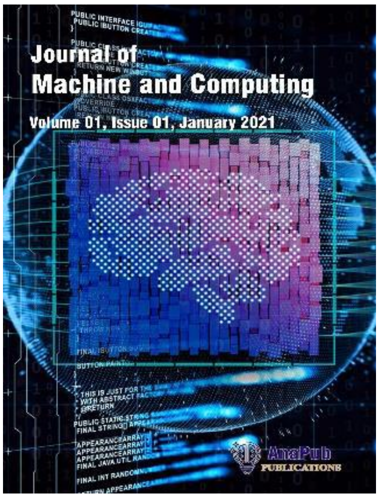
Journal Pre-proof



Intrusion Detection Systems for IoT Based on Machine Learning Under the Learning Environment

Qusay Abdullah Abed and Wathiq Laftah Al-Yaseen

DOI: 10.53759/7669/jmc202505018

Reference: JMC202505018

Journal: Journal of Machine and Computing.

Received 21 July 2024

Revised form 23 October 2024

Accepted 06 November 2024

Please cite this article as: Qusay Abdullah Abed and Wathiq Laftah Al-Yaseen, “Intrusion Detection Systems for IoT Based on Machine Learning Under the Learning Environment”, Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505018

Intrusion Detection Systems for IoT Based on Machine Learning Under the Learning Environment

Qusay Abdullah Abed *1, Wathiq Laftah Al-Yaseen 1

1 Kerbala Technical Institute, Al-Furat Al-Awsat Technical University, 56001, Kerbala, Iraq

Emails: inkr.ks@atu.edu.iq

Abstract

In an ever-evolving global landscape, concerns regarding network security continue to grow. Integrating information technologies into daily life has made safeguarding computer security imperative. The rise of internet connectivity and innovations like the Internet of Things (IoT) have introduced new challenges in breaching computer systems. Organizations are dedicating resources to research methods for enhancing cyber-attack discovery, opting for intelligent approaches to achieve the highest accuracy rates. The combination of IoT and ML is changing how services and applications work. In the classical ML approaches, data are collected and centrally processed. Nevertheless, this approach is challenging to implement in modern IoT networks because they deal with a significant amount of data, and privacy is often an issue. In contrast, federated learning (FL) has been reported as a possible approach to address such limitations. FL enables ML methods to perform collaborative training through model parameter sharing rather than client data. This study comprehensively reviews cutting-edge literature on enhancing computer network security with ML in the FL environment and IoT. This work further explores various methods and applications in intrusion detection (ID) mechanisms within computer networks through a contemporary and thorough examination.

Keywords: Machine Learning; Internet of Things; Detection System; Federated Learning; Intelligent Techniques; Network Security.

1. Introduction

Network security has become an undeniable necessity in light of the extensive Internet utilization. The widespread access to information has led to substantial risks, encompassing everything from viruses to network intrusions, resulting in considerable business losses. Consequently, companies are making significant investments in the study, employing intelligent techniques to enhance security, particularly as tools for intervention discovery [1,2]. The need to continuously update research in intrusion detection (ID) within computer networks is becoming increasingly crucial. Intrusion detection systems are the hardware or software systems that automate ID. Various intrusion-based approaches have been reported, such as statistical-based, pattern-based, rule-based, state-based, and heuristic-based. A significant concern emerges with implementing the Internet Protocol version 6 (IPv6) system, particularly network security and, more specifically, ID. The implementation of IPv6 in ID is considered a new demand for the protection of network mechanisms, and it is a fact that IPv6 is closely linked to the Internet of Things (IoT). The symbiotic relationship between IPv6 and the IoT model facilitates unrestricted internet connectivity for diverse devices, including blenders, microwaves, wearable clothing, cognitive buildings [3], and many more. This proliferation of IPv6 in IoT poses an ongoing challenge in network security, emphasizing the fundamental need for research into intervention discovery techniques tailored for the IoT. Conversely, the necessity to send the data to the centralized cloud, which implies a high probability of energy consumption, privacy issues, and data leakage, is caused by the limited computing power of IoT devices. Some studies propose a Federated Learning (FL) based IDS to transfer learning amongst local devices, not from a cloud [4].

In recent years, IoT has become increasingly integrated into various aspects of daily life, including smart homes, healthcare, transportation, and industrial systems. This widespread adoption of IoT applications has resulted in an exponential increase in data generated. The extensive data generation has led to the need for more sophisticated IDS to protect IoT devices and networks from security threats. Given IoT devices' distributed and heterogeneous nature, FL can be a promising approach for developing IDS [5]. Moreover, machine learning (ML) techniques can potentially analyze large volumes of data in real-time and identify patterns and anomalies that may indicate security breaches.

Many efforts are being made to determine the best ways to detect intrusions in IoT environments. Researchers identified the key factors and desired outcomes for effective intrusion detection in IoT. Studies in the domain of IoT have garnered significant interest both in academic circles and the industry, primarily owing to their potential applications in various human endeavors [6]. IoT holds promise as a means to enhance people's quality of life, for instance, through devices like smart watches that monitor health using sensors, and its popularity has surged alongside declining sensor costs, the widespread adoption of remote storage services, and the rise of big data technologies. The ready availability of these resources bolsters IoT, mainly when diverse resource-rich devices are interconnected, giving rise to novel applications. However, this newfound landscape has a caveat: the imperative need for security. Additionally, questions arise concerning the trustworthiness of data collected from IoT devices, data privacy issues, the purposes, and the locations for which this data may be utilized, serving as crucial motivators for our research [7]. Nonetheless, it is noteworthy that, until now, there has been a conspicuous absence of a comprehensive exploration of the utilization of ML under the environment of FL within the realm of IoT. Specifically with an emphasis on ID.

This comprehensive review aims to explore the literature on IDS for IoT based on FL and ML techniques. The selected studies encompass publications from 2016 to 2024 utilizing authentic internet search engines. This review will provide insights into the current state of research in this area and identify potential opportunities for further advancement in IDS for IoT. This research offers credibility and support for the claims and findings presented in the study and gives credit to the sources of information. An in-depth analysis of the literature used in the research work can provide insight into the validity and reliability of the information presented. FL can be a promising approach for developing IDS for IoT devices' distributed and heterogeneous nature [8]. Large volumes of data can be analyzed in real-time using ML techniques to identify security breaches. IDS can help protect IoT devices and networks from security threats by analyzing patterns and anomalies in the data. In short, the main contribution of this review was based on conducting a retrospective analysis of the methods applied in the past to FL and ML for IoT security augmentation in ID. Further, the gap in research was analyzed. The remainder of this review was structured as follows: Section 2 discusses the background of the related research. Section 3 elaborates on the recent advances in ID for IoT, and section 4 discusses addressing the data security challenges in IoT expansion.

2. Background of the Study

IDS tailored for IoT environments, primarily through ML within FL frameworks, are an essential area for ensuring the security and privacy of IoT-edge devices. While lying at the edge of networks, these systems have a high risk of cyber-attacks; therefore, robust security measures are needed to mitigate these threats. This section, thus, serves the purpose of furnishing a comprehensive background to contextualize the study. It starts by describing the very core of IoT-edge devices, emphasizing their importance and specific problems. Following that, it uses IDS testing and validation to highlight its current developments and modifications made for the IoT edge. Furthermore, the discourse revolves around FL, which explains its basics, workflow, and how aggregation techniques represent the central part of collaborative ML. In this basic description, readers will understand the complex relationship between ML, IoT security, and FL paradigms within IDS.

A. Internet of Things (IoT)

The IoT is a new paradigm in the IT field. "Internet of Things" is a short form of the two-word phrase: Internet and Things. The internet is an international network of interconnected computer networks that use the Internet protocol suite (TCP/IP) as a communications standard for billions of users around the globe. It comprises millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies [9]. The application of IoT ranges from a small network like home automation to an extensive network like a cloud-based industry application. It can be utilized in many areas, such as environmental monitoring, home automation, agriculture, aquaculture, health care, transportation, and logistics.

B. IoT-Edge Devices

IoT-edge devices are advanced devices that analyze and process data at the edge. They are intended to solve the problem of the enormous amount of data produced by IoT devices, which can be a problem when uploaded to the cloud services because of the direct costs related to uploading, processing, and storing the data [10]. AI is used in some industrial sensors to detect defective parts, like intelligent sensors, computer vision systems, and speech recognition devices. These devices are essential in various applications, such as industrial settings where sensors measure temperature, humidity, and other parameters.

As the IoT-edge devices increase, the management and security of these devices become more difficult for organizations. The main issue of IoT-edge devices is the absence of standardization and compatibility among different devices. Such issues can result in incompatibility and security problems in the IoT ecosystem [7]. Besides, the edge devices' low processing power and storage capacity can be problematic when running security measures and managing updates. The edge devices distributed over different locations make monitoring and controlling the security patches and updates impossible. This distribution of edge devices may make edge devices the weak link of the IoT network, resulting in security breaches and the whole network being unprotected [9].

C. IDS Testing and Validation for IoT-Edge

IDS is the most popular mechanism for detecting different types of intrusions. It consists of three components: data collection, feature selection, and the decision engine. The decision engine affects the system's efficiency. IDSs are divided into three main categories depending on the detection methods: signature-based, anomaly-based, and specification-based [8]. Signature-based IDS identifies the attacks using its signatures stored in a database as a reference. Nevertheless, Anomaly-based IDS detects new intrusions by comparing new entries to its regular behavior pattern. Any change exceeding the specified limit is an anomaly [11]. In addition, the specification-based IDS is a hybrid method that integrates the two preceding techniques. This method combines these techniques to detect new attacks while eliminating false positives.

D. Classification of Artificial Intelligence (AI) Learning Method

Castro et al. classify AI learning methods into five main categories: labeled data, learning architecture, learning strategy, learning environment, and explainability-based (**Table 1**). Regarding the data labeling process, there are three supervised, unsupervised, and semi-supervised learning methods [4].

Table 1. Classification of the AI learning approaches based on enhancing the privacy and security of IoT networks.

	Classification	**Learning Approach**
Artificial Intelligence Learning Approach	Labeled Data	• Supervised Learning • Unsupervised Learning • Semi-Supervised Learning
	Learning Architecture	• Machine Learning • Deep Learning • Hybrid Learning
	Learning Strategy	• Reinforcement Learning • Ensemble Learning • Transfer Learning • Meta-Learning • Active Learning
	Learning Environment	• Centralized Learning • Distributed Learning • Federated Learning • Edge Learning
	Based on Explainability	• Black Box Learning • Explainable Learning

Supervised learning is training a model with the labeled data, enabling the model to make predictions for the new, unseen data points. A few standard models in this category are decision tree DT), linear regression LR) model, support vector machine (SVM), Naive-Bayes NB) classifier, logistic regression (Log. R) method, k-nearest neighbor algorithm (KNN), artificial neural network (ANN) [8]. On the contrary, unsupervised learning tries to find patterns or structures in unlabeled data without using any background information. Some remarkable examples of unsupervised learning techniques are the K-means algorithm for clustering and principal component analysis (PCA) for reducing dimensionality. Other examples are hierarchical clustering and auto-encoders AE). Semi-supervised learning is a hybrid of supervised and unsupervised learning. The model is trained on a combination of labeled and unlabeled data. The semi-supervised learning is significant when the labeled data is limited, or the cost of obtaining it is prohibitive. The model learns from the labeled data and later uses what it learned to the unlabeled data [4].

The learning architecture, the basis of traditional ML techniques, is based on various algorithms that can learn from data without deep neural networks. These are the conventional ML models used to predict or classify. In contrast, Deep Learning (DL) techniques are a part of the ML models that use multi-layered neural networks to model the complex patterns within data. Well-known DL models are convolutional neural networks (CNN), recurrent neural networks (RNN), gated recurrent unit (GRU), long short-term memory (LSTM), deep belief network (DBN), restricted Boltzmann machine (RBM), graph neural network (GNN), generative adversarial network (GAN), and Auto encoder (AE). The learning strategy revolves around reinforcement learning RL), which involves an agent learning to make decisions through interaction with its environment. In contrast, transfer learning TL) involves fine-tuning a pre-trained model on a different but related task. Meta-learning represents a learning approach where the model adapts its learning process by learning from various tasks. Ensemble learning combines different models to improve overall predictive performance [5]. A significant model component is active learning, which involves selecting the most informative samples from the data set to learn, reducing the requirement for extensive labeled datasets, and making the learning process more effective.

Centralized learning occurs when a system or central machine processes data and computation. Indeed, distributed learning requires sharing data and computing resources between several machines or nodes for joint model training. However, ML algorithms have numerous applications and analyze several data types from different IoT devices, including text, numeric, videos, photographs, and location [12]. It uses centralized data, which causes several problems, including data privacy. In addition, ML faces other challenges related to optimization and massive scale [6]. The local data disparities happen when many texts, images, and videos are unevenly stored on gadgets, which is a real problem for information transmission. This problem does not end with the application; it expands its scope with data transfer between client devices and servers. To solve these ML problems, Google developed FL. In FL, devices train the model and store data locally [13]. Another noteworthy one is edge learning, which places AI models on IoT network edge devices.

E. Machine Learning and Federated Learning Techniques for Intrusion Detection

Based on the survey, four main types of AI techniques have been reported for ID: supervised ML, unsupervised ML, semi-supervised ML, and DL models, as represented in **Figure 1**. The supervised ML method for the IDS relied on the SVM, DT, Random Forest RF), and Neural Networks. Zhang et al. stressed the significance of high-quality training data for enhancing detection performance. They presented a potent security framework centered on an SVM incorporating enhanced attributes. Indeed, their implementation of the log marginal probability ratio transformation aimed to enhance SVM-based detection. The empirical results showcased positive outcomes characterized by robust performance, high detection rates, and minimal false positive alarms [6]. In 2010, Heba et al. used Principal Component Analysis (PCA) with SVM to detect IDS and select the optimum feature subset [7]. Further, the discussion section elaborates on these learning methods' applicability to the IDS in detail.

For the FL case, datasets related to network intrusion are used to simulate FL methods and evaluate their performance. So far, FL techniques have been simulated with the following datasets: Wireless Sensor Network dataset (WSN-DS) [8], KDDCup99 [9], CICIDS2017 [10], Network Security Laboratory - Knowledge Discovery and Data Mining (NSL-KDD) [11], GPWST [12], Aegean Wi-Fi Intrusion Dataset (AWID), ISCX20 014, UNSW-NB15 [13], and private data sets [14].

Figure 1: Intrusion Detection employed a variety of algorithmic categories.

3. Recent Advances in Intrusion Detection for IoT

The current study highlights recent literature related to ID with IoT under the beneath of ML and FL, including the work of Ahmed et al., which underscores the significance of detection as a crucial task capable of identifying outliers within a specific dataset. The author underlines that ID is a compelling domain with substantial attention in statistics and ML. Costa et al. highlight the importance of utilizing intelligent tools to assist ID: ID, particularly computer networks [8]. The researcher used the unsupervised optimum-path forest classifier for computer network intervention discovery. As the IoT model continues to flourish within computer networks, accompanied by a growing reliance on devices for this purpose [9], the inevitability of concerns surrounding the security of networked devices on an unreliable Internet becomes evident. They are leading the implementation of various techniques aimed at, to some extent, ensuring the reliability of specific equipment and devices [10].

Additionally, Evans' work provides an intriguing chart that delves into users' perspectives regarding IoT devices, highlighting the exponential growth in this area. IoT faces prevalent cyber security risks, including the Man-in-the-middle (MITM) [5] and the Distributed Denial of Service (DDoS) [7] attack. Ongoing efforts aim to establish protective systems for IoT against such threats. One such system is the Fog Computing-based Security (FOCUS) system, which employs a virtual private network (VPN) to secure devices of the IoT and issues alerts in the event of potential DDoS attacks on IoT platforms. This study substantiated its concept with experiments, displaying its effectiveness in swiftly filtering out malicious attacks while conserving network bandwidth with minimal response time.

Furthermore, according to the opinion of Schukat et al., an inherent lack of security in the wireless and internet sensors, pivotal components of the IoT, leaves the IoT susceptible to diverse assaults [10]. The authors introduced a novel framework for real-time ID comprising modules based on anomaly detection and specific protocols for identifying part of routing assaults commonly observed in the IoT. To achieve this objective, ID gents, following a specification-based approach, are positioned at the router devices. These agents evaluate the conduct of their host nodes and convey their local observations through regular data packets to both the central node and anomaly-driven ID module situated at the root node. Experimental outcomes demonstrate that the suggested live hybrid method resulted in a false positive rate of 5.92% and a valid positive rate of 76.19%, even if facing targeted assaults and scenarios. Zarpelao et al. delve into security concerns, particularly in the IoT and connecting physical devices with the internet, given the increasing prevalence of cyber security threats in everyday tasks [11]. Assaults on vital infrastructure, like electricity generation facilities and public transit systems, can significantly affect urban areas and even entire countries. The study focused on IDS procedures tailored for the IoT and introduced the classification to categorize the research papers in this field. Additionally, it was noted that the progress in creating IDS for the IoT is nascent, and the proposed remedies do not comprehensively tackle the diverse array of attacks and IoT technologies.

Yang et al. emphasized the IoT comprising distributed small devices spanning a broad scope [12] and suggested an anomaly detection-centered plan to safeguard data consolidation against (FDI) assaults. The fundamental concept beyond their efforts revolves around leveraging the strong spatial-temporal correlation observed in consecutive readings in the IoT environmental monitoring to forecast future observations using historical data. Consequently, Neisse et al. worried about intrusion vulnerabilities in IoT devices [13]. Its study introduced model-centered protection tools that smoothly integrate into an administration structure for IoT devices. This toolkit airs the definition and practical assessment of security guidelines, ultimately ensuring the protection of user data. This study was implemented within a smart city context to assess its viability and effectiveness. The pattern introduced in this study facilitated the definition of various trust relationships and factors governing interactions among IoT devices. This model incorporates a reference system for outlining trust aspects and enables the creation of comprehensive security policies based on trust.

Further literature of this study is based on the protection issues within the IoT in the quest to identify potential interventions or weaknesses. [illegible]our et al. conducted a study that showed a keen interest in investigating the IoT routing algorithms and their susceptibilities to assaults [14]. Conti et al. presented an intriguing study that delves into the IoT landscape's intricacies, emphasizing its challenges and opportunities [15]. The authors underscore the importance of establishing a robust IoT network that can identify breached devices, monitor them, and safeguard against potential threats while maintaining a record of evidence of possible attacks or malevolent actions.

This investigation primarily centered on elucidating the notable hurdles faced within the realm of IoT. Additionally, the authors pointed out that identifying the existence of the IoT poses considerable difficulty, particularly given that these devices are engineered to operate inactively and independently. Over recent years, integrating ML methods to enhance safety and intrusion discovery within IoT settings has gained paramount significance in tackling the previously mentioned challenges [illegible]. However, it is noteworthy that we have encountered relatively few studies that have leveraged ML and FL to tackle safety issues in IoT surroundings. Deep learning (DL) has garnered substantial interest in recent years. It is now acknowledged as a significant approach not only for network IDS (NIDS) but also for its applications in the fields of text mining, pattern recognition, and image processing. Görmüş et al. also highlighted that security metrics of this nature could prove beneficial not only for users of various internet infrastructures but also for domains like cloud computing and, notably, the IoT, which has been a focal point of growing security concerns [9].

Furthermore, Schukat et al. highlighted challenges and problems associated with planning and implementing IoT systems [10], which explored the intricate relationship between fog computing, cloud computing, extensive data analytics, and the IoT. However, the authors also introduced an innovative, intelligent approach to enhance independent management, data consolidation, and protocol adjustment services to enhance seamless integration across diverse IoT devices. This study mainly focused on targeting IoT guidelines and examining various guidelines across various levels within the IoT ecosystem. The authors further delved into the core functionalities and objectives of these protocols. It encompassed the ramifications of IoT, including Big Data, cloud computing, and fog computing. It underscored the necessity for a novel generation of data analytics algorithms and tools tailored for IoT big data, emphasizing the importance of managing input size efficiently. This study's focus was IoT protocols and standards, examining various protocols and patterns across different layers within an IoT ecosystem. In short, the authors presented three use cases demonstrating how the multiple protocols discussed in this study synergize to facilitate the creation of innovative smart IoT services that offer novel functionalities to users.

Lopez-Martin et al. directed their research towards multidisciplinary solutions facilitated by an appropriate platform. They aimed to explore the possible interplay and mutual influences among different aspects of the IoT systems [1]. This prototype serves as a means to evaluate and enhance various multidisciplinary aspects of the IoT framework, Encompassing aspects of data processing, communications, and hardware design. Zarpelao et al. introduced innovative security monitoring for networks tailored particularly to IoT networks. This method relies on a Conditional Variational Auto encoder (CVAE) with a specialized architecture incorporating intrusion labels within the decoder layers. The introduced model can perform feature reconstruction, rendering it suitable for incorporation into the existing Network IDS, a component of network monitoring systems, with a particular focus on IoT networks. Notably, this method functions within a lone training phase, resulting in efficiency gains and conservation of computational resources. In this study, the authors introduced an approach grounded in automata theory, tailored explicitly for the extensive and diverse landscape of the IoT. This technique utilizes an expanded version of labeled state transition to provide a standardized depiction of the IoT framework. Enabling ID by analyzing action flows and their comparisons [11], this research encompassed the design of a security monitoring approach, the creation of Event Databases, and the development of an Event monitor to identify known cyber-attacks. This scenario highlighted the challenge of even sophisticated methods such as classical ML. Systems encounter in identifying these subtle variations of attacks that evolve gradually.

Conti et al. explored the safety of the IoT configuration that leverages (SDN). Within this situation, the software-defined configuration operates without or with a backbone, referred to as a Software-defined network [15]. Their study elucidated the functioning of the suggested configuration and underscored the potential to enhance network safety with greater efficiency and flexibility through software-defined networks. This article explored network access management and worldwide traffic surveillance in ad-hoc networks. Additionally, it highlighted specific architectural design decisions related to SDN utilizing Open Flow and examined their potential effects. Ramos et al. conducted an investigation centered on quantitative security metrics derived from modeling, which intended to provide a quantifiable assessment of the overall effectiveness of IDS approaches [16]. Their proposed IDS demonstrated the capability to identify three forms of IoT attacks: replay attack, jam attack, and false attack.

Nonetheless, in the context of safety and intrusion avoidance in the IoT, it is apparent that the configuration of the IoT systems has not yet been standardized. Organizations like IEEE and ITU are actively involved in standardizing IoT. Adat et al. note that technologies like IEEE 802.15.4, IPv6, and 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) have been established as foundational platforms for IoT [17]. However, the author also highlights that there are relatively limited standardized IoT configurations, with a more significant part of them emphasizing network layer and IoT-specific layer requirements. The most comprehensive and generic IoT-layer architecture is illustrated in **(Figure 2)**. It uses data management, application, network, and perception layers. Gunupudi et al. emphasized that preserving secrecy and conducting intrusion discovery within the IoT context is inherently challenging and significantly more complex [2]. Their work introduced a membership function to cluster attributes within the global dataset incrementally. The objective was to depict every piece of data in multiple dimensions within the worldwide data set, employing a comparable technique with decreased dimensions. They attained this condensed depiction via a dimensionality reduction technique. That subsequently served as data for the categorizer.

Bhuyan et al. utilized the balanced outcome as the foundation for the effortless intrusion discovery method, drawing upon the principles of game theory [18]. This method primarily focused on forecasting the stable condition, enabling the intrusion detecting system to trigger its aberration discovery mode for Detecting novel attack patterns. Their study's findings demonstrated the generated data's viability, showing casing out standings detection rates, minimal false alerts, and low energy usage. Suo et al. recognized the necessity of IoT middleware mainly because most devices have limited resources [19]. By introducing this enhancement, it became feasible to implement intelligent decision-making mechanisms within the middleware.

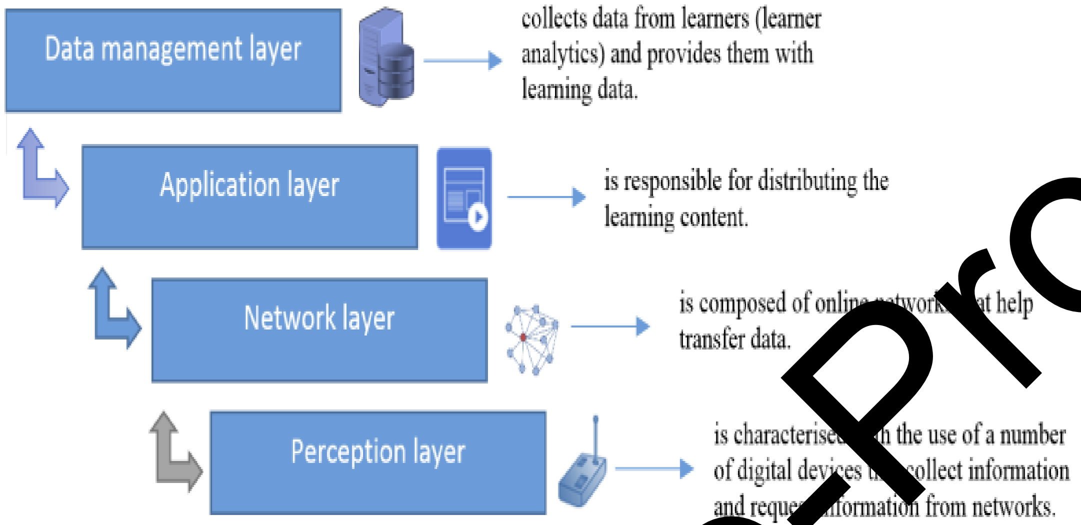


Figure 2: Layers of a generic IoT architecture.

Pasini et al. undertook a research endeavor that delved into the implications of IoT within the industrial automation sector [3]. Their study presented an innovative architecture to facilitate the incorporation of established legacy industry-grade devices for internet-based functionality. The swift proliferation of IoT has sparked apprehensions regarding the amalgamation of established technologies and the integration of novel approaches, particularly in the security domain. Consequently, many significant research initiatives within the IoT sphere have emerged, with a dedicated emphasis on understanding the behavior of IoT-based systems concerning computer network security. Numerous IoT-related studies have introduced fresh technologies that seamlessly integrate with the paradigm, consistently prioritizing security concerns [16]. Security issues, like cyber-attacks, stand in line with pivotal elements - authentication, integrity, confidentiality, availability, and access control. A comparative analysis of different surveys that approach AI-based solutions like IoT security and privacy is represented in the comparative study of Castro et al. [4]. For the security requirements desired, we found out that traditional authentication, like social engineering and password guessing, gives room for attackers to gain access to the network. The survey (Wu[illegible] et al., 2020) provides an in-depth description of how AI approaches recognize human biological and behavioral characters and static and dynamic device operating information to make authentication decisions [5].

Consequently, Hussain et al. delineate approaches to apply ML and DL models for access control systems [20]. Kazi Istiaque et al. offers conventional ML and RF-based methodologies to implement a distribution authentication and authorization algorithm [21]. Data integrity and other methods are covered, including tamper detection and false data injection attack detection. Privacy issues are overshadowed, and the importance of applying block chain technology to this matter is emphasized. Maurya et al. offer the federated transfer learning (FTL) approach to solve the authentication and protection of privacy issues at the same time using the DDPG (S-TD3) method with support from the twin delayed system for industrial-IoT [22]. The approach ensures the privacy and security of all industrial implementations by using block chains. The mechanism of proof of storage by transfer learning (TLS), a standard for tackling the preservation and safety requirements is introduce. The novel significant humane twin routine DDPG trains the user model in recognizing specific areas. The tactic allows the devices to share different data types in businesses' local and "big" data operations, including the more significant forms of data.

The other approaches pay attention to preventing poisoning attacks in decentralized learning networks. Li and his colleagues introduced a multi-tentacle FL (MTFL) framework that responds to adaptive poisoning attacks in the software-defined industrial IoT (SD-IoT). The architecture allows network members of FL to be connected to tentacles when connecting specific attributes to learning obligations. The TD-EPAD algorithm, a tentacle-based efficient poisoning attack detection algorithm, is introduced here, which is employed to detect the poisoned data, and a stochastic tentacle data exchanging (STDE) protocol is put forward to substitute the poisoned data with standard data. Zhang et al. [6]. Zhang et al. pose a defense approach to resisting poisoning attacks in FL systems, particularly IoT scenarios. The authors discuss a strategy called "Pivotal Adversarial Training," which is targeted at making the impact of poisoned local updates less significant. This is done by building a pivotal property of a neural network model, which will induce the model to pivot when it comes to the sensitive attribute by building an additional model on the output log it has to predict which attributes exist in the dataset. Lastly, the anomaly detection system based on an ML model (AD-ML) that detects sensor tampering in IoT systems is also covered [6]. The system leverages both unsupervised and supervised ML algorithms by employing them to analyze network traffic patterns and give an alert when any anomalies are found.

Moreover, the ML derived by the Microcontroller Unit Chip Temperature Fingerprint (MTID) method is also reported, which entails the adoption of an SVM classifier to identify intrusions in IoT systems by exploiting temperature fingerprints [20]. Popoola et al. suggested a Federated Deep Learning (FDL) method to detect zero-day botnet attacks and prevent data leakage in IoT edge devices. This method uses the best DNN architectural design to classify network traffic. A model parameter server on the remote side controls the independent training of DNN models running on multiple IoT edge devices, and the FedAvg algorithm is used to integrate local model updates. A global DNN model is generated when the parameter server and the IoT edge devices exchange parameters over several communication rounds [23].

4. Methods and Results

A. Mathematical Methods

1- Dataset Selection and Preprocessing:

The study utilizes multiple datasets relevant to network intrusion detection, such as the Wireless Sensor Network dataset (WSN-DS), KDD Cup99, CICIDS2017, and others. Each dataset was selected based on its applicability to simulating intrusion detection systems (IDS) in IoT environments. Data preprocessing included steps to normalize and clean the data, ensuring consistency across different datasets. The preprocessing also involved feature extraction and selection, applying techniques like Principal Component Analysis (PCA) to reduce dimensionality and improve computational efficiency. Accuracy, Precision, Recall, and F1-Score: These metrics are commonly used to evaluate the performance of IDS models. They can be calculated using the following formulas:

• Accuracy: is the ratio of true detection over the whole instances.

$$\text{Accuracy} = \frac{TP+TN}{Total\ sample}$$

• Recall is how often does it predicts correctly. Also known as Sensitivity or True Positive Rate (TPR).

$$\text{Recall} = \frac{TP}{TP+FN}$$

• Precision indicates how often it is accurate when it is predicted to be accurate.

$$\text{Precision} = \frac{TP}{TP+FP}$$

• F1-measure is the average of recall and precision weight. The mathematical representation of all measures can be deduced from the confusion matrix.

$$\text{F1-measure} = 2 * \frac{Precision * Recall}{Precision + Recall\ pop}$$

2- Model Training:

For this study, various machine learning (ML) models were employed, including supervised learning models like Support Vector Machines (SVM), Decision Trees (DT), and Neural Networks. These models were trained using a cross-validation approach to ensure robustness. The training process involved fine-tuning hyper-parameters through grid search and validation against a separate validation set to prevent over fitting.

2- Federated Learning (FL) Framework Implementation:

The study implemented an FL framework to address privacy concerns associated with centralized data processing. The FL framework allowed for collaborative model training across distributed IoT devices without sharing raw data. Instead, model updates were aggregated using techniques like Federated Averaging, ensuring that the learning process remained efficient and scalable. The FL framework was tested under various scenarios to assess its performance in terms of accuracy, latency, and resource consumption.

3- Intrusion Detection Evaluation:

The intrusion detection capability of the models was evaluated using metrics such as True Positive Rate (TPR), False Positive Rate (FPR), Precision and F1 Score. The study also analyzed the impact of different types of attacks on detection performance. Additionally, the performance of the FL-based IDS was compared to traditional centralized ML models to assess the trade-offs in terms of security, privacy, and computational efficiency.

4- Validation of Results:

The models' results were validated through repeated experiments under different network conditions and attack scenarios. Sensitivity analyses were conducted to understand how changes in the IoT environment (e.g., varying the number of devices, network latency) impacted model performance. Furthermore, the results were cross-verified using alternative datasets to ensure generalizability.

B. Results of Methods:

- **Performance of Supervised Learning Models:**

The results showed that supervised learning models, particularly SVM and Decision Trees, achieved high accuracy rates in detecting intrusions. SVM, with an optimized kernel function, performed exceptionally well, achieving an accuracy of over 90% on the CICIDS2017 dataset. Decision Trees also demonstrated strong performance, particularly in scenarios involving well-defined attack signatures.

- **Federated Learning Outcomes:**

The FL framework demonstrated comparable accuracy to centralized models, with a marginal decrease of about 2-3% in accuracy due to the distributed nature of data processing. However, the trade-off was justified by significant improvements in data privacy and reduced risk of data breaches. The results also highlighted that FL could effectively handle the heterogeneity of IoT devices, maintaining performance across various network configurations.

- **Anomaly Detection Capability:**

The study revealed that anomaly-based IDS within the FL framework could detect novel attacks that were not part of the training data. The anomaly detection model, using a combination of PCA and

SVM, achieved a true positive rate of 85% with a false positive rate of 7%, indicating its effectiveness in identifying previously unseen threats.

- **Comparative Analysis:**

When comparing FL with traditional centralized ML models, the results indicated that FL provides a more secure and scalable solution for IoT environments. The study noted a slight increase in communication overhead due to model updates, but this was mitigated by the reduced need for raw data transfer.

5. Addressing Data Security Challenges in IoT Expansion

The increasing expansion of the IoT brings a significant rise in concerns related to data security risks. These concerns arise from multiple factors, encompassing vulnerabilities in IoT devices that can lead to intrusion attempts, denial of service attacks, and viruses. Implementing more robust measures to address these risks caused by the mentioned factors adequately is crucial. That enables system programmers and IoT makers to strengthen their protection protocols. Identifying and mitigating all potential vulnerabilities and threats tailored for IoT architectures are paramount. Addressing and mitigating potential threats necessitate a greater emphasis on in-depth studies to enhance our understanding of these threats within the IoT context.

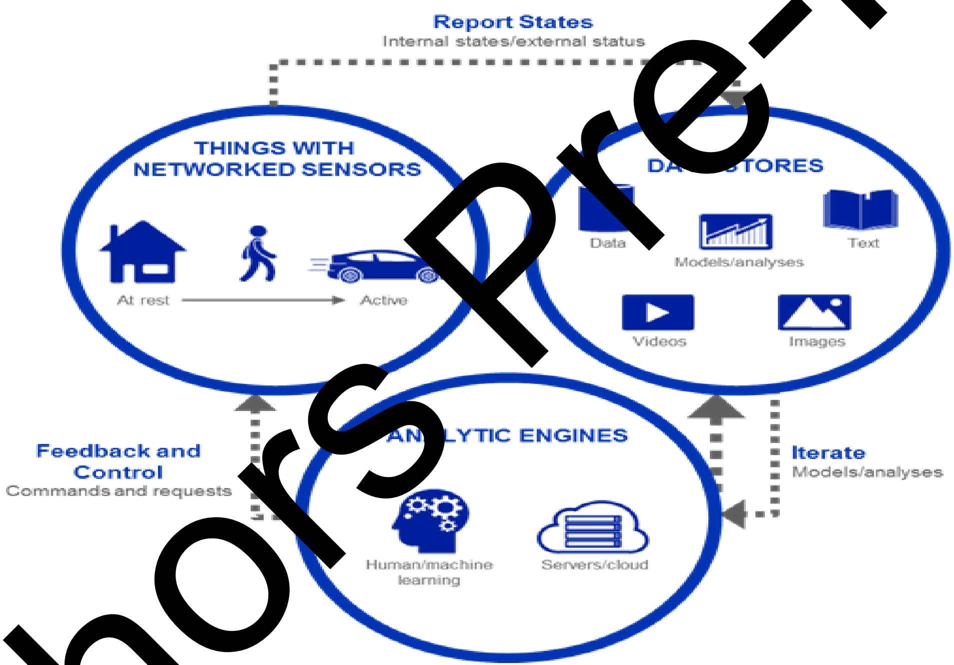


Figure 3: The three main views of IoT.

Furthermore, it is essential to tackle security challenges like concerns about secrecy that have been recognized to minimize their impact and prevent them from compromising IoT systems. Able amount of work must be must. This work should target suppliers and users to enhance IoT application reliability progressively. The trend is to focus more precisely on addressing security challenges within IoT services and devices. According to Karsligel et al., IoT is still rapidly evolving, driven by the increased utilization of sensors to collect, organize, and mine data on the internet, encompassing sensor-equipped hardware [24]. **Figure 3** illustrates three primary perspectives of the IoT to elucidate this setting: (i) the "Things with Networked Sensors," which emphasizes embedded sensors for tracking various entities; (ii) the "Data Stores," focusing on the creation of intelligent objects; and (iii) the "Analytic Engines," addressing challenges related to data interpretation.

Karsligel et al., also underscore a critical concern, highlighting the severe security risks posed by IoT when these devices are deploying within businesses. In such scenarios, attackers could gain access through various intrusion techniques, opening the door to corporate espionage by the malicious infiltrator [24]. The authors also identify several security challenges in the context of IoT, which include IoT's integration with various technologies, scalability concerns, managing Big Data generated by IoT, ensuring the provision of facilities for the IoT, addressing hardware limitations for programs, enabling access in supporting delay-sensitive, dealing with mobility issues and remote locations facilities.

Current IoT research has broadened its horizons, moving beyond concerns related to power consumption. A noteworthy emerging trend involves the integration of IDS across multiple layers within network architectures, departing from the conventional emphasis on the lowest layer. Furthermore, there has been a noticeable shift towards adopting tailor-made IDS tools for IoT support. This shift is poised to capture many substantial interests from software developers, encompassing both commercial software and open-source solutions. Further research on IoT related to IDS moves towards ML in the FL environment.

The RFs, a composite ensemble method of D.T. Nabila Farnaaz and her co-authors, designed an IDS system model based on the RF classifier, and its performance was evaluated on the NSL-KDD dataset. RFs are a group of classifiers and perform relatively well against other traditional classifiers when classifying attacks. This highly efficient model has a minimum false alarm and maximum detection rates. Stefanova and Ramachandran suggested a two-phase network intrusion classification. In the first stage, traffic was classified as "norma" or "attac" giving the second stage a chance to classify attack traffic by type. The proposed method incorporates the RF and partial DT. Popoola et al., proposes using IDS, which utilizes an active learning approach. This method uses the RF classifier and k-means algorithms [23].

Auto-Encoder IDS (AE-IDS) based on a Random Forest (RF) algorithm has been reported in another study. This method consists of the selection of features and their grouping in the training data set. Following training, the network auto-encodes to predict the results, reducing detection time and improving prediction precision. Other RF-based models for detecting IDS have been reported to improve the model's performance.

6. Study Contributions

This study makes several significant contributions to the field of network security, particularly in the context of IoT environments:

A. Advancement in Federated Learning for IDS:

The research introduces a novel application of Federated Learning in the development of Intrusion Detection Systems for IoT. By leveraging FL, the study addresses the critical challenges of data privacy and security inherent in centralized ML approaches, offering a scalable and efficient alternative that reduces the risk of data breaches.

B. Comprehensive Evaluation of ML Techniques:

The study provides an in-depth analysis of various supervised learning models, highlighting their strengths and limitations in detecting network intrusions. This evaluation helps identify the most effective algorithms for deployment in real-world IoT environments.

C. Introduction of Anomaly Detection Mechanisms:

The integration of anomaly detection within the FL framework represents a key innovation, enabling the identification of novel and unknown threats. This capability is crucial for enhancing the resilience of IoT networks against evolving cyber-attacks.

D. Benchmarking with Multiple Datasets:

By utilizing and benchmarking against a wide range of publicly available datasets, the study ensures that its findings are robust, generalizable, and applicable to diverse IoT scenarios. This approach also provides a reference point for future research in the field.

E. Contribution to IoT Security Paradigms:

The study contributes to the ongoing discourse on IoT security by demonstrating how ML and FL can be effectively integrated to protect IoT devices. The findings pave the way for future developments in secure, distributed learning environments, ultimately contributing to the broader goal of securing next-generation IoT ecosystems.

7. Conclusions

This study has concentrated on the latest advancements in ID and the application of intelligent techniques in the IoT sphere to ensure data security. The papers examined in this article primarily addressed the notable concern and extensive endeavors undertaken by the scientific community and industry. These efforts have revolved around the creation of optimized security protocols. These protocols aim to balance delivering adequate protection while keeping energy consumption low or moderate. This research explored various intelligent techniques employed within computer network security, specifically focusing on ID. While these techniques aim to enhance detection accuracy, it remains evident that addressing the false positive rate continues to be a prevalent challenge across all studies. Specific methods can effectively reduce the false grade. Conversely, some techniques follow the opposite approach: they stabilize the false grade but demand substantial computational resources for training and testing. This matter is relevant in the ID context, emphasizing the need for real-time identification.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot," *Sensors,* vol. 17, p. 1967, 2017.

[2] R. K. Gunupudi, M. Nimmala, N. Gugulothu, and S. R. Gali, "CLAPP: A self constructing feature clustering approach for anomaly detection," *Future Generation Computer Systems,* vol. 74, pp. 417-429, 2017.

[3] D. Pasini, S. M. Ventura, S. Rinaldi, P. Bellagente, A. Flammini, and A. L. C. Ciribini, "Exploiting Internet of Things and building information modeling framework for management of cognitive buildings," in *2016 IEEE International smart cities conference (ISC2),* 2016, pp. 1-6.

[4] O. E. L. Castro, X. Deng, and J. H. Park, "Comprehensive Survey on AI-Based Technologies for Enhancing IoT Privacy and Security: Trends, Challenges, and Solutions," *HUMAN-CENTRIC COMPUTING AND INFORMATION SCIENCES,* vol. 13, 2023.

[5] J. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing internet of things security: A survey," *Ieee Access,* vol. 8, pp. 153826-153848, 2020.

[6] Y. Zhang, Q. Yang, D. An, D. Li, and Z. Wu, "Multistep multiagent reinforcement learning for optimal energy schedule strategy of charging stations in smart grid," *IEEE Transactions on Cybernetics*, 2022.

[7] F. E. Heba, A. Darwish, A. E. Hassanien, and A. Abraham, "Principle components analysis and support vector machine based intrusion detection system," in *2010 10th international conference on intelligent systems design and applications*, 2010, pp. 363-367.

[8] K. A. Costa, L. A. Pereira, R. Y. Nakamura, C. R. Pereira, J. P. Papa, and A. X. Falcão, "A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks," *Information Sciences,* vol. 294, pp. 95-108, 2015.

[9] S. Görmüş, H. Aydın, and G. Ulutaş, "Security for the internet of things: a survey of existing mechanisms, protocols and open research issues," *Journal of the Faculty of Engineering and Architecture of Gazi University,* vol. 33, pp. 1247-1272, 2018.

[10] M. Schukat, P. C. Castilla, H. Melvin, and F. Hu, "Trust and trust models for the iot," *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations,* 2016.

[11] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications,* vol. 84, pp. 25-37, 2017.

[12] L. Yang, C. Ding, M. Wu, and K. Wang, "Robust detection of false data injection attacks for data aggregation in an Internet of Things-based environmental surveillance," *Computer Networks,* vol. 129, pp. 410-428, 2017.

[13] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: a model-based security toolkit for the internet of things," *computers & security,* vol. 54, pp. 60-76, 2015.

[14] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," *Journal of Network and Computer Applications,* vol. 66, pp. 198-213, 2016.

[15] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," vol. 78, ed: Elsevier, 2018, pp. 544-546.

[16] A. Ramos, M. Lazar, R. Holanda Filho, and J. J. Rodrigues, "Model-based quantitative network security metrics: A survey," *IEEE Communications Surveys & Tutorials,* vol. 19, pp. 2704-2734, 2017.

[17] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems,* vol. 67, pp. 423-441, 2018.

[18] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *Ieee communications surveys & tutorials,* vol. 16, pp. 303-336, 2013.

[19] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering,* 2012, pp. 648-651.

[20] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials,* vol. 22, pp. 1686-1721, 2020.

[21] K. Istiaque Ahmed, M. Tahir, M. Hadi Habaebi, S. Lun Lau, and A. Ahad, "Machine learning for authentication and authorization in iot: taxonomy, challenges and future research direction," *Sensors,* vol. 21, p. 5122, 2021.

[22] S. Maurya, S. Joseph, A. Asokan, A. A. Algethami, M. Hamdi, and H. T. Rauf, "Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT," *Sensors,* vol. 21, p. 7793, 2021.

[23] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices," *IEEE Internet of Things Journal,* vol. 9, pp. 3930-3944, 2021.

[24] M. E. Karsligel, A. C. Yavuz, M. A. Güvensan, K. Hanifi, and H. Bank, "Network intrusion detection using machine learning anomaly detection algorithms," in *2017 25th Signal Processing and Communications Applications Conference (SIU),* 2017, pp. 1-4.