# Protecting Smart Homes: Cyber Attack Detection in IoT

Sure Mamatha[1]
Assistant Professor
VNR VJIET

M Radha[2]
Assistant Professor
VNR VJIET

***ABSTRACT - Cybersecurity remains a significant worry for all sectors involved in digital operations, particularly with the occasional surge in security breaches. With the increasing utilization of Internet of Things (IoT) devices in various environments such as homes, offices, transportation, and healthcare, the frequency of malicious attacks is also on the rise. Fog computing can easily be incorporated into IoT for detecting attacks due to IoT and fog devices being closer together than IoT devices and the cloud. ML is commonly utilized for detecting attacks because IoT devices generate large amounts of data. This research proposes a new approach for analyzing network traffic to detect malicious attacks using IoT artificial intelligence techniques, with the goal of developing a sustainable smart home. A kernel quadratic vector discriminant machine was utilized for traffic analysis to enhance data transmission efficiency by reducing network traffic. Improved energy efficiency is a result of decreased traffic. Adversarial Bayesian belief networks are next applied to identifying malicious attacks. An experimental analysis has investigated throughput, data traffic analysis, packet delivery ratio, energy efficiency, end-to-end delay, and quality of service. The proposed approach obtained an 80% quality of service, a 98% data transfer rate, a 75% assessment of data traffic, a 44% total delay, a 93% rate of successful packet delivery, and a 94% utilization of energy.***

***Keywords – Internet of Things, Machine Learning, kernel quadratic vector discriminant machine***

## I. INTRODUCTION

Physical systems are more susceptible to cyberattacks due to increased internet connectivity. Due to the development of automated attack tools and the complexity of cyberattacks, organized hacking clusters have started to take part. Effective cyberattacks could have fatal, catastrophic, or even disastrous effects on a CPS. It is challenging to defend CPSs against cyberattacks, though. Determining fraudulent data injection attacks is challenging because many CPS systems lack cybersecurity features like message authentication. The lack of universal encryption makes it challenging to defend against eavesdropping attacks, particularly on systems running outdated technologies. Referring to system states is required to prevent replay attacks[1].

The Internet of Things (IoT) has had a significant impact on our lives, and deep learning (DL) techniques have proven to be more effective than traditional machine learning (ML) approaches. DL models are being used to detect cyberattacks against CPS, which is difficult due to the complexity of implementing cybersecurity measures. ML methods are used in regression and classification to extract useful insights from data generated by machines and humans, whereas DL methods address cybersecurity issues in CPSs. The Internet of Things is a significant technological advancement with numerous applications and implications for our daily lives[2].

In an IoT network, machine learning (ML) can be used to provide security services. The cybersecurity industry is using machine learning (ML) in more and more applications, and the use of ML to detect attacks is becoming a hotly contested topic. The following is the research's contribution, To put forth a novel approach for a sustainable smart home that uses IoT artificial intelligence techniques for network traffic analysis based on cybersecurity and malicious attack detection, Adversarial Bayesian belief networks are used to detect malicious attacks, while a kernel quadratic vector discriminant machine has been used for traffic analysis. This machine improves data transmission by minimizing network traffic.

This article is structured as follows: The current method for detecting network traffic and attacks is provided in Section II, the suggested research is presented in Section III, and an experimental analysis of the results is completed in Section IV. Section V wraps up research by implications for the future.

## II. RELATED WORK

Deep learning research has thrived in areas involving image processing, pattern recognition, and text processing, but there are a few interesting projects in cybersecurity. Earlier research [3, 4] shows that DLNN, alone or in fusion with optimization or ML methods, can accurately forecast assaults. [5] combining SVMs with ANNs significantly improves detection rates compared to DL or ML alone. In particular, [6] generates hybridization by incorporating SVM and ANN and integrating a genetic algorithm (GA) and PSO. This hybridization achieves an impressive 99.3% accuracy. [7] tested the man shift technique on the KDD99 network traffic dataset to identify network invasion. The authors believe a mean shift in the network dataset may indicate an assault. The algorithm did not detect user to root (U2R) or remote-to-local (R2L) assaults. Serra et al. [8] developed ClusterGAN, a new method for adaptive clustering based on GANS. Choi et al. developed a network intrusion detection system (NIDS) that utilized

unsupervised learning and unlabeled data. Work [9] evaluated SVM, KNN, and ANN to detect FDI (False Data Injection) assaults. The trial proved that KNN and SVM outperformed ANN in terms of accuracy. Supervised learning uses labeled data to learn a function that maps an input to an output. In a study [10], two open-source NIDS and two supervised ML approaches were used to analyze backscatter darknet traffic and identify cyber-attacks, precisely SYN-DOS attacks on IoT. The authors of [11] documented the development of wireless sensor networks (WSN), correspondence innovation, and Internet of Things innovation. The authors of [12] used IDS-applicable ML methods, including KNN, SVM, DT, NB, NN, and RF. The authors compared ML methods for collecting Bot-IoT data using multi- and binary-class combinations. These models were used to calculate F1 scores, recall, precision, and accuracy. In [2], an online dataset was used to compare ML and deep-learning neural networks for identifying assaults in FOG designs. Grunt [13], a popular location framework, is also a mark-based framework that uses attack signature rules to identify digital attacks. The authors utilize AhoCorasick [14], a search calculation, to determine whether approaching traffic patterns are assaults or not. Suricata [15] is a popular public IDS that supports multithreading and is suitable for large-scale network frameworks. The review used Suricata to run the discovery framework on the asset limitation device, Raspberry Pi. They anticipate recognizing the port-checking assault on the IoT environment. Several studies [16] proposed an attack detection framework for the IoT environment, focusing on port scanning, MITM, DNS store harming, and flood attacks. According to the review [17], Grunt weighs less than Suricata. They proposed an AI-based discovery structure to enhance the Grunt framework. The expansion resulted in better recognition outcomes than the initial Grunt. Table 1 shows a comparison between energy analysis and cyber-attack detection.

## III. SYSTEM MODEL

This section introduces an advanced approach for analyzing network traffic that relies on cybersecurity and IoT artificial intelligence methods to detect malicious attacks in order to create a sustainable smart home. A kernel quadratic vector discriminant machine has been utilized for traffic analysis to enhance data transmission through minimizing network traffic. With reduced traffic, there is an enhancement of energy efficiency. The following stage includes utilizing adversarial Bayesian belief networks for identifying malicious attacks. Figure 1 shows the proposed design.

A Core E7400 processor, 3.00 GB of RAM, a 32-bit operating system, and the proposed design with fog and cloud nodes are tested on a server.

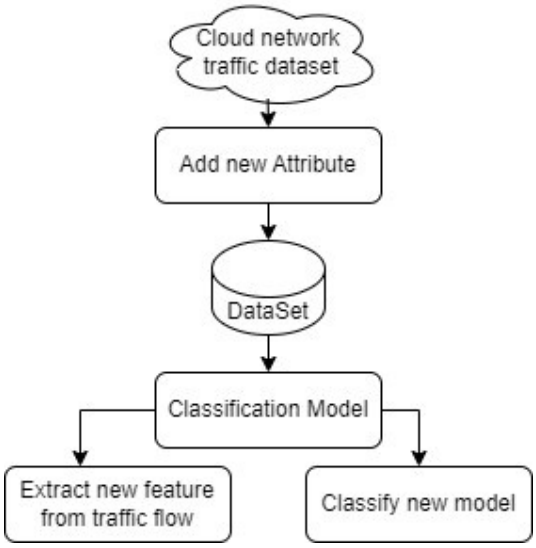



Fig 1: System design for analysis of network traffic and identification of malicious attacks

Pre-processing processing methods are applied to convert a dataset into a structure suitable for machine learning. Eliminating inaccurate or superfluous data that could compromise the dataset's accuracy is another way that this cleaning process increases the dataset's efficacy.

UKSVM computes the similarity between uncertain samples using a kernel function. The decision function and classification models can be derived after the kernels have been computed. Fortunately, there exist kernel functions like Hellinger's kernel [r1], HIK, and $\chi 2$ kernel [r2] that can be used to determine the degree of similarity between probability distributions. These additive kernels are added to SVMs by us.

A subfamily of additive positive definite kernels includes additive kernels HIK, $\chi 2$ kernel [r2], and Hellinger's kernel. These kernels have demonstrated strong performance in the area of image classification [r2]. The first use of histogram intersection for color indexing in object recognition was in 1991. It calculates how similar two histograms are to one another. It is resilient to changes in scale. Let the histograms of the two images be $x_1$ and $x_2$. Both histograms have m bins; $x_{1jb}$ and $x_{2jb}$ represent the $j_b$ $^{th}$ b in for $j_b$=1,…m.$\sum_{jb=1}^{m} x1jb = N$ and $\sum_{jb=}^{m} x2jb = N$. the histogram intersection is derived with the following equation:$= K_{HIK}(X_1, X_2) = \sum_{j_b=1}^{m}\{x_1 x_2 jb\}$

## IV. EXPERIMENTAL ANALYSIS

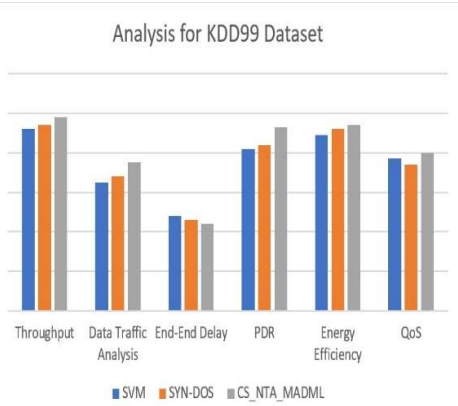
A Core E7400 processor, 3.00 GB of RAM, a 32-bit operating system, and the proposed design with fog and cloud nodes are tested on a server.

Description of the dataset: A number of those datasets remain private, primarily due to security concerns, but some are now accessible to the public, including KDD99. There are a lot of datasets available, but few of them are realistic datasets of IoT and network traffic that include new instances of botnets. Furthermore, IoT-generated traffic is absent from some databases, and new features are absent from others. A validation dataset is a collection of instances that are used to modify the hyperparameters, or architecture, of a classifier. It is also known as a "dev set" or development set. One example of a hyperparameter for artificial neural networks is the number of hidden units in each layer. The validation set is used in the hyperparameter tuning procedure. In the end, the test set is used to evaluate the best model. If hyperparameter tuning is not implemented, the validation set becomes unnecessary and redundant. The analysis in Table is predicated on multiple malicious attack datasets. The datasets analyzed in this case are KDD99. Throughput, data traffic analysis, packet delivery ratio, energy efficiency, end-end delay, and quality of service are all considered in the parametric analysis.

| Techniques | Throughput | Data Traffic | End-End Delay | PDR | Energy Efficiency | QoS |
|---|---|---|---|---|---|---|
| SVM | 92 | 65 | 48 | 82 | 89 | 77 |
| SYN-DOS | 94 | 68 | 46 | 84 | 92 | 74 |
| CS_NTA_MADML | 98 | 75 | 44 | 93 | 94 | 80 |

**Table 1 :** Analyses based on the KDD99 dataset of malicious attacks.

The proposed and present methods are compared using a KDD99 dataset, as seen in the figure. The existing SVM achieved throughput of 92%, data traffic analysis of 65%, end-end delay of 48%, packet delivery ratio of 82%, energy efficiency of 89%, QoS of 77%; and SYN-DOS achieved throughput of 94%, data traffic analysis of 68%, end-end delay of 46%, packet delivery ratio of 84%, energy efficiency of 92%, and QoS of 74%. The proposed technique achieved these results.




## V. DISCUSSION

Utilizing neural networks and network traffic features, various feature combinations are obtained for the detection of cyber virus attacks. This research uses a 442,240 data point dataset that integrates information from previous datasets and results from laboratory experiments to facilitate learning. Currently, available neural network models are recommended for use in the detection of malware in Internet of Things devices. The system can detect anomalous network activity and trigger alarms in response with a reduced false alarm rate. Using the KDD 99 datasets, we evaluated the binary classification of network traffic. The results exhibited that using filtering based on association rules could greatly improve the system's detection accuracy. Furthermore, our detection technique fared well in a multi-class experimental setup. This two-level detection system, which first classifies and then filters network traffic, provides better detection results with fewer false positives.

## VI. CONCLUSION

This research proposes an innovative IoT artificial intelligence-based cybersecurity plan for a sustainable smart home. Malicious attacks are identified using adversarial Bayesian belief networks, and traffic analysis is done using a kernel quadratic vector discriminant machine. This device reduces network traffic, which enhances data transmission. 98% throughput, 75% data traffic analysis, 44% end-end delay, 93% packet delivery ratio, 94% energy efficiency, and 80% quality of service were all attained by the recommended approach. The architecture of a deep neural network can still be greatly enhanced, and future studies can tackle the problem of raising precision without lowering recall. To strengthen its decision-making ability and resistance to further attempts, the suggested method will be extended in the future to include data from various attack types and sources. It is believed that further research on enhancing the suggested method should focus on studying a network evolutionary algorithm, such as the imperialist competitive algorithm.

## REFERENCES


[1] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: a survey," IEEE/CAA J. Autom. Sinica, vol. 9, no. 3, pp. 377–391, Mar. 2022. doi: 10.1109/JAS.2021.1004261

[2] Prabakar, D., M. Sundarrajan, R. Manikandan, N. Z. Jhanjhi, Mehedi Masud, and Abdulmajeed Alqhatani. 2023. "Energy Analysis-Based Cyber Attack Detection by IoT with Artificial Intelligence in a Sustainable Smart City" Sustainability 15, no. 7: 6031. https://doi.org/10.3390/su15076031

[3] Zagrouba, Rachid & Alhajri, Reem. (2021). Machine Learning based Attacks Detection and Countermeasures in IoT. International Journal of Communication Networks and Information Security. 13. 158-167. 10.17762/ijcnis.v13i2.4943.

[4] Salam, Abdu & Ullah, Faizan & Amin, Farhan & Abrar, Muhammad. (2023). Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. Technologies. 11. 107. 10.3390/technologies11040107.

[5] Do Xuan, Cho. 2021. "Detecting APT Attacks Based on Network Traffic Using Machine Learning". Journal of Web Engineering 20 (1):171-90. https://doi.org/10.13052/jwe1540-9589.2019.

[6] Do, Cho & Tran Duc, Duong & Hoang, Dau. (2021). A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic. Journal of Intelligent and Fuzzy Systems. 40. https://content.iospress.com/articles/journal-of. 10.3233/JIFS-20246.

[7] Anusha, M. & Karthika, M.. (2022). Investigation on Malware Detection Using Deep Learning Methods for Sustainable Development. 10.1007/978-981-16-8721-1_57.

[8] Matheus P. Novaes, Luiz F. Carvalho, Jaime Lloret, Mario Lemes Proença,Adversarial Deep Learning approach detection and defense against DDoS attacks in SDN environments,Future Generation Computer Systems,Volume 125,2021,Pages 156-167,ISSN 0167-739X, https://doi.org/10.1016/j.future.2021.06.047.

[9] Shahid, Waleed & Aslam, Baber & Abbas, Haider & Khalid, Saad & Afzal, Hammad. (2021). An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling. Journal of Network and Computer Applications. 198. 103270. 10.1016/j.jnca.2021.103270.

[10] Ahmad Ali AlZubi, Mohammed Al-Maitah, and Abdulaziz Alarifi. 2021. Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Comput. 25, 18 (Sep 2021), 12319–12332. https://doi.org/10.1007/s00500-021-05926-8

[11] Waqas, Muhammad & Kumar, Kamlesh & Laghari, Asif & Saeed, Umair & Rind, Muhammad & Shaikh, Aftab & Hussain, Fahad & Rai, Athaul & Qazi, Abdul. (2021). Botnet attack detection in Internet of Things devices over cloud environment via machine learning. Concurrency and Computation Practice and Experience. 34. 1-23. 10.1002/cpe.6662.

[12] Khan, Muhammad Ashfaq. 2021. "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System" Processes 9, no. 5: 834. https://doi.org/10.3390/pr9050834

[13] Amiya Kumar Sahu, Suraj Sharma, M. Tanveer, and Rohit Raja. 2021. Internet of Things attack detection using hybrid Deep Learning Model. Comput. Commun. 176, C (Aug 2021), 146–154. https://doi.org/10.1016/j.comcom.2021.05.024

[14] Ullah, Safi, Muazzam A. Khan, Jawad Ahmad, Sajjad Shaukat Jamal, Zil e Huma, Muhammad Tahir Hassan, Nikolaos Pitropakis, Arshad, and William J. Buchanan. 2022. "HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles" Sensors 22, no. 4: 1340. https://doi.org/10.3390/s22041340

[15] Ravi, V., Pham, T. D., & Alazab, M. (2023). Attention-Based Multidimensional Deep Learning Approach for Cross-Architecture IoMT Malware Detection and Classification in Healthcare Cyber-Physical Systems. IEEE Transactions on Computational Social Systems, 10(4), 1597 - 1606. https://doi.org/10.1109/TCSS.2022.3198123

[16] Abu Al-Haija Q. Top-Down Machine Learning-Based Architecture for Cyberattacks Identification and Classification in IoT Communication Networks. Front Big Data. 2022 Jan 13;4:782902. doi: 10.3389/fdata.2021.782902. PMID: 35098112; PMCID: PMC8792902.

[17] Mihoub, Alaeddine & Fredj, Ouissem & Cheikhrouhou, Omar & Derhab, Abdelouahid & Krichen, Moez. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering. 98. 107716. 10.1016/j.compeleceng.2022.107716.

[18] Miragaia, Rolando, Francisco Chávez, Josefa Díaz, Antonio Vivas, Maria Henar Prieto, and Maria José Moñino. 2021. "Plum Ripeness Analysis in Real Environments Using Deep Learning with Convolutional Neural Networks" Agronomy 11, no. 11: 2353. https://doi.org/10.3390/agronomy11112353

[19] Sarker, I. H.; Furhad, M. H.; Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2021, 2. https://doi.org/10.1007/s42979-021-00557-0.

[20] Sun, Cong, Jianfeng Ma and Qingsong Yao. "On the architecture and development life cycle of secure cyber-physical systems." Journal of Communications and Information Networks 1 (2016): 1-21.