An Intrusion Detection System Using Machine Learning and Deep Learning Algorithms

P M Vijayan
Department of Electronics and Communication Engineering ,
Siddhartha Institute of Science and Technology ,
Puttur, Andhara Pradhesh, India
vijayangce@gmail.com

K Mounika
Department of Electronics and Communication Engineering ,
Siddhartha Institute of Science and Technology ,
Puttur, Andhara Pradhesh, India
mounikakalivi@gmail.com

O Mounika
Department of Electronics and Communication Engineering ,
Siddhartha Institute of Science and Technology ,
Puttur, Andhara Pradhesh, India
Ontelamounika9@gmail.com

J Niranjan Reddy
Department of Electronics and Communication Engineering ,
Siddhartha Institute of Science and Technology ,
Puttur, Andhara Pradhesh, India
niranjanreddy1073@gmail.com

V Nagajyothi
Department of Electronics and Communication Engineering ,
Siddhartha Institute of Science and Technology,
Puttur, Andhara Pradhesh, India
nagajyothi2327@gmail.com

P Munisekhar
Department of Electronics and Communication Engineering ,
Siddhartha Institute of Science and Technology ,
Puttur, Andhara Pradhesh, India
pandlurusekhar@gmail.com

Abstract: The rapid development of IoT systems, IoT networks remain highly vulnerable to a wide range of security attacks, which can cause severe disruption to IoT services. To address these challenges, a novel intrusion detection system (IDS) is proposed using Message Queuing Telemetry Transport (MQTT) datasets. Initially, IoT data is collected from standard MQTT sources and processed in a pre-processing phase. The processed data is then used to extract three sets of features: the first set is optimally selected using the Improved Vulture Starvation–based African Vultures Optimization Algorithm (IVS-AVOA); the second set consists of statistical features refined by IVS-AVOA; and the third set is derived from an autoencoder optimized by the same algorithm. This proposed model effectively enhances attack detection in IoT environments.

KEY WORDS: Internet of things, intrusion detection system, Message Queuing Telemetry Transport (MQTT), Improved Vulture Starvation-based African Vultures Optimization Algorithm.

Introduction:

An Intrusion Detection System (IDS) is a security mechanism designed to monitor network or system activities and identify suspicious behaviour , such as attempts to gain unauthorized access. IDS continuously applying, data sources including network traffic, system logs, and user activities to detect potential threats. IDS are broadly classified into two categories: signature-based IDS and anomaly-based IDS. Signature-based IDS detects attacks by matching known attack patterns or signatures, whereas anomaly-based IDS identifies intrusions by detecting deviations from normal system behaviour [1], [2]..

Cybersecurity analysts use different methods to detect botnet attacks in networks. IoT networks are more vulnerable because of weak security and complex device design. Deep learning models can detect botnet attacks, but most studies use only one model. A single model may not work well for changing attack patterns and unbalanced data. Therefore, ensemble learning can improve the accuracy and reliability of botnet detection in IoT networks.

Intrusion Detection Systems (IDS) are software or hardware tools that monitor activities in computer systems and networks. They apply events such as network traffic and system logs to identify security threats. With the rapid growth of cyberattacks, IDS have become essential components of organizational security. IDS can be configured according to specific system and network requirements. By providing timely alerts, IDS help organizations detect and respond to intrusions effectively.

Intrusion detection involves monitoring activities in a computer system or network to identify security breaches. These breaches attempt to compromise confidentiality, integrity, or availability of data. Intrusions can be caused by external attackers or by authorized users misusing privileges. Some users may try to gain access beyond their authorization. Intrusion Detection Systems (IDS) automate the process of detecting and applying such intrusions.

Intrusion Detection Systems (IDS) are used to detect attacks on computer systems and networks. Ensuring complete security is difficult due to system complexity and operational constraints. Therefore, IDS monitor system usage to identify insecure or abnormal states. They detect misuse by authorized users as well as attacks from external sources. IDS help identify attempts to exploit system vulnerabilities and abuse privileges.

LITERATURE SURVEY :

1. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study

Hindy et al. (2020) proposed a machine-learning-based intrusion detection system for IoT environments using the MQTT protocol. The study utilized the MQTT-IDS2020 dataset and applied various machine learning classifiers such as Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), and K-Nearest Neighbour (KNN) to detect MQTT-based attacks. The work introduced a standardized MQTT attack dataset and provided benchmark results for comparison. However, the study observed that traditional machine learning

models struggle with high-dimensional data, and deep learning methods were not extensively explored, limiting scalability and detection performance.

2. Deep Learning-Based Intrusion Detection System for MQTT

Khan et al. (2021) developed a deep learning-based intrusion detection system using Deep Neural Networks (DNN) for applied MQTT traffic. The model effectively learned complex non-linear patterns present in MQTT messages and demonstrated superior detection accuracy compared to classical machine learning approaches. Despite its improved performance, the approach requires a large amount of training data and lacks efficient feature optimization techniques. Additionally, the system's performance degrades when trained on imbalanced datasets, which is a common challenge in real-world IoT environments.

3. An Automated Intrusion Detection System Using Improved Heuristic Autoencoder and LSTM-based DBN for MQTT

Vijayan and Sundar (2023) proposed an automated intrusion detection system that combines an improved heuristic-optimized autoencoder with an LSTM-based Deep Belief Network (DBN) for MQTT traffic analysis. The autoencoder was used for effective feature extraction, while the improved heuristic optimization enhanced sequential attack detection. The model demonstrated strong performance in identifying complex MQTT attacks. However, the approach suffers from high computational complexity and is difficult to deploy on resource-constrained IoT devices due to its heavy processing requirements.

4. RSSI-Based Intrusion Detection Technique for IoT Networks

Bhosale and Sonavane et al. (2020) introduced an intrusion detection technique based on the Received Signal Strength Indicator (RSSI) for IoT networks. The method achieved improved detection performance by increasing the True Positive Rate (TPR) while reducing the False Positive Rate (FPR). This lightweight approach is suitable for IoT sensor networks. However, the detection accuracy decreases significantly as the hop count increases, limiting its effectiveness in large-scale or multi-hop IoT networks.

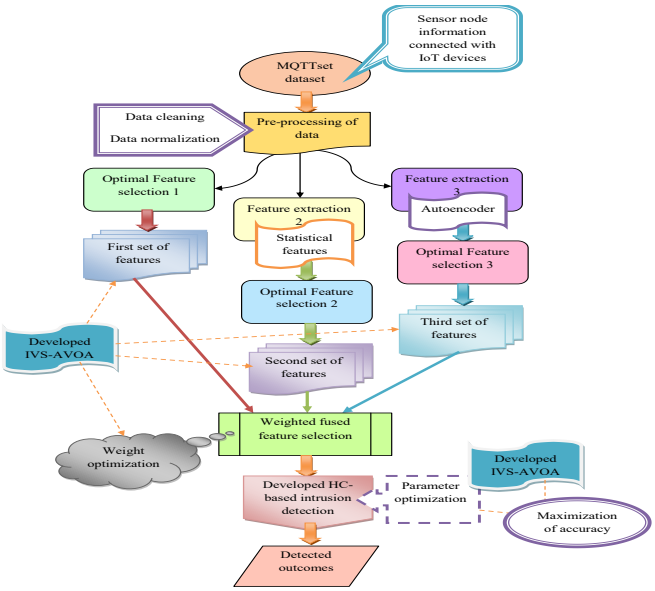
5 . Machine Learning-Based Security Solutions for IoT Attack Detection

Syeda Manija Tahsin, Hadis Karimi pour et al. (2020) presented a comprehensive machine learning-based security framework capable of detecting various types of IoT attacks. The system demonstrated the ability to identify multiple attack categories effectively. Nevertheless, the model faces challenges in precisely identifying specific attack types due to increased complexity. This limitation highlights an ongoing issue in IoT security where accurate attack classification remains difficult.

6 . Fuzzy Logic-Based Intrusion Detection System for IoT Environment

Haripriya and Koluthungan (2019) proposed a fuzzy logic-based intrusion detection system for IoT environments. The model improved detection efficiency by handling uncertainty in network behaviour and provided accurate detection for certain attack patterns. However, the approach fails to detect multiple attack types simultaneously and does not incorporate optimization techniques. As a result, its applicability in dynamic and large-scale IoT networks is limited.

PROPOSED METHOD :



The proposed methodology diagram illustrates a sophisticated, end-to-end pipeline for an advanced machine learning system powered by the Improved Vulture-Based African Vulture Optimization Algorithm (IVB-AVOA). Starting from raw input data—likely from sensors or real-world sources—the process systematically transforms unrefined information into high-fidelity predictions through sequential stages of pre-processing, feature engineering, optimization, fusion, refinement, and hybrid classification. This structured approach ensures robustness, efficiency, and superior performance in handling complex datasets, as evidenced by the flowchart's clear directional flow from left to right, with parallel branches for feature handling converging into a unified output .Data Pre-processing and Feature Extraction Raw data enters the pipeline and immediately undergoes pre-processing, which includes essential steps like noise removal, handling of missing values, and normalization. This stage standardizes the data scale, mitigating issues from varying sensor ranges or distributions. Following this, three distinct sets of features are extracted: statistical features (e.g., mean, variance, skewness), and two other categories—possibly texture-based or domain-specific ones tailored to the application. These branches highlight the diagram's emphasis on multi-modal feature capture to enrich representational power .Optimization with IVB-AVOAA core innovation shines here: each of the three feature sets is independently optimized using IVB-AVOA, an enhanced bio-inspired metaheuristic algorithm mimicking vulture foraging behaviours for superior exploration and exploitation. This optimization selects the most salient features, discarding redundancies and irrelevant ones, which is crucial for dimensionality reduction and preventing overfitting. The algorithm's "improved" aspect likely incorporates adaptive parameters or hybrid mechanisms, enabling it to outperform standard optimizers in converging to global optima faster, especially with high-dimensional data .Feature Fusion and Autoencoder Refinement The three optimized feature sets converge into a fused representation, combining statistical and deep-learned attributes for a holistic view. This fused vector then feeds into an autoencoder—a neural architecture that learns compressed, latent representations by reconstructing inputs while minimizing reconstruction error. The autoencoder acts as a bottleneck, further distilling the data into essential components, enhancing compactness and generalization while suppressing noise amplified during fusion .Hybrid Classification and Output Finally, the refined features reach the classification stage, employing a hybrid model that integrates fuzzy logic (for handling uncertainty via membership functions) with 1D Convolutional Neural Networks (1D-CNN, suited for sequential

data like time-series), and potentially other classifiers (e.g., SVM or ensemble methods). This synergy leverages fuzzy logic's interpretability and CNN's pattern recognition prowess, yielding precise decisions. The output represents the system's prediction or categorization, closing the loop on a methodology designed for real-world efficacy, such as in IoT monitoring, biomedical signal analysis, or industrial fault detection. This diagram not only visualizes the workflow but also underscores the system's novelty in leveraging IVB-AVOA for feature optimization alongside hybrid deep-fuzzy classification, promising state-of-the-art results in accuracy and efficiency.

RESULT & DISCUSSION :

Comparative validation of the proposed IDS for IoT devices with existing classifiers :

Measure	DNN (Nguyen et al., 2019)	RNN (Chowdhury and Kaiser, 2018)	Fuzzy (Hartpence and Kalafsat, 2019)	1DCNN (Ke et al., 2021)	Fuzzy-1DCNN (Zhao et al., 2021)	IVS-AVOA-HC (Proposed)
Accuracy	88.73	90.72	91.45	92.64	93.95	**96.63**
Sensitivity	83.35	83.36	87.37	87.97	100	**100**
Specificity	89.76	90.74	91.43	92.62	93.93	**96.65**
Precision	81.48	84.72	84.86	87.74	90.92	**94.06**
F1-score	84.74	87.37	88.52	90.26	92.74	**95.27**
FPR	11.25	09.26	08.54	07.32	06.05	**03.34**
FNR	19.61	16.62	16.69	14.31	12.86	**10.27**
NPV	88.76	90.75	91.42	92.69	93.32	**96.68**
FDR	14.52	16.23	16.35	17.53	12.14	**11.89**
MCC	75.51	80.18	81.69	84.72	89.62	**92.62**

The table presents a comparative validation of the proposed Intrusion Detection System (IDS) framework for IoT devices against several existing classification techniques, namely DNN, RNN, Fuzzy-based models, 1DCNN, and Fuzzy–1DCNN, using multiple evaluation metrics. This comprehensive comparison highlights the effectiveness and robustness of the proposed IVS-AVOA-HC method by analyzing its performance across both positive and negative classification measures. The results clearly show a consistent improvement of performance from conventional deep learning approaches toward hybrid models, with the proposed method achieving the best overall results.

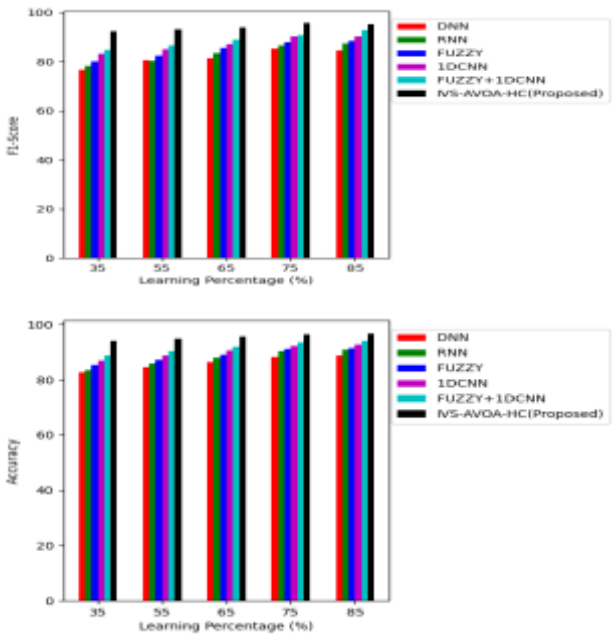
In terms of accuracy, the proposed IVS-AVOA-HC framework achieves 96.63%, which is significantly higher than DNN (88.73%), RNN (90.72%), Fuzzy (91.45%), 1DCNN (92.64%), and Fuzzy-1DCNN (93.95%). This improvement indicates that the proposed model is highly capable of correctly classifying both normal and malicious IoT traffic. Similarly, sensitivity, which reflects the system's ability to correctly detect actual intrusions, reaches 100% for the proposed method, matching the best-performing hybrid model and outperforming all other techniques. This demonstrates that the proposed IDS can detect all attack instances without missing any, which is a critical requirement for security-sensitive IoT environments.

The specificity of the proposed model is also the highest at 96.65%, indicating a strong ability to correctly identify legitimate traffic and minimize false alarms. This is further supported by the precision value of 94.06%, which shows that the majority of detected intrusions are truly malicious. When both precision and sensitivity are jointly considered, the F1-score of the proposed method reaches 95.27%, surpassing all other classifiers. This highlights the balanced and reliable detection capability of the proposed IDS, especially under class-imbalanced conditions commonly found in IoT datasets.

Error-related metrics further emphasize the superiority of the proposed framework. The False Positive Rate (FPR) is reduced to 3.34%, which is the lowest among all methods, indicating fewer false alarms. Similarly, the False Negative Rate (FNR) is minimized to 10.27%, showing that the proposed IDS misses fewer attack instances compared to existing models. The Negative Predictive Value (NPV) of 96.68% confirms that traffic classified as normal is highly reliable, enhancing trust in the system's predictions. Additionally, the False Discovery Rate (FDR) is comparatively low at 11.53%, demonstrating improved reliability over other hybrid techniques.

Finally, the Matthews Correlation Coefficient (MCC), which provides a balanced measure even for imbalanced datasets, reaches 92.62% for the proposed IVS-AVOA-HC framework. This high MCC value indicates strong overall classification quality and robustness. Overall, the table clearly demonstrates that the proposed IDS framework significantly outperforms existing classifiers across all evaluation metrics, proving its effectiveness, reliability, and suitability for securing IoT environments against diverse and evolving cyber-attack.

Proposed IDS framework for IoT devices with different techniques over "(a)accuracy, (b) F1-score



The given figure presents a detailed performance evaluation of a proposed Intrusion Detection System (IDS) framework for IoT devices by comparing it with several existing and hybrid techniques using two key performance metrics, namely accuracy and F1-score, under different learning percentages (35%, 55%, 65%, 75%, and 85%). The techniques considered for comparison include Deep Neural Network (DNN), Recurrent Neural Network (RNN), Fuzzy-based approach, 1D Convolutional Neural Network (1DCNN), Fuzzy + 1DCNN hybrid model, and the proposed IVS-AVOA-HC method. The variation in learning percentage represents the proportion of training data used to train the IDS, allowing the evaluation of model scalability and learning capability under limited and large datasets.

Figure (a) illustrates the accuracy comparison of different IDS techniques. It can be observed that as the learning percentage increases, the accuracy of all models improves steadily, indicating that a higher amount of training data enhances the intrusion detection capability. Traditional deep learning models such as DNN and RNN achieve moderate accuracy due to their limited ability to handle complex attack patterns and uncertainty in IoT traffic. The fuzzy-based approach improves accuracy by incorporating rule-based reasoning, while the 1DCNN model further enhances performance through effective feature extraction from network traffic data. The hybrid Fuzzy + 1DCNN approach achieves higher accuracy by combining

uncertainty handling with deep feature learning. However, the proposed IVS-AVOA-HC method consistently outperforms all other techniques across all learning percentages, achieving the highest accuracy even at lower training data levels. This superior performance indicates the effectiveness of the proposed framework in optimizing feature selection, learning discriminative patterns, and accurately identifying intrusion activities in IoT networks.

Figure (b) presents the F1-score comparison, which is a crucial metric for intrusion detection systems as it balances both precision and recall, especially in scenarios involving imbalanced datasets. Similar to the accuracy results, the F1-score increases for all models as the learning percentage grows, showing improved classification balance with more training data. DNN and RNN models exhibit lower F1-scores due to higher misclassification rates, whereas fuzzy and 1DCNN approaches show better performance by reducing false alarms and missed detections. The hybrid Fuzzy + 1DCNN method further improves the F1-score by effectively integrating fuzzy inference with deep learning features. Nevertheless, the proposed IVS-AVOA-HC technique achieves the highest F1-score at all learning percentages, demonstrating its strong ability to accurately detect intrusions while maintaining a low false positive and false negative rate.

Overall, the figure clearly indicates that the proposed IDS framework provides superior and consistent performance compared to existing methods in terms of both accuracy and F1-score. The consistent improvement across varying learning percentages highlights the robustness, scalability, and effectiveness of the proposed approach for real-time intrusion detection in IoT environments. This makes the proposed IVS-AVOA-HC method highly suitable for deployment in resource-constrained and security-critical IoT applications.

CONCLUSION :

The paper introduces a comprehensive and innovative intrusion detection system (IDS) designed specifically to address the growing security challenges in Internet of Things (IoT) environments. Given the heterogeneous, resource-constrained, and highly connected nature of IoT networks, traditional intrusion detection approaches often fail to deliver sufficient accuracy, adaptability, and efficiency. To overcome these limitations, the proposed work develops a hybrid intrusion detection framework that strategically integrates hybrid classifiers (HC) with an advanced optimization technique known as the Improved Vulture Starvation-based African Vultures Optimization Algorithm (IVS-AVOA).

At the core of the proposed framework lies an intelligent feature weighting and selection mechanism, where IVS-AVOA plays a critical role in optimizing the most informative features from high-dimensional network traffic data. By assigning appropriate weights to features, the system reduces redundancy and noise, thereby improving detection accuracy while also lowering computational overhead. This optimization step ensures that the classifiers focus on the most relevant behavioral patterns associated with both normal and malicious network activities, which is particularly important in dynamic IoT scenarios.

The detection phase employs a hybrid classification strategy that combines fuzzy logic and a one-dimensional Convolutional Neural Network (1DCNN). The fuzzy logic component effectively handles uncertainty, imprecision, and overlapping boundaries in network traffic patterns, which are common in real-world IoT data. It enables rule-based reasoning and interpretability, making the system more robust to ambiguous attack behaviors. In parallel, the 1DCNN captures complex temporal and spatial relationships within sequential network data by automatically learning deep hierarchical features. The fusion of these two classifiers results in a powerful hybrid model that leverages the interpretability of fuzzy systems and the strong feature-learning capability of deep learning.

Extensive experimental evaluations were conducted to validate the effectiveness of the proposed IVS-AVOA-HC-based IDS. The results clearly demonstrate that the proposed framework significantly outperforms several widely used conventional and deep learning-based classifiers, including standalone Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), fuzzy models alone, 1DCNN alone, and even a basic hybrid Fuzzy-1DCNN model without optimization. The improvements are particularly evident in terms of detection accuracy, indicating the system's enhanced ability to correctly identify both known and unknown intrusion patterns while minimizing false alarms.

Overall, the analysis strongly confirms that the integration of IVS-AVOA for optimized feature weighting with a hybrid fuzzy-1DCNN classifier leads to a highly efficient and reliable intrusion detection framework. The proposed IDS not only improves detection accuracy but also enhances scalability and adaptability, making it well-suited for real-time IoT security applications. Consequently, this work provides a robust and effective alternative to existing intrusion detection approaches, offering superior security assurance for IoT devices and networks in comparison to traditional and standalone machine learning or deep learning methods.

REFERENCES :

1 . Abdollahzadeh, B., F. S. Gharehchopogh, and S. Mirjalili. 2021. African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems. Computers & Industrial Engineering 158:107408. **2 .** Alkadi, O., N. Moustafa, B. Turnbull, and K.-K R. Choo. 2021. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal 8 (12):9463–72. doi:10.1109/JIOT.2020.2996590.

3.Babu, M. R., and K. N. Veena. 2021. Implementing optimized classifier for distributed attack detection and BAIT-based attack correction in IoT. International Journal of System Assurance Engineering and Management. doi:10.1007/s13198-021-01115-w.

4 . Basati, A., and M. M. Faghih. 2022. PDAE: Efficient network intrusion detection in IoT using parallel deep auto-encoders. Information Sciences 598:57–74.

5 . Bedi, P., S. Mewada, R. A. Vatti, C. Singh, K. S. Dhindsa, M. Ponnusamy, and R. Sikarwar. 2021. Detection of attacks in IoT sensors networks using machine learning algorithm. Microprocessors and Microsystems 82:103814. doi:10.1016/j.micpro.2020.103814.

6 . Bhosale, S. A., and S. S. Sonavane. 2021. Wormhole attack detection system for IoT network: A hybrid approach. Wireless Personal Communications 124:1081–108.

7 . Chowdhury, N., and M. A. Kashem. 2008. A comparative analysis of Feed-forwards neural network & Recurrent Neural network to detect intrusion. 2008 International Conference on Electrical and Computer Engineering. doi:10.1109/ICECE.2008.4769258.

8 . Ciklabakkal, E., A. Donmez, M. Erdemir, E. Suren, M. K. Yilmaz, and P. Angin. 2019. ARTEMIS: An intrusion detection system for MQTT attacks in internet of things. 2019 38th Symposium on Reliable Distributed Systems (SRDS). doi:10.1109/SRDS47363.2019. 00053.

9. Haripriya, A. P., Kulothungan, K. 2019. Secure-MQTT: An efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. EURASIP Journal on Wireless Communications and Networking 2019:90. doi:10.1186/s13638-0191402-8.

10 . Huang, C., L. Wang, R. S.-C. Yeung, Z. Zhang, H. S.-H. Chung, and A. Bensoussan. 2018. A prediction model-guided Jaya algorithm for the PV system maximum power point tracking. IEEE Transactions on Sustainable Energy 9 (1):45–55.

11 . Jithu, P., J. Shareena, A. Ramdas, and A. P. Haripriya. 2021. Intrusion detection system for IoT botnet attacks using deep learning. SN Computer Science 2:205. doi:10.1007/s42979021-00516-9.

12 . Kan, X., Y. Fan, Z. Fang, L. Cao, N. N. Xiong, D. Yang, and X. Li. 2021. A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network. Information Sciences 568:147–62. doi:10.1016/j.ins.2021. 03.060.

13 . Ke, L., Y. Yang, X. Liu, and Y. Liu. 2021. Fault diagnosis of modular multilevel converter based on 1DCNN and LSTM network. 2021 China Automation Congress (CAC), 7441–6.

14 . Krishna, E. S. P., and A. Thangavelu. 2021. Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm. International Journal of System Assurance Engineering and Management. doi:10.1007/ s13198-021-01150-7.

15 . Kumar, P. M., and U. D. Gandhi. 2020. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. The Journal of Supercomputing 76 (6):3963–83. doi:10.1007/s11227-017-2169-5.

16 . Kumar, P., G. P. Gupta, and R. Tripathi. 2021. Toward, design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks. Arabian Journal for Science and Engineering 46 (4):3749–78. doi:10.1007/s13369-020-05181-3.

17 . Kunang, Y. N., S. Nurmaini, D. Stiawan, Zarkasi, and J. Firdaus. 2018. Automatic features extraction using autoencoder in intrusion detection system. International Conference on Electrical Engineering and Computer Science (ICECOS).

18 . Li, F., R.-J. Zhao, S. Wang, L.-B. Chen, A. W.-C. Liew, and W. Ding. 2022. Online intrusion detection for IoT systems with full Bayesian possibilistic clustering and ensembled fuzzy classifiers. IEEE Transactions on Fuzzy Systems 30 (11):4605–17. doi:10.1109/ TFUZZ.2022.3165390.

19 . Li, R., Q. Li, J. Zhou, and Y. Jiang. 2021. ADRIoT: An edge-assisted anomaly detection framework against IoT-based network attacks. IEEE Internet of Things Journal 9 (13): 10576–87. doi:10.1109/JIOT.2021.3122148.

20 . Liu, J., D. Yang, M. Lian, and M. Li. 2021. Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access 9:38254–68. doi:10.1109/ACCESS.2021. 3063671.