Journal of Integrated
SCIENCE & TECHNOLOGY

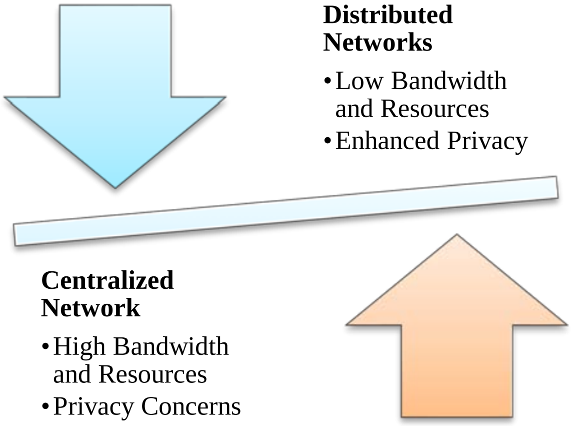
A review on intrusion detection system for distributed network based on Machine Learning

Vineeta Shrivastava,* Anoop Kumar Chaturvedi

Department of Computer Science & Engineering, Lakshmi Narain College of Technology Excellence, LNCT University, Bhopal, M.P., India.

Received on: 01-Aug-2023, Accepted and Published on: 12-Oct-2023

ABSTRACT



The distributed mobility management (DMM) in ID/locator separation architectures has recently received extensive attention to provide load-balanced and scalable mobility services. Since IDs cannot be aggregated, it has limitations in terms of network mobility (NEMO) support. The benefits of decentralized systems over centralized systems along with security issues and distributed systems' challenges form the basis of current work. A wider perspective has been envisioned while examining various intrusion detection strategies and potential applications of blockchain technology, which has drawn significant interest from both academia and business about supply chain management, open banking, online payment, and other areas. The processing of IDSs involves integrating blockchain technology to improve Collaborative IDSs (CIDSs). Blockchain's decentralized and tamper-resistant data storage enables secure information sharing among CIDS nodes without a central authority. This enhances detection and response capabilities, and blockchain also facilitates post-incident analysis and forensics.

Keywords: Unified Threat Management, Distributed Network, Internet of Medical Things, Network Latency, Intrusion Detection System

INTRODUCTION

Securing network systems is a pivotal component of information technology security. Devices such as firewalls, network-based intrusion detection and prevention systems (NIDS/NIPS), and unified threat management (UTM) tools play a significant role in identifying and thwarting attacks targeting the network. Firewalls focus on filtering certain traffic types to bolster security, whereas NIDS/NIPS aims to identify and counteract potentially harmful network activities. A combined approach using both firewalls and NIDS/NIPS can amplify the defense against network breaches. UTM tools amalgamate the features of firewalls, NIDS/NIPS, and more, offering detection capacities akin to their standalone counterparts. Another technique, Deep Packet Inspection (DPI), delves into the application layer, facilitating the discernment of different applications and their data. Although DPI boosts the precision of intrusion detection, it demands more time when juxtaposed with conventional packet header scrutiny. This study delves into the utility of NIDS within the broader landscape of detecting network-based threats.

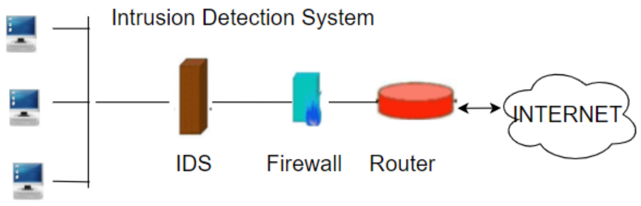


Figure 1. Intrusion Detection System

*Corresponding Author: Vineeta Shrivastava, Assistant Professor, Department of Computer Science & Engineering, Lakshmi Narain College of Technology Excellence, Bhopal.
Email shrivastavavinita21@gmail.com
Tel (M): +91 9575448606

Cite as: *J. Integr. Sci. Technol., 2024, 12(2), 739. URN:NBN:sciencein.jist.2024.v12.739*

ISSN: 2321-4635
http://pubs.thesciencein.org/jist

This study explores Network Intrusion Detection Systems (NIDS) that leverage machine learning. These systems aim to autonomously identify both familiar and novel threats to a network by deriving patterns and insights from the underlying data. The machine learning methods used for NIDS can be classified into three categories: statistics-based, data mining-based, and classification-based. These methods extract low-level features from the data and utilize rules or models to identify intrusions. Utilizing machine learning methodologies, NIDS can proficiently scrutinize network data, pinpointing unfamiliar threats through patterns discerned from both anomalous and regular network activities. This study underscores several unresolved challenges in the realm of intrusion detection, indicating areas that warrant deeper investigation:

- Rapidly Changing Network Environments and Training Data: The continuous advent of novel attack methodologies causes network settings and intrusion training datasets to undergo swift transformations. The increasing size of training data poses a challenge for handling it effectively. Existing algorithms are mostly offline, leading to time-consuming periodic retraining. Online training, which updates the detector with new data and discards old data, is more suitable for dynamic intrusion detectors. However, maintaining accuracy during online training remains a challenge.
- Handling Various Attribute Types in Network Connection Data: Network connection records encompass a mix of attribute types, from categorical to numerical, each with its spectrum of values. Integrating this multifaceted data, while preserving its inherent information, is pivotal for ensuring the efficacy of intrusion detection systems.
- Centralized vs. Distributed Intrusion Detection: Centralized Intrusion Detection Systems (IDS) process all network data centrally, consuming significant bandwidth and resources, with potential privacy concerns for local node data. Alternatively, Distributed IDS reduces data communication and computational load by sharing models learned at local nodes, offering enhanced privacy protection.

Intrusion Detection in Decentralized Network

The decentralized intrusion detection framework operates on the premise that every node generates its localized intrusion detection model, drawing upon its specific data. These individualized models are subsequently aggregated to formulate a comprehensive global model at each respective node. This aggregation is based on a limited selection of samples from the node in question. Importantly, there's no interchange of raw training data between the nodes. The globally synthesized model is then employed for intrusion detection tasks at its node. This architecture is underpinned by three primary components: data refinement, individual node models, and overarching global models, as depicted in Figure 2.

The prevalence of distributed networks is on the rise, with Secure Access Service Edge (SASE) and Edge computing for IoT standing out as notable instances. SASE provides a dispersed network framework tailored for remote teams, ensuring secure pathways to applications and services via distinct SASE nodes. On the other hand, Edge computing for IoT deploys various edge processing nodes, ensuring brisk network connectivity for the acquisition and interpretation of data in IoT setups.

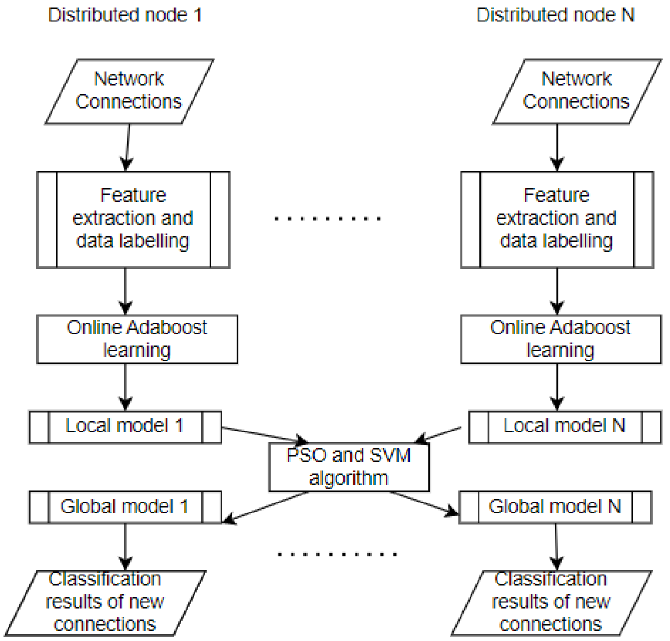


Figure 2. Overview of the intrusion detection framework

When assessing diverse network frameworks, such as centralized, decentralized, and distributed, each presents unique characteristics. Centralized networks have endpoints linking to a solitary application or resource, operating in a client-server dynamic, which may be susceptible to disruptions. Conversely, distributed networks embrace a modular approach; these networks comprise interconnected server clusters that collaboratively allocate resources and reroute users for enhanced dependability and application efficiency. This methodology bolsters fail-safety and minimizes the likelihood of significant disruptions.

For instance, traditional remote access VPN designs, especially in the context of remote teams, frequently rely on a centralized layout with a unique VPN gateway at the enterprise network boundary, creating potential vulnerability. Distributed frameworks present a sturdier alternative by capitalizing on modular setups to amplify redundancy and efficacy. Figure 3 elucidates the structural variances between centralized and distributed systems.

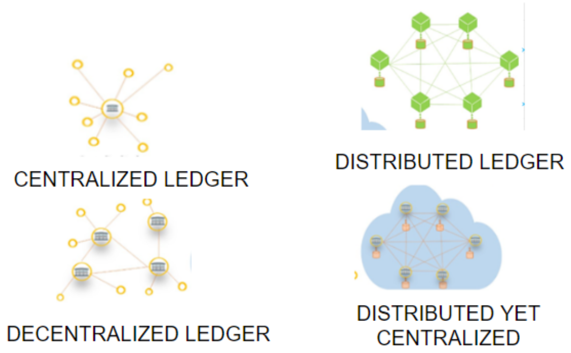


Figure 3. Centralized vs. Distributed System

In comparing decentralized and distributed networks, their distinct differences become evident. Decentralized networks disperse workloads, services, and data across specific locations, relying on each other for operation, while distributed networks contain all necessary resources at each node, enabling independent functioning. Decentralized networks lack a centralized control plane, managing workloads separately, whereas distributed networks typically have a central control mechanism.

Distributed networks offer various advantages, including increased redundancy, improved application performance, and scalability. However, they also present challenges such as managing complexity, ensuring data consistency, and maintaining security. As businesses undergo digital transformation and rapid shifts in technology, distributed networks prove beneficial in adapting to these changes. Examples of these shifts include virtualization, cloud computing, containers, edge computing, and remote work policies. Distributed networks offer flexibility, scalability, efficient resource utilization, enhanced application performance, and improved resilience, meeting the demands of modern technology and remote work environments.

Distributed networks offer several advantages, such as improved application and service reliability, easy scalability, flexibility in traffic flows, and centralized control. Each node in a distributed network can operate independently, ensuring better reliability as outages in one section do not lead to service disruptions. Scalability is achieved by adding or removing nodes as needed for desired redundancy and performance. The network can reconfigure traffic flows rapidly to accommodate new applications or changes in usage, avoiding bottlenecks and ensuring efficient data flow. Additionally, distributed networks offer centralized control for unified management of network performance configurations and security policies across all nodes, ensuring consistency and uniformity.

A distributed network consists of independently run networks that are collectively managed, often geographically separated, providing improved reliability and performance across various locations. Despite operating independently, the management and monitoring of the networks are centralized, allowing for unified policies and comprehensive visibility through a single NetOps management panel. This enables better service resiliency, performance, and resource sharing among the networks.

There are several types of distributed networks, each with its unique characteristics and use cases:

- Client/Server Systems: This basic communication method involves clients sending requests to servers, which respond with the required output. Multiple servers can be utilized in this system.
- Peer-to-Peer Systems: In this decentralized model, each node can function as both a client and a server. Nodes perform tasks on their local memory and communicate directly with other nodes without any hierarchical structure.
- Middleware: Middleware serves as an intermediary application between two separate applications, providing services to both and enabling data transfer between them.
- Three-tier: This system uses separate layers and servers for different functions of a program, with client data stored in the middle tier. It is commonly used in web or online applications.
- N-tier: Also known as a multitier distributed system, N-tier systems can have any number of functions in the network. They are commonly used in web applications and data systems.

Each distributed network architecture has its specific roles and applications, as illustrated in Figure 4.

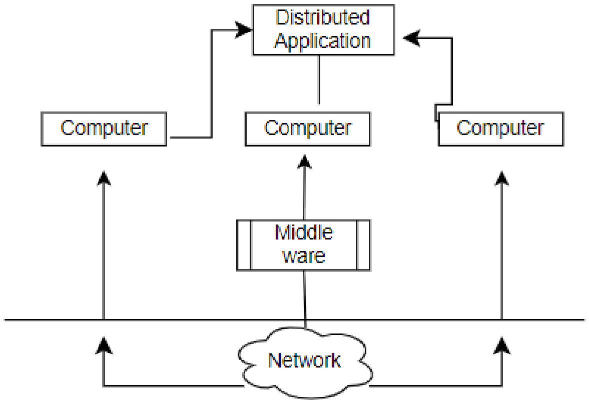
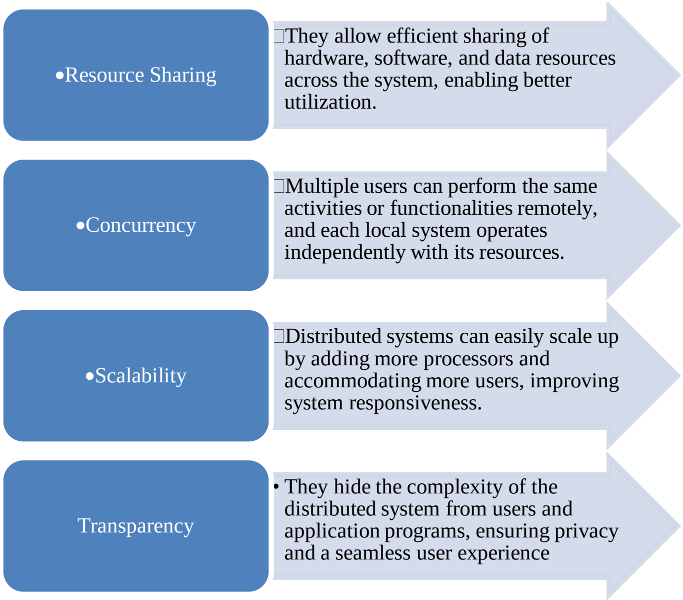


Figure 4. Types of Distributed Network

Characteristics of Distributed System

Distributed systems offer several key characteristics as presented in figure 5.


•Resource Sharing

They allow efficient sharing of hardware, software, and data resources across the system, enabling better utilization.

•Concurrency

Multiple users can perform the same activities or functionalities remotely, and each local system operates independently with its resources.

•Scalability

Distributed systems can easily scale up by adding more processors and accommodating more users, improving system responsiveness.

Transparency

• They hide the complexity of the distributed system from users and application programs, ensuring privacy and a seamless user experience

Figure 5. Characteristics of Distributed Network

Security Concerns

In summary, security in distributed systems encompasses several key concepts:

- Confidentiality: Ensuring that important data remains undisclosed and protected from unauthorized access.

- Data Integrity: Maintaining the accuracy and consistency of data throughout its lifecycle, preventing unauthorized modifications or destruction.
- Authentication: Establishing mutual trust between parties, and verifying the identity of involved parties to ensure authenticity.
- Authorization and Access Control: Managing access to authorized resources through secure access points, preventing unauthorized individuals from accessing the system.
- Non-Repudiation: Ensuring that parties cannot deny sending or receiving messages, providing proof of communication.
- Accountability: The ability to detect errors and identify responsible entities for system failures, addressing an important facet of security in distributed systems.

INTRUSION DETECTION IN USING SUPERVISED MACHINE LEARNING IN DISTRIBUTED NETWORK

Singh et al.[1] introduced a Dew-Cloud-based model employing Hierarchical Federated Learning (HFL) for secure IoMT applications, achieving 99.31% training accuracy. Shin et al.[2] developed a discretization technique for model training, with a classification accuracy of 0.9722 on the NSL-KDD dataset. Alasmary et al.[3] presented a defense strategy for IoT devices including a novel method, ShieldRNN, showing superior performance on the CIC-IDS2017 dataset. Siddii et al.[4] proposed a statistical approach for dataset normalization, achieving 98.27% accuracy. Bagaa et al.[5] introduced a framework combining supervised learning and neural networks, detecting anomalies with 99.71% accuracy. Finally, Loannau et al.[6] designed an SVM-based Intrusion Detection System (IDS) for IoT, achieving up to 99.8% accuracy. Das et al.[7] introduced a framework for detecting DDoS intrusions using machine learning ensemble techniques, enhancing both security and interpretability. Gohil et al.[8] achieved 96.25% accuracy in classifying DDoS attacks from legitimate flows using the CICDDoS2019 dataset and supervised classification algorithms. Zekri et al.[9] designed a DDoS detection system with 98.8% accuracy using the C.4.5 algorithm and signature detection. Rajimol et al.[10] showcased the effectiveness of ensemble-based classifiers, like Adaboost with Random Forest, for intrusion detection. Teixeira et al.[11] proposed a vote-based architecture for IDSs, achieving 98.2% accuracy and 96.7% precision. Yao et al.[12] introduced the MSML framework, which outperformed existing systems with 96.6% accuracy. Khonde et al.[13] improved detection accuracy and system performance using an intelligent IDS with ensembling techniques. Moulla et al.[14] achieved 99.44% accuracy with a novel network IDS. Divyatmika et al.[15] developed an autonomous network intrusion detection model with high true positive and low false positive rates. Ravipati et al.[16] evaluated machine learning algorithms for anomaly detection, identifying top performers. Anti et al.[17] proposed a three-layer intrusion detection system for IoT with high F-measures. Bertoli et al.[18] presented the AB-TRAP framework with an average f1-score of 0.95 and an area under the ROC curve of 0.98 for internet traffic. Dang et al.[19] suggested a method for selecting training data for Intrusion Detection Systems (IDSs) that enhances performance while minimizing costs. Rani et al.[20] introduced an efficient intrusion detection technique for IoT networks using the Random Forest classifier, boasting a 99.9% accuracy rate. Dina et al.[21] outlined two main classifications for network intrusions: signature-based and anomaly-based IDSs. Grammatikis et al.[22] developed the DIDEROT model, which uses both supervised and unsupervised machine learning alongside SDN technology to detect specific DNP3 cyberattacks. Baraneetharan et al.[23] provided a survey focusing on the application of machine learning techniques for security in Wireless Sensor Networks (WSNs). Ravi et al.[24] unveiled a comprehensive deep learning model, particularly utilizing recurrent architectures, for detecting and categorizing network attacks with high accuracy. Finally, Belavagi et al.[25] designed frameworks for intrusion detection classification and prediction, with their results underscoring the superior performance of the Random Forest Classifier compared to other methods.

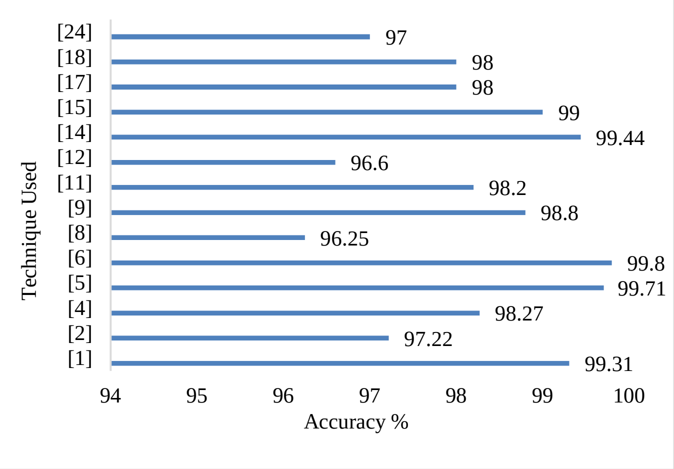


Figure 6. Comparison of accuracy of supervised machine learning algorithm

In Figure 6, a comparison of the accuracy of supervised machine learning algorithms for intrusion detection in distributed networks is presented.

INTRUSION DETECTION IN USING UNSUPERVISED MACHINE LEARNING IN DISTRIBUTED NETWORK

The provided list includes several research papers focusing on unsupervised machine-learning techniques for various aspects of intrusion detection and network security. Let's summarize the key contributions of each paper:

Nair et al.[26] introduced an unsupervised algorithm for fingerprinting LoRa-modulated chirps in RF signals, achieving 100% success in identifying legitimate and rogue transmitters. Singh et al.[27] presented a Dew-Cloud-based model with hierarchical federated learning, achieving 99.31% training accuracy and outperforming existing models in various metrics. Lefoane et al.[28] explored pattern-centric feature selection for botnet detection, with some models showing a 100% true positive rate and zero false positives. Wang et al.[29] developed a method using stacked contractive autoencoders for unsupervised feature derivation, improving detection efficiency. Alasmary et al.[3] presented ShieldRNN, a strategy for RNN/LSTM models, that excels in IoT device protection. Yang et al.[31] introduced Griffin, a NIDS using unsupervised learning for efficient intrusion detection. Pu et al.[32]

proposed a combination of Sub-Space Clustering and Class SVM for anomaly detection, outperforming other techniques. Lastly, Wen et al.[33] unveiled PSubCLUS, a parallel subspace clustering algorithm, ensuring efficient load balancing and parallel speedup for high-dimensional big data clustering.

Hanselmann et al.[34] unveiled CANet for intrusion detection in CAN networks, outperforming other ML methods. Zoppi et al.[35] reviewed unsupervised algorithms for zero-day attack detection. Filho et al.[36] introduced FID-GAN, an efficient unsupervised IDS for Cyber-Physical Systems. Xu et al.[37] proposed a 5-layer autoencoder model for network irregularity detection, outshining rivals in intrusion detection. Zavrak et al.[38] used unsupervised and semi-supervised learning for deviant network traffic detection, highlighting the effectiveness of the Variational Autoencoder. Chadza et al.[39] implemented a transfer learning approach for intrusion detection with high prediction accuracy. Xie et al.[40] presented a model for predicting parameters in industrial control systems, exhibiting excellent precision, recall, and F1-score. Rao et al.[41] introduced a two-stage hybrid intrusion detection method, surpassing conventional models in performance. Alom et al.[42] employed an Unsupervised Extreme Learning Machine for network intrusion detection with high accuracy. Lastly, Narsimhan et al.[43] developed a robust real-time CAN Intrusion Detection System.

Mighan et al.[44] proposed a hybrid deep network and machine learning scheme for large-scale network intrusion detection. Zanero et al.[45] introduced a two-tier architecture using unsupervised clustering and anomaly detection for efficient intrusion detection. Mokhtar et al.[46] achieved 98% accuracy in detecting stealthy attacks in control systems with unsupervised learning. Rawat et al.[47] identified an effective intrusion detection approach using Principal Component Analysis, comparing classical and deep learning methods. Casas et al.[48] proposed UNIDS, an effective system for detecting unknown network attacks without labeled data. Verkeren et al.[49] found autoencoders to be effective and computationally efficient in detecting malicious network behavior through unsupervised methods. Idrissi et al.[50] introduced EdgeIDS, an unsupervised IoT IDS based on GANs with high detection rates and low false positives. Zhang et al.[51] offered a privacy-preserving approach for anomaly-based intrusion detection in IIoT, outperforming baseline models with 95.97% accuracy for AdaBoost and 73.70% for Random Forest.

Houda et al.[52] introduced MiTFed, a framework allowing SDN domains to collaboratively develop intrusion detection models without sharing private datasets, using the Ethereum blockchain for decentralized collaboration. Nguyen et al.[53] improved the accuracy of cloud IDSs through two deep generative models designed to synthesize harmful samples. Brenner et al.[54] proposed a network-based intrusion detection system, focused on risk management and applicability in smart factories and similar cyber-physical systems. Kim et al.[55] developed Panop, an ANN-based Network Intrusion Detection System (NIDS) designed for distributed networks, providing high accuracy with minimal performance reduction on low-end hardware. Marir et al.[56] presented a distributed method for detecting anomalies in large networks, combining deep feature extraction and ensemble SVMs, showing improved performance over existing models. Deng et al.[57] introduced a label-limited intrusion detection method for IoT networks using a Flow Topology-based Graph Convolutional Network (FT-GCN) and a Node-Level Spatial (NLS) attention mechanism. Singh et al.[58] designed a Dew-Cloud-based model with hierarchical federated learning, achieving high training accuracy (99.31%) and superior performance in various metrics. Finally, Kamaldeep et al.[59] proposed an ML model, demonstrating that significant feature reduction enhances the efficiency of ML-based IDSs in detecting DDoS attacks in standardized IoT networks using the 6LoWPAN stack.

Shan et al.[60] introduced Polygraph, a system for fake news detection that is decentralized and intrusion-tolerant, with throughput only 4%-7% slower than a single-server setup. Alcazar et al.[61] evaluated differential privacy techniques applied during the training of a Federated Learning (FL)-enabled Intrusion Detection System (IDS) for industrial IoT, comparing accuracy under various privacy criteria and aggregation procedures. Khan et al.[62] proposed an autoencoder-based framework using convolutional and recurrent networks for cyber threat detection in IIoT, outperforming contemporary methods. Zeng et al.[63] presented a detection system based on causal deep learning that maintains stability across various network conditions, increasing average stability by over 10%. Khan et al.[64] suggested DFF-SC4N, a federated learning-based model, for intrusion detection in SC 4.0 networks, optimizing global model accuracy. Alrowaily et al.[65] conducted experiments with seven machine-learning methods on the CICIDS 2017 malware detection dataset. Zegeye et al.[66] introduced a Multi-Layer Hidden Markov Model (HMM)-based IDS with high accuracy, precision, recall, and F1-score. Kye et al.[67] proposed a hierarchical network intrusion detection method through self-supervised learning, detecting 99% of aberrant data. Gao et al.[68] presented a fuzziness-based semi-supervised learning strategy for network intrusion detection in robotic cloud systems, achieving accuracy rates of 84.54% and 71.29% on specific datasets. Yao et al.[69] developed MSML, a multilevel intrusion detection model, showing improved performance over previous systems. Finally, Arugzzese et al.[70] showcased the potential and risks of ML-NIDS through the XeNI framework, designed for trustworthy cross-evaluations of ML-NIDS.

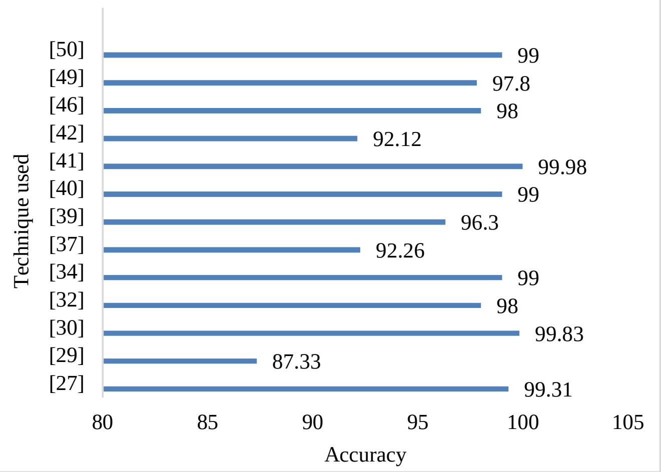


Figure 7. Comparison of accuracy of unsupervised machine learning algorithm

Figure 7 presents a comparison of accuracy achieved by various unsupervised machine learning algorithms for intrusion detection in distributed networks. Among the techniques evaluated, the one proposed by Alasmary et al.[3] achieves the highest accuracy of 99.83%, indicating its effectiveness in detecting intrusions in distributed network environments.

Current Challenges and Future Scope

Distributed systems face several challenges including:

- Network Latency: Network latency refers to the time it takes for data to travel from one node to another in the distributed system. High latency can lead to delays in communication and response times, affecting overall system performance.
- Distributed Coordination: Coordinating multiple nodes in a distributed system is complex, as there is no centralized authority. Ensuring that different nodes work together efficiently and in a synchronized manner can be a challenging task.
- Data Consistency: In distributed systems, maintaining data consistency across multiple nodes is crucial to avoid data corruption and ensure that all nodes have the same view of the data at any given time.
- Heterogeneity: Distributed systems often involve various hardware, software, and networking components, making it essential to address compatibility issues and ensure seamless integration.
- Scalability: As the workload and number of users increase, distributed systems should be able to scale up to handle the load without experiencing bottlenecks or performance degradation.
- Transparency: Distributed systems should provide a unified and coherent view to users, hiding the underlying complexity of the distributed nature of the system.
- Concurrency: Managing shared resources and ensuring proper access control in a distributed environment where multiple processes may access the same resources concurrently is critical to avoid conflicts and ensure data integrity.
- Security: Security is a major concern in distributed systems. Protecting data, preventing unauthorized access, and ensuring data privacy are essential for maintaining the system's integrity and user trust.
- Failure Handling: In distributed systems, failures are more common due to the increased number of components. Handling failures gracefully and recovering from them efficiently is vital to maintaining system availability and reliability.

Conclusion

Traditional Intrusion Detection Systems (IDSs) may struggle to detect sophisticated and distributed attacks due to evolving cyber threats. The paper emphasizes exploring various IDS types, anomaly detection techniques, and machine learning models to enhance intrusion detection accuracy and efficiency. Machine learning-based approaches have shown promise in detecting unknown and complex attacks by leveraging large datasets and data pre-processing. The future of IDSs involves integrating blockchain technology to improve Collaborative IDSs (CIDSs). Blockchain's decentralized and tamper-resistant data storage enables secure information sharing among CIDS nodes without a central authority. This enhances detection and response capabilities, and blockchain also facilitates post-incident analysis and forensics. The broader perspective of blockchain in IDSs offers potential solutions for identity management, data privacy, and secure communication in cybersecurity.

Conflict of Interest: None

Acknowledgement : None

Data Availability : None

Funding : None

References

1. P. Singh, G.S. Gaba, A. Kaur, M. Hedabou, A. Gurtov. Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT. *IEEE J. Biomed. Heal. Informatics* **2023**, 27 (2), 722–731.
2. G.Y. Shin, D.W. Kim, M.M. Han. Data Discretization and Decision Boundary Data Point Analysis for Unknown Attack Detection. *IEEE Access* **2022**, 10, 114008–114015.
3. F. Alasmary, S. Alraddadi, S. Al-Ahmadi, J. Al-Muhtadi. ShieldRNN: A Distributed Flow-based DDoS Detection Solution For IoT Using Sequence Majority Voting. *IEEE Access* **2022**, 10, 88263–88275.
4. M.A. Siddiqi, W. Pak. An Agile Approach to Identify Single and Hybrid Normalization for Enhancing Machine Learning-Based Network Intrusion Detection. *IEEE Access* **2021**, 9, 137494–137513.
5. M. Bagaa, T. Taleb, J.B. Bernabe, A. Skarmeta. A Machine Learning Security Framework for Iot Systems. *IEEE Access* **2020**, 8, 114066–114077.
6. C. Ioannou, V. Vassiliou. Experimentation with Local Intrusion Detection in IoT Networks Using Supervised Learning. In *Proceedings - 16th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2020*; **2020**; pp 423–428.
7. S. Das, S. Shiva. Machine Learning application lifecycle augmented with explanation and security. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2021*; **2021**; pp 171–177.
8. M. Gohil, S. Kumar. Evaluation of Classification algorithms for Distributed Denial of Service Attack Detection. In *Proceedings - 2020 IEEE 3rd International Conference on Artificial Intelligence and Knowledge Engineering, AIKE 2020*; **2020**; pp 138–141.
9. M. Zekri, S. El Kafhali, N. Aboutabit, Y. Saadi. DDoS attack detection using machine learning techniques in cloud computing environments. In *Proceedings of 2017 International Conference of Cloud Computing Technologies and Applications, CloudTech 2017*; **2018**; Vol. 2018-January, pp 1–7.
10. R.R.R. Robinson, C. Thomas. Ranking of machine learning algorithms based on the performance in classifying DDoS attacks. In *2015 IEEE Recent Advances in Intelligent Computational Systems, RAICS 2015*; **2016**; pp 185–190.
11. D. Teixeira, S. Malta, P. Pinto. A Vote-Based Architecture to Generate Classified Datasets and Improve Performance of Intrusion Detection Systems Based on Supervised Learning. *Futur. Internet* **2022**, 14 (3), 14 3.
12. H. Yao, D. Fu, P. Zhang, M. Li, Y. Liu. MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. *IEEE Internet Things J.* **2019**, 6 (2), 1949–1959.
13. S.R. Khonde, V. Ulagamuthalvi. Ensemble-based semi-supervised learning approach for a distributed intrusion detection system. *J. Cyber Secur. Technol.* **2019**, 3 (3), 163–188.
14. S. Moualla, K. Khorzom, A. Jafar. Improving the Performance of Machine Learning-Based Network Intrusion Detection Systems on the UNSW-NB15 Dataset. *Comput. Intell. Neurosci.* **2021**, 2021.
15. Divyatmika, M. Sreekesh. A two-tier network based intrusion detection system architecture using machine learning approach. In *International*

Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016; **2016**; pp 42–47.

16. R. Rama Devi, M. Abualkibash. Intrusion Detection System Classification Using Different Machine Learning Algorithms on KDD-99 and NSL-KDD Datasets - A Review Paper. *Int. J. Comput. Sci. Inf. Technol.* **2019**, 11 (03), 65–80.
17. E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, P. Burnap. A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet Things J.* **2019**, 6 (5), 9042–9053.
18. G. De Carvalho Bertoli, L.A. Pereira Junior, O. Saotome, et al. An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System. *IEEE Access* **2021**, 9, 106790–106805.
19. Q.V. Dang. Studying Machine Learning Techniques for Intrusion Detection Systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Dang, T. K., Küng, J., Takizawa, M., Bui, S. H., Eds.; Springer International Publishing, Cham, **2019**; Vol. 11814 LNCS, pp 411–426.
20. D. Rani, N.C. Kaushal. Supervised Machine Learning Based Network Intrusion Detection System for Internet of Things. In *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*; **2020**; pp 1–7.
21. A.S. Dina, D. Manivannan. Intrusion detection based on Machine Learning techniques in computer networks. *Internet of Things (Netherlands)* **2021**, 16, 100462.
22. P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.A. Karypidis, A. Sarigiannidis. DIDEROT: An intrusion detection and prevention system for DNP3-based SCADA systems. In *ACM International Conference Proceeding Series*; New York, NY, USA, **2020**.
23. Dr. E. Baraneetharan. Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey. *J. Inf. Technol. Digit. World* **2020**, 02 (03), 161–173.
24. V. Ravi, R. Chaganti, M. Alazab. Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Comput. Electr. Eng.* **2022**, 102, 108156.
25. M.C. Belavagi, B. Muniyal. Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection. *Procedia Comput. Sci.* **2016**, 89, 117–123.
26. M. Nair, T.A. Cappello, S. Dang, M.A. Beach. Rigorous Analysis of Data Orthogonalization for Self-Organizing Maps in Machine Learning Cyber Intrusion Detection for LoRa Sensors. *IEEE Trans. Microw. Theory Tech.* **2023**, 71 (1), 389–408.
27. P. Singh, G.S. Gaba, A. Kaur, M. Hedabou, A. Gurtov. Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT. *IEEE J. Biomed. Heal. Informatics* **2023**, 27 (2), 722–731.
28. M. Lefoane, I. Ghafir, S. Kabir, I.U. Awan. Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks. *IEEE Trans. Ind. Informatics* **2023**, 19 (1), 921–929.
29. W. Wang, X. Du, D. Shan, R. Qin, N. Wang. Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine. *IEEE Trans. Cloud Comput.* **2022**, 10 (3), 1634–1646.
30. S. Rawat, A. Srinivasan, V. Ravi, U. Ghosh. Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. *Internet Technology Letters*. **2022**.5(1), e232.
31. L. Yang, Y. Song, S. Gao, A. Hu, B. Xiao. Griffin: Real-Time Network Intrusion Detection System via Ensemble of Autoencoder in SDN. *IEEE Trans. Netw. Serv. Manag.* **2022**, 19 (3), 2269–2281.
32. G. Pu, L. Wang, J. Shen, F. Dong. A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Sci. Technol.* **2021**, 26 (2), 146–153.
33. X. Wen, H. Juan. PSubCLUS: A Parallel Subspace Clustering Algorithm Based on Spark. *IEEE Access* **2021**, 9, 2535–2544.
34. M. Hanselmann, T. Strauss, K. Dormann, H. Ulmer. CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data. *IEEE Access* **2020**, 8, 58194–58205.
35. T. Zoppi, A. Ceccarelli, A. Bondavalli. Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application. *IEEE Access* **2021**, 9, 90603–90615.
36. P. Freitas De Araujo-Filho, G. Kaddoum, D.R. Campelo, et al. Intrusion Detection for Cyber-Physical Systems Using Generative Adversarial Networks in Fog Environment. *IEEE Internet Things J.* **2021**, 8 (8), 6247–6256.
37. W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, F. Sabrina. Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset. *IEEE Access* **2021**, 9, 140136–140146.
38. S. Zavrak, M. Iskefiyeli. Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder. *IEEE Access* **2020**, 8, 108346–108358.
39. T. Chadza, K.G. Kyriakopoulos, S. Lambotharan. Learning to Learn Sequential Network Attacks Using Hidden Markov Models. *IEEE Access* **2020**, 8, 134480–134497.
40. X. Xie, B. Wang, T. Wan, W. Tang. Multivariate Abnormal Detection for Industrial Control Systems Using 1D CNN and GRU. *IEEE Access* **2020**, 8, 88348–88359.
41. K. Narayana Rao, K. Venkata Rao, P.R. Prasad. A hybrid Intrusion Detection System based on Sparse autoencoder and Deep Neural Network. *Comput. Commun.* **2021**, 180, 77–88.
42. M.Z. Alom, T.M. Taha. Network intrusion detection for cyber security using unsupervised deep learning approaches. In *Proceedings of the IEEE National Aerospace Electronics Conference, NAECON*; **2017**; Vol. 2017-June, pp 63–69.
43. H. Narasimhan, V. Ravi, N. Mohammad. Unsupervised Deep Learning Approach for In-Vehicle Intrusion Detection System. *IEEE Consum. Electron. Mag.* **2023**, 12 (1), 103–108.
44. S.N. Mighan, M. Kahani. A novel scalable intrusion detection system based on deep learning. *Int. J. Inf. Secur.* **2021**, 20 (3), 387–403.
45. S. Zanero, S.M. Savaresi. Unsupervised learning techniques for an intrusion detection system. In *Proceedings of the ACM Symposium on Applied Computing*; New York, NY, USA, **2004**; Vol. 1, pp 412–419.
46. S. Mokhtari, K.K. Yen. Measurement data intrusion detection in industrial control systems based on unsupervised learning. *Appl. Comput. Intell.* **2021**, 1 (1), 61–74.
47. S. Rawat, A. Srinivasan, V. Ravi, U. Ghosh. Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. *Internet Technol. Lett.* **2022**, 5 (1).
48. P. Casas, J. Mazel, P. Owezarski. Unsupervised Network Intrusion Detection Systems: Detecting the Unknown without Knowledge. *Comput. Commun.* **2012**, 35 (7), 772–783.
49. M. Verkerken, L. D'Hooge, T. Wauters, B. Volckaert, F. De Turck. Unsupervised Machine Learning Techniques for Network Intrusion Detection on Modern Data. In *2020 4th Cyber Security in Networking Conference, CSNet 2020*; **2020**; pp 1–8.
50. I. Idrissi, M. Azizi, O. Moussaoui. An unsupervised generative adversarial network based-host intrusion detection system for internet of things devices. *Indones. J. Electr. Eng. Comput. Sci.* **2022**, 25 (2), 1140–1150.
51. J. Zhang, C. Luo, M. Carpenter, G. Min. Federated Learning for Distributed IIoT Intrusion Detection Using Transfer Approaches. *IEEE Trans. Ind. Informatics* **2023**, 19 (7), 8159–8169.
52. Z.A. El Houda, A.S. Hafid, L. Khoukhi. MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2023**, 10 (4), 1985–2001.
53. L. Vu, Q.U. Nguyen, D.N. Nguyen, D.T. Hoang, E. Dutkiewicz. Deep Generative Learning Models for Cloud Intrusion Detection Systems. *IEEE Trans. Cybern.* **2023**, 53 (1), 565–577.
54. B. Brenner, S. Hollerer, P. Bhosale, et al. Better Safe Than Sorry: Risk Management Based on a Safety-Augmented Network Intrusion Detection System. *IEEE Open J. Ind. Electron. Soc.* **2023**, 4, 287–303.
55. H. Kim, S. Ahn, W.R. Ha, et al. Panop: Mimicry-resistant ANN-Based distributed NIDS for IoT networks. *IEEE Access* **2021**, 9, 111853–111864.

56. N. Marir, H. Wang, G. Feng, B. Li, M. Jia. Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using spark. *IEEE Access* **2018**, 6, 59657–59671.
57. X. Deng, J. Zhu, X. Pei, et al. Flow Topology-Based Graph Convolutional Network for Intrusion Detection in Label-Limited IoT Networks. *IEEE Trans. Netw. Serv. Manag.* **2023**, 20 (1), 684–696.
58. P. Singh, G.S. Gaba, A. Kaur, M. Hedabou, A. Gurtov. Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT. *IEEE J. Biomed. Heal. Informatics* **2023**, 27 (2), 722–731.
59. Kamaldeep, M. Malik, M. Dutta. Feature Engineering and Machine Learning Framework for DDoS Attack Detection in the Standardized Internet of Things. *IEEE Internet Things J.* **2023**, 10 (10), 8658–8669.
60. G. Shan, B. Zhao, J.R. Clavin, H. Zhang, S. Duan. Poligraph: Intrusion-Tolerant and Distributed Fake News Detection System. *IEEE Trans. Inf. Forensics Secur.* **2022**, 17, 28–41.
61. P. Ruzafa-Alcazar, P. Fernandez-Saura, E. Marmol-Campos, et al. Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT. *IEEE Trans. Ind. Informatics* **2023**, 19 (2), 1145–1154.
62. I.A. Khan, N. Moustafa, D. Pi, et al. A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks. *IEEE Internet Things J.* **2022**, 9 (13), 11604–11613.
63. Z. Zeng, W. Peng, D. Zeng. Improving the Stability of Intrusion Detection With Causal Deep Learning. *IEEE Trans. Netw. Serv. Manag.* **2022**, 19 (4), 4750–4763.
64. I.A. Khan, N. Moustafa, D. Pi, Y. Hussain, N.A. Khan. DFF-SC4N: A Deep Federated Defence Framework for Protecting Supply Chain 4.0 Networks. *IEEE Trans. Ind. Informatics* **2023**, 19 (3), 3300–3309.
65. M. Alrowaily. Investigation of Machine Learning Algorithms for Intrusion Detection System in Cybersecurity. *Graduate Theses and Dissertations*. March 2020, pp 1–88.
66. W.K. Zegeye, R.A. Dean, F. Moazzami. Multi-Layer Hidden Markov Model Based Intrusion Detection System. *Mach. Learn. Knowl. Extr.* **2019**, 1 (1), 265–286.
67. H. Kye, M. Kim, M. Kwon. Hierarchical Detection of Network Anomalies : A Self-Supervised Learning Approach. *IEEE Signal Process. Lett.* **2022**, 29, 1908–1912.
68. Y. Gao, Y. Liu, Y. Jin, J. Chen, H. Wu. A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System. *IEEE Access* **2018**, 6, 50927–50938.
69. H. Yao, D. Fu, P. Zhang, M. Li, Y. Liu. MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. *IEEE Internet Things J.* **2019**, 6 (2), 1949–1959.
70. G. Apruzzese, L. Pajola, M. Conti. The Cross-Evaluation of Machine Learning-Based Network Intrusion Detection Systems. *IEEE Trans. Netw. Serv. Manag.* **2022**, 19 (4), 5152–5169.