

# Implementation of a multi-stage intrusion detection systems framework for strengthening security on the internet of things

K. Swapna Rani<sup>1\*</sup>, Gayatri Parasa<sup>2</sup>, Dr.D. Hemanand<sup>3</sup>, Dr.S.V. Devika<sup>4</sup>,  
Dr.S. Balambigai<sup>5</sup>, Dr.M.I. Thariq Hussan<sup>6</sup>, and Koppuravuri Gurnadha Gupta<sup>7</sup>, YJ  
Nagendra Kumar<sup>8</sup>, Alok Jain<sup>9</sup>

<sup>1</sup> Assistant Professor, Department of CSE, KG Reddy College of Engineering and Technology, Chilukuru Village Hyderabad

<sup>2</sup> Assistant Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India - 522502

<sup>3</sup> Professor, Department of Computer Science and Engineering, S.A. Engineering College, Poonamallee-Avadi Road, Thiruverkadu, Chennai-600077, Tamil Nadu, India

<sup>4</sup> Professor, Department of ECE, Hyderabad Institute of Technology and Management, Hyderabad

<sup>5</sup> Associate Professor, Department of ECE, Kongu Engineering College, Tamil Nadu

<sup>6</sup> Professor and Head, Department of IT and CSE (IOT), Guru Nanak Institutions Technical Campus, Hyderabad

<sup>7</sup> Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh - 522302, India

<sup>8</sup> Department of IT, GRIET, Hyderabad, Telangana, India

<sup>9</sup> Lovely Professional University, Phagwara, Punjab, India.

**Abstract.** The Internet of Things (IoT) expansion has introduced a new era of interconnectedness and creativity inside households. Various independent gadgets are now controlled from a distance, enhancing efficiency and organization. This results in increased security risks. Competing vendors rapidly develop and release novel connected devices, often paying attention to security concerns. As a result, there is a growing number of assaults against smart gadgets, posing risks to users' privacy and physical safety. The many technologies used in IoT complicate efforts to provide security measures for smart devices. Most intrusion detection methods created for such platforms rely on monitoring network activities. On multiple platforms, intrusions are challenging to detect accurately and consistently via network traces. This research provides a Multi-Stage Intrusion Detection System (MS-IDS) for intrusion detection that operates on the host level. The study employs personal space and kernel space data and Machine Learning (ML) methods to identify different types of intrusions in electronic devices. The proposed MS-IDS utilizes tracing methods that automatically record device activity, convert this data into numerical arrays to train multiple ML methods, and trigger warnings upon detecting an incursion. The research used several ML methods to enhance the ability to see with little impact on

---

\* Corresponding author: [r.swapna.k@gmail.com](mailto:r.swapna.k@gmail.com)

the monitoring devices. The study evaluated the MS-IDS approach in a practical home automation system under genuine security risks.

## 1 Overview of intrusion detection systems

The research now lives in a perpetually linked and more intelligent environment. Internet of Things (IoT) applications are becoming prevalent in several fields, such as smart homes, healthcare systems, autonomous vehicles, and industrial automation [1]. However, this situation is very vulnerable to any cyber assault. Therefore, security is a crucial matter that has to be addressed. Cyber-attacks occur at several levels inside the IoT systems [2]. For instance, sniffer assaults, control of access assaults, and many assaults that might arise at the application level. Phishing attempts, man-in-the-middle assaults, distributed denials of service, and other attacks are present on the networking layer. Potential attacks on the perceptual layer include node extraction, malware injections, and eavesdropping [3]. Regarding IoT, a significant expense is required to establish infrastructure, emphasizing scaling, efficiency, and user-friendliness. The absence of security upgrades on connected devices will create obstacles to the system's stability.

Intrusion refers to unauthorized or potentially harmful access to the system, allowing an attacker to access or alter data. Intrusion Detection Systems (IDS) are tools used to enhance the safety of systems by preventing unwanted infiltration and harmful access [4]. Security is a significant risk in connected devices. The selection and optimization of the IDS technique are critical areas of concern due to the importance of accuracy in these systems. An unreliable IDS might generate several false warnings, disrupting the system's smooth operation [5]. Unexpected new threats also threaten the whole system.

This study presents a comprehensive framework for automated real-time IoT evaluation. The research gathers detailed data from the observed devices using tracing methods. It transmits to research engines on a network gadget, a dedicated workstation at home, or the public cloud. The evaluation engine uses many machine learning methods to identify irregularities in device operation. Alerts are generated by the analysis system as necessary, including the device identifier and the kind of threat discovered.

The rest of the sections are as follows: section 2 indicates the related works and survey. Section 3 proposes a Multi-Stage Intrusion Detection System (MS-IDS) using Machine Learning (ML) to detect intrusions in IoT. Section 4 analyses the results of the proposed method, which are compared with other ML models. The conclusion and future scope are listed in section 5.

## 2 Background and analysis

The rise in Internet-connected devices necessitates attention to network administration duties such as device administration, tracking traffic, and cybersecurity. Prasant et al. predict that there will be 50 billion gadgets linked to the Internet, with each person owning around seven gadgets [6]. The rapid advancement of IoT technology is leading to an increased amount of IoT data being transferred via networks and the Internet, making it increasingly vulnerable to cyber security assaults.

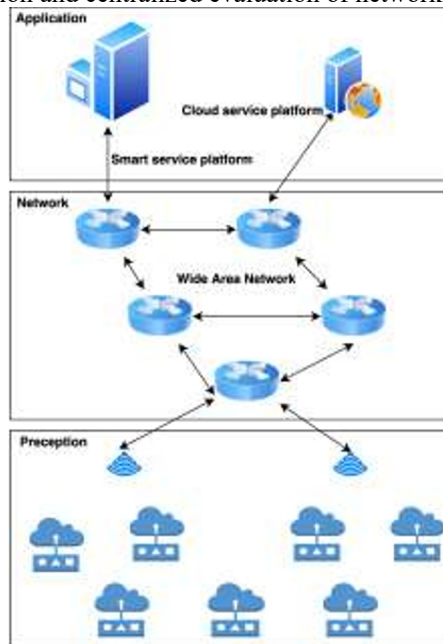
Dias et al. have indicated that creating a tailored security system for IoT devices is complex due to the IoT environment's diverse, divided, and non-interoperable nature [7]. Various security measures have been suggested to enhance information safety, authorization, access management, confidence, and privacy in connected devices. Despite these protections, IoT networks are still vulnerable to assaults and breaches.

Otoum et al. emphasize the need to create more security tools focused on the IoT and suggest that solutions such as IDS might be used to meet this need [8]. Current IDS systems used in traditional networks are unsuitable for IoT networks because they need more flexibility in dealing with the intricate and diverse IoT environment. The unique characteristics of IoT elements, including resource limitations, extensive scope, diversity, prioritization of functionality above security, increased privacy needs, cost-effective design, and complex trust administration, pose challenges for traditional IDS systems. Burhan et al. argue that network construction, flexibility, multiple devices, interaction, cooperation with the real world, limited resources, confidentiality, broad scale, trust administration, and insufficient security preparation necessitate the creation of IDS for the IoT [9].

They analyzed the available literature on IDS solutions for IoT networks to comprehend their development background. Martins et al. highlighted that only a few studies on IDS developments have concentrated on IoT networks [10]. The research mentioned the need to offer systems that can (a) protect against various threats, (b) offer diverse detection techniques, (c) cover a broader spectrum of IoT devices, and (d) protect IDS warning traffic and administration.

### 3 Multi-stage intrusion detection system

Intrusion detection methods for connected things should use minimum resources from restricted IoT gadgets. They use the excellent capabilities of devices like boundary routers or cloud-based services. Based on the objectives mentioned earlier, a solution that guarantees software integrity on IoT gadgets and minimizes the consumption of resources should utilize a hybrid deployment method. The most suitable approach for these circumstances is a mix of dispersed data collection and centralized evaluation of network traffic information.



**Fig. 1.** Architecture of the proposed MS-IDS system

Fig. 1 displays the structure of the suggested MS-IDS designed for connected devices. The proposed artifact aims to enhance the ability to detect threats in connected devices by monitoring and capturing communications between devices across the IoT design's three

layers: perception, network, and applications. This three-tier approach guarantees the identification of intrusions that might happen in any layer of a connected device. Communication interception will be conducted by deploying probes across all network tiers. The placements of these probes offer a comprehensive perspective of IoT applications and might be advantageous for detecting breaches or assaults.

### 3.1 Architectural design

The proliferation of IoT gadgets and intelligent systems across several sectors has created new vulnerabilities for cyber assaults. Data theft is a significant risk for many companies. Current IDS need an intelligent agent to monitor automated systems consistently to detect irregularities. The anomalies must be documented in an attack database to assist in creating defensive strategies. The difficulty lies in the fact that these measures are ineffective in detecting recent assaults. Therefore, there is an urgent need to create an intelligent security architecture specifically designed for deployment in IoT networks.



**Fig. 2.** Workflow of the proposed MS-IDS

The suggested MS-IDS architecture integrates the intrusion identification and mitigation system, as shown in Fig. 2.

### 3.2 Requirement of the MS-IDS system

IoT-based control networks and structures are necessary in practically every part of the planet. IoT security needs are crucial for several applications, from home security devices to tracking and managing parameters in mission-critical scenarios. The hackers might take control of whole networks to obtain access to the entire thing by intercepting gateways, servers, or both. Therefore, there is a significant need to safeguard the host computers in the IoT network, as they serve as the main point of contact for the whole network. These devices will likely be the entire system's entrance or entry point. The recommended design provides a comprehensive solution for detecting and preventing attacks by integrating analysis and implementing a preventive system based on the results from the preceding IDS study.

### 3.3 Multi-stage IDS system

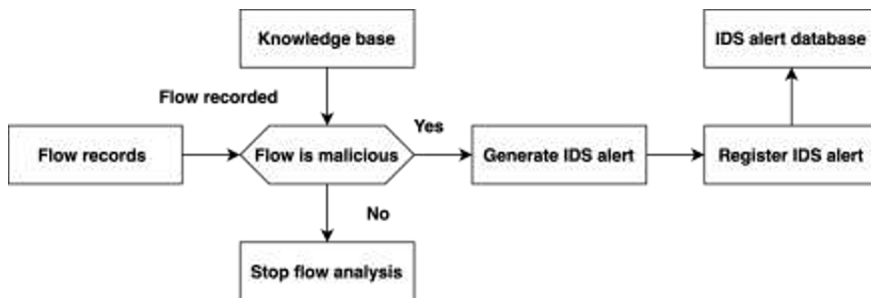
MS-IDS is designed to detect attackers who try to get past and attack an infrastructure via a vulnerable application by creating a replica interface that does not reveal the real one. It is likely a honeypot designed to gather data about the attack's characteristics, instruments, technologies, and locations. Based on the collected observations, a more robust system with improved security measures will be developed. IoT networks face a hurdle due to their limited ability to provide advanced security measures. However, hackers refrain from targeting a primary sensor node due to the inability to infiltrate the system. An IoT network

often includes a central gateway server that manages the entire network. Accessing this gateway grants attackers the ability to access the whole system. The proposed design offers remedies for host-based assaults on gateway services and utilizes ML methods for classifying and predicting attack information. An efficient system for preventing intrusions was developed by anticipating assaults.

### 3.4 Intrusion prevention system

An intrusion preventive system, whether hardware or software-based, safeguards the whole network by tracking, preventing, reporting, and perhaps isolating a segment when hostile activity is identified. This system is readily implemented on servers to track and handle all incoming requests. By pinpointing security assaults on the IDS, the Intrusion Prevention System (IPS) is constructed to safeguard the whole network against such attacks. To implement the IPS, the research needs Artificial Intelligence (AI) assistance to classify assaults using different ML methods. These methods are evaluated using fuzzy-based rankings and recommendation engines to choose the most suitable one for the issue. The research uses these assessments to select the appropriate ML technique and categorize the attack database. The research uses the categorization report and conclusions to create and revise IPS rules to safeguard IoT networks periodically.

### 3.5 Flow-based analysis

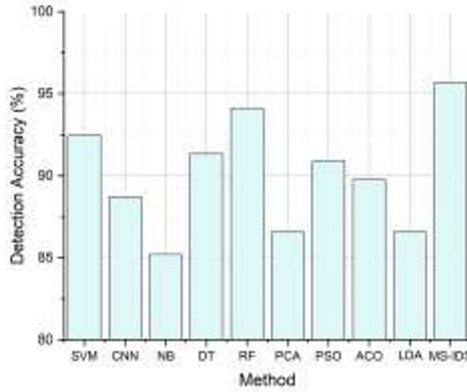


**Fig. 3.** Flow-based IDS system

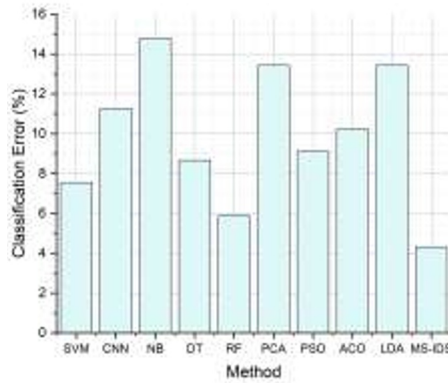
The flow-based IDS system is shown in Fig. 3. It is suggested that intruders be detected by analyzing the Internet Protocol (IP) flow data on both a local device and a distant device inside a cloud-based platform. Analyzing individual IP flow data must adhere to the pattern shown in Figure 5. Local and remote IDS components analyze the obtained IP traffic data according to their anticipated computational capacity.

## 4 Simulation outcomes and discussions

The assigned task involves categorizing instances connected to host-based assaults found in the botnet dataset. The dataset has 40k occurrences and 33 characteristics, beginning with the source address. The analysis is done in Matlab, and the proposed MS-IDS method results are compared with other ML models: Support Vector Machine (SVM) [11], Convolutional Neural Network (CNN) [12], Naïve Bayes (NB) [13], Decision Tree (DT) [14], Random Forest (RF) [15], Principle Component Analysis (PCA) [16], Particle Swarm Optimisation (PSO) [17], Ant Colony Optimisation (ACO) [18], and Linear Discriminant Analysis (LDA) [19].

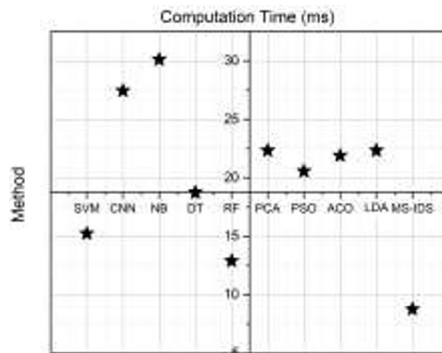


**Fig. 4(a).** Detection accuracy evaluation results

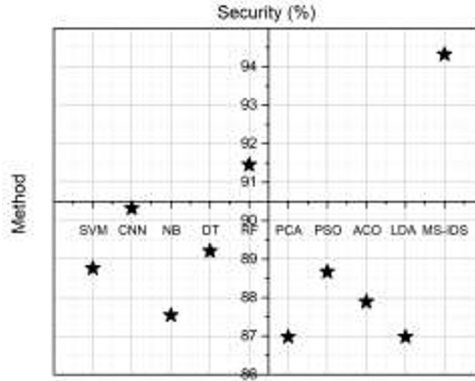


**Fig. 4(b).** Classification error evaluation results

Fig. 4(a) displays the Detection Accuracy results, with MS-IDS achieving the highest accuracy at 95.68%, surpassing SVM (92.45%), DT (91.34%), and other methods. Fig. 4(b) shows that the categorization mistake percentages indicate MS-IDS's better performance, with the lowest mistake rate of 4.32%, highlighting its effectiveness in reducing misclassifications compared to SVM (7.55%) and other methods. The MS-IDS proposal achieves superior outcomes using a multi-stage strategy that integrates personal and kernel space data with ML techniques, resulting in improved accuracy and decreased misclassifications.

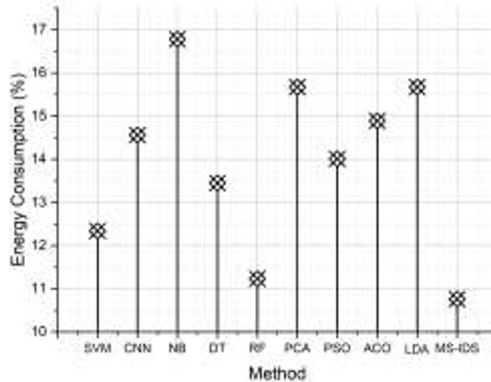


**Fig. 5(a).** Computation time evaluation results

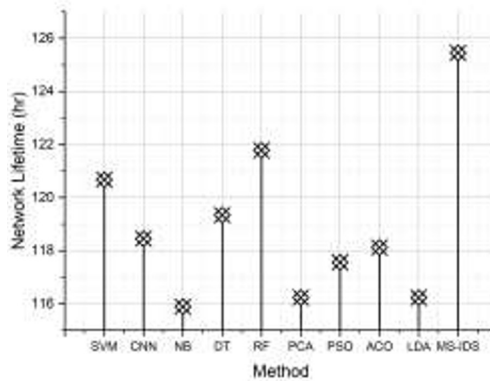


**Fig. 5(b).** Security evaluation results

Fig. 5(a) shows the calculation Time findings, with MS-IDS having the shortest calculation time at 8.76 milliseconds, outperforming SVM (15.23 ms), CNN (27.45 ms), and other methods. Fig. 5(b) shows that MS-IDS is the most secure approach, with a security percentage of 94.32%, surpassing RF (91.45%), CNN (90.32%), and other methods. The fast processing time of MS-IDS is due to its streamlined multi-stage methodology, and its robust security outcomes are a consequence of integrating personal and kernel space information with ML techniques to improve overall security protocols.



**Fig. 6(a).** Energy consumption evaluation results



**Fig. 6(b).** Network lifetime evaluation results

Fig. 6(a) displays the Energy Consumption findings, indicating that MS-IDS is the most excellent energy-efficient approach with a consumption rate of 10.76%, outperforming SVM (12.34%), CNN (14.56%), and other methods. Fig. 6(b) shows that MS-IDS has the most extended network lifespan at 125.45 hours, surpassing SVM (120.67 hrs), RF (121.78 hrs), and other methods. MS-IDS improves Energy Consumption efficiency via optimized multi-stage processes, leading to decreased energy use. The prolonged Network Lifetime is due to the method's efficiency in reducing resource depletion and maximizing energy use, improving the network's sustainability.

## 5 Conclusion and discussions

This study introduces a comprehensive and adaptable framework for detecting intrusions on intelligent gadgets. It utilizes many ML techniques and tracking methods on the observed devices. The system has shown exact intrusion-detecting outcomes. The research detailed the process of adjusting it to suit various devices and discussed the high performance of this technique due to its host-based approach. The program might have been modified to function with the live tracking mode for real-time intrusion detection. While the research achieved high precision in identifying breaches with existing models, there is room for enhancing the system's usability.

Studying the capacity of the analytical engine could be intriguing. The MS-IDS approach is distributed and scaled to multiple devices in small or more significant networks because the captured pictures can be evaluated separately. The resources required to expand the monitored networks need to be analyzed. Future research might investigate the processing speed of the learning phase since the training stage has to be continually modified to address constantly emerging novel risks.

## References

1. I.H. Sarker, A.I. Khan, Y.B. Abushark, F. Alsolami. *Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions*. Mob. Netw. Appl., **28**, 1, 296-312, (2023)
2. M.K. Kagita, N. Thilakarathne, T.R. Gadekallu, P.K.R. Maddikunta, S. Singh. *A review on cybercrimes on the Internet of Things*. Deep Learning for Security and Privacy Preservation in IoT, 83-98, (2022)
3. A.J. Hintaw, S. Manickam, M.F. Aboalmaaly, S. Karuppayah. *MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT)*. IETE J. Res., **69**, 6, 3368-3397, (2023)
4. A. Heidari, M.A. Jabraeil Jamali. *Internet of Things intrusion detection systems: A comprehensive review and future directions*. Clust. Comput., **26**, 6, 3753-3780, (2023)
5. S. Ali, Q. Li, A. Yousafzai. *Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey*. Ad Hoc Netw., **152**, 1-31, (2024)
6. P. Prasant, S. Bhardwaj, M. Gupta, M. Srivastava, J. Singh, R.K. Maurya. *Role of internet of things in protecting different wearable gadgets and materials*. Mater. Today: Proc., **56**, 3387-3393, (2022)
7. L.M. Dias, J.F. Ramalho, T. Silvério, L. Fu, R.A. Ferreira, P.S. André. *Smart optical sensors for Internet of things: Integration of temperature monitoring and customized security physical unclonable functions*. IEEE Access, **10**, 24433-24443, (2022)

8. Y. Otoum, D. Liu, A. Nayak. *DL-IDS: a deep learning-based intrusion detection framework for securing IoT*. Trans. Emerg. Telecommun. Technol., **33**, 3, 1-16, (2022)
9. M. Burhan, H. Alam, A. Arsalan, R.A. Rehman, M. Anwar, M. Faheem, M.W. Ashraf. *A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: layered architecture, real-time security issues, and solutions*. IEEE Access, **11**, 73303-73329, (2023)
10. I. Martins, J.S. Resende, P.R. Sousa, S. Silva, L. Antunes, J. Gama. *Host-based IDS: A review and open issues of an anomaly detection system in IoT*. Future Gener. Comput. Syst., **133**, 95-113, (2022)
11. A. Alsarhan, M. Alauthman, E.A. Alshdaifat, A.R. Al-Ghuwairi, A. Al-Dubai. *Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks*. J. Ambient Intell. Humaniz. Comput., **14**, 5, 6113-6122, (2023)
12. A. Halbouni, T.S. Gunawan, M.H. Habaebi, M. Halbouni, M. Kartiwi, R. Ahmad. *CNN-LSTM: hybrid deep neural network for network intrusion detection system*. IEEE Access, **10**, 99837-99849, (2022)
13. R. Islam, M.K. Devnath, M.D. Samad, S.M.J. Al Kadry (2022). *GGNB: Graph-based Gaussian naive Bayes intrusion detection system for CAN bus*. Veh. Commun., **33**, 1-27, (2022)
14. M.H.L. Louk, B.A. Tama. *Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system*. Expert Syst. Appl., **213**, (2023)
15. Z. Liu, Y. Shi. *A hybrid IDS using GA-based feature selection method and random forest*. Int. J. Mach. Learn. Comput, **12**, 02, 43-50, (2022)
16. M. Al-Fawa'reh, M. Al-Fayoumi, S. Nashwan, S. Fraihat. *Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior*. Egypt. Inform. J., **23**, 2, 173-185, (2022)
17. S. Subramani, M. Selvi. *Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks*. Optik, **273**, (2023)
18. J.K. Samriya, R. Tiwari, X. Cheng, R.K. Singh, A. Shankar, M. Kumar (2022). *Network intrusion detection using ACO-DNN model with DVFS based energy optimization in cloud framework*. Sustain. Comput.: Inform. Syst., **35**, (2022)
19. M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, M. Portmann. *Feature extraction for machine learning-based intrusion detection in IoT networks*. Digit Commun Netw., (2022)