Latharani T R[1*], Dr. Mouneshachari S[2]

Leveraging Machine Learning for Behavioral Analysis and Mitigation of APT Attacks in WSNs

JES Journal of Electrical Systems

Abstract
Advanced Persistent Threats (APTs) pose a significant challenge to cybersecurity especially in Wireless Sensor Networks (WSNs) due to their sophisticated, prolonged and targeted nature. Traditional detection methods often struggle to identify and counteract these evasive threats effectively. This paper explores the application of ML (Machine Learning) models for behavioral analysis of APT attacks, aiming to enhance detection and response mechanisms through the enhanced dataset using CGAN (Conditional Generative Adversarial Network) models. It mainly focuses on integration of the dataset generated using CGAN with ML classification techniques. Also on exploration of SCVIC-APT-2021 dataset along with all its features based on CICFlowmeter-V4.0 and applying classification techniques such as SVM (Support Vector Machine), RF(Random Forest) and KNN(K Nearest Neighbor) to label arrived sample from the environment. The proposed model has made a comparative analysis corresponding to performance on precision and f1-scores of the classification models. The paper also evaluates feature selection techniques and data preprocessing methods to improve model accuracy and reduce false positives. Experimental results demonstrate that ML-based approaches can significantly outperform traditional signature-based methods in detecting and mitigating APTs, offering more adaptive and scalable solutions. The findings highlight the importance of continuous learning and model updating to keep pace with evolving APT tactics. This paper contributes to the growing system of knowledge in cybersecurity by providing insights into the practical implementation of machine learning models for Advanced Persistent Threat detection and presenting a framework for integrating these models into existing security infrastructures. The practical results indicate that among SVM, RF and KNN, RF has emerged as the most suitable classifier for derived datasets using CGAN models.

Keywords: cybersecurity, mitigating, CGAN, cybersecurity, exploration

1. INTRODUCTION

Within the realm of cybersecurity, APTs constitute a giant and evolving mission. Unlike conventional cyber threats which are regularly opportunistic or unsophisticated, APTs are characterized with the aid of their stealthy, continual and centered nature [1]. These threats are generally achieved by extraordinarily professional adversaries who coin a number of strategies to infiltrate and preserve manipulation over a network for prolonged intervals, regularly to obtain strategic objectives or get entry into sensitive statistics. Detecting and mitigating APTs requires a deep knowledge of their behavioral patterns and a capacity to become aware of anomalies that deviate from everyday network activities. Traditional security features, including signature based detection and rule-based systems often fall behind in addressing the complicated and adaptive nature of APTs[2]. This has spurred interest in leveraging superior technology, mainly Deep Learning (DL) and ML to decorate the detection and analysis of these state-of-the-art threats.

WSNs consist of numerous small, low-power devices or sensor nodes that communicate wirelessly to collect and transmit data about their environment. These networks are widely used in various applications, including environmental monitoring, military surveillance, healthcare and smart cities. Qualities of WSNs namely resource constraints, open nature, dynamic, ad-hoc and remote deployments make them more susceptible to APT attacks [3][4]. By studying network site visitors, user behavior and other relevant information, ML models can discover hidden anomalies and analyze potential threats in APTs with greater accuracy and speed. This paper explores the behavioral analysis of APT attacks using Machine Learning models by involving Datasets enhanced by Conditional Generative Adversarial Network (CGAN) models. It starts with a top level view of APT characteristics in the form of dataset enhancement which is previously constructed by involving SCVIC-APT-2021 [5]. The discussion then shifts to the classification of samples on various clusters based on the process of APT attacks later to behavioral analysis of APT attacks using these labels based on duration in days.

2. REVIEW OF LITERATURE

The review of literature of this paper mainly focuses on exploring APT attacks with its various phases, dataset SCVIC-APT-2021 and its enhancement using CGAN models and ML models for classification of APT attacks at various stages. Advanced Persistent Threats (APTs) pose serious cybersecurity issues, specifically in industrial and critical infrastructure systems. Numerous researches have looked into different methods for identifying and reducing these

[1*]Ph.D. Scholar, Department of Computer Science and Engineering, Jain Institute of Technology, Davangere, Affiliated to Visvesvaraya Technological University, Belagavi, India, lathaquick@gmail.com
[2]Professor and Head, Department of Computer Science and Engineering, Jain Institute of Technology, Davangere, Affiliated to Visvesvaraya Technological University, Belagavi, India, drmounesh.cs@gmail.com

risks. By examining behavioral patterns, Authors [6] proposed a novel method for connecting APT attack groups. Their methodology achieves a 90.9% correlation accuracy rate by comparing attack methods and malware features using rough set theory to identify latent links among APT groups. By exposing relationships between APT groups, this method provides insightful information for proactive threat defense and threat attribution. Authors [7] have expanded on this by using hypergame theory to APT security. Their concept reduces detection system false positives and extends system security life by utilizing defensive deception, which takes use of the attacker's subjective perception to deceive them. By providing a proactive protection, this technique makes it harder and demands more resources for attackers to carry out APTs. Authors[8] conducted a comprehensive examination of APT detection methods, looking at important APT phases such as Reconnaissance, Initial Compromise, Pivoting, Lateral movement, Data exfiltration and Normal Traffic. They stressed the need for better early-stage detection methods because current approaches frequently fail to detect advanced multi-staged attacks.

To further improve APT defenses in industrial settings, authors [9] have proposed an adversarial defense mechanism tailored to Industrial IoT (IIoT) environments. Their framework uses a GAN model to capture complex attack behaviors, achieving detection accuracies of 96.97% and 95.97% on the DAPT2020 and Edge I-IoT datasets, respectively. Their approach outperformed conventional ML approaches, proving effective in safeguarding IIoT systems from sophisticated APTs. Authors [10] introduced another novel strategy that emphasizes attack intent-driven and sequence-based learning. Their dual approach boosts cybersecurity defences by precisely anticipating and thwarting multi-step, covert attacks by examining malicious behavior sequences and attacker intent. Authors [11] looked into how machine learning might be used to identify APTs through network traffic analysis. Also their work illustrates the potential of ML in detecting unusual behaviors connected to APTs by using decision trees, Support Vector Machines and Neural Networks to examine network traffic patterns. The study highlights the difficulty of striking a balance between low false positives and detection accuracy, a recurring trade-off in APT detection, not withstanding progress. Authors [12] proposed a model which offers a perceptive examination of threat modeling strategies designed especially for Advanced Persistent Threats (APTs). Given the particular difficulties presented by APTs long duration, covert attacks targeted at vital assets the authors assess a number of threat modeling frameworks and techniques. They draw attention to the shortcomings of conventional methods, which frequently overlook the intricate, multi-phase structure of APTs. The article provides suggestions for creating more potent threat modeling techniques that improve early detection, response and resilience against APTs by contrasting different models.

The necessity of sophisticated, multi-layered defenses against APTs is highlighted by this research taken together. Each strategy has its own advantages for strengthening cyber defenses against more sophisticated APT attacks, ranging from intent-driven analysis and machine learning to defensive deception and behavior correlation.

3. METHOD

Figure 1 shows the proposed methodology for behavioral analysis of APT attacks using machine learning models. The initial process of the methodology is to access, study and analyze the dataset SCVIC-APT-2021. The detailed description about the mentioned dataset is provided in the literature section of this paper

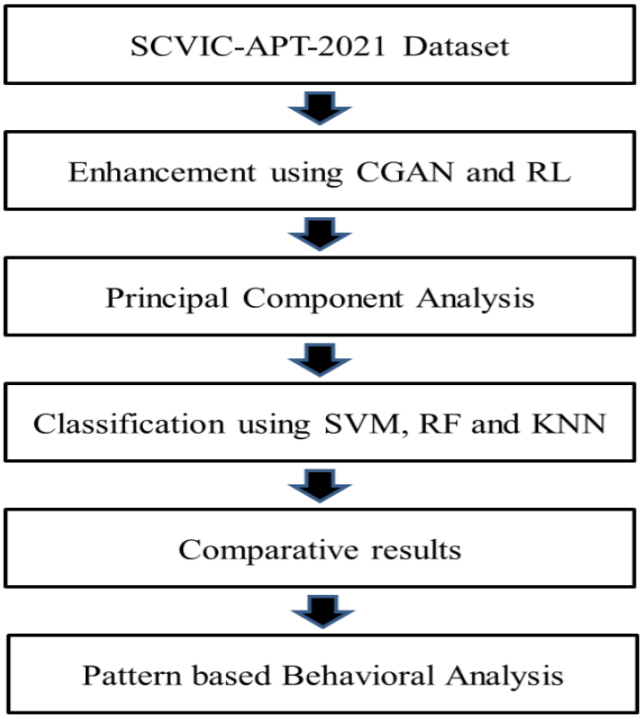

Figure 1. Proposed methodology for behavioral analysis of APT attacks

3.1 Enhancement of SCVIC-APT-2021 Dataset using CGAN and RL (Reinforcement Learning)

Behavioral analysis of the APT attacks essentially needs the data samples of the attacker at all the dimensions. More the number of data samples more will be the accuracy of the model. In this connection, the description related to the enhancement of the dataset is proposed in the previous research work [13].

3.2 Dimensionality reduction process using Principal Component Analysis

Enhanced dataset from SCVIC-APT-2021 includes 84 attributes as per CICFlowmeter-V4.0 [14] format. Processing of these 84 attributes for machine learning algorithms implementation lead to unsolvable complications. Hence, Principal Component Analysis is applicable for dimensionality reduction to lesser number. The proposed methodology aims to reduce them upto two, three or four dimensions or features.

3.3 Classification using SVM, RF and KNN

The proposed methodology explores the classification of APT attack behaviors at six phases as classes using Support Vector Machine, Random Forest and K Nearest Neighbor algorithms. PCA converts eighty four into two, three and four dimension dataset, the complexity of the computation may reduce but at the same time efficiency of the model corresponding to classification plays a major role. Hence, three classifiers are experimented to verify the performance of the labeling. Since dataset includes labeled samples, supervised algorithms are involved in this paper for the classification process. Around 56,487 samples are provided in the available dataset. These samples are divided in the ratio of 60:40 as training and testing samples during classification process.

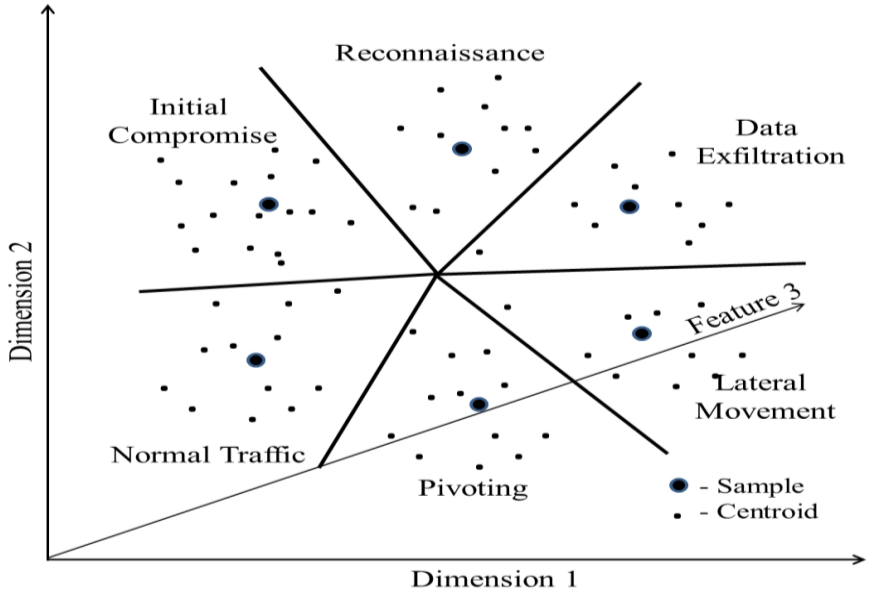

Figure 2a. Division of clusters based on planes in SVM classification model

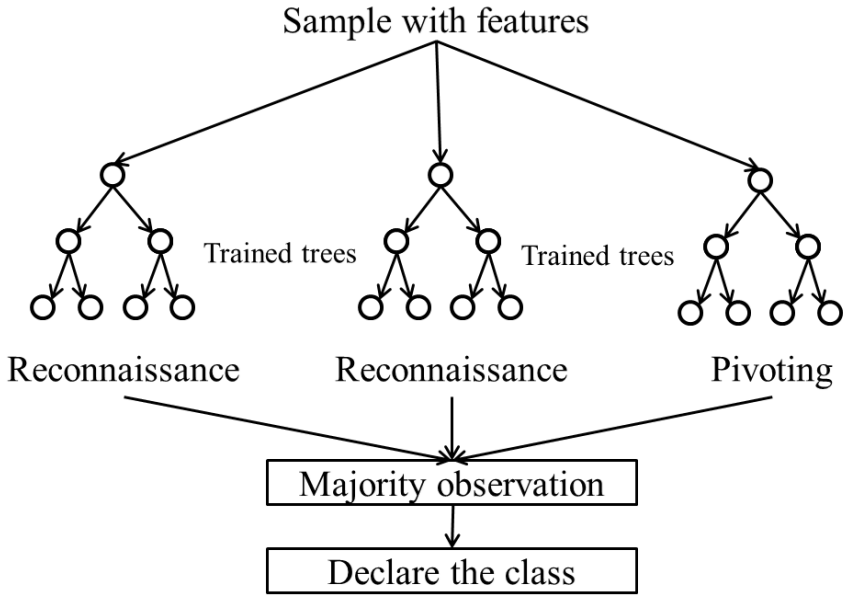

Figure 2b. Decision trees in Random Forest Classification model

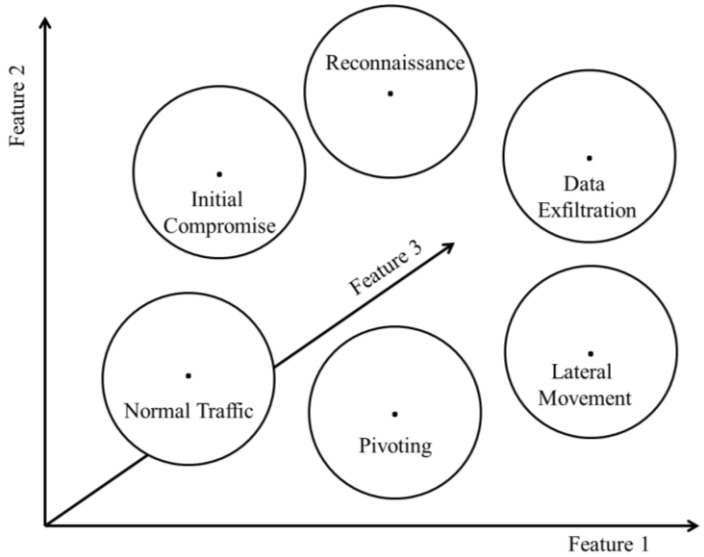

Figure 2c. Clusters in KNN classification model

Figure 2a, Figure 2b and Figure 2c shows the clusters model among the classifiers SVM, RF and KNN respectively. As per the derived dataset and APT attacker behaviors, six predefined clusters are identified namely Reconnaissance, Initial Access, Lateral Movement, Pivoting, Data Exfiltration and Normal Traffic. Classification figures are clearly depicting these six clusters. These clusters are the progressive behaviors of APT attacks. Classification of the test sample is conducted based on knowledge base. Testing phase is processed for all the test samples and examined confusion matrix to record the performance of the classification model on precision, accuracy and f1-score (harmonic mean).

3.4 Comparative analysis

The performance analysis of all the mentioned machine learning techniques corresponding to accuracy, precision and f1-score are plotted on graph. Conclusions are drawn based on the performances.

3.5 Pattern based behavioral analysis

Newly arrived transaction from the network is classified to assign its label. The labels remain unchanged for subsequent transactions for a set period of days. Durations between previous labels to the subsequent labels are recorded. This recorded duration is plotted on the graph as shown in Figure 3, indicating behavioral patterns of the APT attacker's and environment. Cyber security Investigation reports [16] approximated the total duration of the APT attacks till data exfiltration is from 100 to 200 days. According to these documents the average durations in days are estimated as avg_dur among all the phases of APT attacks. If the avg_dur fall less than 40 days then it suggests that environment is highly vulnerable or APT attackers are rapidly trying to exploit environment for valuable data. Certain measures can be applied immediately to mitigate vulnerability in the environment. Table 1 show certain behavior pattern of APT attackers based on duration between labels. The proposed research has tried to identify five behavior patterns of the attacker or environment.

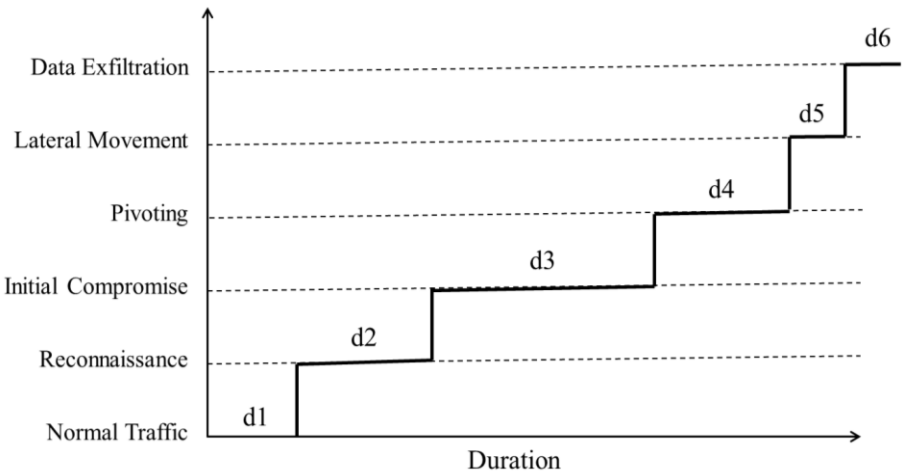

Figure 3. Duration pattern based behavioral model of APT attackers

Table 1. Approximated behaviors of APT attackers and environment based on durations

SN	Duration pattern	Expected Behavior
1	d1 ≈ d2 ≈ d3 ≈ d4 ≈ d5	Attackers are beginners and planned execution
2	d1 is larger than all	Environment is highly protective or attacker may be beginner
3	d6 is larger than all	Attackers are expecting higher returns or results. Other words highly valuable environment
4	Durations are unequal or random	Attacker is highly intelligent and carefully handling the environment
5	Any duration is longer	Environment is highly protective at that point

4. RESULTS AND DISCUSSION

Result section is organized according to the proposed methodology as shown in Figure 1. And it is implemented in python programming language under Anaconda environment.

4.1 Results of Principal Component Analysis

PCA applied on the enhanced dataset containing eighty four dimensions to convert it into two, three or four dimension dataset as shown in Figure 4a, 4b and 4c respectively. Observation indicate that the four dimensional dataset is providing a proper divergence between the samples for assigned labels. Hence, the same is used during the further classification process.

The above dimensionality reduction process using PCA may reduce the dimensions to two, three and four dimensions but the efficiency of the classification also matter corresponding to accuracy and precision of the classification.

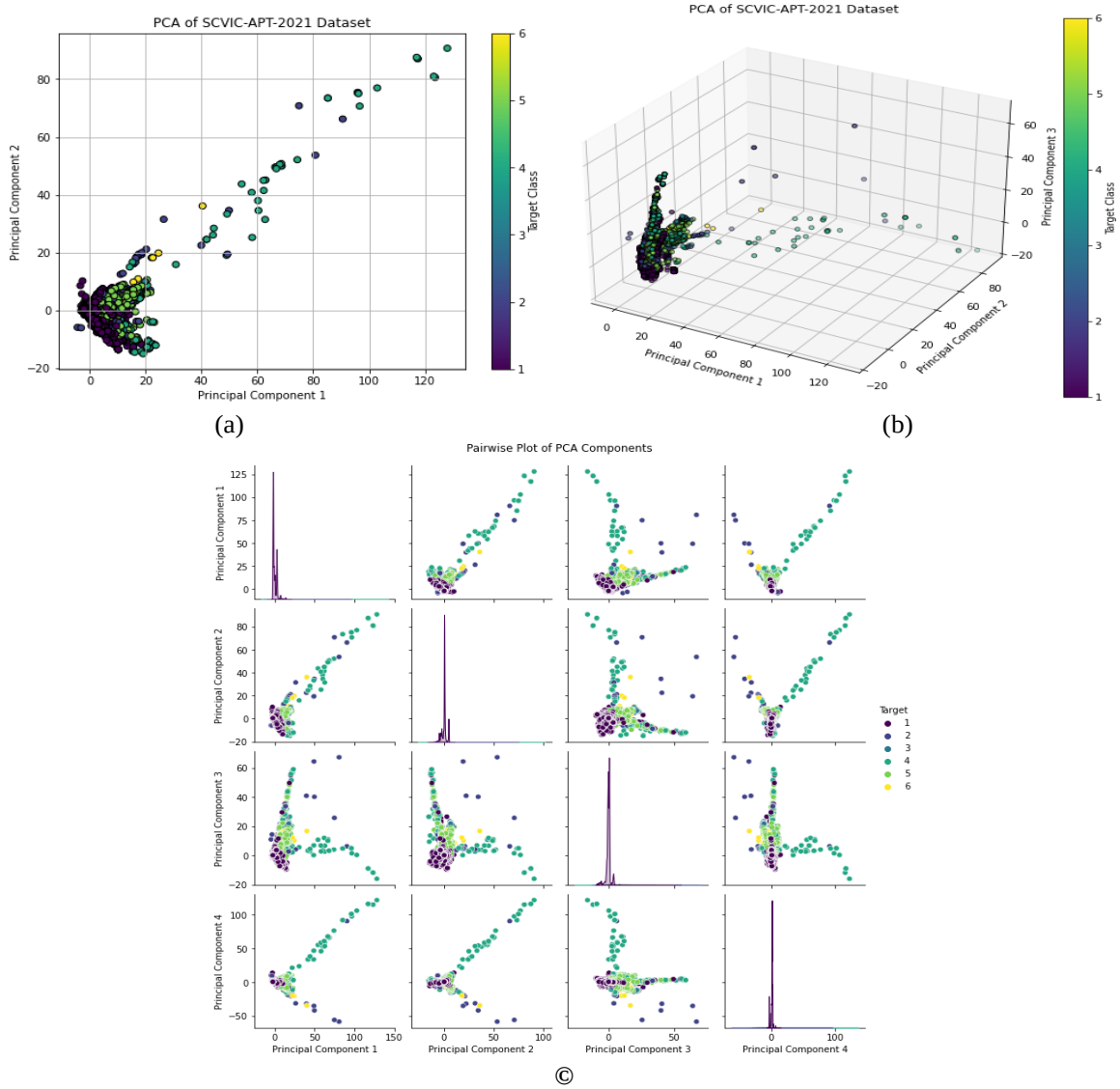

Figure 4. (a) PCA with two components (b) PCA with three components (c) PCA with four components

6.3 Comparative analysis of classification

Figure 5 depict the comparative analysis of various classifiers involved in classification process of the derived dataset. All the classifiers performing almost similar corresponding to accuracy parameter, but there is versatile behavior on average precision and f1-score parameters. The performance of the classifiers on four dimensions space shows gradual improvement compared to three dimensions. But, Random Forest is performing better on precision and f1-score parameters compared to other two classifiers. SVM showed lower performance compared to other classifier on the derived SCVIC-APT-2021 dataset.

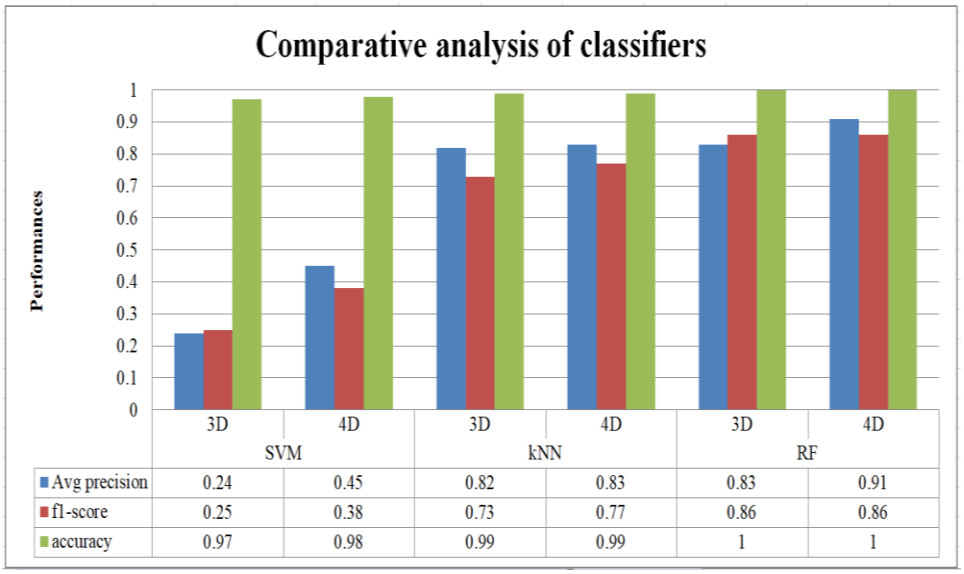

Figure 5. Comparative analysis of classifiers

6.3 Behavioral analysis

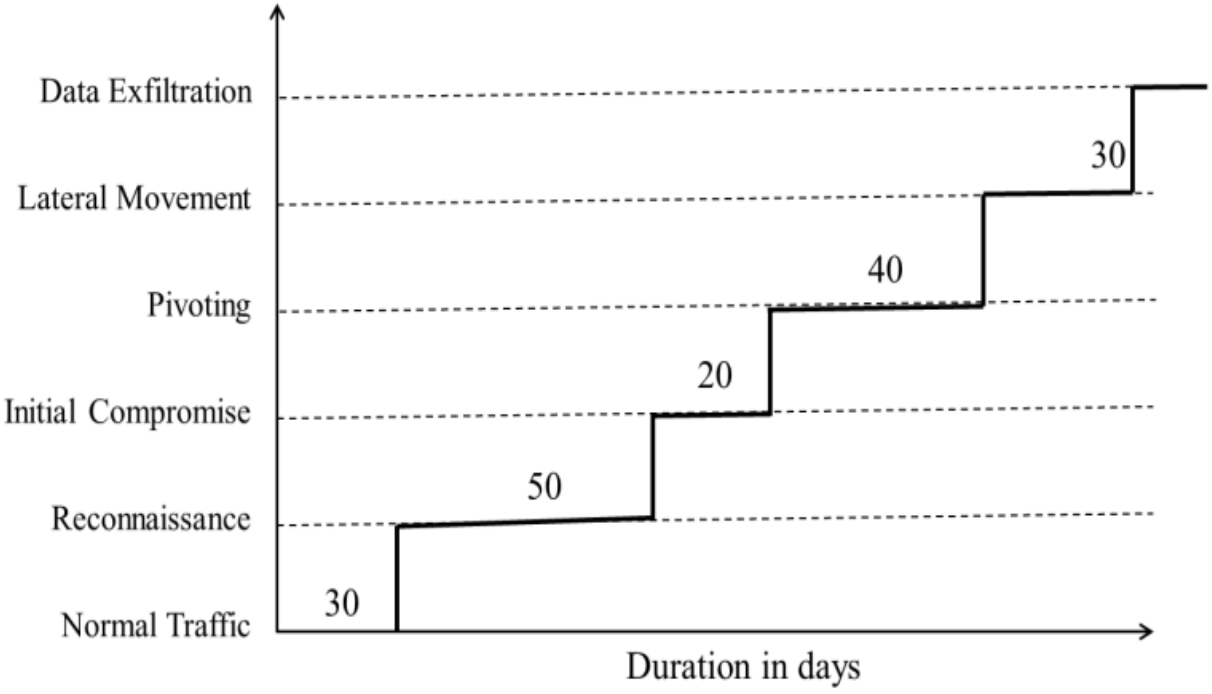

Figure 6. Sample behavioral pattern of APT attack

As per study there are six behaviors of APT attackers namely Reconnaissance, Initial Access, Lateral Movement, Pivoting, Data Exfiltration and Normal Traffic. Each transaction in the network traffic should belong to one among these behaviors. The newly received transaction is labeled and verified along with its duration; if the label changes, the new duration is recorded. Figure 6 shows a sample behavioral pattern of APT attack based on test sample classification using the proposed model. The pattern indicates the attacking speed with respect to duration and the security measures of the system. Here the avg_dur is estimated approximately to thirty five days. As per the proposed model, the estimated avg_dur is within forty days. Hence, It indicates that the environment is highly vulnerable and need some

measures for protection. These behavioral analyses enable the environment to implement precautionary measures for safeguarding the system.

5. CONCLUSION

APT attacks in WSNs represent a significant threat to cybersecurity. These attacks sustain longer duration and target the system to achieve their goals. These attacks can be tackled only through their behavioral analysis. Due to insufficient or limited amount of samples in dataset sometimes model fails to provide accurate results. Hence, sample generation to improve the existing dataset has been borrowed from the previous experiments. The derived dataset is involved for the classification process in the proposed research work. Labeling of newly arrived transaction from the network is one of the needy tasks in the proposed research. Also, the performance corresponding to accuracy, precision and f1-score of classification models plays a major role. Three classification models were undertaken for labeling the transaction, also their performances were recorded. RF classifier outperformed compared to other two classifications namely SVM and KNN. Labeling process leads to draw a behavioral pattern of the attacker. These patterns clarify about the attack necessity, vulnerability rate and attacking skills. The proposed research can be extended to quantify vulnerability rate and analyze attacking skills.

REFERENCES

[1] Yue, Hao, et al. "Detecting APT attacks using an attack intent-driven and sequence-based learning approach." Computers & Security 140 (2024): 103748.
[2] Mutalib, Noor Hazlina Abdul, et al. "Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review." Artificial Intelligence Review 57.11 (2024): 1-47.
[3] Singh, S.; Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. A Comprehensive Study on APT Attack and Counterasures for Future Network and Communications: Challenges and Solutions. J. Supercomput. 2019, 75, 4543–4574.
[4] Li, M.; Huang, W.; Wang, Y.; Fan, W.; Li, J. The study of APT attack stage model. In Proceedings of the 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, Japan, 26–29 June 2016; pp. 1–5.
[5] Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein Mouftah, Mehran Bagheri, Petar Djukic, “A New Realistic Benchmark for Advanced Persistent Threats in Network Traffic”, IEEE Networking Letters, 2022.
[6] Li, Jingwen, Jianyi Liu, and Ru Zhang. "Advanced Persistent Threat Group Correlation Analysis via Attack Behavior Patterns and Rough Sets." Electronics 13.6 (2024): 1106.
[7] Wan, Zelin, et al. "Resisting multiple advanced persistent threats via hypergame-theoretic defensive deception." IEEE Transactions on Network and Service Management 20.3 (2023): 3816-3830.
[8] Krishnapriya, Singamaneni, and Sukhvinder Singh. "A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques." Computers, Materials & Continua 80.2 (2024).
[9] Javed, Safdar Hussain, Maaz Bin Ahmad, Muhammad Asif, Waseem Akram, Khalid Mahmood, Ashok Kumar Das, and Sachin Shetty. "APT adversarial defence mechanism for industrial IoT enabled cyber-physical system." IEEE Access 11 (2023): 74000-74020.
[10] Yue, Hao, et al. "Detecting APT attacks using an attack intent-driven and sequence-based learning approach." Computers & Security 140 (2024): 103748.
[11] Do Xuan, Cho. "Detecting APT attacks based on network traffic using machine learning." Journal of Web Engineering 20.1 (2021): 171-190.
[12] Tatam, Matt, Bharanidharan Shanmugam, Sami Azam, and Krishnan Kannoorpatti. "A review of threat modelling approaches for APT-style attacks." Heliyon 7, no. 1 (2021).
[13] Mouneshachari S., “Intelligent Model Using CGAN and RL for Efficient Contextual Dataset Generation”, Int J Intell Syst Appl Eng, vol. 12, no. 23s, pp. 1051 –1056, Aug. 2024.
[14] Habibi Lashkari, Arash. (2018). CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyser for anomaly detection. https://github.com/ISCX/CICFlowMeter. 10.13140/RG.2.2.13827.20003
[15] Mohibullah, Md, Md Zakir Hossain, and Mahmudul Hasan. "Comparison of euclidean distance function and manhattan distance function using k-mediods." International Journal of Computer Science and Information Security (IJCSIS) 13.10 (2015): 61-71.
[16] Langlois, Philippe. "2020 data breach investigations report." (2020).

BIOGRAPHIES OF AUTHORS

	**Dr. Mouneshachari S** received the B.Eng. degree in Computer Science and Engineering from Kuvempu University, India, in 2000 and the M.Tech in Computer Science and Engineering from VTU, Belagavi, India and Ph.D. degree in Computer Science and Engineering from Jain University, Bengaluru, India in 2017. Currently, he is working as Professor at the Department of Computer Science and Engineering under VTU, Belagavi, India. His research interests include Cybersecurity, Internet of Things, EEG Analysis and Cloud computing. Also he has developed software solutions to societal and organization challenges. He is a reviewer for many reputed national and international journals and conferences. He can be contacted at email: drmounesh.cs@gmail.com.
	**Latharani T R** is a Ph.D. scholar from Department of Computer Science and Engineering, Jain Institute of Technology, Davangere. Received B.E. degree in Computer Science and Engineering from Visveswaraya Technological University, Belagavi, in 2007 and M.Tech. from Visveswaraya Technological University, Belagavi, in 2011. Currently she is working as Assistant Professor, in the department of Computer Science and Engineering under VTU, Belagavi, India. Her research interests include Cybersecurity and Internet of Things. email: lathaquick@gmail.com