ISSN: 2959-6386 (Online), Vol. 2, Issue 2, 2023

Journal of Knowledge Learning and Science Technology

journal homepage: https://jklst.org/index.php/home

JKLST

EXPLORING THE INTERSECTION OF KNOWLEDGE, LEARNING, AND SCIENCE & TECHNOLOGY:

UNLEASHING THE POWER OF SYNERGY IN THE 21ST CENTURY

Exploring Machine Learning Intrusion Detection: Addressing Security and Privacy Challenges in IoT - A Comprehensive Review

Gowrisankar Krishnamoorthy[1]Sai Mani Krishna Sistla[2]

[1] HCL America, USA

[2]Soothsayer Analytics, USA

Abstract:

With billions of IoT devices in operation globally, vast amounts of data are generated, posing significant security challenges throughout the data lifecycle. Machine learning (ML) offers a promising approach to safeguarding IoT systems by swiftly detecting anomalies and enforcing real-time security and privacy (S&P) measures. This systematic literature review investigates ML-based intrusion detection in IoT, examining academic journals from 2011 to 2021 through the IEEE and ProQuest databases. Utilizing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, we identify key insights and challenges. Our review reveals that while ML-based Intrusion Detection Systems (IDS) exhibit superior performance in detecting emerging attack trends, they also introduce complexities such as increased computational demands, susceptibility to adversarial attacks, scalability issues, and trade-offs between accuracy and false positives. Furthermore, deep learning methods outperform traditional ML techniques in anomaly detection. Addressing the evolving nature of attacks remains a continuous endeavor, underscoring the ongoing development of IDS.

Keywords: Internet of Things, Intrusion Detection, Machine Learning, Security and Privacy, Systematic Review

Article Information:

Article history: 12/10/2023 *Accepted:* 15/10/2023 *Online:* 30/10/2023 *Published*: 30/10/2023

DOI: https://doi.org/10.60087/jklst.vol2.n2.P125

Correspondence author: Gowrisankar Krishnamoorthy

Introduction

The advent and proliferation of the Internet of Things (IoT) have revolutionized various facets of modern living, from smart cities to intelligent transportation systems. However, this convenience also brings forth significant challenges, particularly concerning security risks and privacy concerns that necessitate careful consideration. Given the pervasive nature of IoT, its impact can be either constructive or detrimental across multiple domains.

Security and Privacy (S&P) issues within IoT frameworks are often delineated based on varying architectural models, which may range from three-layered to more complex configurations, depending on researchers' preferences. Despite the absence of a standardized IoT architecture, this study focuses on the fundamental three-layered structure, depicted in Figure 1.

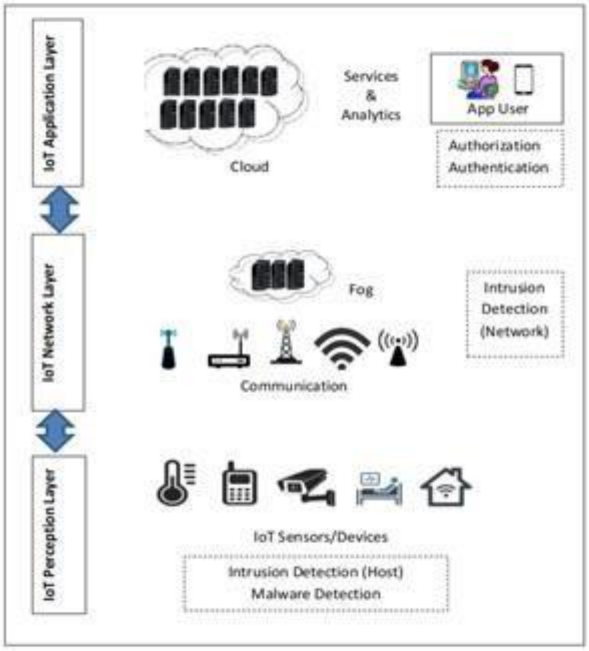
- IoT Application Layer: This tier encompasses Cloud servers, furnishing tailored computational and storage services to individuals and enterprises alike.

- IoT Network Layer: Comprising diverse networks and devices such as cellular networks, local area networks, and the Internet, along with essential components like hubs, routers, and gateways. Communication technologies like Bluetooth, LTE, Wi-Fi, and mobile networks underpin this layer.

- IoT Perception Layer: Primarily constituted by sensors, responsible for collecting environmental data for subsequent transmission to upper layers. Additionally, it incorporates actuators and controllers tasked with monitoring processes and initiating actions based on analyzed data.

Data generated by IoT sensors traverse through the network layer to the application layer (Cloud) for further processing. Subsequently, outcomes or commands are disseminated to end devices, actuators, or users. Irrespective of the architectural model chosen, IoT data undergoes vulnerability to attacks throughout its lifecycle - from collection at the source to storage, with each layer posing its own set of vulnerabilities and associated threats.

These attacks often culminate in data breaches, encompassing unauthorized access to confidential or personal information, potential financial fraud through misappropriated data, and even threats to national security should sensitive government data fall into adversary hands. Addressing these vulnerabilities and associated threats necessitates the deployment of robust protective measures to alleviate user concerns, foster confidence, encourage global adoption, and facilitate the commercialization of IoT technologies. Forecasts indicate substantial growth in the IoT market, with an anticipated value of approximately $163.2 billion in 2020, projected to escalate to around $493 billion over the subsequent five years (2021-2026) (Businesswire, 2021).



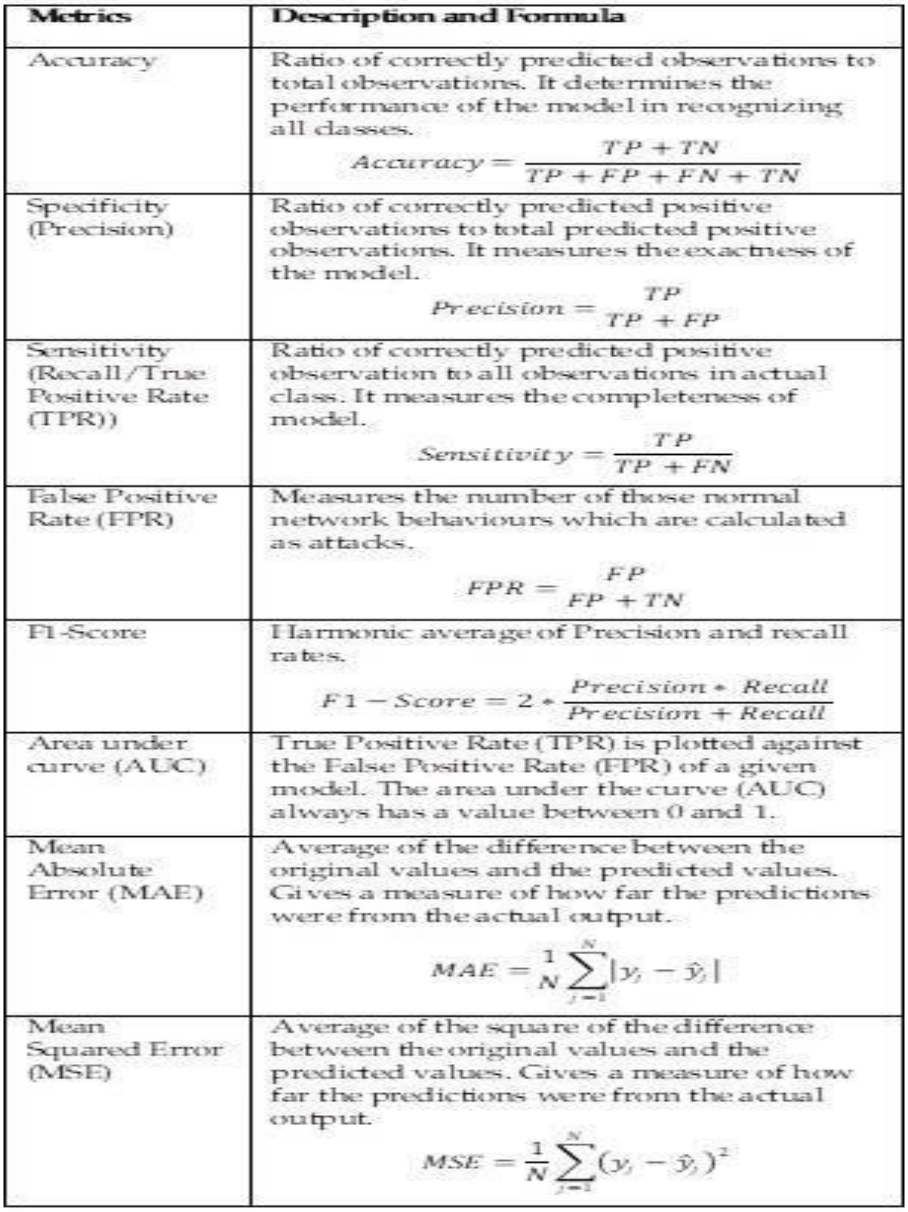
The IoT ecosystem faces significant vulnerabilities at the device layer due to the proliferation of unsecured IoT devices, with projections estimating 30.9 billion connected units globally by 2025 (Statista, 2021). These devices, originating from diverse manufacturers and utilizing disparate protocols and specifications, lack standardized security measures, thereby exposing the entire IoT system to potential threats and attacks (Rani et al., 2021). While managing existing threats presents challenges, emerging threats, comprising novel combinations of known threats, are dynamic and more formidable. Exploiting the vast data generated by IoT devices, as well as their limited computational and storage capabilities, these threats require real-time responses for effective mitigation. However, traditional device-cloud-device data processing routes suffer from high latency, hindering the swift implementation of mitigating measures.

To address latency issues, Fog computing and Edge Computing have emerged, extending computational capabilities closer to the devices (at the edge), thereby reducing latency and enabling real-time threat responses (Bonomi, 2011; Dastjerdi et al., 2016; Zhang and Chiang, 2016; Ni et al., 2018).

In the realm of data protection and preservation, specific requirements such as Confidentiality, Integrity, Non-Repudiation, Authentication, Authorization, Availability, and Freshness have been identified (Rayes and Salam, 2019). Different applications necessitate varying sets of requirements to be fulfilled. Notably, machine learning (ML) has been successfully employed in Security and Privacy (S&P) domains, particularly in intrusion detection. ML leverages the wealth of IoT-generated data to discern patterns and behaviors, enabling the prediction and detection of vulnerabilities, threats, and attacks (Hussain et al., 2020; Thamilarasu et al., 2020; Kasongo, 2021). Unlike traditional methods reliant on predefined rules, ML empowers systems to make decisions based on learned data patterns.

ML techniques encompass four main categories: Supervised, Unsupervised, Semi-supervised, and Reinforcement Learning. Supervised learning employs labeled input and output data for training, facilitating classification and regression tasks (Kubat, 2021). Unsupervised learning operates on unlabeled data, clustering or reducing dimensionality based on inherent similarities. Semi-supervised learning utilizes a mix of labeled and unlabeled data, leveraging labeled data features for classification. Reinforcement learning, devoid of labeled data, relies on environmental interactions to adjust classifications, guided by a reward system (Mohammed et al., 2016).

This review focuses on ML techniques as a solution to IoT security and privacy challenges, with particular emphasis on intrusion detection—an imperative within IoT networks. Intrusion Detection Systems (IDS) can assume various forms, including device-based, network-based, or hybrid systems combining both approaches. Network-based IDS (NIDS) analyze network traffic for intrusion detection, while host-based IDS (HIDS) focus on individual devices.

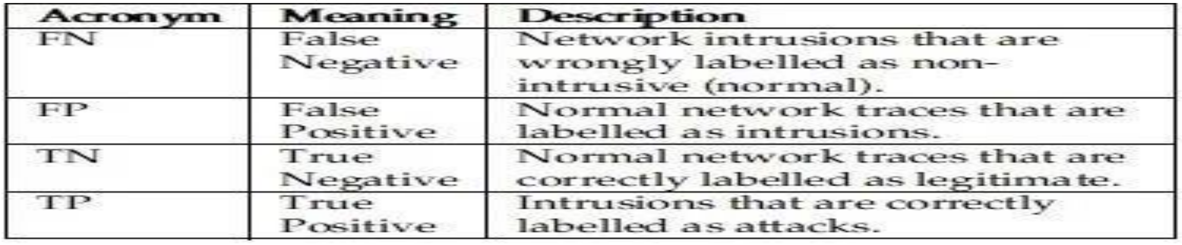


Metrics	Description and Formula
Accuracy	Ratio of correctly predicted observations to total observations. It determines the performance of the model in recognizing all classes. $Accuracy = \frac{TP + TN}{TP + FP + FN + TN}$
Specificity (Precision)	Ratio of correctly predicted positive observations to total predicted positive observations. It measures the exactness of the model. $Precision = \frac{TP}{TP + FP}$
Sensitivity (Recall/True Positive Rate (TPR))	Ratio of correctly predicted positive observation to all observations in actual class. It measures the completeness of model. $Sensitivity = \frac{TP}{TP + FN}$
False Positive Rate (FPR)	Measures the number of those normal network behaviours which are calculated as attacks. $FPR = \frac{FP}{FP + TN}$
F1-Score	Harmonic average of Precision and recall rates. $F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall}$
Area under curve (AUC)	True Positive Rate (TPR) is plotted against the False Positive Rate (FPR) of a given model. The area under the curve (AUC) always has a value between 0 and 1.
Mean Absolute Error (MAE)	Average of the difference between the original values and the predicted values. Gives a measure of how far the predictions were from the actual output. $MAE = \frac{1}{N}\sum_{j=1}^{N}\lvert y_j - \hat{y}_j \rvert$
Mean Squared Error (MSE)	Average of the square of the difference between the original values and the predicted values. Gives a measure of how far the predictions were from the actual output. $MSE = \frac{1}{N}\sum_{j=1}^{N}(y_j - \hat{y}_j)^2$

Host-based Intrusion Detection Systems (HIDS) leverage sensor and device log data for detection (Meera et al., 2021; Singh and Singh, 2014).

For identifying anomalies (unknown-attacks), IDS analyze patterns that deviate from normal network traffic or sensor data patterns. Conversely, for detecting signatures (known-attacks), patterns are compared against known patterns in the IDS database. Upon flagging an intrusion, appropriate countermeasures are enacted. Examples include signature-based detection (Eskandari et al., 2020; Swarna et al., 2020), anomaly-based detection (Ahmad et al., 2020; Eskandari et al., 2020; Sheikhan and Bostani, 2017), and methods for mitigating adversarial attacks on ML techniques (Sagar et al., 2020; Miyato et al., 2018; Zhang et al., 2019; Santana et al., 2021).

The architecture of the IoT system, whether centralized or distributed, also influences intrusion detection strategies. The effectiveness of ML techniques in this context depends on their performance, evaluated through various metrics such as:



Acronym	Meaning	Description
FN	False Negative	Network intrusions that are wrongly labelled as non-intrusive (normal).
FP	False Positive	Normal network traces that are labelled as intrusions.
TN	True Negative	Normal network traces that are correctly labelled as legitimate.
TP	True Positive	Intrusions that are correctly labelled as attacks.

This study stands out due to its comprehensive review of existing ML-based Intrusion Detection Systems (IDS) and its identification of novel techniques, such as blockchain integration, multi-layer approaches, and federated learning, which aim to enhance privacy preservation in IoT systems. The subsequent sections are structured as follows: Section 2 discusses related works, Section 3 outlines the research methodology employed, Section 4 presents the review findings along with the performance metrics utilized, and identifies gaps and limitations in the existing studies. Finally, Section 5 concludes by summarizing the main findings of the study and proposes avenues for future research.

RELATED WORK

Numerous surveys and reviews have delved into the application of machine learning (ML) to address security and privacy challenges within the realm of IoT, with a particular focus on intrusion detection. Several notable studies are outlined in this section.

Amiri-Zarandi et al. (2020) conducted a comprehensive review of studies employing ML techniques to tackle privacy concerns in IoT, addressing issues such as scalability, interoperability, and resource limitations (computation, storage, and energy). They categorized data generated across different IoT layers and applied ML for robust privacy management.

Chaabouni et al. (2019) conducted a comparative review of traditional and ML-based Network Intrusion Detection Systems (NIDS) within IoT architectures. Their analysis encompassed detection methodologies, validation strategies, identified threats/attacks, and deployed algorithms. Results indicated that ML-based approaches offer advantages in terms of enhanced detection accuracy and reduced false positive alarms.

Hameed et al. (2021) focused on Implantable Medical Devices (IMDs) due to their critical impact on patient health and safety. Their study investigated security solutions including anomaly detection, authentication, access control, and network layer security. While traditional ML techniques demonstrated efficacy, attention was drawn to considerations regarding resource utilization, time complexity, and energy consumption to ensure effectiveness.

Thamilarasu et al. (2020) proposed an Intrusion Detection System (IDS) tailored for IoT sensor and network data within connected medical devices. Their model exhibited high detection accuracy with minimal computational resource requirements.

Iwendi et al. (2021) aimed to detect network-based attacks and privacy violations in smart healthcare using ML methods, specifically employing Random Forest (RF) and feature optimization techniques. Their approach yielded a high detection rate coupled with a lower false alarm rate.

Verma et al. (2021) explored the application of ML techniques for intrusion detection in the Internet of Medical Things (IoMT) and privacy preservation of patients' medical records, demonstrating the effectiveness of ML in safeguarding sensitive healthcare data.

Various studies have contributed significantly to the understanding and advancement of machine learning (ML) in cybersecurity, particularly within the domain of cyber-physical systems (CPS). Liang et al. (2019) elucidated the benefits, vulnerabilities, and emerging trends associated with ML applications in CPS, defining CPS as integrated collections of physical and computer components aimed at safe and efficient process operation (Munirathinam, 2020). Noteworthy examples of CPS include industrial control systems and smart grids, where ML techniques offer improved intrusion detection and decision-making accuracy. However, concerns arise from the escalating trend of ML exploitation in cyberattacks and intrusions.

Skowron and Janicki (2020) proposed a novel method for detecting traffic fingerprinting attacks, while also addressing vulnerabilities stemming from ML adversarial usage against IoT devices. Sharma and Liu (2021) evaluated six supervised learning algorithms for detecting misbehavior in the Internet of Vehicles (IoV), highlighting challenges posed by the similarity between normal and abnormal data, despite achieving commendable performance.

Weng and Liu (2019) introduced anomaly detection for mobile service computing, aiming to mitigate data transfer hacking risks to the Cloud. Other studies, such as those by Hassan et al. (2020), Shahid et al. (2020), Kasongo (2021), and Liu et al. (2020), demonstrated the efficacy of ML and deep learning models in countering cyber-attacks and safeguarding the integrity of industrial IoT (IIoT) networks, crucial for industries facing evolving threats.

Nie et al. (2021) proposed a deep learning-based Intrusion Detection System (IDS) for Social IoT, achieving enhanced accuracy through multiple attack handling models. Liu and Lang (2019) provided a taxonomy of IDS utilizing ML and DL approaches, emphasizing the computational resource requirements of deep learning techniques.

Furthermore, researchers have explored innovative ML techniques, such as federated learning (FL), blockchain, and multi-layer/deep learning, to enhance privacy preservation. FL, a decentralized privacy-preserving method, safeguards raw data on devices for local computation, thereby thwarting unauthorized access. Blockchain integration, fog computing, edge computing, and ML synergies have been proposed by Hassija et al. (2019) and Alkadi et al. (2021) to bolster IoT security.

The combination of blockchain and FL by Lu et al. (2020) enables secure and efficient data sharing, while hierarchical blockchain-enabled FL algorithms by Chai et al. (2021) and Iftikhar et al. (2021) ensure safe knowledge sharing in IoT applications. Ibrahim et al. (2022) introduced a blockchain-enabled protocol (BEP) and Software Defined Networking (SDN) architectures to fortify IoT security against Denial of Service (DoS) and Distributed DoS (DDoS) attacks.

Multi-layer ML/DL approaches, as demonstrated by Lee et al. (2020) and Khater et al. (2019), leverage deep networks to enhance intrusion detection accuracy, particularly in resource-constrained IoT environments. Qaddoura et al. (2021) incorporated two detection stages for improved classification quality, while Gassais et al. (2020), Bica et al. (2019), and Pajooh et al. (2021) implemented ML and DL algorithms with minimal computational overhead on IoT devices.

Hameed et al. (2021) proposed a combined host and network IDS for simultaneous detection of malicious sensor and network data, underscoring the importance of integrated security measures. Table 3 provides a summary of some of the reviewed studies, showcasing the diverse approaches and techniques employed in ML-based cybersecurity research.

Research Methodology

This study centers on the application of machine learning (ML) techniques in intrusion detection, a critical challenge within IoT networks. To achieve this, a systematic literature review (SLR) was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework (Azevedo et al., 2017; Guelph-Humber, 2021). PRISMA, a widely recognized standard, outlines a structured approach for document identification, screening, and inclusion/exclusion criteria, thereby enhancing review accuracy and facilitating replication of review methods.

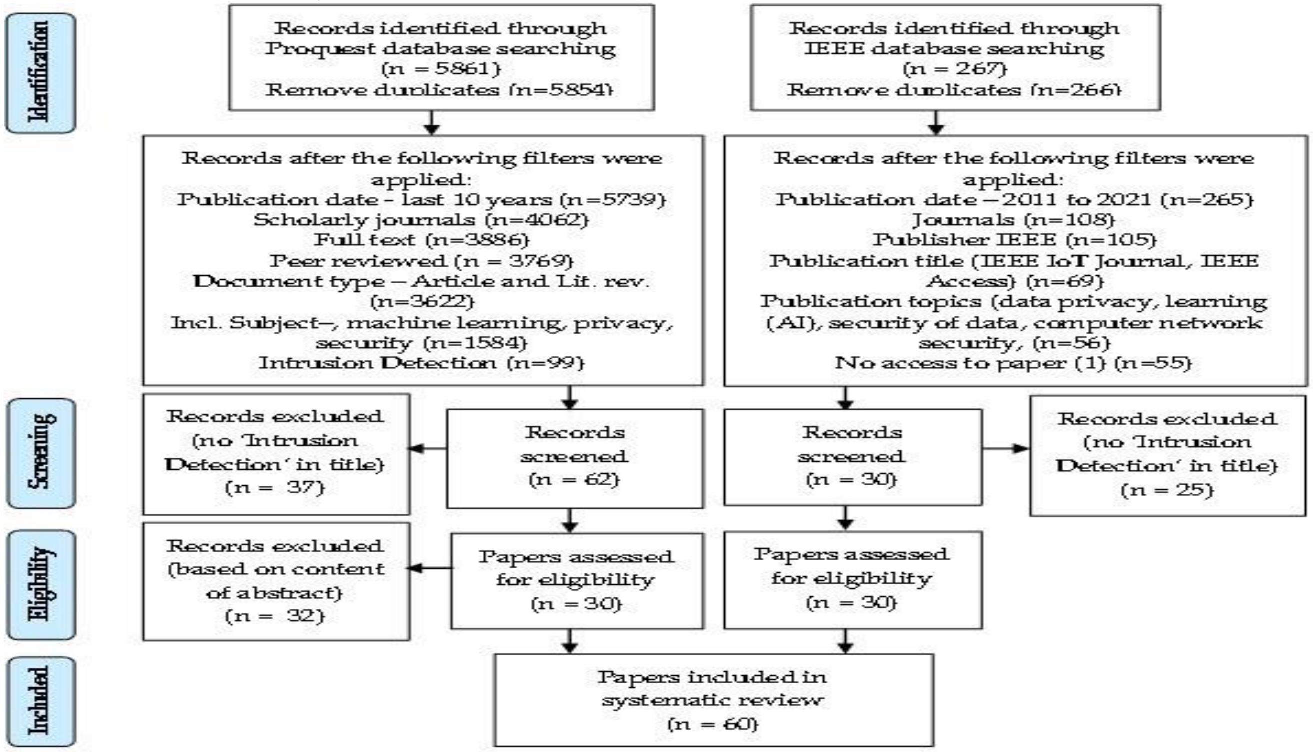
The search for relevant papers was conducted across two prominent databases: IEEE and ProQuest (comprising 4 databases in total). Keywords including "Internet of Things," "IoT," "Intrusion Detection," "Machine Learning," "Security and Privacy," and "Systematic Review" were employed to retrieve pertinent literature. Subsequently, identified papers underwent screening based on specific inclusion/exclusion criteria. Eligible papers were subjected to further scrutiny, including evaluation of title, abstract content, and overall relevance to the study's objectives.

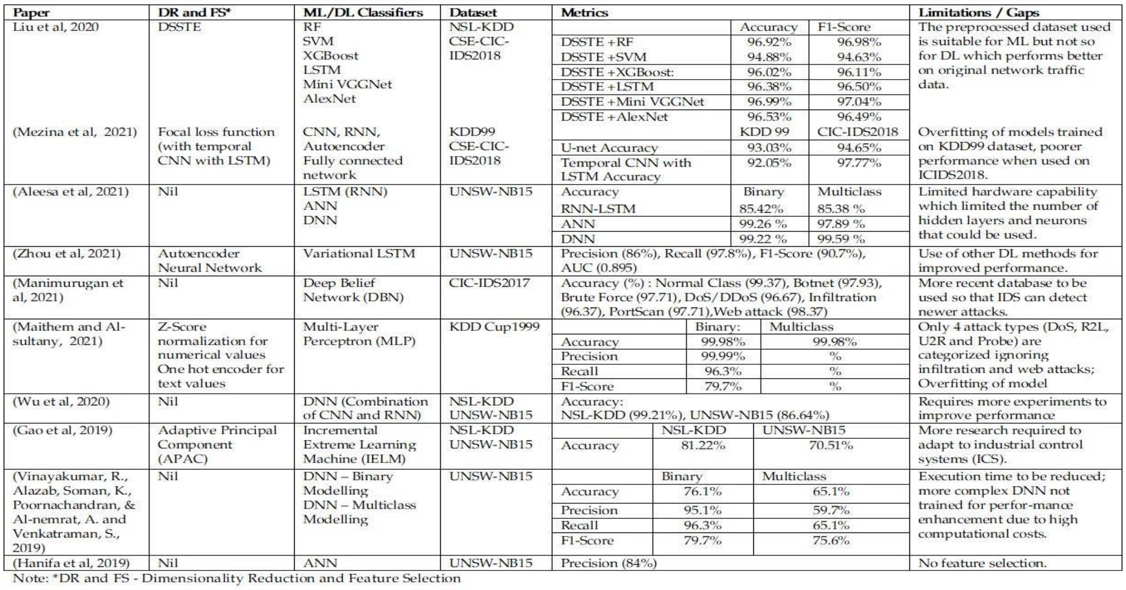
RESULTS AND DISCUSSION

Utilizing the PRISMA framework and conducting an advanced search with relevant keywords, a total of 6,128 papers were retrieved from both the ProQuest and IEEE databases. The advanced search query included terms such as "Internet of Things," "IoT," "Security and Privacy," "Machine Learning," and "Intrusion Detection," as depicted in Fig. 2. Various filters, including publication type (journal articles, conference papers, or book chapters) and publication date, were applied during the search process.

Following the application of inclusion/exclusion criteria, the number of potential papers for review was narrowed down to 99 from the ProQuest database and 55 from the IEEE database. Subsequently, further refinement based on abstract content and relevance led to the final selection of 60 papers—30 from each database—to ensure equitable representation in the review process.

Paper Details	**Contributions**	**Limitations/Gaps**
(Chaabouni et al. 2019)	Compared current defense techniques in traditional and ML NIDS in terms of architecture, detection methodologies, validation strategies, treated threats, and algorithm deployments; with the latter providing increased detection accuracy and decreased false positive alarms.	Standard public benchmark dataset is required for improved validation strategy such that a clear, practical and convenient comparison of the different NIDS can be carried out.
(Hassija et al. 2019)	Identified threats at the various layers of IoT architecture and proposed solutions using blockchain, fog computing, edge computing, and machine learning; the aim being to enhance the level of security of the system.	Blockchain: Leakage of private information of users. Scalability and availability issues as number of miners increase. Fog & Edge Computing: data security and user privacy due to leakage and misuse of a user's private data. ML: Effectiveness and accuracy of IDS is dependent on choice of algorithm and dataset.
(H. Liu and Lang 2019)	Proposed a taxonomy of IDS that takes data objects as the main dimension to classify and summarize machine learning-based and deep learning-based IDS literature.	Lack of available datasets, low detection accuracy in actual environments, low efficiency due to complicated models and extensive data preprocessing methods required between effectiveness and efficiency in order for the IDSs to detect attacks in real time.
(Liang, et al, 2019)	Proposed mechanisms to enhance IDS accuracy in "cyber-physical systems (CPS)" using various ML algorithms.	Ability of attackers to use ML techniques in the execution of cyberattacks and intrusions and vulnerabilities at all stages of the data life-cycle.
(AbdulRahman et al., 2020)	Presented how ML techniques can be utilized for S&P issues and resource management in IoT using FL.	Being a new research direction, more studies need to be carried out to develop more robust FL systems.
(Amiri-Zarandi et al, 2020)	Identified merits and demerits of utilizing data in ML-based solutions for privacy in IoT.	Identified limitations include lack of standard data practices and policies, interoperability of devices and regulatory compliance. Need for new ideas such as using Blockchain and ML techniques to be further investigated.
(Asharf et al. 2020)	Presented various aspects of IoT systems in terms of architecture, protocols, technologies, and emerging threats from compromised IoT devices. An overview of intrusion detection models using ML and DL techniques for attack detection was also presented.	Lack of suitable datasets, assumption of real-time IDS that there is no attack traffic during the learning phase which sometimes leads to false alarms, resource limitation of IoT devices, heterogeneity of IoT system and scalability issues.
(Hussain et al. 2020)	Identified requirements for IoT network security, attack types and current solutions proposed using existing ML and DL solutions.	Shortcomings in MD/DL techniques such as computational complexity, learning efficiencies and parameter tuning strategies.
(Leevy and Khoshgoftaar 2020)	Presented and analyzed IDS based on the CSE CICIDS2018 dataset; this being the most recent intrusion detection dataset that is big data, publicly available and covers a wide range of attack types.	Unusually high performance scores which may be a consequence of overfitting, class imbalance of dataset and lack of the data cleaning to enhance dataset usability.
(Hameed, et al, 2021)	Provided security solutions (sensor anomaly detection, device authentication, access control and network layer security) to Implantable Medical Devices (IMDs) by applying ML techniques.	Effectiveness is determined by resource capacity, time complexity and energy usage which must be given proper consideration.
(Nguyen et al. 2021)	Used federated learning (FL) in IoT networks to enhance privacy preservation.	Resource requirements are not always met.


Identification
Screening
Eligibility
Included
Records identified through Proquest database searching (n = 5861) Remove duplicates (n=5854)
Records identified through IEEE database searching (n = 267) Remove duplicates (n=266)
Records after the following filters were applied: Publication date - last 10 years (n=5739) Scholarly journals (n=4062) Full text (n=3886) Peer reviewed (n = 3769) Document type – Article and Lit. rev. (n=3622) Incl. Subject–, machine learning, privacy, security (n=1584) Intrusion Detection (n=99)
Records after the following filters were applied: Publication date – 2011 to 2021 (n=265) Journals (n=108) Publisher IEEE (n=105) Publication title (IEEE IoT Journal, IEEE Access) (n=69) Publication topics (data privacy, learning (AI), security of data, computer network security, (n=56) No access to paper (1) (n=55)
Records excluded (no 'Intrusion Detection' in title) (n = 37)
Records screened (n = 62)
Records screened (n = 30)
Records excluded (no 'Intrusion Detection' in title) (n = 25)
Records excluded (based on content of abstract) (n = 32)
Papers assessed for eligibility (n =30)
Papers assessed for eligibility (n = 30)
Papers included in systematic review (n = 60)



Paper	DR and FS*	ML/DL Classifiers	Dataset	Metrics			Limitations / Gaps
Liu et al, 2020	DSSTE	RF SVM XGBoost LSTM Mini VGGNet AlexNet	NSL-KDD CSE-CIC-IDS2018		Accuracy	F1-Score	The preprocessed dataset used is suitable for ML but not so for DL which performs better on original network traffic data.
				DSSTE +RF	96.92%	96.98%	
				DSSTE +SVM	94.88%	94.63%	
				DSSTE +XGBoost:	96.02%	96.11%	
				DSSTE +LSTM	96.38%	96.50%	
				DSSTE +Mini VGGNet	96.99%	97.04%	
				DSSTE +AlexNet	96.53%	96.49%	
(Mezina et al, 2021)	Focal loss function (with temporal CNN with LSTM)	CNN, RNN, Autoencoder Fully connected network	KDD99 CSE-CIC-IDS2018		KDD 99	CIC-IDS2018	Overfitting of models trained on KDD99 dataset, poorer performance when used on ICIDS2018.
				U-net Accuracy	93.03%	94.65%	
				Temporal CNN with LSTM Accuracy	92.05%	97.77%	
(Aleesa et al, 2021)	Nil	LSTM (RNN) ANN DNN	UNSW-NB15	Accuracy	Binary	Multiclass	Limited hardware capability which limited the number of hidden layers and neurons that could be used.
				RNN-LSTM	85.42%	85.38 %	
				ANN	99.26 %	97.89 %	
				DNN	99.22 %	99.59 %	
(Zhou et al, 2021)	Autoencoder Neural Network	Variational LSTM	UNSW-NB15	Precision (86%), Recall (97.8%), F1-Score (90.7%), AUC (0.895)			Use of other DL methods for improved performance.
(Manimurugan et al, 2021)	Nil	Deep Belief Network (DBN)	CIC-IDS2017	Accuracy (%) : Normal Class (99.37), Botnet (97.93), Brute Force (97.71), DoS/DDoS (96.67), Infiltration (96.37), PortScan (97.71),Web attack (98.37)			More recent database to be used so that IDS can detect newer attacks.
(Maithem and Al-sultany, 2021)	Z-Score normalization for numerical values One hot encoder for text values	Multi-Layer Perceptron (MLP)	KDD Cup1999		Binary:	Multiclass	Only 4 attack types (DoS, R2L, U2R and Probe) are categorized ignoring infiltration and web attacks; Overfitting of model
				Accuracy	99.98%	99.98%	
				Precision	99.99%	%	
				Recall	96.3%	%	
				F1-Score	79.7%	%	
(Wu et al, 2020)	Nil	DNN (Combination of CNN and RNN)	NSL-KDD UNSW-NB15	Accuracy: NSL-KDD (99.21%), UNSW-NB15 (86.64%)			Requires more experiments to improve performance
(Gao et al, 2019)	Adaptive Principal Component (APAC)	Incremental Extreme Learning Machine (IELM)	NSL-KDD UNSW-NB15		NSL-KDD	UNSW-NB15	More research required to adapt to industrial control systems (ICS).
				Accuracy	81.22%	70.51%	
(Vinayakumar, R., Alazab, Soman, K., Poornachandran, & Al-nemrat, A. and Venkatraman, S., 2019)	Nil	DNN – Binary Modelling DNN – Multiclass Modelling	UNSW-NB15		Binary	Multiclass	Execution time to be reduced; more complex DNN not trained for perfor-mance enhancement due to high computational costs.
				Accuracy	76.1%	65.1%	
				Precision	95.1%	59.7%	
				Recall	96.3%	65.1%	
				F1-Score	79.7%	75.6%	
(Hanifa et al, 2019)	Nil	ANN	UNSW-NB15	Precision (84%)			No feature selection.

Note: *DR and FS - Dimensionality Reduction and Feature Selection

Overall, the primary objective of intrusion detection in IoT is to deploy an Intrusion Detection System (IDS) that is robust, dependable, and precise in identifying and thwarting diverse attacks, including both anomalous and signature-based threats, against the system. To achieve this goal, a plethora of machine learning (ML) and deep learning (DL) methods have been employed, either individually or in hybrid combinations. Significant emphasis has been placed on ensuring the suitability and efficacy of the dataset for learning purposes. Various data transformation techniques and feature selection/extraction methods have been leveraged to balance the dataset and reduce the number of features, respectively. The nature of the dataset (balanced or imbalanced; historical or current) and the choice of feature selection/extraction techniques profoundly influence the IDS's performance, impacting its ability to accurately detect attacks.

Despite the extensive research in this domain, several gaps and limitations persist, each study presenting its unique challenges. Some of the identified gaps and limitations include:

1. The selection of dimensionality reduction and feature selection methods during the preprocessing stage significantly affects the IDS's ability to detect attacks accurately.

2. The computational complexity associated with data preprocessing, feature reduction, model training, and deployment of ML- and DL-based NIDS escalates resource requirements (CPU, storage, energy), posing challenges, particularly for resource-constrained IoT devices. This underscores the necessity for developing efficient NIDS with minimal computational demands.

3. Balancing detection accuracy with false positive events is crucial to prevent unnecessary deployment of mitigating actions, which could disrupt services.

4. The utilization of ML in executing adversarial attacks on IoT devices and networks has emerged as a concern.

5. IDS may struggle to detect certain attacks hidden within imbalanced network datasets, as the abundance of normal data often biases towards higher false-positive rates.

6. The inability of IDS to capture all potential normal observations in heterogeneous IoT networks may result in elevated false-negative rates.

7. The scalability challenges posed by the adoption of ML/DL techniques in large, distributed IoT networks, owing to their heterogeneous nature.

8. While DL models demonstrate superior efficiency in attack detection compared to ML, they often entail longer running times, rendering them occasionally unsuitable for meeting the real-time requirements of IDS.

Given the dynamic nature of attacks, it remains arduous for any single IDS to detect all types of threats comprehensively. With new and emerging attacks continually evolving and growing in complexity, the development of IDS remains an ongoing endeavor.

Conclusions

The role of machine learning (ML) in addressing security and privacy concerns within IoT has been extensively examined by researchers, with ML techniques playing a significant role in securing both the device and network layers. This study conducted a systematic review focusing on various ML techniques applied to intrusion detection. The review encompassed relevant studies published over the past decade (2011-2021) sourced from two major databases, IEEE and ProQuest.

From the final selection of 60 papers, it was evident that deep learning (DL) methods exhibited superior suitability compared to traditional ML approaches, particularly for anomaly detection in IoT. This conclusion was drawn based on the comprehensive analysis of performance metrics employed across the studies. Furthermore, researchers demonstrated a concerted effort to enhance IoT system performance through the exploration of hybrid techniques, including federated learning, blockchain, and multi-layer classification approaches. Notably, models combining multiple ML techniques showcased enhanced performance outcomes.

However, despite the progress achieved, several gaps and challenges persist, as delineated earlier. Future research endeavors should focus on further enhancing system performance and efficiency, with particular emphasis on improving dataset balancing and feature selection methodologies. The development of efficient Intrusion Detection Systems (IDS) holds significant promise in bolstering the broader acceptance and commercialization of IoT technology, projected to reach a staggering $493 billion by 2026.

References

[1] AbdulRahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2020). A Survey on Federated Learning: The Journey from Centralized to Distributed On-Site Learning and Beyond. IEEE Internet of Things Journal, 0(0). https://doi.org/10.1109/JIOT.2020.3030072

[2]Adekunle, B. O., Akinyemi, J. B., Aladesanmi, T. A., Aderounmu, A. G., & Kamagate, B. H. (2019). An Improved Anomalous Intrusion Detection Model. FUOYE Journal of Engineering and Technology, 4(2). https://doi.org/10.46792/fuoyejet.v4i2.418

[3] Ahmad, I., Yousaf, M., Yousaf, S., & Ahmad, M. O. (2020). Research Article Fake News Detection Using Machine Learning Ensemble Methods. Wiley Hindawi. Retrieved from https://doi.org/10.1155/2020/8885861

[4] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2021). A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. IEEE Internet of Things Journal, 8(12), 9463–9472. https://doi.org/10.1109/JIOT.2020.2996590

[5]Amiri-Zarandi, M., Dara, R. A., & Fraser, E. (2020). A survey of machine learning-based solutions to protect privacy in the Internet of Things. Elsevier Computers & Security. https://doi.org/10.1016/j.cose.2020.101921

[6] Ayogu, B. A., Adetunmbi, A. O., & Ayogu, I. I. (2019). A Comparative Analysis of Decision Tree and Bayesian Model for Network Intrusion Detection System. FUOYE Journal of Engineering and Technology, 4(2). https://doi.org/10.46792/fuoyejet.v4i2.362

[7] Bica, I., Chifor, B. S., Arseni, S., & Matei, I. (2019). Multi-Layer IoT Security Framework for Ambient Intelligence Environments. MDPI Sensors, 19. https://doi.org/10.3390/s19184038

[8] Businesswire. (2021). Global IoT Connectivity Market Analysis and Forecast Report 2021. In Businesswire. Retrieved from https://www.businesswire.com/news/home/20211015005387/en/Global-IoT-connectivity-Market-Analysis-and-Forecast-Report-2021/

[9] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE - Communications Surveys and Tutorials, 21(3), 2671–2701.

[10] Chai, H., Leng, S., Chen, Y., & Zhang, K. (2021). A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(7), 3975–3986. https://doi.org/10.1109/TITS.2020.3002712

[11] Hasan, M. R. (2023). NetSuite's Next Frontier: Leveraging AI for Business Growth. International Journal of Science, Engineering and Technology, Volume 11 Issue 6. Retrieved from: https://www.ijset.in/volume-11-issue-6/

[12]Hasan, M. R. (2022). Cybercrime Techniques in Online Banking. Journal of Aquatic Science. Retrieved from https://www.journal-aquaticscience.com/article_158883.html

[13] Islam, M., &Shuford , J. . (2024). A Survey of Ethical Considerations in AI: Navigating the Landscape of Bias and Fairness. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006- 4023*, *1*(1). https://doi.org/10.60087/jaigs.v1i1.27

[14] Akter, most. S. (2024). Interdisciplinary Insights: Integrating Artificial Intelligence with Environmental Science for Sustainable Solutions. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *1*(1). https://doi.org/10.60087/jaigs.v1i1.28

[15] khan , M. R. . (2024). Advancements in Deep Learning Architectures: A Comprehensive Review of Current Trends. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *1*(1). https://doi.org/10.60087/jaigs.v1i1.29

[16] Rana , M. S. ., &Shuford , J. . (2024). AI in Healthcare: Transforming Patient Care through Predictive Analytics and Decision Support Systems. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *1*(1). https://doi.org/10.60087/jaigs.v1i1.30

[17] Mia , M. R. ., &Shuford , J. . (2024). Exploring the Synergy of Artificial Intelligence and Robotics in Industry 4.0 Applications . *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-*