A Secure And Privacy Aware Federated Deep Learning System for Home Intrusion Detection

Kavitha C[1], Aravinda T V[2], Krishnareddy K R[3], Ramesh B E[4]

[1] Student, Dept. of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India
[2]Professor, Dept. of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India
[3]Professor & HOD, Dept. of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India
[4]Associate Professor, Dept. of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India
[1]ckavitha021@gmail.com, [3]krkrishnareddy69@gmail.com,
[2]tvaravinda@gmail.com [4]ramesh.be@gmail.com

Abstract – With the rapid growth of smart home technologies and intelligent surveillance systems, ensuring security while protecting user privacy has become increasingly important. Traditional surveillance systems usually rely on centralized servers where video data is continuously stored and processed. However, this method can expose sensitive personal information, increase communication costs, and create risks related to data leakage and unauthorized access. To overcome these challenges, the proposed work introduces a hybrid software-based and hardware-assisted Home Intrusion Detection System that uses Federated Learning for secure and efficient surveillance.

In this system, multiple smart home environments are simulated as virtual clients within a single platform. Each client captures video data from cameras and trains its own local intrusion detection model independently. Instead of sending raw video footage to a central server, only model parameters are shared, helping preserve user privacy and reduce network overhead. The framework applies computer vision and anomaly detection techniques to identify suspicious activities such as unauthorized access, unknown persons, and unusual movements. A central server aggregates the locally trained models to create a global model, which is redistributed to clients for continuous improvement. Overall, the system provides a scalable, privacy-preserving, and cost-effective solution for next-generation smart home security.

Index Words**:** Home Intrusion Detection, Federated Learning, Anomaly Detection, Computer Vision, Multi-Camera Surveillance, Privacy-Preserving Learning, YOLO (You Only Look Once)

I. INTRODUCTION

With the growing adoption of smart home technologies, ensuring household security has become increasingly important. Conventional surveillance systems generally depend on centralized cloud-based processing, where captured video and sensor information are transferred to remote servers for analysis. Although effective, these methods often create concerns related to user privacy, data exposure, network dependency, and increased communication costs. Because of these challenges, researchers are now focusing on intelligent decentralized approaches that can provide stronger privacy protection while maintaining reliable security monitoring.

The proposed Home Intrusion Detection System is designed using Federated Learning integrated with artificial intelligence and computer vision techniques. In this approach, different smart homes are represented as separate clients, each using cameras to monitor activities in real time. Rather than sending raw surveillance footage to a central server, every client processes its own data locally and trains an intrusion detection model within its environment. The system is capable of identifying unusual events such as unauthorized access, unfamiliar individuals, or suspicious movement patterns.

Federated learning plays a key role in improving the overall detection model while preserving user privacy. Only trained model parameters are shared with the aggregation server, ensuring that sensitive user data remains stored locally within each client device. This collaborative learning process allows the global model to benefit from information learned across multiple environments without directly accessing personal data. As a result, the system achieves better accuracy, adaptability, and security.

To strengthen monitoring capabilities, the framework supports multiple camera inputs and continuous real-time surveillance. Advanced computer vision techniques, including object detection and face recognition, are used to identify potential intrusions and trigger alerts whenever suspicious activities are detected. The proposed system offers a scalable, privacy-aware, and efficient smart home security solution while also serving as a practical research model for studying federated learning–based surveillance systems.

II. LITERATURE SURVEY

The rapid growth of IoT networks has increased the need for intelligent and privacy-preserving intrusion detection systems (IDS). Recent research has focused on integrating federated learning, deep learning, and hybrid models to improve cybersecurity performance in distributed IoT environments. Devine et al. [1] proposed a Transformer-based IDS for smart home IoT environments that combines network traffic and telemetry data to enhance cyberattack detection accuracy using attention mechanisms. However, the study mainly relied on benchmark datasets and faced challenges such as false alarms and limited explainability. Similarly, Puviarasu and Sudha [2] introduced a privacy-preserving federated learning framework using an FT-Transformer model for real-time intrusion detection across IoT devices. Their work emphasized secure distributed learning while preserving data privacy.

Khraisat et al. [3] presented a survey on federated learning for IDS and discussed major challenges including communication overhead, non-IID data distribution, scalability issues, and adversarial attacks. Buyuktanir et al. [4] also explored advancements in federated learning-based IDS and highlighted the importance of robust aggregation

methods and lightweight edge-based models for efficient deployment. Albanbay et al. [5] evaluated federated learning-based IDS performance and identified issues such as model drift, aggregation complexity, and data imbalance in distributed environments.

Hybrid and deep learning approaches have also gained significant attention in intrusion detection research. Agoramoorthy et al. [6] analyzed hybrid IDS models that combine signature-based and anomaly-based detection methods to improve system accuracy. Altunay and Albayrak [7] proposed a CNN+LSTM-based IDS capable of extracting both spatial and temporal features for detecting industrial IoT attacks effectively. Ding et al. [8] developed the DeepAK-IoT model, which achieved high detection accuracy using deep neural networks. Furthermore, Dong et al. [9] introduced a real-time deep learning-based IDS capable of efficiently monitoring live network traffic and detecting abnormal activities in dynamic environments.

III. PROPOSED METHODOLOGY

The proposed Home Intrusion Detection System is developed using a combination of computer vision techniques and federated learning to enable secure, decentralized anomaly detection. The methodology is organized into several stages, including data acquisition, preprocessing, local model training, federated aggregation, and real-time detection.

1) Data Acquisition

The system captures real-time video streams from **multiple camera sources**, including laptop webcams, external cameras, or IP-based cameras. Each simulated smart home acts as an independent client, continuously collecting visual data from its environment. This multi-camera setup ensures wider coverage and improves the reliability of intrusion detection.

2) Data Preprocessing

Captured video frames are processed before analysis:

- Frames are resized and converted into appropriate formats.
- Noise reduction and normalization techniques are applied.
- Face regions and objects of interest are extracted using computer vision methods.

This step ensures that the input data is optimized for efficient model processing.

3) Local Intrusion Detection Model

Each client runs a local detection pipeline consisting of:

- **Object Detection (YOLO):** Identifies the presence of humans or suspicious objects in the frame.
- **Face Recognition:** Compares detected faces with a predefined dataset of authorized individuals to distinguish between known and unknown persons.
- **Anomaly Detection Logic:** Flags intrusion if:
  - A person is detected in restricted conditions, or
  - An unknown face is identified.

The detection process operates in real-time, enabling immediate identification of potential threats.

Algorithm YOLO _Object _Detection

Input: Image I
Output: Detected objects (Bounding Boxes, Class Labels, Confidence Scores)

Step 1: Preprocessing
I_ resized ← Resize(I, 416 × 416)
I_ normalized ← Normalize(I _resized)

Step 2: Feature Extraction
Feature_ Map ← CNN(I_ normalized)

Step 3: Grid Creation
S ← grid size
Divide Feature_ Map into S × S grid cells

Step 4: Bounding Box Prediction
For each grid cell i in S × S:
For each bounding box b in B:
Predict (x, y, w, h)
Compute Confidence:
Confidence ← P(object) × IoU

Step 5: Class Prediction
For each grid cell i:
Predict class probabilities:
P(Class_i | Object)

Step 6: Score Calculation
For each bounding box:
Score ← P(Class_i) × Confidence

Step 7: Threshold Filtering
Remove boxes where Score < Threshold

Step 8: Non-Maximum Suppression (NMS)
For overlapping boxes:
Keep box with highest score
Remove others

Step 9: Output Results
Return final Bounding Boxes, Class Labels, Confidence Scores

End Algorithm

4) Local Model Training

Each client independently trains its model using locally generated or stored data. The training process updates model parameters based on observed patterns such as motion behaviour and detected intrusions. This ensures that each client adapts to its specific environment.

5) *Federated Learning Process*

Instead of transmitting raw data, each client shares only its **model parameters (weights)** with a central server. The server performs aggregation using the Federated Averaging (FedAvg) algorithm:

- Collect model weights from multiple clients

Each client k trains a local model on its data:

$$w_k^{(t)} = \text{LocalTrain}(w^{(t)}, D_k) \quad (1)$$

- $w_k^{(t)}$: Updated weights from client k
- $\mathbf{w^{(t)}}$: Global model at round t
- D_k : Local dataset of client k

Compute the average of these weights

$$w^{(t+1)} = \sum_{k=1}^{K} n_k / n \; w_k^{(t)} \quad (2)$$

· Weighted average based on data size
· n_k: samples at client k, $n=\sum n_k$

- Generate a global model

$$w_{global} = w^{(t+1)} \quad (3)$$

The updated global model is then redistributed to all clients, improving overall system performance while preserving privacy.

Generate Global Model
The aggregated weights form the new global model:

$$w_{global} = w^{(t+1)} \quad (4)$$

Redistribute Global Model to Clients

$$w_k^{(t+1)} \longleftarrow w_{global} \quad (5)$$

· Each client receives the updated global weights
· Used for the next training round

Overall Iterative Process

$$w^{(t+1)} = \sum_{k=1}^{K} \frac{nk}{n} . \text{LocalTrain}(w^{(t)}, D_k) \quad (6)$$

6) *Real-Time Monitoring and Alert System*

The system provides a user interface dashboard for:

- Live video monitoring from multiple cameras
- Displaying detection results (Normal / Intrusion)
- Logging intrusion events

When an anomaly is detected, the system generates alerts and stores evidence (captured images or logs) for further analysis.

IV. SYSTEM ARCHITECTURE

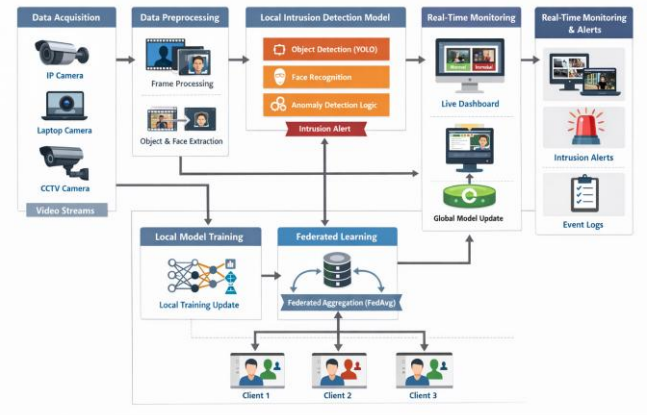


Figure 1: System Architecture

The Figure 1 represents the system architecture of a Home Intrusion Detection System using Computer Vision and Federated Learning.

1. Data Acquisition

Multiple cameras, including laptop cameras, continuously capture live video from different environments, where each camera serves as an independent data source for separate clients.

2. Data Preprocessing

Raw video frames are processed through resizing, formatting, object and face extraction, while noise reduction and normalization techniques enhance entire data quality and analysis accuracy.

3. Local Intrusion Detection Model

Each client performs real-time monitoring using YOLO object detection, face recognition, and anomaly detection to identify unknown individuals or suspicious activity in restricted areas.

4. Local Model Training

Each client independently trains its local model using private data, allowing the system to learn environmental patterns, user movements, and previous intrusion activities effectively.

5. Federated Learning (Central Server)

Instead of sending video data, clients send model weights.
The server performs:
Federated Aggregation (FedAvg)which averages model parameters from all clients
A Global Model is created and sent back to clients.

6. Real-Time Monitoring

A dashboard display:
Live video feeds
Detection status (Normal / Intrusion)
Shows global model updates applied to clients.
purpose: Provide user-friendly system control and visualization.

7. Alert System & Logging

When intrusion is detected:
Alerts are triggered
Evidence (images/video frames) is stored
Event logs are maintained

V. Results And Discussions

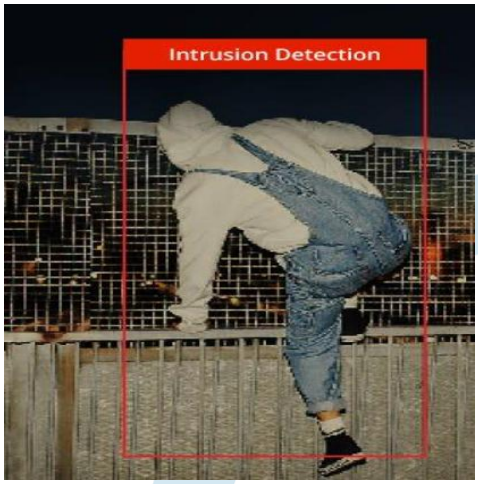


Figure 2: Intrusion Detected

The Figure 2 shows an intrusion detection system identifying a person climbing over a fence, which is considered a suspicious activity. The system uses object detection to locate the person and highlights them with a red bounding box labelled “Intrusion Detection.” This indicates an unauthorized entry attempt, triggering an alert and logging the event for security monitoring.

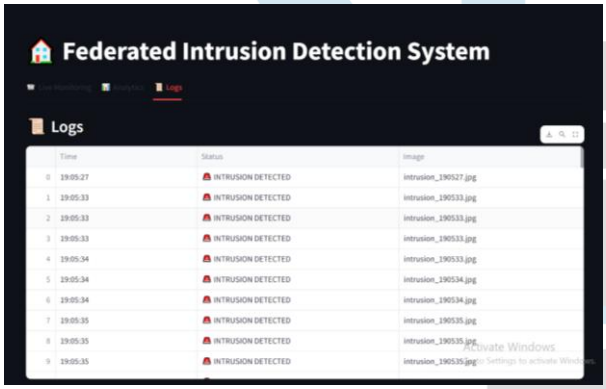


Figure 3: Log Report

The Figure 3 shows the Logs section of the Federated Intrusion Detection System dashboard, where all detected intrusion events are recorded. Each entry includes the timestamp, the status (“Intrusion Detected”), and the saved image filename as evidence. This log helps in tracking security incidents over time and provides stored visual proof for further analysis or investigation.

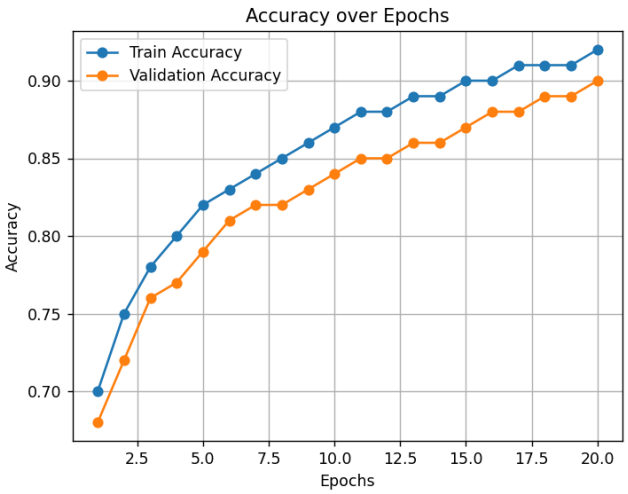
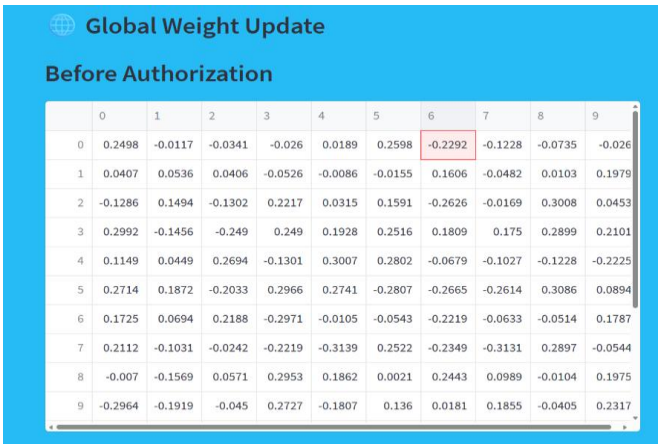


Figure 4: Accuracy

The Figure 4 shows the model’s training and validation accuracy over epochs, indicating how performance improves during learning. The training accuracy steadily increases, while the validation accuracy follows a similar trend, showing that the model is generalizing well without significant overfitting. The small gap between the two curves suggests good model stability and effective learning.

Figure 5: Metrics of federated Home intrusion detection

The Figure 5 shows the after the federated round and metrics like accuracy ,precision ,Recall and F1-score changes after every federated round by storing the intrusion activity in the log.

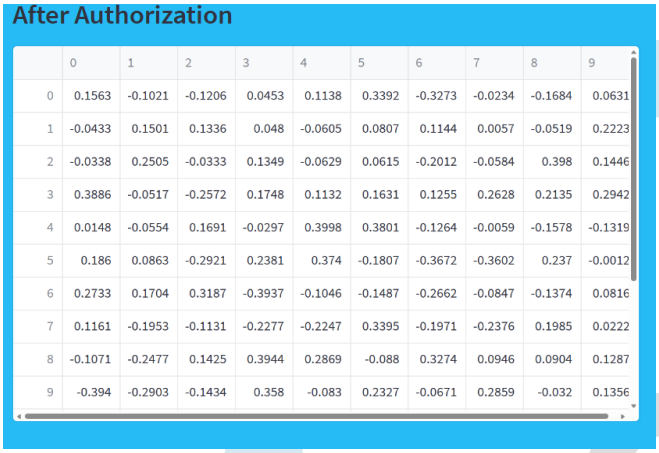


	0	1	2	3	4	5	6	7	8	9
0	0.2498	-0.0117	-0.0341	-0.026	0.0189	0.2598	-0.2292	-0.1228	-0.0735	-0.026
1	0.0407	0.0536	0.0406	-0.0526	-0.0086	-0.0155	0.1606	-0.0482	0.0103	0.1979
2	-0.1286	0.1494	-0.1302	0.2217	0.0315	0.1591	-0.2626	-0.0169	0.3008	0.0453
3	0.2992	-0.1456	-0.249	0.249	0.1928	0.2516	0.1809	0.175	0.2899	0.2101
4	0.1149	0.0449	0.2694	-0.1301	0.3007	0.2802	-0.0679	-0.1027	-0.1228	-0.2225
5	0.2714	0.1872	-0.2033	0.2966	0.2741	-0.2807	-0.2665	-0.2614	0.3086	0.0894
6	0.1725	0.0694	0.2188	-0.2971	-0.0105	-0.0543	-0.2219	-0.0633	-0.0514	0.1787
7	0.2112	-0.1031	-0.0242	-0.2219	-0.3139	0.2522	-0.2349	-0.3131	0.2897	-0.0544
8	-0.007	-0.1569	0.0571	0.2953	0.1862	0.0021	0.2443	0.0989	-0.0104	0.1975
9	-0.2964	-0.1919	-0.045	0.2727	-0.1807	0.136	0.0181	0.1855	-0.0405	0.2317

Figure 6: Global Weight update Before Authorization of a person

The figure 6 “Global Weight Update” table before authorization in a machine learning or federated learning

system. The matrix contains numerical weight values used by the model during training. Positive and negative values represent parameter adjustments. It highlights the model's internal state before secure validation, synchronization, or aggregation across connected devices.



	0	1	2	3	4	5	6	7	8	9
0	0.1563	-0.1021	-0.1206	0.0453	0.1138	0.3392	-0.3273	-0.0234	-0.1684	0.0631
1	-0.0433	0.1501	0.1336	0.048	-0.0605	0.0807	0.1144	0.0057	-0.0519	0.2223
2	-0.0338	0.2505	-0.0333	0.1349	-0.0629	0.0615	-0.2012	-0.0584	0.398	0.1446
3	0.3886	-0.0517	-0.2572	0.1748	0.1132	0.1631	0.1255	0.2628	0.2135	0.2942
4	0.0148	-0.0554	0.1691	-0.0297	0.3998	0.3801	-0.1264	-0.0059	-0.1578	-0.1319
5	0.186	0.0863	-0.2921	0.2381	0.374	-0.1807	-0.3672	-0.3602	0.237	-0.0012
6	0.2733	0.1704	0.3187	-0.3937	-0.1046	-0.1487	-0.2662	-0.0847	-0.1374	0.0816
7	0.1161	-0.1953	-0.1131	-0.2277	-0.2247	0.3395	-0.1971	-0.2376	0.1985	0.0222
8	-0.1071	-0.2477	0.1425	0.3944	0.2869	-0.088	0.3274	0.0946	0.0904	0.1287
9	-0.394	-0.2903	-0.1434	0.358	-0.083	0.2327	-0.0671	0.2859	-0.032	0.1356

Figure 7: Global Weight update After Authorization of a person

The figure 7 presents the "After Authorization" stage of a global weight update process in a machine learning system. The numerical values indicate updated model parameters after security verification and authorization. Compared to the previous stage, the weights are refined and synchronized, showing how the system securely improves model learning and maintains reliable data consistency.

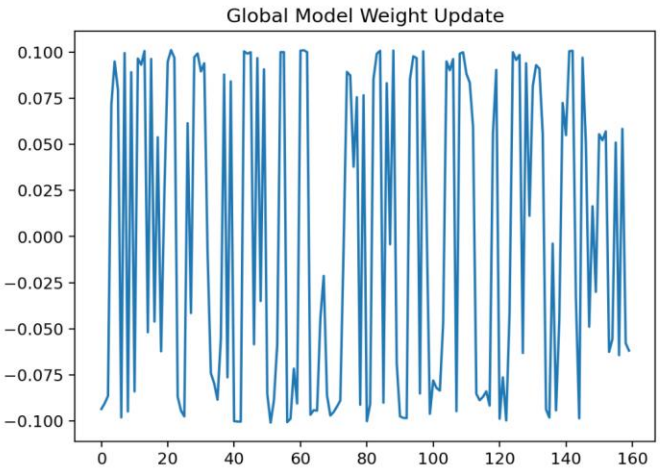


Figure 8: Global weight update to central server

The Figure 8 illustrates the global model weight update process in a machine learning system. The fluctuating line represents continuous changes in model weights during training and optimization. Positive and negative variations indicate parameter adjustments made to improve learning accuracy. The visualization highlights how the model dynamically adapts and updates itself throughout the training process

VI. Conclusion and Future Works

The proposed System combines computer vision and Federated Learning to provide a smart, secure, and privacy-preserving surveillance solution for homes. The system uses various camera sources and real-time video analysis to detect suspicious activities through object detection, face recognition, and anomaly detection techniques. One of the major advantages of the system is its decentralized learning approach, where each client trains their local model independently and shares only model parameters instead of raw video data. This helps maintain user privacy and data security while enabling collaborative learning among all the clients. The aggregated global model continuously improves detection accuracy and system performance. In addition, the system supports real-time monitoring, instant alert generation, and event logging, allowing users to respond quickly to potential threats and analyze incidents effectively. Its scalable and adaptable architecture makes it suitable for smart home environments and future surveillance applications. Overall, the proposed framework provides an efficient, reliable, and intelligent intrusion detection solution by integrating artificial intelligence with distributed learning technologies.

Future Works

The proposed System provides a strong foundation for smart home security, but it can be further enhanced through several future improvements. Advanced AI models such as Vision Transformers and improved YOLO versions like YOLOv8 can be integrated to achieve more accurate object detection and surveillance performance. Behaviour analysis techniques using models such as LSTM or 3D CNN can also help identify suspicious activities like loitering, forced entry, or unusual movement patterns. These improvements can increase detection accuracy, especially in low-light conditions or crowded environments.

Another important enhancement is Edge AI deployment, where the system can run on devices such as Raspberry Pi or NVIDIA Jetson. This allows video processing and intrusion detection to occur directly on local devices instead of depending entirely on cloud servers. As a result, the system can provide faster real-time responses, reduce latency, minimize bandwidth usage, and improve overall efficiency and reliability for smart home surveillance applications.

References

[1] Devine, M., Ardakani, S. P., Al-Khafajiy, M., & James, Y. (2025). *Federated machine learning to enable intrusion detection systems in IoT networks*. Electronics,14(6),1176. https://doi.org/10.3390/electronics14061176 (MDPI)

[2] Puviarasu, A., & Sudha, V. K. (2024). *Enhanced IoT security: Privacy-preserving federated learning model for accurate, real-time intrusion detection across devices*. International Journal of Intelligent Systems and Applications in Engineering.

[3] Khraisat, A., Alazab, A., Singh, S., Jan, T., & Gomez, A. J. (2022). *Survey on federated learning for intrusion detection system*. Computer Communications, 195, 346–361.

[4] Buyuktanir, B., Altinkaya, S., Baydogmus, G. K., & Yildiz, K. (2024). *Federated learning in intrusion detection: Advancements, applications and future directions*. Future Generation Computer Systems.
[5]Albanbay, N., Tursynbek, Y., Graffi, K., Uskenbayeva, R., Kalpeyeva, Z., Abilkaiyr, Z., & Ayapov, Y. (2024). *Federated learning-based intrusion detection in IoT networks: Performance evaluation and data scaling study*. Journal of Network and Computer Applications.
[6] Agoramoorthy, M., Ali, A., Sujatha, D., M. R., T. F., & Ramesh. (2023). *An analysis of signature-based components in hybrid intrusion detection systems*. International Journal of Information Security and Privacy.
[7] Altunay, H. C., & Albayrak, Z. (2024). *A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks*. Computers & Security.
[8] Ding, W., Abdel-Basset, M., & Mohamed, R. (2023). *An effective deep learning model for cyberattack detection in IoT networks*. Information Sciences, 647, 119–132.
[9] Dong, Y., Wang, R., & He, J. (2022). *Real-time network intrusion detection system based on deep learning*. IEEE Access, 10, 45678–45689.