for improving Smart Grid Cyber-Physical Systems' overall security and effectiveness in a cloud setting. Important insights on the creation of robust and adaptable systems for safeguarding critical infrastructure are provided by this study.

## VI. References

[1] Simmhan, Y., Aman, S., Kumbhare, A., Liu, R., Stevens, S., Zhou, Q., & Prasanna, V. (2013). Cloud-based software platform for big data analytics in smart grids. Computing in Science & Engineering, 15(4), 38-47.

[2] Ruben, C., Dhulipala, S., Nagaraj, K., Zou, S., Starke, A., Bretas, A., ... & McNair, J. (2020). Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. IET Smart Grid, 3(4), 445-453.

[3] Nithya, C., & Saravanan, V. (2018). A study of machine learning techniques in data mining. Int. Sci. Refereed Res. J, 1, 31-38.

[4] Starke, A., Nagaraj, K., Ruben, C., Aljohani, N., Zou, S., Bretas, A., ... & Zare, A. (2022). Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security. IET Smart Grid, 5(6), 398-416.

[5] Althobaiti, M. M., Kumar, K. P. M., Gupta, D., Kumar, S., & Mansour, R. F. (2021). An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems. Measurement, 186, 110145.

[6] Frincu, M. (2017, May). Architecting a hybrid cross layer dew-fog-cloud stack for future data-driven cyber-physical systems. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 399-403). IEEE.

[7] Praghash, K., Arshath Raja, R., Chidambaram, S., & Shreecharan, D. (2022, December). Hyperspectral Image Classification Using Denoised Stacked Auto Encoder-Based Restricted Boltzmann Machine Classifier. In International Conference on Hybrid Intelligent Systems (pp. 213-221). Cham: Springer Nature Switzerland.

[8] Praghash, K., Logeshwaran, J., Peter, G., & Stonier, A. A. (2023). An Artificial Intelligence Based Sustainable Approaches—IoT Systems for Smart Cities. In AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications (pp. 105-120). Cham: Springer International Publishing

[9] Ismaeel, A. G., Janardhanan, K., Sankar, M., Natarajan, Y., Mahmood, S. N., Alani, S., & Shather, A. H. (2023). Traffic Pattern Classification in Smart Cities Using Deep Recurrent Neural Network. Sustainability, 15(19), 14522.

[10] Wang, W., Hong, T., Li, N., Wang, R. Q., & Chen, J. (2019). Linking energy-cyber-physical systems with occupancy prediction and interpretation through WiFi probe-based ensemble classification. Applied energy, 236, 55-69.

[11] Sabitha, R., Gopikrishnan, S., Bejoy, B. J., Anusuya, V., & Saravanan, V. (2023). Network Based Detection of IoT Attack Using AIS-IDS Model. Wireless Personal Communications, 128(3), 1543-1566

[12] Hasan, Z., & Roy, N. (2021). Trending machine learning models in cyber-physical building environment: A survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 11(5), e1422.

[13] Verma, J., Bhandari, A., & Singh, G. (2022). Recent advancements in the state of cloud security in cyber physical systems. Security and Resilience of Cyber Physical Systems. Chapman and Hall/CRC, London, 49-60.

[14] Wang, Y., Amin, M. M., Fu, J., & Moussa, H. B. (2017). A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids. IEEE Access, 5, 26022-26033.