International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
***Article Received**: 09 December 2022 **Revised**: 10 January 2023 **Accepted**: 26 January 2023*

Auto Deep Learning-based Automated Surveillance Technique to Recognize the Activities in the Cyber-Physical System

M.Archana[1], Dr.S.Kavitha[2], Dr.A.Vani Vathsala[3]
[1]Research Scholar in CSE,
SRM Institute of Science and Technology, Kattankulathur,
Tamil Nadu, India.
Senior Assistant professor,Department of CSE,
CVR College of Engineering,
Hyderabad, Telangana, India
mogullaarchana23@gmail.com
[2]Department of CTECH,
SRM Institute of Science and Technology, Kattankulathur,
Tamil Nadu, India
kavithas@srmist.edu.in
[3]Department of CSE,
CVR College of Engineering,
Hyderabad, Telangana, India
vani_vathsala@cvr.ac.in

Abstract— In recent days, the Internet of Things (IoT) plays a significant role and increasing in rapid usage in various applications. As IoT is being developed for cyber-physical systems in the specific domain of e-health care, military, etc. Based on real-time applications, security plays a vital role in certain activities in educational institutions. In the institutions, there are multiple videos are collected and stored in the data repositories. Those datasets are developed specifically for certain activities and no other datasets are developed for academic activities. As there is a large number of videos and images are collected and considered, advanced technologies like, deep learning and IoT are used to perform certain tasks. In this paper, a Auto Deep learning-based Automated Identification Framework (DLAIF) is proposed to consider and reconsider the activities based on image pre-processing, model can be trained through the proposed GMM model and then predication to make an effective surveillance process based on HMM. This proposed process makes to recognize the activities through EM and log Likelihood for cyber-physical systems. In the performance analysis, the proposed model efficiency can be determined through Accuracy detection, False Positive rate and F1 Score requirement. Then calculating the accuracy is more effective for the proposed model compared to other existing models such as BWMP and LATTE.

Keywords: Internet of Things, Deep Learning, Neural Networks, Computational time, and Accuracy.

I. Introduction

In the recent era, Network related activities are increased rapidly in day to day and it has various confidential information's, which is increasing enormously. In this situation, network faces issues related to security as intruders i.e., unauthorized users, which contains those activities are malicious and has any unwanted activities [1]. Intrusion-based network system will play a vital role in the area of research and there are various machine learning approaches still exists and that are proposed as the related study in the current scenario [2].

Then there are various datasets are used as generated one and that are analyzed and refined through various learning models. Initially these machine learning models are being used on the intrusion network systems [3-6] that are added and integrated to make salient information's such as, selection of features, paradigm integration and various deep learning models as represented in Figure1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
***Article Received**: 09 December 2022 **Revised**: 10 January 2023 **Accepted**: 26 January 2023*

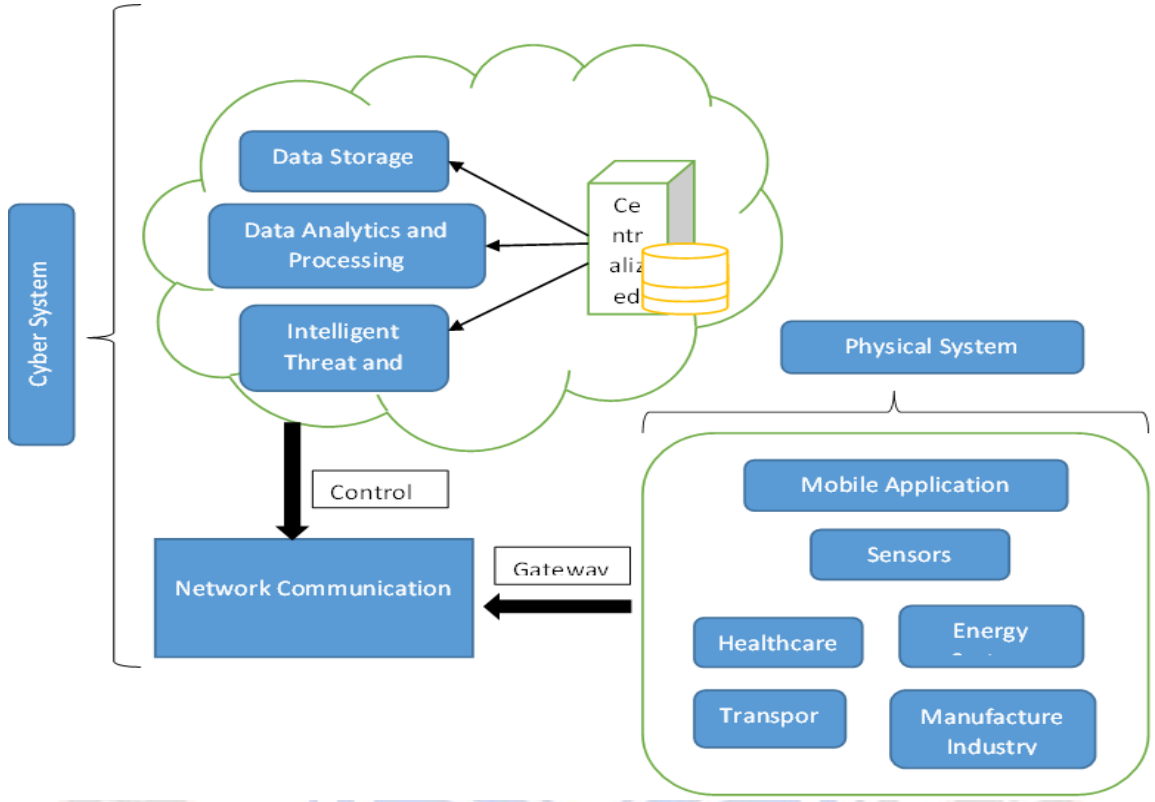

Figure. 1. Cyber Physical System

The important activities that are prevailed on the cyber physical systems are intrusion detection systems that are emerged and able to keep tract the essential feature with effective quality that are able to identify the data and to remove the unwanted data or irrelevant information feature and it make to reduce the feature dimension based on the datasets that are used [7]. Then propose the hybrid method, which integrates both Support Vector Machine (SVM) and Genetic Algorithm (GA) [8] and [9]. It results in analyzing and extracting the datasets through learning algorithm, which results in making the genetic algorithm more efficient than the support vector machine. Then the learning algorithm will makes integrates with feature subset selection. Proposed a malware detection model associated with cloud computing based on packet networking [10,34]. The identification of packets, which is considered as the input uses data mining technique to reduce the packet knowledge and this helps to validate whether malware detection or not. As data mining will analyze the extraction of data but learning algorithm will learn the input dataset. So, SMMDS based malware detection model will follow the concept of machine learning technique [11].

Mainly, the intruder intension is to attempt the confidential data. Based on the various security-based network methods, they are overcoming the different attacks and illegal activities happens on the physical systems through cyber-attacks and it still exists on it even the methods are applied on it [12]. So, there should be an effective intrusion system is needed to avoid those attacks based on the system related to network intrusion approach to prevent them. There are several intrusion systems exists on the current scenario as there are broadly classified as Denial of Service (DoS), Cross-Site Scripting (CSS), etc [13] and [14] are used to overcome the attacks that still exist. So, there must be a low-cost and better identification approach to detect the anomalies activities but the existing techniques fail to detect in the complex system. The existing learning algorithm make to improve the accuracy detection, which results in fast and scalable way to perform the detection process [15].

In this, a Deep Learning-based Automated Identification Framework (DLAIF) is proposed to make improved decision-making to identify the anomaly activities in Cyber-Physical Systems (CPS). In the proposed framework, Auto DL based learning model is proposed, which helps to learn the activities performed in the system. This DL-based model helps to influence and gather some information at the execution time and identify the anomalies activities as the abnormal changes are identified from the normal behavioral system. Then the proposed work is analyzed based on the performance metric of detection

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
***Article Received**: 09 December 2022 **Revised**: 10 January 2023 **Accepted**: 26 January 2023*

accuracy, F1 Score, False positive rate and AUC value and it is compared to other existing methods such as,

II. Related Works

There are various detection systems deployed for performing multiple activities in automated systems. In this different automated approaches and communication techniques are discussed and explain how those models perform the process of identifying anomalies activities in the cyber-physical system. Then the Deep learning role has been explored to make effective progress of monitoring the activities in the network [16-19]. Then anomalies detection activities are modeled to communicate with messages and perform attacks so that the illegitimate activities are identified with certain pattern matching [20] and [21]. This method makes some failure to identify the activity and that information in the process attack stages. In order to reduce the failure, CAN packets are being used to check the matching pattern between the packets and CAN packet in order to identify the anomalies activities. Then [22] has used CAN IDs as the metrics to pair the information sequences and it achieves a false positive rate but fails to identify the attacks.

[23] has calculated the time interval among the requested node information to the receiving information as how much the time it takes to reach the destination via CAN bus to identify certain attacks like reply attack. Based on the pattern matching, [24] has proposed a detection system with the integration of the Myers algorithm in order to improve and speed the process matching process. Then to identify multiple anomaly identification, [25] has proposed an approach to make analysis on time-frequency based on the injection of CAN messages. Thus, the above approaches proposed are related to anomaly detection system but it is not specific to more complex networks and various attacks. Then [26] has proposed the anomaly based detection technique as it monitors the offline system activities and able to identify the anomaly as there is a change as compared to the normal behavior. Based these kind of approaches, the various attacks can be identified.

Then [27], has proposed the learning method to be integrated with detection system and it helps to identify and monitor the attacks happening in the system. This approach has performed well with the integration of learning method but suffers from improper latency. [28] and [29] has proposed technique, which uses 4 classifier with nearest neighbor as it categories the CAN payload normally and their attacks performed on it. With respect to the attacks like DoS and fuzzy, this classifier approach will perform poorer and able to manage only the low-priority messages. Then [30] has proposed the detection model associated with decision tree as it monitors and identifies the detection of attacks in some of the aspects and it faces the problem of high latency on the networks. Then there are various approaches are used as it including as it fails with high latency problems.

Then deep learning-based approaches are proposed as it helps to manage the communication messages in the network. The deep learning-based approach makes low-priority monitoring to be applied and it is difficult to apply the high-priority systems [31] and [32]. The deep-based auto encoder approach is proposed in order to identify the attacks as it uses the LSTM model and it contains message ID to identify the complex networks. Then LSTM based prediction model is proposed to the value message as it takes longer message variation to detect the anomaly in networks. With the LSTM classifier, supervised learning models are applied and to classify the attacks on the networks. Then [33] proposed the LSTM-based encoder and decoder architecture as it uses certain messages to make them construct the given input. This encoder and decoder use K-nearest neighbor and estimator to identify the intrusion on the networks. The models proposed above attempts to improve the detection accuracy on the anomaly activities performed on the network and make the approach to be light weight, fast, and data scalable to monitor and detect the attacks in the network.

III. Problem Definition

The existing models used to identify and monitor the anomaly detection approach make to attain reduced cost and improved detection time and it is not applied to complex networks. Then various other approaches are deployed with the integration of learning algorithms as makes attempt to increase the accurate detection and it faces the problem of accurate detection and identifying the attacks and anomaly activity happening in the system. Then it faces the problem of computational overhead in order to achieve high performance.

IV. Research Methodology

In this aspects, the data's are collected under the framework of DLAIF under a regular interval in time as it helps to improve the data confidence level and it helps to identify the anomaly activity performed in the system. After collecting the data information, those data are pre-processed by applying the training model. The data which is represented as the datasets are classified into certain groups and make each group work independently based on the message identifier. Each group has certain featured attributes such as,

a. Message timestamp
b. Signal Values

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
***Article Received**: 09 December 2022 **Revised**: 10 January 2023 **Accepted**: 26 January 2023*

c. Message represented as single bit
d. Message Identifier
e. Message signals

$$Message\ Label = \begin{cases} 0 & Non\ Anomalies\ Samples \\ 1 & Anomalies\ Samples \end{cases} \quad (1)$$

In the above eqn. (1), Non-Anomalies samples are trusted one, and anomalies samples are experienced with certain attacks. Then the signal values are represented as 0's and 1's. and if the data variance is high, getting the data's are very slow and unstable one.

Then the prediction model is designed, which helps to identify the attacks as it persists to anomaly activity that happen during the normal activity in the system. The information's that are collected from the system that are applied to data pre-processing and this helps to make the learning algorithm to learn the relationship among the information's that are collected. Then this processed information's helps to predict the activity that is doing to happen at the next instance of time and this prediction will be more accurate among the identification of anomalies behavior happen in the system. During the prediction model, it faces the problem of out of distribution for detecting purpose. The model is developed to make effective decision making

In the prediction model, anomaly detection is confirmed as it represents the input set as 'Y' = {Y_1, Y_2, Y_3, …. Y_n} and it makes the datasets to be tested. Here the training datasets make nonconformity measure function, which uses numerical values. Then this function makes to measure the distance between the Z_n of next data with the K-Nearest Neigbour from the datasets 'Y'. Then P-value is represented 'P' based on the two non-conformity value with the next value of 'Y_n'.

$$P_{n+1} = \frac{|\{1,2,\ldots m\}\ Z_n \geq Z_{n+1}|}{m} \quad (2)$$

Then the given input set 'Y' = {Y_1, Y_2, Y_3, …. Y_n} is categorized into Y_1, Y_2, Y_3, …. Y_k and other sets as Y_{k+1}, Y_2, Y_3, …. Y_n and the P value is redefined as,

$$P_{n+1} = \frac{|\{m+1,\ldots\ldots K\}\ Z_n \geq Z_{n+1}|}{m-k} \quad (3)$$

The P-value makes the conformity anomalies value to make the high probability of detecting the anomaly activity. During the process of prediction, proposed model makes the distribution of nonconformity measure function to calculate the prediction value. In the presence of attack, information not able to maintain the relationship among them and makes θ Gaussian Mixture Model (GMM) as it represents the system behavior,

$$P(X_i = x) = \sum_{K=1}^{K} \prod_k P(X_i = x |\ Z_i = k) \quad (4)$$

Where Z_i *belongs to* {1,2,3. ….. K} for X_i

$P(X_i | Z_i)$ → Component Mixture

Then Expectation-Maximization (EM) is applied to determine the optimal bounded value 'B' as $B(\theta; \theta^t)$ and extend the bounded value to determine θ^{t+1}. Then formulate the expected and Maximization Step as represented in Figure 2.

Expected Step: $f^t(J) \triangleq P(J|U, \theta^t)$

Maximization Step: $\theta^{t+1} = \text{argmax}_\theta (Q^t(\theta) + \log P(\theta))$

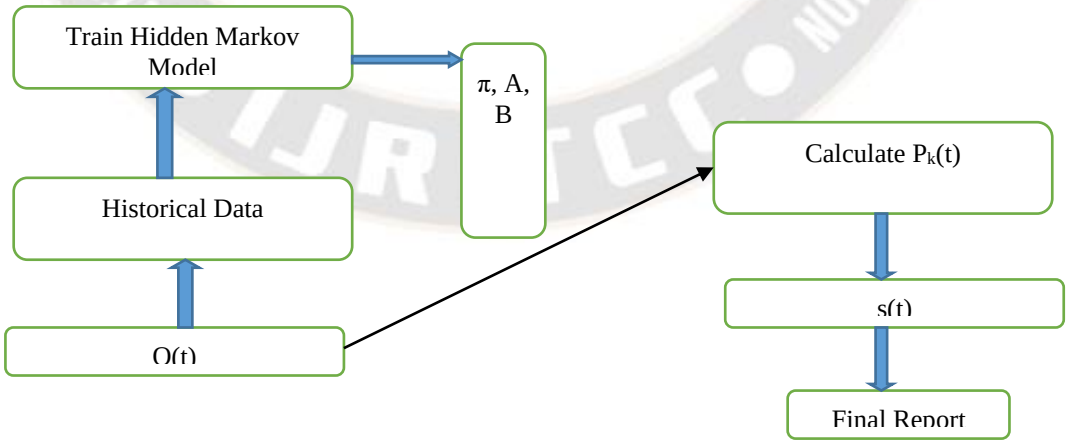

Figure. 2. Anomalies Data detection model based on the training data

Algorithm 1: Anomalies Data detection model based on the training data.

Input: Training Data

Output: Detecting the anomalies activity in the system.

1. Train the data
2. GMM to target the multimode behavior

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
***Article Received**: 09 December 2022 **Revised**: 10 January 2023 **Accepted**: 26 January 2023*

3. The component weight is calculated as $P\ (x|\Theta_m)$ and then P value is calculated based on Eqn (3) and (4) and then it is formulated as,

$P\ (x|\Theta)= \sum_{K=1}^{K} \emptyset_m\ P(x|\theta_m)$

Where, $\emptyset_m$ weight of the component

θ_m Mean and Covariance Matrix.

$\Theta \rightarrow Guassian\ Mixture$

4. GMM uses EM algorithm to determine the mean and covariance $\mu_m, \sum m$
5. Validate the P value.
6. The sequence of non-conformity measures with respect to $(y - \overline{y})^{abs}$
7. Pool sets are generated $\{Y_1, Y_2, Y_3, \ldots. Y_{n-1}, Y_n\}$
8. P values $\{P_1, P_2, P_3, \ldots. P_{n-1}, P_n\}$ then define the threshold value.

In the role of classifying the anomalies in the system, discrepancy changes are identified and anomalies are identified, as same as training data, anomaly detection also performed. Using HMM, Detecting the anomaly, with increased detection rate, learning ability and improved stability.

Algorithm 2: Anomalies Data classification model based on the training data

Input: Training the data

Output: Anomaly classifier using HMM

1. Train the input data
2. Train the linear models $\{L_1, L_2, L_3, \ldots. L_p\}$
3. As Vector Parameters are represented as Θ and parameters $\{\Theta_1, \Theta_2, \Theta_3, \ldots. \Theta_p\}$are recorded.
4. HMM-based anomaly classifier has set of pair H,

Where $Q = \{Q_1, Q_2, Q_3, \ldots. Q_p\}$ and $V = \{V_1, V_2, V_3, \ldots. V_S\}$

Q → Hidden States and V → Observations and both determined based on time.

5. Probability Matrix,

$A= [a_{ij}], belongs\ to\ R^{NXN}$

$Where,\ a_{ij} \rightarrow data\ moves\ from\ state\ 'i'\ to\ 'j'$

$a_{ij}=P(Q_{t+1} = j|Q_t=i)$

$B= [b_j(k)], belongs\ to\ R^{NXM}$

Whereas, $b_j(k)=P(V_t = k|Q_t=j)$

6. Hidden Markov Model $H = (Q, A, V, B, \pi)$

Where Q → Hidden States

V → Observations

π → Initial Probabilities

A → Transition Probabilities

B → Emission Probabilities

7. Training Phase, Vector Parameters → $\{\Theta_1, \Theta_2, \Theta_3, \ldots. \Theta_p\}$
8. Apply HMM on training phase for every variable V_i, calculate Log-likelihood for sequence $L_{ij,}$

$L_{ij}=Log(P\ (\Theta_n|q_n))$ Whereas, $P\ (\Theta_n|q_n)= \prod_{i=1}^{n} P\ (\Theta_i|q_i)$

9. Validating the data through Likelihood Estimation. $L_{ij}=\{L_{i1}, L_{i2}, L_{i3}, \ldots.. L_{ij}\}$
10. Threshold: $h_2^{V_i}$

Based on anomaly detection and classification, effective decision-making is generated.

V. Performance Analysis

In the performance analysis, the proposed DLAIF framework effectiveness where proposed model uses prediction process with a threshold value in order to identify the anomalies and normal activities performed in the system. With this proposed framework, various scenario are addressed as listed below,

1. Static Threshold
2. Signal value difference
3. Signal Deviation sum
4. Signal Deviation mean
5. Signal Deviation maximum absolute

Then the proposed framework is analyzed on various performance metrics such as, Detection accuracy, false positive rate and F1 Score.

Table 1. Accuracy Value based on the DLAIF framework

Accuracy	DLAIF ST	DLAIF AVG	DLAIF SUM	DLAIF MAX	DLAIF DIFF
No Attack	0.8	0.99	0.98	0.98	0.99
Relay Attack	0.85	0.920	0.925	0.89	0.93
DDoS Attack	0.58	0.89	0.89	0.84	0.91
Dropping Attack	0.77	0.86	0.855	0.81	0.88

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
Article Received: 09 December 2022 Revised: 10 January 2023 Accepted: 26 January 2023

From the Table 1, Accuracy value probability is calculated based on the proposed framework category of ST, AVG, SUM, MAX and DIFF. and it is calculated under the scenario of No attack, replay attack, DDOS Attack and Dropping Attack.

Table 2. False Positive Rate Value based on the DLAIF framework

False Positive Rate	DLAIF ST	DLAIF AVG	DLAIF SUM	DLAIF MAX	DLAIF DIFF
Constant Attack	0.42	0.29	0.29	0.31	0.58
Relay Attack	0.03	0.031	0.032	0.032	0.027
DDoS Attack	0.018	0.017	0.019	0.017	0.018
Dropping Attack	0.04	0.042	0.043	0.044	0.045

From the Table 2, False Positive Rate probability is calculated based on the proposed framework category of ST, AVG, SUM, MAX and DIFF. and it is calculated under the scenario of Constant attack, replay attack, DDOS Attack and Dropping Attack.

Table 3. F1 Score Value based on the DLAIF framework

F1 Score	DLAIF ST	DLAIF AVG	DLAIF SUM	DLAIF MAX	DLAIF DIFF
Constant Attack	0.67	0.84	0.84	0.81	0.83
Relay Attack	0.81	0.94	0.94	0.91	0.96
DDoS Attack	0.58	0.86	0.86	0.76	0.92
Dropping Attack	0.78	0.94	0.94	0.77	0.92

From the Table 3, F1 Score probability is calculated based on the proposed framework category of ST, AVG, SUM, MAX and DIFF. and it is calculated under the scenario of Constant attack, replay attack, DDOS Attack and Dropping Attack.

Table 4. Accuracy Value based on the DLAIF framework

F1 Score	BWMP	LATTE	Proposed DLAIF
Constant Attack	1.0	1.0	1.0
Relay Attack	0.84	0.87	0.92
DDoS Attack	0.78	0.92	0.96
Dropping Attack	0.78	0.98	0.997

From the Table 4, Accuracy probability is calculated based on the proposed framework and compared with BWMP and LATTE and infer that the proposed one will perfrom better in term of accuracy under the scenario of No attack, replay attack, DDOS Attack and Dropping Attack

Table 5. False Positive Rate Value based on the DLAIF framework

False Positive Rate	BWMP	LATTE	Proposed DLAIF
Constant Attack	0.021	0.038	0.021
Relay Attack	0.011	0.012	0.009
DDoS Attack	0.000	0.009	0.005
Dropping Attack	0.000	0.019	0.014

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 2
DOI: https://doi.org/10.17762/ijritcc.v11i2.6111
***Article Received**: 09 December 2022 **Revised**: 10 January 2023 **Accepted**: 26 January 2023*

From the Table 5, False Positive Rate probability is calculated based on the proposed framework and compared with BWMP and LATTE and infer that the proposed one will perfrom better in term of accuracy under the scenario of No attack, replay attack, DDOS Attack and Dropping Attack.

Table 6. F1 Score Value based on the DLAIF framework

F1 Score	BWMP	LATTE	Proposed DLAIF
Constant Attack	0.78	0.85	0.88
Relay Attack	0.78	0.97	0.985
DDoS Attack	0.66	0.965	0.974
Dropping Attack	0.671	0.985	0.944

From the Table 6, F1 Score probability is calculated based on the proposed framework is compared with BWMP and LATTE and infer that the proposed one will perform better in term of accuracy under the scenario of No attack, replay attack, DDOS Attack and Dropping Attack.

VI. Conclusion

Novel Deep learning-based Automated Identification Framework (DLAIF) is proposed to consider and reconsider the activities based on image pre-processing, model can be trained through the proposed GMM model and then predication to make an effective surveillance process based on HMM. This proposed process makes to recognize the activities through EM and log Likelihood for cyber-physical systems. In the performance analysis, Accuracy detection, F1 Score and False Positive rate probability is calculated based on the proposed framework category of ST, AVG, SUM, MAX and DIFF. and it is calculated under the scenario of Constant attack, replay attack, DDOS Attack and Dropping Attack. Then proposed DLAIF framework is compared with existing BWMP and LATTE to calculate Accuracy detection, F1 Score and False Positive rate probability. In the analysis, Proposed DLAIF performs effectively in terms of Accuracy detection, F1 Score and False Positive rate probability.

References:

[1] H. M. Song, H. R. Kim and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in International Conference on Information Networking (ICOIN), 2016.

[2] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in IEEE Intelligent Vehicles Symposium (IV), 2017.

[3] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—

[4] Practical examples and selected short-term countermeasures," Reliability Engineering & System Safety, vol. 96, no. 11, pp. 11-25, 2011.

[5] M. Gmiden, M. H. Gmiden and H. Trabelsi, "An intrusion detection method for securing in vehicle CAN bus," in International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2016.

[6] H. Lee, S. H. Jeong and H. K. Kim, "OTIDS: A Novel Intrusion Detection System for Invehicle Network by Using Remote Frame," in Annual Conference on Privacy, Security and Trust (PST), 2017.

[7] U. E. Larson, D. K. Nilsson and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in IEEE Intelligent Vehicles Symposium, 2008.

[8] M. Aldwairi , A. M.Abu-Dalo and M. Jarrah, "Pattern matching of signature-based IDS using Myers algorithm under MapReduce framework," EURASIP Journal on Information Security, 2017.

[9] E. W. Myers, "An O(ND) difference algorithm and its variations," Algorithmica, vol. 1, pp. 251-266, 1986.

[10] T. Hoppe, S. Kiltz, and J. Dittmann, "Applying intrusion detection to automotive IT-early

[11] insights and remaining challenges," Journal of Information Assurance and Security (JIAS), pp. 226-235, 2009.

[12] D. Stabili, M. Marchetti and M. Colajanni, "Detecting attacks to internal vehicle networks through Hamming distance," in AEIT International Annual Conference, 2017.

[13] K. T. Cho and K. G. Shin, "Viden: Attacker identification on in-vehicle networks," in ACM SIGSAC Conference on Computer and Communications Security, 2017.

[14] K. T. Cho and K. G. Shin, "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection," in 25th USENIX Security Symposium, 2016.

[15] X. Ying, S. U. Sagong, A. Clark, L. Bushnell and R. Poovendran, "Shape of the Cloak: Formal Analysis of

Clock Skew-Based Intrusion Detection System in Controller Area Networks," IEEE Transactions on Information Forensics and Security, vol. 14, pp. 2300-2314, 2019.

[16] M. Yoon, S. Mohan, J. Choi and L. Sha, "Memory Heat Map: Anomaly detection in realtime embedded systems using memory behavior," in IEEE Design Automation Conference, (DAC), 2015.

[17] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in IEEE Intelligent Vehicles Symposium (IV), 2011.

[18] W. Wu, Y. Huang, R. Kurachi, G. Zeng, G. Xie, R. Li, and K. Li, "Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks," IEEE Access, vol. 6, pp. 45233-45245, 2018.

[19] M. Müter, A. Groll and F. C. Freiling, "A structured approach to anomaly detection for invehicle networks," in International Conference on Information Assurance and Security, 2010.

[20] A. Taylor, N. Japkowicz and S. Leblanc, "Frequency-based anomaly detection for the automotive CAN bus," in World Congress on Industrial Control Systems Security (WCICSS), 2015.

[21] F. Martinelli, F. Mercaldo, V. Nardone and A. Santone, "Car hacking identification through fuzzy logic algorithms," in IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2017.

[22] T. P. Vuong, G. Loukas and D. Gan, "Performance Evaluation of Cyber-Physical Intrusion Detection on a Robotic Vehicle," in IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015.

[23] M. Levi, Y. Allouche and A. Kontorovich, "Advanced analytics for connected cars cyber security," in IEEE Vehicular Technology Conference (VTC Spring), 2017.

[24] M. Kang and J. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in IEEE 83rd Vehicular Technology Conference (VTC Spring), 2016.

[25] S. F. Lokman, A. T. Othman, S. Musa, and M. H. Abu Bakar, "Deep contractive autoencoder-based anomaly detection for in-vehicle controller area network (CAN)," Progress in Engineering Technology. Advanced Structured Materials, vol. 119, 2019.

[26] M. Hanselmann, T. Strauss, K. Dormann and H. Ulmer, "CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data," IEEE Access, vol. 8, pp. 58194-58205, 2020.

[27] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," IEEE Access, vol. 6, pp. 3491-3508, 2018.

[28] A. Taylor, S. Leblanc and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in IEEE International Conference on Data Science and Advanced Analytics (DSAA), 2016.

[29] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle can bus communications," IEEE Access, vol. 8, pp. 185489-185502, 2020.

[30] V. K. Kukkala, S. V. Thiruloga and S. Pasricha, "INDRA: Intrusion Detection using Recurrent Autoencoders in Automotive Embedded Systems," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), vol. 39, 2020.

[31] M. O. Ezeme, Q. H. Mahmoud and A. Azim, "Hierarchical Attention-Based Anomaly Detection Model for Embedded Operating Systems," in IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), 2018.

[32] M. Weber, G. Wolf, B. Zimmer, and E. Sax., "Online Detection of Anomalies in Vehicle Signals using Replicator Neural Networks," in ESCAR USA, 2018.

[33] M. Weber, S. Klug, B. Zimmer, and E. Sax, "Embedded Hybrid Anomaly Detection for Automotive CAN Communication," in European Congress on Embedded Real Time Software and Systems(ERTS),2018.

[34] Bandi, R., Ananthula, V.R. & Janakiraman, S. Self Adapting Differential Search Strategies Improved Artificial Bee Colony Algorithm-Based Cluster Head Selection Scheme for WSNs. Wireless Pers Commun 121, 2251–2272 (2021). https://doi.org/10.1007/s11277-021-08821-5