*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 2207–2217
DOI : 10.47974/JDMSC-2092

# A novel approach to IoT security for intrusion detection system using ensemble network and heuristic-assisted feature fusion

Atul B. Kathole [‡]
Kapil Vhatkar [†]
*Department of Computer Engineering*
*Dr. D. Y. Patil Institute of Technology*
*Pune 411018*
*Maharashtra*
*India*

Gulbakshee Dharmale [§]
*Department of Information Technology*
*Pimpri Chinchwad College of Engineering*
*Pune 411044*
*Maharashtra*
*India*

Shwetambari Chiwhane *
*Department of Computer Science and Engineering*
*Symbiosis Institute of Technology*
*Symbiosis International (Deemed University)*
*Pune*
*Maharashtra*
*India*

Vinod V. Kimbahune [@]
*Department of Computer Engineering*
*Dr. D. Y. Patil Institute of Technology*
*Pune 411018*
*Maharashtra*
*India*

[‡] *E-mail:* atul.kathole1910@gmail.com
[†] *E-mail:* kapilnv@gmail.com
[§] *E-mail:* gulbakshi.dharmale@pccoepune.org
* *E-mail:* shwetambari.chiwhane@sitpune.edu.in (Corresponding Author)
[@] *E-mail:* vinod.kimbahune@dypvp.edu.in

Ankur Goyal [#]
*Department of Computer Science & Engineering*
*Symbiosis International Deemed University*
*Symbiosis Institute of Technology*
*Pune 411016*
*Maharashtra*
*India*

**Abstract**

The area of "Internet of Things (IoT)" has gained popularity recently as a method for developing intelligent models. Security and privacy are regarded as the two main issues in every real-world IoT application. The security risks posed by IoT-enabled devices are serious threats to the development of the smart industry. Thus, to reduce the security dangers that emanate from IoT devices and give birth to numerous security concerns, Intrusion Detection Systems (IDSs) specifically tailored for the IoT sectors are important. Conventional intrusion detection systems (IDSs) are unsuitable for use in standard Internet of Things (IoT) networks for a variety of reasons, including memory, battery life, and processing power. Various Intrusion Detection Systems (IDSs) have been proposed in academic research to address these problems. However, while identifying anomalies, various intrusion detection systems (IDSs) have issues with low accuracy and numerous false alarms. To counteract the shortcomings of conventional systems, it is recommended that an ensemble deep learning model be utilized to identify intrusions within the Internet of Things (IoT) domain. The final result is then determined by averaging the scores, which is accomplished by combining them. Divergent measurements are thus used to validate the model. On the other hand, by prohibiting unwanted access, the recommended method not only increases the detection rate but also improves network security.

***Subject Classification:*** *Primary 93A30, Secondary 49K15.*

***Keywords:*** *Intrusion detection system, Internet of Things, Weighted feature fusion, Fitness value of pelican optimization algorithm, Ensemble networks.*

## 1. Introduction

The IoT [1] refers to the interconnectedness of physical systems through network connectivity, software, and sensors, enabling them to communicate and gather data. The IDSs monitor the behavior of the system and analyze the network traffic in order to identify significant security breaches [2]. The traditional IDS approaches are generally ineffective for IoT platforms due to the inherent characteristics of IoT networks such as dynamic topologies, heterogeneity, and resource

[#] *E-mail:* **Ankur_gg5781@yahoo.co.in**

constraints. Deep learning has emerged as an effective approach for detecting intrusions in IoT due to its capacity to comprehend complex features and patterns from vast amounts of data. The intrusion identification in IoT is enhanced by deep learning, namely through the utilization of "Artificial Neural Networks (ANN)" to analyze and predict sensor data, network traffic, and other relevant information [3]. Based on prior knowledge, deep learning methods have the ability to identify intrusion attempts and anomalous patterns, as well as classify different types of attacks.

The intrusion detection in IoT-aided deep learning approaches involves utilizing the capabilities of artificial neural networks (ANNs) to automatically detect and learn hostile actions or anomalies in IoT systems. The intrusion attack and pattern techniques arise in response to changing circumstances and require the deep learning approach to be updated simultaneously [4]. The system's retraining process, which utilizes currently created knowledge, helps it adapt to increasing threats and improve its effectiveness. The trained system is predicted to employ a confidential repository of labelled data that is not utilized throughout the training process. This evaluation confirms the effectiveness of the system by considering parameters such as F1 score, recall, precision, and accuracy. The evaluation helps determine the system's efficiency and identify any necessary improvements and adjustments [5]. To ensure the effectiveness of new intrusion methods, it is necessary to consider the chosen system structure, the presence of computing assets, and the ongoing observation and model update [6].

The recommended IoT-aided IDS task's contributions are listed as follows.

- The objective is to create an IDS specifically for the IoT industry. This system will effectively prevent unauthorised access and achieve higher detection capabilities by utilising ensemble deep learning techniques.
- To derive the distinctive characteristics from the initial dataset, by utilising the TSNE, PCA, and statistical metrics. The weights are ideally combined with the features using the designed FVPOA.
- The performance rates of the constructed IoT-aided IDS task were estimated using several optimisation algorithms and classifiers, and evaluated using multiple functionality metrics.

The framework of the suggested IoT-aided IDS task comprises of following parts. Related work of exiting approach with research gap in Part II. The novel idea of the IDS in IoT network is demonstrated in Part III. conventional experiments of IDS are given in Part IV. The conclusion of the suggested IDS task is given in Part V.

## 2. Related Work

In 2023, [2] and the colleagues suggested a practical and effective IDS for IoT networks, utilizing deep learning methods. A filter-based attribute selection method known as "Deep Neural Network (DNN)" was employed to identify and eliminate correlated attributes. Subsequently, the system underwent optimization by adjusting several parameters. The job that was developed had an accuracy rate of 84%. The "Generative Adversarial Networks (GANs)" were employed to produce artificial data for targeted attacks on minority groups.

In 2022, [3] proposed a methodology for anomaly-aided Intrusion Detection Systems (IDS) that utilizes Convolutional Neural Networks (CNNs). This approach leverages the advantages of IoT's capabilities and provides a framework for efficiently validating the traffic within IoT networks. The recommended solution demonstrated the capacity to identify any anomalous traffic patterns and potential breaches.

In 2023, [4] utilized the LSTM approach to address the IDS and accurately identify cyber threats. They also provided a detailed description of the system's conclusions. This strategy employed a combination of input attributes extracted using the "SPIP method to estimate and train the LSTM system.

### 2.1 *Problem statement*

Although there have been improvements in IDS for ensuring network security in the IoT industry, there is a notable lack of research on combining Ensemble Networks with Enhanced Heuristic-assisted Weighted Feature Integration [7]. Ensemble learning and heuristic-assisted feature integration have been found to enhance detection accuracy and robustness in traditional IDS [8]. However, their potential and usefulness in IoT environments have not been thoroughly investigated.

## 3. Proposed Concept of Intrusion Detection System in IoT Network: Ensemble Network and Enhanced Heuristic Algorithm

The IoT has garnered significant attention in recent times due to its advancements and contributions to numerous sectors such as smart environments, automation, healthcare, industrial processes, and more. The IoT facilitates the connection of several disparate advancements through the internet, enabling the convergence of smart objects and determining the interaction between the cyber and physical domains. The IoT advancements have diverse purposes, although they share common characteristics. The IoT consists of three distinct stages: collection and transmission. This objective is achieved by the utilization of short-range transmission technology and sensor devices [9]. The transmission step is dedicated to conveying the information gathered in the collection phase to the candidates. During this phase, technologies such as wifi and Ethernet are interconnected using various protocols to establish a network that connects candidates and objects over large distances [8]. Finally, during the processing stage, the applications carry out operations on the collected data in order to obtain valuable information. The applications are responsible for making decisions based on the data. The following are a number of IoT security features [10].

Data confidentiality is crucial for both personal and industrial progress, as any alterations to the data might lead to significant issues. The preservation of data confidentiality is a crucial element inside the IoT industry.

Data integrity is an essential and vital aspect. Validating the data resource and identifying harmful assaults are crucial for describing data integrity in the IoT sector [11].

Continuous accessibility of acquired data is crucial in the IoT business. The Internet of Things (IoT) should provide the candidate with unrestricted access to information, regardless of their location or the time of day. However, there is a potential for security vulnerabilities. Therefore, it is crucial to provide secure data access.

Authentication: The Internet of Things (IoT) requires a robust verification process. This will improve the equilibrium between the data and the IoT system [12].

Considering these security factors, it is crucial to bolster the security system for the IoT sector. The threats should be promptly discovered to minimise network disruptions [13]. The Intrusion Detection System (IDS) recognises and disregards unauthorised access, thereby safeguarding the

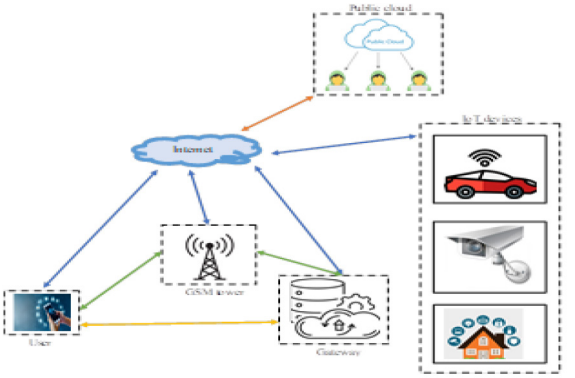


**Figure 1**

**The pictorial representation of IDS in the IoT environment**

data and network. The depiction of the IDS in the IoT sector is visually presented in Figure 1.

*Dataset Details*

The implemented intrusion detection framework has utilized the below-mentioned benchmark datasets.

**Dataset 1 ("NSL-KDD dataset"):** The implemented intrusion detection system utilized the significant data from the link "https://www.unb.ca/cic/datasets/nsl.html". This data resource emerged from the traditional KDD'99 data resource to resolve the inherent issues of the traditional KDD'99. This data resource includes 8 data files and each data file includes a subset of the conventional KDD dataset.

The acquired data from the above datasets are pointed as $J_m$. Here $m = 1, 2..., M$. The total collected data is denoted as $M$.

The objective function of the term $y_{a,b}^{Q2}$ is referred to as $G_a^{Q2}$. The designed FVPOA's pseudo-code is offered in Algorithm 1 and the flowchart is given in Figure 1.

**Algorithm 1: Developed FVPOA**

The iteration counts and population matrix initialization
Objective function validation
For $t = 1$ *to* $T_{\max}$
For $a = 1$ *to* $N_{pop}$
**Random value estimation utilizing**
Perform the POA task
Process the exploration operation utilizing
Estimate the hunting process applying
Perform the positing updating adopting
End
End
Iterate the process to achieve the optimal solutions
Acquire the optimum values
End

## 4. Experimental Setup

Implementing an Intrusion Detection System (IDS) for providing network security using Ensemble Network with Enhanced Heuristic-assisted Weighted Feature Integration [14] in the IoT sector involves several steps. Here in this section gives the overview of how you can approach the implementation using Python using some parameters,

### 4.1 *Confusion matrix estimation of the recommended IDS for three datasets*

The suggested IDS framework is processed with the confusion matrix estimation for the three datasets and illustrated in Figure 2. According to the actual and predicted values, the recommended IDS is examined [15]. From Figure 2, it is known that the initial dataset attained 94.73% accuracy. This confirms that the examined IDS has better efficacy.

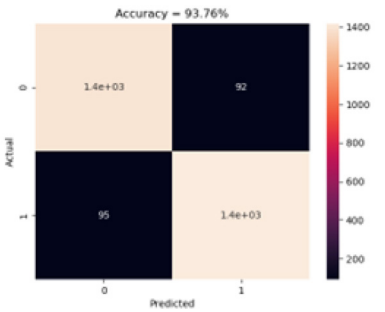


**Figure 2**

**The confusion matrix estimation of the suggested IDS concerning "**

**(a) Dataset 1**

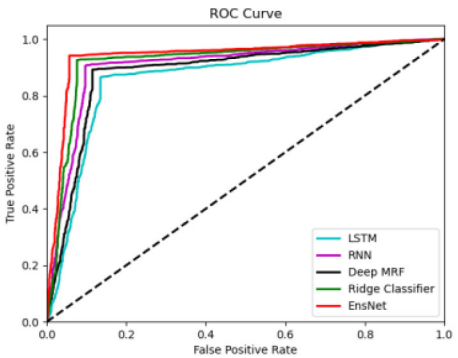


**Figure 3**

**The ROC examination of the suggested IDS over various classifiers concerning " (a) Dataset 1**

ROC estimation of the implemented IDS task over divergent classifiers for three datasets

The ROC validation of the suggested IDS task in the IoT sector is conducted over divergent classifiers and presented in Figure 3. According to the "false and true positive rates" the process is estimated [16]. When taking the third dataset false positive rate as 0.2, the recommended IDS is advanced by 31.5 % of LSTM, 32.5 % of RNN, 35 % of Deep MRF, and 36.5 % of Ridge classifier correspondingly. Hence, it is described that the suggested IDS in the IoT sector has high functionality **[17].**

*The overall comparative validation of the designed IDS over conventional classifiers*

Table 1 presents a comparative analysis of the built IDS using different algorithms and classifiers for three datasets [8]. When considering the accuracy value for the initial dataset in Table 1, the suggested IDS increased by 6.2% for LSTM, 2.9% for RNN, 4.9% for Deep MRF, and 1.16% for Ridge classifier respectively. The comprehensive analysis demonstrated that the proposed IDS)has superior functionality [10].

**Table 1**

**The comparative validation of the recommended IDS over multiple conventional classifiers for three datasets**

| Terms | LSTM | RNN | Deep MRF | Ridge classifier | EnsNet |
|---|---|---|---|---|---|
| "Dataset-1" | | | | | |
| "Accuracy" | 89.9 | 91.16666667 | 92.23333333 | 92.96666667 | 93.76666667 |

*Contd...*

| | | | | | |
|---|---|---|---|---|---|
| **"Recall"** | 90.1986755 | 91.25827815 | 92.18543046 | 93.04635762 | 93.90728477 |
| **"Specificity"** | 89.59731544 | 91.0738255 | 92.28187919 | 92.88590604 | 93.62416107 |
| **"Precision"** | 89.78246539 | 91.1978822 | 92.36894492 | 92.98477829 | 93.72108394 |
| **"FPR"** | 89.59731544 | 91.0738255 | 92.28187919 | 92.88590604 | 93.62416107 |
| **"FNR"** | 89.9900892 | 91.22807018 | 92.27709645 | 93.01555776 | 93.81409196 |
| **"NPV"** | 79.79934272 | 82.33248789 | 84.46635234 | 85.93266469 | 87.53278808 |
| **"FDR"** | 10.40268456 | 8.926174497 | 7.718120805 | 7.11409396 | 6.375838926 |
| **"F1-Score"** | 9.801324503 | 8.741721854 | 7.814569536 | 6.953642384 | 6.092715232 |
| **"MCC"** | 10.21753461 | 8.802117803 | 7.631055076 | 7.015221707 | 6.278916061 |

## 5. Conclusion

The improved Intrusion Detection System (IDS) work in the Internet of Things (IoT) sector for providing security has been developed to tackle the challenges faced by traditional methods that utilize ensemble deep learning procedures. Initially, the primary data was collected from the conventional data sources. Additionally, the feature extraction approach was implemented using TSNE, PCA, and statistical features. Furthermore, the acquired characteristics were combined with the assistance of weights that were optimally estimated using the enhanced FVPOA. Finally, the combined characteristics were analyzed using the EnsNet, which was created using a different classifier. Furthermore, the result was obtained using the procedure of average-based fusion. Therefore, the model was validated using several factors. When the second dataset epoch value was set to 150 for the suggested IDS, the accuracy of LSTM improved by 43%, RNN by 42%, Deep MRF by 40%, and Ridge classifier by 38% respectively. Thus, it has been demonstrated that the implemented IDS in the IoT industry achieved superior detection rates and effectively thwarted unauthorized access by external entities to the network.

## 6. Future Work

The combination of edge computing with AI-driven IDS is the key to ensuring the security of IoT in the future. Ensemble networks equipped with improved heuristic-assisted weighted feature integration can be implemented at the network edge to facilitate immediate identification and reaction to threats, hence minimizing delays and decreasing the need for extensive network capacity. The research in this field should priorities the optimization of ensemble learning algorithms for edge environments, the creation of lightweight heuristic models for edge devices with limited resources, and the investigation of federated learning methods for sharing distributed threat knowledge among edge nodes.

**References**

[1] A. Dhumane, S. Chiwhane, A. Mangore, and S. Ambala, "Cluster-based energy-efficient routing in Internet of Things," in *ICT with Intelligent Applications*, J. Choudrie, P. Mahalle, T. Perumal, and A. Joshi, Eds., vol. 311. Singapore: Springer, pp. 1-10 (2023). doi: 10.1007/978-981-19-3571-8_40.

[2] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Computers and Electrical Engineering*, vol. 107, p. 108626, Apr. (2023).

[3] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, p. 107810, Apr. (2022).

[4] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," *Information Sciences*, vol. 639, p. 119000, Aug. (2023).

[5] M. Abd Elaziz, M. A. A. Al-qaness, A. Dahou, R. A. Ibrahim, and A. A. Abd El-Latif, "Intrusion detection approach for cloud and IoT environments using deep learning and Capuchin Search Algorithm," *Advances in Engineering Software*, vol. 176, p. 103402, Feb. (2023).

[6] M. Vishwakarma and N. Kesswani, "DIDS: A deep neural network-based real-time intrusion detection system for IoT," *Decision Analytics Journal*, vol. 5, p. 100142, Dec. (2022).

[7] M. Catillo, A. Pecchia, and U. Villano, "CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders," *Computers & Security*, vol. 129, p. 103210, Jun. (2023).

[8] S. D. Patil, A. B. Kathole, S. Kumbhare, and K. Vhatkar, "A blockchain-based approach to ensuring the security of electronic data," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1, pp. 1-8 (2024).

[9] S. Nagaraj, A. B. Kathole, L. Arya, N. Tyagi, S. B. Goyal, A. S. Rajawat, M. S. Raboaca, T. C. Mihaltan, C. Verma, and G. Suciu, "Improved secure encryption with energy optimization using random permutation pseudo algorithm based on Internet of Things in wireless sensor

networks," *Energies*, vol. 16, no. 1, p. 8, Jan. (2023). [Online]. Available: https://doi.org/10.3390/en16010008

[10] A. B. Kathole, J. Katti, D. Dhabliya, V. Deshpande, A. S. Rajawat, S. B. Goyal, M. S. Raboaca, T. C. Mihaltan, C. Verma, and G. Suciu, "Energy-aware UAV based on blockchain model using IoE application in 6G network-driven cyber twin," *Energies*, vol. 15, no. 21, p. 8304, Nov. (2022). [Online]. Available: https://doi.org/10.3390/en15218304.

[11] S. D. Patil, A. B. Kathole, S. Kumbhare, K. Vhatkar, and V. V. Kimbahune, "A blockchain-based approach to ensuring the security of electronic data," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 11s, pp. 649–655 (2024).

[12] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning-based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, pp. 102211, Oct. (2023).

[13] B. Madhu, M. V. G. Char, R. Vankdothu, A. K. Silivery, and V. Aerranagula, "Intrusion detection models for IoT networks via deep learning approaches," *Measurement: Sensors*, vol. 25, p. 100641, Feb. (2023).

[14] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882-6897, Aug. (2020).

[15] Kumar, S. S. R. N. P. Bhat, and S. Gupta, "An enhanced quantum key distribution protocol for security authentication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 499-507, (2019).

[16] R. Mills, A. K. Marnerides, M. Broadbent and N. Race, "Practical Intrusion Detection of Emerging Threats," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 582-600, March (2022).

[17] S. Kumar, P. K. Srivastava, G. K. Srivastava, P. Singhal, D. Singh, and D. Goyal, "Chaos based image encryption security in cloud computing," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1041-1051, Jul. (2022).

*Received March, 2024*