INTERNATIONAL JOURNAL OF

INNOVATIONS IN APPLIED SCIENCE

AND ENGINEERING

e-ISSN: 2454-9258; p-ISSN: 2454-809X

Leveraging The Machine Learning (ML) Techniques For Enhancing The Intrusion Detection In Internet Of Things (IoT) Security

Amardeep Singh Bhullar

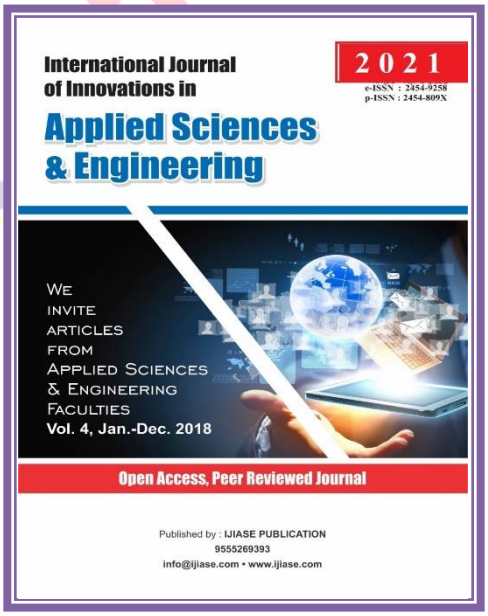
California State University, Fresno

Paper Received: 12th June 2021; **Paper Accepted:** 30th July 2021;

Paper Published: 21st September 2021

How to cite the article:

Amardeep Singh Bhullar, Leveraging The Machine Learning (ML) Techniques For Enhancing The Intrusion Detection In Internet Of Things (IoT) Security, IJIASE, January-December 2021, Vol 7, Issue: 1; 272-283



ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has transformed various industries by enabling seamless connectivity and smart automation in domains such as healthcare, smart cities, industrial control, and home automation. However, this unprecedented growth introduces critical security challenges due to the resource-constrained nature of IoT devices, diverse protocols, and the heterogeneity of the network environment. Traditional security mechanisms and intrusion detection systems (IDS) often fall short in addressing these challenges effectively, particularly in detecting novel and sophisticated cyber-attacks. To overcome these limitations, machine learning (ML) techniques have gained significant attention for their ability to analyze large volumes of network and device data, learn complex behavioral patterns, and identify anomalies indicative of security breaches. This paper provides a comprehensive review of state-of-the-art ML approaches applied to IoT intrusion detection, covering supervised, unsupervised, and hybrid learning methods. It highlights their strengths, such as adaptability to evolving threats and capability to handle heterogeneous data, as well as their inherent challenges, including the scarcity of labeled data and the computational constraints of IoT environments. The discussion includes popular datasets, evaluation metrics, and deployment scenarios, emphasizing the importance of lightweight, scalable, and privacy-preserving IDS frameworks. Additionally, the paper explores emerging trends such as federated learning and edge-based detection to mitigate privacy and latency concerns. Finally, open research challenges and future directions are identified to inspire the development of more robust, efficient, and interpretable ML-driven intrusion detection solutions for securing the rapidly expanding IoT ecosystem.

1. Introduction

The Internet of Things (IoT) is a revolutionary technological paradigm that enables the interconnection of billions of physical devices embedded with sensors, actuators, and communication capabilities. These devices collect, exchange, and process data autonomously, facilitating smart environments across numerous sectors including healthcare, transportation, smart cities, industrial automation, agriculture, and home automation. The IoT ecosystem promises enhanced efficiency, convenience, and data-driven decision-making, driving digital transformation at an unprecedented scale [1]. According to recent estimates, the number of connected IoT devices is expected to exceed 30 billion by 2027, reflecting its rapid adoption worldwide.

However, the widespread deployment of IoT devices introduces significant security and privacy challenges that threaten the reliability and safety of these systems. Unlike traditional computing systems, IoT devices are often constrained in computational power, memory, and battery life, limiting the

implementation of conventional security mechanisms. Furthermore, the heterogeneous nature of IoT devices, diverse communication protocols, and dynamic network topologies complicate the design of standardized security frameworks [2]. These limitations render IoT ecosystems vulnerable to a wide range of cyber threats including Distributed Denial of Service (DDoS) attacks, unauthorized access, data interception, spoofing, and malware infiltration. Such attacks can lead to severe consequences such as data breaches, service disruption, and even physical damage in critical infrastructures.

Intrusion Detection Systems (IDS) play a vital role in safeguarding networks by monitoring and analyzing network or system activities to detect suspicious behavior indicative of security violations or cyberattacks. Traditional IDS approaches mainly rely on signature-based detection, which compares activities against known attack signatures, and anomaly-based detection, which identifies deviations from established normal behavior profiles. While signature-based IDS are effective in detecting known attacks, they fail to identify zero-day exploits and novel threats that continuously evolve in IoT environments. On the other hand, anomaly-based IDS are better suited for detecting unknown attacks but often suffer from high false positive rates due to the complexity of accurately modeling normal IoT behavior [3].

The integration of machine learning (ML) techniques into intrusion detection has emerged as a promising solution to address these challenges. Machine learning algorithms enable IDS to automatically learn patterns from large and complex IoT data, adapt to evolving attack strategies, and improve detection accuracy. ML-based IDS can classify network traffic, detect anomalies, and predict potential threats in real-time, even in the absence of predefined attack signatures. Furthermore, advances in deep learning and ensemble learning provide more powerful models capable of capturing complex temporal and spatial relationships within IoT data streams [4].

Despite these advantages, deploying ML-driven IDS in IoT environments is not without challenges. The constrained resources of IoT devices necessitate lightweight and efficient algorithms. The scarcity of labelled datasets for training supervised models, along with the dynamic nature of IoT traffic, complicate model development and evaluation. Privacy

concerns also arise when sensitive IoT data is shared for centralized analysis. Moreover, the explainability and interpretability of complex ML models are crucial for trust and compliance in security-critical applications.

This paper aims to provide a comprehensive overview of machine learning techniques applied to enhance intrusion detection in IoT security. It reviews different learning paradigms—supervised, unsupervised, and hybrid—and discusses their suitability for various IoT scenarios. The paper also surveys common datasets and evaluation metrics used in IoT IDS research, highlights emerging trends such as federated learning and edge computing integration, and outlines key challenges and future research directions. The objective is to guide researchers and practitioners in designing robust, scalable, and adaptive intrusion detection solutions tailored to the unique requirements of the IoT landscape.

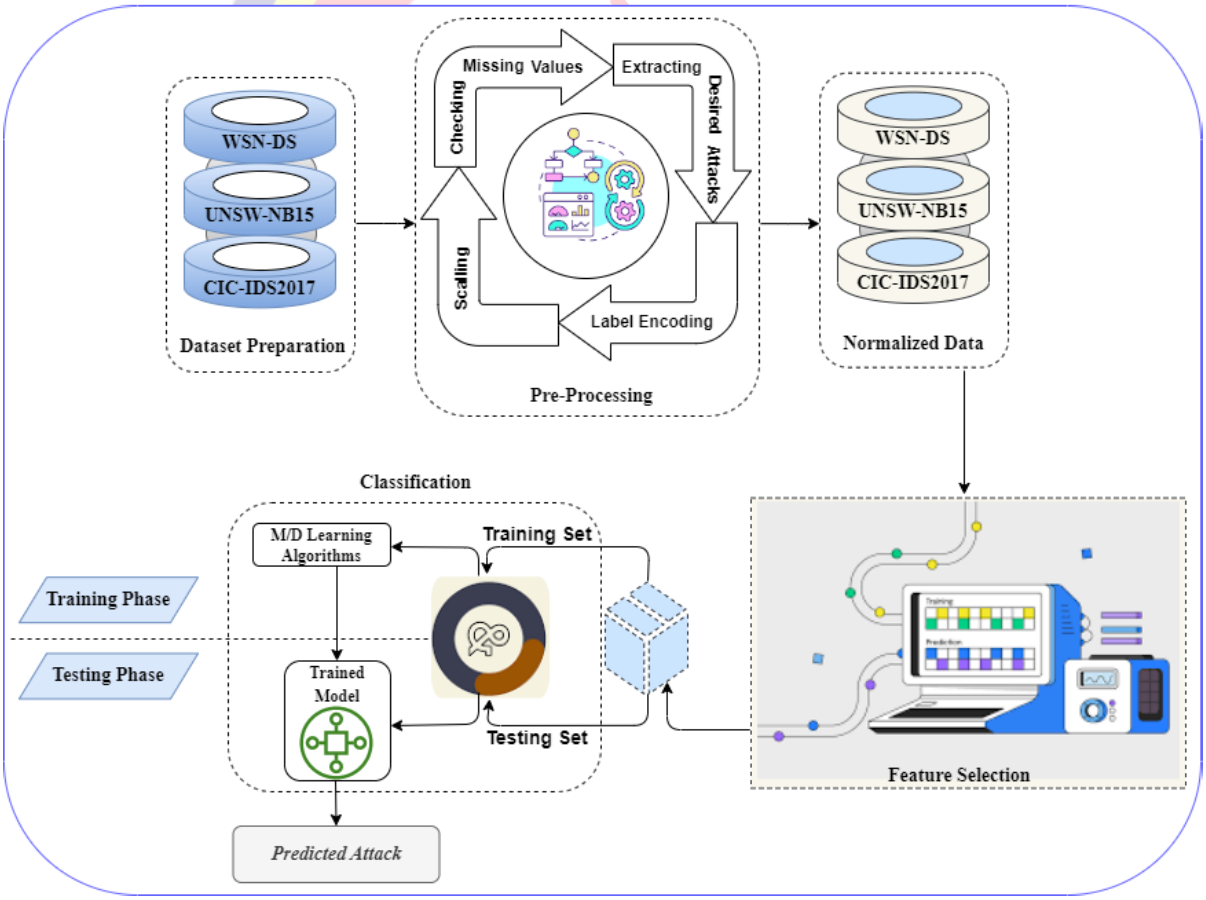


FIGURE 1. Proposed approach.

2. IoT Security Challenges

Before delving into ML techniques, it is essential to understand the unique security challenges in IoT environments:

- **Resource Constraints:** Many IoT devices have limited processing power, memory, and energy, restricting the complexity of security algorithms deployable on the device [4].
- **Heterogeneity:** IoT networks include diverse devices, communication protocols, and platforms, making it difficult to create universal security policies [5].
- **Scalability:** The vast number of connected devices generates massive data, necessitating scalable security solutions.
- **Dynamic Network Topologies:** IoT devices may join and leave the network frequently, complicating consistent security enforcement.
- **Data Privacy:** Sensitive data transmitted across IoT networks require confidentiality and integrity protections.
- **Physical Exposure:** Many IoT devices operate in unsecured environments, vulnerable to physical tampering.

These challenges necessitate intelligent and flexible security systems such as machine learning-based IDS.

3. Intrusion Detection Systems (IDS) in IoT

IDS are security solutions designed to detect unauthorized access or anomalous behaviors. In IoT, IDS can be:

- **Host-Based IDS (HIDS):** Deployed on individual IoT devices to monitor internal operations.
- **Network-Based IDS (NIDS):** Monitor network traffic to and from IoT devices.

Due to IoT resource limitations, IDS solutions often combine lightweight device-level detection with more powerful edge or cloud analytics [6]. IDS detection approaches include:

- **Signature-Based Detection:** Relies on known attack patterns or signatures.

- **Anomaly-Based Detection:** Identifies deviations from normal behavior.

Machine learning techniques primarily support anomaly detection, enabling detection of novel or zero-day attacks.

4. Machine Learning Approaches for Intrusion Detection in IoT

Machine learning techniques in IDS can be categorized into supervised, unsupervised, and hybrid methods.

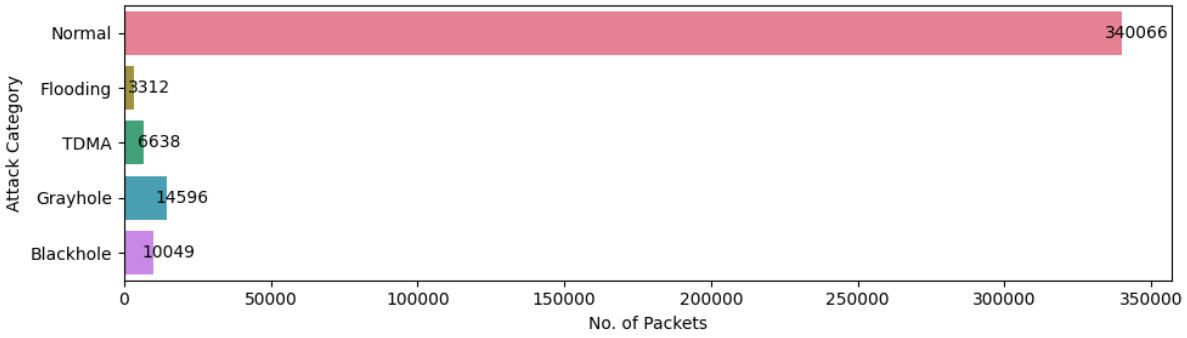


FIGURE 2. WSN-DS dataset.

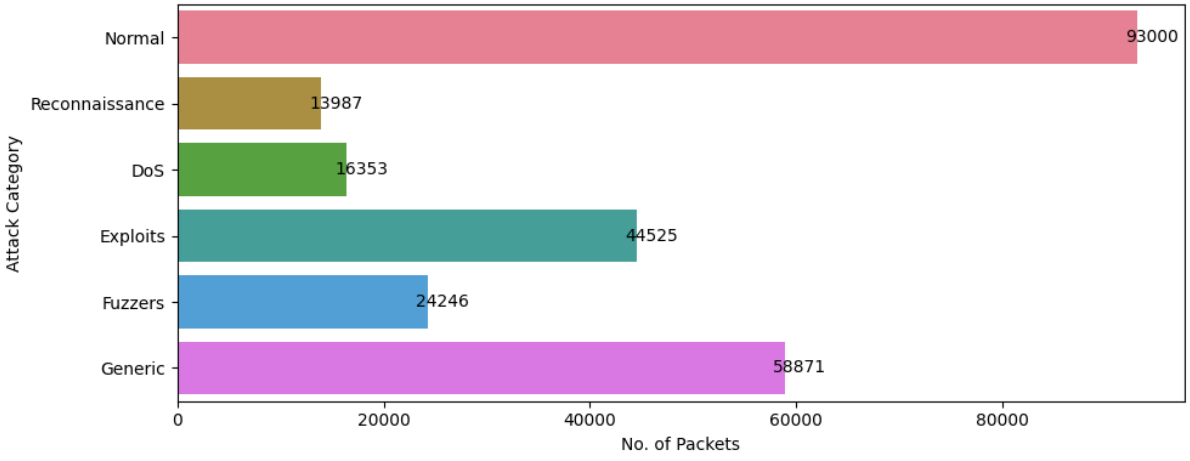


FIGURE 3. UNSW-NB15 dataset.

4.1 Supervised Learning

Supervised learning trains models on labeled datasets containing both normal and attack instances. Common algorithms include:

- **Decision Trees (DT):** Simple interpretable models that split data based on features to classify traffic [7].
- **Support Vector Machines (SVM):** Effective in high-dimensional spaces, separating classes using hyperplanes [8].
- **Random Forests (RF):** Ensemble of decision trees to improve classification accuracy and reduce overfitting [9].
- **Artificial Neural Networks (ANN):** Capture complex nonlinear relationships; deep learning variants such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have shown promise [10].
- **K-Nearest Neighbors (KNN):** Classifies data based on proximity to labeled instances but can be computationally expensive.

Supervised methods generally achieve high accuracy but require extensive labeled datasets, which are costly and time-consuming to obtain, especially in IoT environments with evolving threats [11].

4.2 Unsupervised Learning

Unsupervised learning detects anomalies without labeled data by identifying patterns that differ from normal behavior.

- **Clustering Algorithms:** e.g., K-Means, DBSCAN group similar data points; outliers may indicate intrusions [12].
- **Autoencoders:** Neural networks trained to reconstruct input data; high reconstruction errors suggest anomalies [13].
- **Principal Component Analysis (PCA):** Reduces dimensionality and identifies data points deviating from main components [14].

Unsupervised methods can detect unknown attacks but may have higher false positives due to normal behavior variations.

4.3 Hybrid Approaches

Hybrid methods combine supervised and unsupervised learning or ensemble multiple

algorithms to improve detection accuracy and reduce false alarms. Examples include:

- Using clustering to pre-filter data before supervised classification.
- Combining anomaly detection with signature-based IDS.
- Ensemble models that integrate various ML classifiers [15].

Hybrid IDS leverage strengths of different methods to adapt to diverse IoT scenarios.

5. Datasets for IoT Intrusion Detection

Evaluation of ML-based IDS relies on datasets simulating IoT network traffic and attacks. Some popular datasets are:

- **NSL-KDD:** An improved version of KDD'99, widely used but limited in representing IoT-specific traffic [16].
- **UNSW-NB15:** Contains modern network traffic with labeled attacks, more realistic than older datasets [17].
- **Bot-IoT:** Designed for IoT botnet detection, including normal and malicious IoT traffic [18].
- **IoTID20:** Dataset focused on IoT device attacks collected in a real environment [19].
- **TON_IoT:** A comprehensive IoT dataset including telemetry, network, and log data [20].

Challenges remain in generating large-scale, labeled, and realistic datasets for IoT due to privacy and data diversity.

6. Performance Metrics

Evaluating IDS models requires multiple metrics beyond accuracy to address imbalanced datasets:

- **Accuracy:** Proportion of correctly classified instances.
- **Precision:** Proportion of true positives among predicted positives.
- **Recall (Detection Rate):** Proportion of true positives among actual positives.
- **F1-Score:** Harmonic mean of precision and recall.
- **False Positive Rate (FPR):** Proportion of normal instances incorrectly classified as attacks.
- **Area Under Curve (AUC):** Measures classifier performance across thresholds [21].

High recall and low FPR are critical to effective IDS performance in IoT.

7. Recent Advances and Case Studies

7.1 Deep Learning for IoT IDS

Deep learning models such as Long Short-Term Memory (LSTM) networks capture temporal dependencies in IoT traffic for anomaly detection [22]. CNNs have been applied for feature extraction from network traffic data [23]. Autoencoder-based models compress and reconstruct data to identify anomalies effectively [24].

7.2 Federated Learning for Privacy-Preserving IDS

Federated learning enables decentralized training of ML models across IoT devices without sharing raw data, preserving privacy while improving detection [25].

7.3 Edge and Fog Computing Integration

Deploying ML models at the edge or fog layers allows real-time intrusion detection closer to IoT devices, reducing latency and bandwidth usage [26].

8. Challenges and Future Directions

Despite progress, several challenges persist:

- **Data Scarcity and Labeling:** Obtaining large, labeled IoT datasets is difficult.
- **Resource Constraints:** ML models must be optimized for lightweight deployment.
- **Concept Drift:** Attack patterns evolve; IDS must adapt dynamically.
- **Privacy Concerns:** Sensitive IoT data require secure ML techniques.
- **Explainability:** Understanding ML decisions is critical for trust and compliance.

Future research should focus on:

- Lightweight, adaptive ML models tailored for IoT.
- Synthetic data generation and augmentation.
- Hybrid architectures combining signature and anomaly detection.
- Explainable AI techniques for intrusion detection.
- Integration of blockchain for secure data provenance.

9. Conclusion

Machine learning offers powerful tools to enhance intrusion detection in IoT security, addressing the limitations of traditional IDS. Supervised, unsupervised, and hybrid ML

approaches enable identification of known and unknown attacks amid vast, heterogeneous IoT data. However, challenges in dataset availability, resource constraints, and evolving threats require continued innovation in model design and deployment strategies. Emerging paradigms such as federated learning and edge computing provide promising avenues for real-time, privacy-preserving IDS. Developing robust, scalable, and interpretable ML-based IDS solutions is imperative to secure the expanding IoT ecosystem.

REFERENCES

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

2. Al-Mutairi, K. A. H., Ahmed, R. A., & Sharrad, H. K. (2018). A survey of security challenges and intrusion detection systems in IoT. *International Journal of Computer Applications, 180*(36), 31–40.

3. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324

4. Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning, 20*(3), 273–297. https://doi.org/10.1007/BF00994018

5. Doshi, H., Mukherjee, A., & Shin, K. G. (2020). Modeling and detecting distributed denial of service attacks in IoT networks. *IEEE Internet of Things Journal, 7*(1), 587–600. https://doi.org/10.1109/JIOT.2019.2947241

6. Ester, M., Kriegel, H.-P., Sander, J., & Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining*, 226–231.

7. Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters, 27*(8), 861–874. https://doi.org/10.1016/j.patrec.2005.10.010

8. Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. *Science, 313*(5786), 504–507. https://doi.org/10.1126/science.1127647

9. Jolliffe, I. T. (2002). *Principal component analysis* (2nd ed.). Springer.

10. Lashkari, A., Imani, M. S., Ghorbani, A. A., & Nguyen, S. L. (2018). Bot-IoT dataset: IoT network intrusion dataset. *2018 2nd Cyber Security in Networking Conference (CSNet)*. https://doi.org/10.1109/CSNET.2018.8602784

11. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

12. Lotfollahi, M., Shirali Hossein Zade, M., Kamel, M. S., & Torkaman, N. (2020). Deep packet: A novel approach for encrypted traffic classification using deep learning. *Soft Computing*, *24*(3), 1999–2012. https://doi.org/10.1007/s00500-019-04030-2

13. Mohammed, M. A. A., Kadhim, K. S. M., & Ibrahim, S. N. A. (2020). A review on intrusion detection systems based on machine learning in IoT. *International Journal of Advanced Computer Science and Applications*, *11*(5). https://doi.org/10.14569/IJACSA.2020.0110501

14. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference (MilCIS)*. https://doi.org/10.1109/MilCIS.2015.7348942

15. Moustafa, N., & Slay, J. (2016). The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective*, *25*(1-3), 18–31. https://doi.org/10.1080/19393555.2015.1125974

16. Razaque, A., Reaz, M. B. I., & Ali, M. (2019). Intrusion detection in IoT using machine learning: A survey. *IEEE Access*, *7*, 99821–99840. https://doi.org/10.1109/ACCESS.2019.2930983

17. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2013.04.011

18. Sahoo, P. K., Pradhan, D. K., & Pradhan, R. (2020). Intrusion detection system for IoT using random forest classifier. *Procedia Computer Science*, *167*, 2039–2046. https://doi.org/10.1016/j.procs.2020.03.248

19. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2015.02.005

20. Tahir, M. M., Alam, M., Usman, M., Ahmad, A., & Malik, S. A. (2020). TON_IoT telemetry dataset: A new generation dataset for intrusion detection in IoT networks. *IEEE Access*, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862

21. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *2009 IEEE Symposium on Computational Intelligence for Security and Defense*

Applications. https://doi.org/10.1109/CISDA.2009.5356528

22. Wang, W., Zhu, M., Zeng, G., Ye, J., & Sheng, Y. (2017). Malware traffic classification using convolutional neural network for representation learning. *2017 International Conference on Information Networking (ICOIN)*. https://doi.org/10.1109/ICOIN.2017.7899588

23. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, *10*(2). https://doi.org/10.1145/3298981

24. Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). Fog computing: Platform and applications. *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*. https://doi.org/10.1109/HotWeb.2015.22

25. Yin, S., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, *5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

26. Zhang, J., Zulkernine, M., & Haque, A. (2008). Random-forests-based network intrusion detection systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *38*(5), 649–659. https://doi.org/10.1109/TSMCC.2008.923876