Machine Learning-based Techniques for Secure and Efficient IoT Data Management

Tim Kramer

Supervisor(s): Mauro Conti, Chhagan Lal

EEMCS, Delft University of Technology, The Netherlands

A Thesis Submitted to EEMCS Faculty Delft University of Technology,
In Partial Fulfilment of the Requirements
For the Bachelor of Computer Science and Engineering
January 29, 2023

Name of the student: Tim Kramer
Final project course: CSE3000 Research Project
Thesis committee: Mauro Conti, Chhagan Lal, Jorge Martinez

Abstract

The dramatic increase in the number of Internet of Things (IoT) devices has created rapid growth for exploitation of security flaws and vulnerabilities. Particularly for critical infrastructure and real-time systems security threats can be highly damaging. Machine Learning (ML) algorithms have demonstrated the ability to combat the security threats and improve the efficiency of data management within IoT networks. This paper addresses how ML methods improve security and efficiency. A review of the current approaches is conducted and these approaches are categorized into detection systems as well as privacy and efficiency enhancements. The proposed future research directions are then presented to address the limitations of the state-of-the-art ML-based IoT security methods.

***Keywords*—Internet of Things; Machine Learning; Security; Efficiency**

1 Introduction

In recent years the number of Internet of Things (IoT) devices has increased, both in the business and consumer sectors. As of 2022 an estimated 12 billion [1] IoT connected devices exist and that number is expected to increase to 30 billion by 2030, with a third being consumer internet and media devices. With this increase in devices and the use of IoT in critical infrastructure applications (e.g. power plants, autonomous vehicles, military) secure, privacy-preserving and efficient data management are crucial. The attack surface of IoT devices is increased in comparison to widespread IT, due to its more heterogeneous data, communication protocols and data management [2]. There is a high demand for secure IoT applications and accelerated growth in the IoT industry.

Due to the steady advance and improvements in Machine Learning and IoT the applicability in their merge is promising, yet the challenges of current Machine Learning techniques for IoT data security and efficiency are evident [3]. With the computational limitation of the IoT devices, security methods have to be carefully selected, and traditional internet security mechanisms are not always applicable. Machine Learning's promising role in improving the security of IoT systems suggests that further research into this field is proposed.

The following research question will be answered based on the findings in section 4 of this paper: *How does the use of Machine Learning methods support secure and efficient data management in IoT domain?*

The main methodology used in this paper to answer the research question is as follows:

1. Identify the metrics for IoT data management security, efficiency, and privacy (e.g. network uptime, scalability and performance)
2. Discuss the Machine Learning techniques that can be used for IoT data management security, privacy, and efficiency (e.g. (un-)supervised- or reinforcement learning)
3. Evaluate how these approaches improve the security, efficiency, and privacy of IoT data management.
4. Determine the pros and cons of the studied machine learning solutions for IoT security, privacy, and efficiency.
5. Propose future research directions addressing the challenges in IoT data management security, privacy, or efficiency, based on the previous findings.

The structure of this paper begins with the background of the research in section 2, including IoT security and ML. Related work and the gaps in research are presented in section 3. Section 4 follows with the main evaluation and analysis of the state-of-the-art in ML-based IoT security solutions. In section 5 the discussion of results and future research directions are presented. The responsible research and conclusion in sections 6 and 7 finalize the paper.

2 Background

To evaluate how ML methods can be used to support secure and efficient IoT data management the background of each of the technologies needs to be studied. In this section the Internet of Things and its attack vectors are explained. Lastly ML algorithms and their categories are described.

2.1 Characteristics and Types of Attacks in IoT

The Internet of Things (IoT) describes the multitude of wireless and wired, internet connected devices that share a number of characteristics. The characteristics include heterogeneity of data, heterogeneity of communication protocols, interconnectivity in global and local ranges, low-power, low-cost and dynamic organization [3]. As illustrated by Butun et al. [4], IoT is the convergence of Wireless Sensor Networks (WSNs), Real-Time Computing, Embedded Systems and Actuation, allowing for a multitude of tasks including data creation (sensing), processing, computation and actuation into the environment. Hence the division into four layers: sensing layer, network layer, middleware layer, and application layer by Hassija et al. [2]. With these characteristics the security and efficiency issues can be defined and categorized.

Attacks on IoT devices can be categorized into passive and active attacks. The types of attacks, as mentioned in [2] for each layer can be listed as follows. For sensing, node capture attacks, where a malicious user gains control of the device, malicious code or false data injection, side-channel attacks, based on processor architecture, power consumption and electromagnetism, eavesdropping and more. Common attacks in the network layer are denial of service (DoS) or dedicated DOS (DDoS) attacks, routing attacks and advanced persistent threats. The middleware layer is exposed to man-in-the-middle attacks, malware injection, and sql injection. Within the gateway layer, used for connecting a multitude of devices, secure on-boarding, extra interfaces, end-to-end encryption, and firmware updates are pose security issues. Finally for the application layer data theft, service interruption and access control attacks are prevalent. Advanced persistent threats (APT) [5] in particular can compromise a network over a longer time-frame and target a specific network

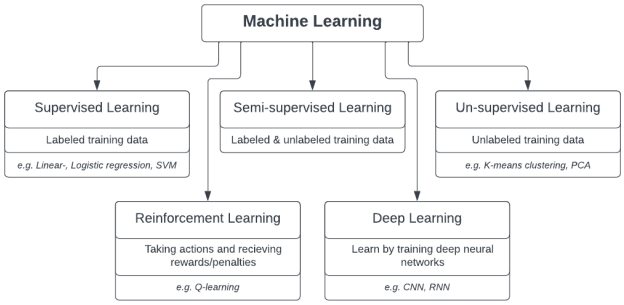

Figure 1: Machine Learning types

or device. Owing to that they are more advanced than other attacks. The strategy of an APT is defined during the reconnaissance, then malicious code is delivered and installed. Lateral movement in the network is then possible and data can be ex-filtrated. Lastly remaining evidence is erased.

2.2 Machine Learning

Methods that can utilize the large amount of data and increase task performance, are the Machine Learning (ML) and Deep Learning (DL) algorithms. These algorithms can be categorized into supervised, unsupervised and reinforcement learning. Figure 1 shows these categories with the addition of semi-supervised learning and deep learning (DL). When considering ML in IoT security Hussain et al. [3] describe the general use cases for the different types of ML algorithms. The main use of supervised and unsupervised learning is for data analysis, while reinforcement learning is mainly used for comparison and decision making.

Some of the algorithms that should be highlighted are, random forest (RL), neural networks, auto encoders, generative adversarial networks (GAN), and deep Q-networks (DQN) [6].

Random forest is comprised of multiple decision trees, each trained on different randomly chosen subsets of data and features. Finally the predictions of each decision tree are averaged.

The **auto encoder** is a deep learning model that has two parts, the encoder and the decoder. The encoder abstracts the input into a lower feature space code and the decoder tries to recreate the input from the code.

Generative adversarial networks generate data samples from the learnt distribution, and train the two models of the generative and discriminative sort.

Finally **deep q-networks** are a form of deep reinforcement learning that is trained by learning the q-function value, which is based on the state and the action selected.

3 Related work

Already established work on the issues of current ML methods for IoT security is discussed in this section. Some of these surveys compile and study research on ML methods and IoT security individually, which are highlighted in the first part of this section. Finally the survey of surveys is conducted with a summary and review of surveys on machine learning-based security approaches.

In Butun et al. [4] IoT attacks are grouped into passive and active attacks. The OSI-layer model is used to further distinguish active attacks. The gathered defense mechanisms against attacks towards wireless sensor networks (WSNs) and IoT cover multiple facets. These include cryptography, encryption algorithms, machine learning methods (e.g. swarm intelligence), hardware and networking protocols, among others. This survey focuses on IoT security more heavily than the following five surveys.

There exist various literature surveys on the use of Machine Learning methods for IoT Security [2, 4, 6]. In the following section a number of these surveys are summarized and reviewed. Table 1 contains the summary of the review and the specialization and focus of the surveys are compared with regard to security, efficiency and privacy.

Machine Learning in IoT Security: Current Solutions and Future Challenges [3] Hussain et al. have written a survey that categorizes the security threats into layers, similar to the OSI-layers with the addition of multi-layered and cloud-based attacks. These security and privacy issues found in IoT are then further described in terms of the security requirements and attack surfaces of IoT devices. The current use of Machine Learning for IoT security is described and grouped by ML algorithm type. Furthermore the limitations of traditional ML techniques and the typical limitations of using ML approaches in IoT environments are discussed, including processing power, energy, data management and data analytics. The survey continues with a description of the existing ML-based solutions for a number of IoT security issues corresponding to authentication, detection and analysis. DoS and Distributed DoS attacks are examined separately from the general attack and anomaly/intrusion detection methods. Finally the open issues and future research directions are identified, which include the limitations of DL, DRL, IoT Data and efficiency.

The survey by Hussain et al. gives a well structured and well-defined overview over the intersection of IoT security and ML solutions. Having the taxonomy of the survey gives a clear outline for readers to identify specific attacks or ML solutions to read about. Furthermore providing the lessons learned provides a good summary of the key takeaways from the previous section. Compared to other surveys studied in this section, access control methods and authentication are discussed by Hussain et al. to a greater extent. Their survey of research papers on ML- and DL-based access control and authentication methods provides variety when the majority of methods studied are detection-based. A disadvantage is that only a limited amount of security issues that are addressed by ML techniques are included, either due to lack of research in those areas or non-applicability and scope. Overall the survey is a good snapshot of the current research on ML techniques for IoT security and provides a detailed direction for further research.

A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security [6] Al-Garadi et al. pro-

Survey, Year	Description	Specialization	Sec.	Eff.	Priv.	Advantages	Disadvantages
[3], 2020	ML based security solutions grouped by threat layers: physical, physical and link, network, transport, and application layers.	General	●	●	●	Clear structure and outline Includes authentication and access control	Limited amount of IoT security issues
[6], 2020	Evaluation of ML and DL methods for IoT security for each layer and description of open issues, limitations, future research directions (e.g. data quality, learning strategies and integration of technologies).	General	●	○	●	Detailed taxonomy of ML/DL for IoT security Privacy included Extensive security properties listed and discussed	Limited amount of non-detection based ML/DL methods discussed Authorization not discussed
[7], 2022	Advanced persistent threat and network intrusion detection using ML and signature-based, anomaly-based, hybrid, and collaborative methods. The PASTA threat model is used to analyze the attacks.	APT	●	○	○	High cost security issue APT is broad enough but remains in a specific workflow Evaluation of IoT datasets Recently published	Limited amount of papers on fully encompassing APT detection, mitigation and avoidance
[8], 2022	Application of ML algorithms for real time systems. Evaluation of ML algorithms in terms of schedule-ability and adaptability discussed.	RTS	○	●	○	RTS has high importance for critical infrastructure Applicability of ML solutions to industry sectors ML-solution efficiency discussed	Limited discussion of ML-based privacy and security of IoT RTS
[9], 2022	ML based smart attacks, categorized into data analysis, behavioral deduction, data generation and behavioral diversion	ML-based attacks	◑	○	●	IoT Security from offense perspective Growth of ML-based attacks	Lacking discussion of future research in terms of defensive security

Table 1: Summary of surveys on ML based IoT security solutions and comparison of their coverage (High: ●, Medium: ◑, Low: ○, Sec: Security, Eff: Efficiency, Priv: Privacy)

vide a general ML and DL survey for IoT security. Their contribution contains the individual description of the state-of-the-art in IoT system attack vectors and the use of ML and DL methods to combat these attack vulnerabilities. Additionally the general IoT system characteristics and layers are described, providing a bases for why risks for IoT security are present. Following these system characteristics the security properties are provided upon which different methods can be compared. The threats mentioned in the paper are categorized into physical, network, cloud, web and application, and new attack surfaces. An extensive review of a majority of machine learning and deep learning methods is conducted. The advantages and disadvantages of each method are provided and the applicability to IoT security is mentioned. Most methods can be used for varying forms of detection. The studies on the state-of-the-art methods are summarized and compared. Finally, after gathering the background and state-of-the-art research, the issues, challenges and future research directions are proposed. These include the improvement of security related datasets, the need for ML and DL methods to maintain high accuracy on low-fidelity data, the augmentation of IoT security data, the choice of different learning strategies based on the type and timeframe of the attack, and the use of ML and DL in different environments. Lastly ML and DL issues, DL/ML integration approaches (e.g. blockchain) and security trade-offs are presented.

The survey by Al-Garadi et al. provides a well-structured and comprehensive taxonomy of the application of Machine Learning and Deep Learning for IoT security. Their graph of the taxonomy provides a visual overview of the survey and guides the reader along the concepts and structure. In terms of breadth of discussion on ML and DL methods, this survey provides a wider range compared to the other surveys studied. Another advantage of the survey is the extensive list of security properties and their threats, for which the related work is highlighted. On the other hand, some of these properties (e.g. non-repudiation) are not further used to evaluate and compare the ML methods and ML-integrated approaches. The inclusion of ML and DL privacy related issues and future research directions is a beneficial quality of the paper, due to the limited amount of research on privacy preserving methods by the other surveys. A slightly different naming convention to the OSI model is used and cloud services is included. Their categorization is more granular but the structure is different from what the majority of the studied surveys have. Finally another disadvantage is the limited discussion on authorization and ML/DL solutions for access control security. The majority of approaches center around detection, where a lack of mitigation techniques is evident.

Machine Learning-enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats [7] Chen et al. survey the literature on Machine Learning-enabled IoT security with a special focus on Advanced Persistent Threats (APT) in IoT Security. The defense against advanced persistent threats is important yet challenging considering their long time frame and hidden nature. The survey opens with security features of IoT and industrial IoT, discussing the different IoT layers. Then the typical attacks, APT attacks and threat model analysis on IoT are explained. In terms of intrusion detection, signature-based, anomaly-based, and hybrid approaches are discussed and categorized. Three groups of machine learning algorithms are evaluated: supervised, unsupervised and deep learning algorithms. Statistical results and datasets are presented alongside the algorithm evaluations. Finally the main contributions are the compilation of open issues, challenges and opportunities. These are given for network intrusion as well as APT attack detection. The issues for network intrusion are updated attack detection, IoT data characteristics (e.g. heterogeneity), and ML algorithm selection and configuration. For APT attack detection the lack of a dedicated dataset, AML-based detection and the combination with malware detection are suggested future research directions.

The advantage of the survey by Chen et al. is that the relatively low amount of research into APT detection is a good basis to build further research in this topic. Advanced persistent threats can be highly damaging when hidden compared to other attacks that do not continue over a longer

period of time [5]. Additionally the low amount of research into APT compared to other attack vectors such as DoS detection, is another reason why the survey by Chen et al. is beneficial. Compared to the other surveys the ML-based solutions are categorized into the APT framework. APT's are still broad in terms of the specific attacks and methods that are used within it, since it has six stages. Multiple mitigation, detection and avoidance opportunities exist in these stages (e.g. reconnaissance, initial compromise, later movement, asset discovery, data ex-filtration) [10]. Another advantage of the survey is the evaluation of IoT data sets. The datasets are listed and evaluated, which assists researchers that use the survey by Chen et al. for their own research. Finally having been published in 2022 the recency of the survey is advantageous. The disadvantage of the survey is the limited amount of papers evaluated that fully encompass an APT detection, mitigation and avoidance approach. The majority of papers focus on intrusion detection, while research into avoidance and mitigation is discussed to a lesser extent.

Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey [8] A survey by Bian et al. discusses the current state-of-the-art in addressing the challenges of using ML in real time systems. Real-time systems take the timing component into account are important for critical infrastructure applications, as mentioned by the paper. The structure for their analysis on ML in real-time IoT systems is divided into three sections. The scheduling analysis is important for providing a guarantee of timely execution. Adapting deep neural networks to real-time systems requires model compression and pipeline optimization. Lastly privacy and security related challenges in the aggregation and processing of sensitive information are discussed. A grouping of ML/DL-based solutions to different applications (i.e. industries) and their problems follows. The future research directions for ML for RTS are utilizing a more probabilistic approach towards predictability, malicious behavior detection and real-time system recovery, which tackles mitigation. Lastly the inference and training time limitations of RTS should be handled and a guarantee on meeting time constraints should be researched further.

Bian et al. provide a survey with a number of advantages and disadvantages. An advantage central to the survey is the high importance of research into real-time systems and their security. The use of RTS in critical infrastructure in the industries of transportation, industrial environments, healthcare and smart cities requires further research into how machine learning can be effectively used in these environments. Efficiency of ML techniques is important in these systems. Having a survey on the state-of-the-art in scheduleability and time constraint ML gives a different perspective for researchers in extension to the accuracy of threat detection methods. Another advantage is the direct connection to industry applications. The survey provides a clear overview of the different industries that have RTS, their problems, a description of devices and the solutions using traditional and ML/DL-based methods. This section gives a connection between the research and industry and assists researchers in finding case studies to direct their research towards. One issue of the survey by Bian et al. is the limited amount of focus on security and privacy. Issues in terms of privacy and security data processing and analysis are discussed to some extent, yet not as comprehensively as other surveys.

How Machine Learning Changes the Nature of Cyberattacks on IoT Networks: A Survey [9] From the offensive direction Bout et al. survey the state-of-the art in ML-based attacks. Described are smart attacks that are less easily detectable, more targeted, self-configuring and can analyze and generate data to use for injection. To do so Bout et al. review surveys on general IoT attacks, ML use in IoT networks and ML-based solutions to IoT security issues. An overview of smart ML-based attacks divided into four categories is provided and countermeasures and open issues are presented. Finally the increased complexity, robustness and adaptability of ML-based attacks guide to further research into these methods. The current challenges presented are learning optimization, improved datasets, updated evaluation methods, utilizing adversarial attacks for security robustness and defense testing.

The advantages of the survey by Bout et al. is that it targets the area of IoT security from a different perspective that the other surveys studied. An increased understanding of smart ML-based attacks can assist researchers in finding solutions to these and improving the security and efficiency of IoT networks. Another advantage is the increased research and growth of ML-based attacks, which highlights the importance. As a main disadvantage the future research directions are not as extensive as other surveys. An increased amount of research into smart attacks without more extensive research into, for example the robustness of machine learning methods against adversarial attacks, could decrease the security and efficiency of IoT networks overall.

4 ML Solutions for IoT Security: A Study

The study of state-of-the-art ML-based IoT security solutions and the current limitations is comprised of the following sections: identification of security metrics, a summary of the state-of-the-art papers and the evaluation, review and comparison of these papers.

4.1 Security and ML Metrics

Common metrics used for internet and IoT security are presented in table 2. The CIA triad is comprised of confidentiality, integrity and availability. The Risk matrix is another security metric and categorization tool used in bug reporting and more. It assists in prioritizing bugs and security vulnerabilities by looking at the two components likelihood and damage. For likelihood questionnaires such as [11] can be used to gauge the attack distribution to some extent.

Metrics for ML can vary from accuracy (e.g. prediction accuracy, F1-score) and statistical significance to computational cost and scalability.

IoT Security

Metric type	*Description*
CIA	Confidentiality, Integrity, Availability
Risk matrix	likelihood vs damage

ML

Metric type	*Description*
Classification	Accuracy, precision, recall, F1-score
Scalability	Memory and processing power requirements
Computation cost	Training and inference time, memory
Statistical Significance	Hypothesis testing, Normal distribution, p-value

Table 2: Description of IoT security and ML metrics

4.2 State-of-the-Art: A Review and Comparison

In this section the state-of-the-art ML-based IoT security solutions are reviewed. The review contains the problem description and proposed approach of each paper, followed by the review of advantages and disadvantages. These are summarized in table 3. Finally based on the reviews the approaches are compared in table 4. The approaches can be grouped into two main categories: firstly the detection-based solutions and secondly the privacy enhancing solutions.

Solutions for Attack and Intrusion Detection in IoT Networks

In the work by **Doshi** et al. [12] DDoS detection is performed by identifying the IoT network features and classifying packets into "normal IoT packets"and DoS packets. This classification improves the security of the IoT network. Multiple machine learning classification methods were assessed including: k-nearest neighbour (KNN), support vector machine (SVM) with linear kernel, decision trees, random forest and a 4-layer neural network with binary cross-entropy loss.

Increasing the resistance to anomalies and DDoS attacks requires detection methods. Machine Learning-based detection methods are explored and evaluated by Doshi are evaluated. Through the packet simulation of common Mirai-type DoS attacks, including TCP SYN, UDP and HTTP GET flood, the task of DDoS traffic identification is addressed. The features for classification are categorized into stateless (e.g. packet size, inter-packet interval, protocol) and stateful (e.g. bandwidth, IP destination address cardinality and novelty). KNN, linear kernel SVM, DT, RF and NN are the 5 machine learning algorithms that were evaluated. The advantages are the very high accuracy of all 5 Machine Learning classifiers (0.91 - 0.99). Due to the low computational overhead the solution is well suited for real-time classification, especially when solely using stateless features. Furthermore removing stateful features reduces the F1 score by an accuracy rating of only 0.01 to 0.05. Finally applying the model to the smart home gateway router of a consumer is possible owing to the fulfilment of three characteristics: lightweight features, protocol-agnostic features and low memory implementation. Conversely the disadvantages consist of a high baseline accuracy of 0.93 for the classification of all data points as DoS traffic. This is due to the dataset imbalance, where 15 times more attack packets than "normal packets "are contained in the dataset. Additionally the data set is simulated and not composed of real-world samples. Finally the dataset has a limited amount of variety in the number of IoT traffic patterns that were included.

To increase the anomaly detection speed and reduce communication delay in IoT networks, **Ngo** et al. [19] propose a hierarchical edge computing scheme that is adaptable and distributed. The use of a central cloud computing generates communication delay, compared to local computing, that is undesirable in certain time critical applications. The proposed solution makes use of varying sized auto-encoders for each hierarchical level of computational power. Then a separate policy selection model is used to select the final prediction from the models. This is done as a contextual-bandit problem. The trade-off between accuracy and delay is considered through the alpha value selection.

The problem Ngo et al. are solving is the unused processing power in IoT and edge devices and the communication delay when running an ML model in the cloud. Furthermore data privacy, communication delay and congestion are issues when training and deploying anomaly detection models. While keeping in mind the computational limitations of common IoT devices and the resource requirements of moving complex models from the cloud to the edge, Ngo et al. propose their hierarchical edge computing (HEC) solution. This distributed and adaptive approach uses long short-term memory (LSTM) in addition to the auto-encoders. With the 3 HEC layers: IoT devices, edge servers and cloud the test bed and contextual-bandit approach was implemented and evaluated. The advantages of the proposed approach is the use of computation power of the IoT and edge nodes, while reducing the computational resources needed on the cloud server. The data being closer to the source can be advantageous for reducing computational delay and privacy. The disadvantage of having the inference on edge and IoT nodes requires the necessary computational power, which might not be available. Privacy considerations and improvements of the proposed approach are not discussed in the paper. Lastly the model is prone to adversarial neural network attacks, due to the high amount of relatively open ML models, negatively impacting the security.

The paper by **Chowdhury** et al. [17] displays and compares machine learning models to detect network anomalies that occur due to a Loophole attack in an IoT network. The packets and their parameters collected from the simulated loophole attack where used as input for the machine learning models. The XGBoost algorithm performed highest in classification accuracy with 93.8%.

Chowdhury et al. designed the insider attack with the name loophole attack to run on the RPL (Routing over Low Power and Lossy Networks). Their proposed solution classifies the data packets into normal packets and insider packets with the use of various machine learning algorithms (NN, LSTM, RF, XGBoost, SVM). XGBoost performed the the highest with 93.8% accuracy and the packet metadata are used as features. The advantages of the proposed approach is the high accuracy (above 90%) for all the machine learning methods. The main disadvantage lies in the narrow target

Paper, Year	Description	Advantages	Limitations
[12], 2018	DDoS traffic detection using network-flow based features and various machine learning algorithms.	Very high accuracy (0.91 - 0.99) for the 5 ML classifiers Good real-time detection (especially using only stateless features) Has lightweight and protocol-agnostic features Low memory requirements	Imbalanced dataset with high baseline accuracy of 0.93 Simulated data set Limited variety in IoT traffic patterns in data set
[13], 2019	Identification of device type and individual devices. Once identified: authorization level matching or quarantining is applied.	Individual device instance identification Improvements in F1-score Authorization and quarantining	Whitelisted malicious nodes Mimicking nodes Only F1-score for evaluation Lacking continuous updating of classifier
[14], 2020	Proxy and MitM detection using GAN-DQN.	High accuracy Implementation approach on edge nodes for real-time monitoring	Non-malicious proxy connections
[15], 2021	Partial homomorphic encryption for privacy-preserving aggregate ML model training.	Low loss in accuracy from cryptography No un-trusted servers required Good scalability	Highest level of semantic security not possible High resource consumption and computational overhead on the side of the data owner
[16], 2021	Independent random projection of deep neural network training data to increase confidentiality.	Good scalability and practicality Addresses confidentiality well in an honest-but-curious coordinator model	High-complexity data patterns not as easily identifiable Requires homogeneous data from nodes Computation vs accuracy trade-off varies by projection type Low confidentiality with additive noise based solutions
[17], 2021	Insider attack/loophole attack detection in RPL networks using Machine Learning classification	High accuracy of $\geq 90\%$ Study of multiple classification methods	Narrow attack type researched Narrow network protocol studied Simulated dataset, where real-world could enhance evaluation Non-adaptive and non-incremental.
[18], 2021	Frequency-based feature normalization to lower re-identification accuracy while maintaining high activity recognition with motion tracking IoT devices.	Better privacy and high (87%) activity recognition Better utility-privacy trade-off compared to other approaches Higher control over feature weight in protection Lower cost for application server	Issue with pseudonym messaging Real-time non-batched approach not as applicable Evaluated on high power device (mobile phone) Only include features needed for application on the server
[19], 2022	Adaptive and distributed hierarchical edge computing system that uses autoencoders on three levels: IoT, edge and cloud devices. Based on the contextual-bandit approach the model is then chosen to do anomaly detection.	Makes use of computational power of IoT and edge nodes Close to data source Reduced communication delay Reduced resource use on cloud infrastructure	Security of model limited, prone to adversarial attacks Increased computational cost on edge and IoT nodes

Table 3: Summary of papers using ML to address IoT security or efficiency

in terms of the attack surface of IoT devices. The paper focuses on a specific subset of vulnerabilities for a specific protocol IPv6 and RPL. IPv4 is still widely used [20] and RPL cannot be used for IPv4. Furthermore other protocols for IPv6 exist hence conducting experiments with other protocols and other types of attacks is needed. Additionally the data is generated with simulation results, whereas further research on real-world data and systems is required. Finally as discussed by Chowdhury the non-incremental nature of their solution is another disadvantage. Therefore the addition of continuous training of the model is suggested.

Hamad et al. [13] use supervised machine learning to fingerprint and identify IoT devices and their type. The packet information and network flow data is used to generate the features and input into the model. Their proposition for a security framework using privileges based on the previous identification is given.

Compromised devices that target other devices and pivot into compromising the whole IoT network is a security threat that is addressed by Hamad et al.. The solution in the paper, to identify devices with machine learning and network behavior, and authorize the devices at certain levels based on the identification, aims to increase security by reducing the likelihood of external malicious nodes gaining unauthorized access to the network. The advantages of the solution are the improvements in device type and individual device instance identification as seen by their respective F1-score 91% and 89%. On the other hand no other metrics for evaluation were used. By using authorization levels and quarantining, a promising model for security in data integrity is given. Some of the issues are that defense against compromised devices, that are whitelisted, is not sufficiently provided. A malicious node could mimic the previous normal network behavior while injecting data, since data packet statistics are used as fingerprinting features. Furthermore the continuous training of the classifier and its use in Real-Time systems is not discussed.

The paper [14] by **Kayode** et al. proposes the use of a DQN-GAN network to classify network connections into proxied vs non-proxied connections. Their model uses the GAN discriminator as a robust target network for training the DQN and the GAN generator to generate new connection data, including malicious traffic. In terms of precision and accuracy, the average approximate value is 0.95 for the model.

Proxy connections in IoT networks are often used as attacks on the network and create vulnerabilities in terms of man-in-the-middle attacks. To combat this attack vector classification into proxied vs non-proxied connections using DQN-GAN is proposed. The advantages are the high approximate accuracy of 0.95. Furthermore the distributed federated-learning based structure allows for the IoT devices to contribute their computational power to the whole system. One of the disadvantages is that non-malicious proxies are

Paper, Year, Author	CIA	Likelihood	Damage	ML-Score	Statistical Significance	Scalability	Computational Cost
[12], 2018, Doshi	A	◕	◕	●	○	●	○
[13], 2019, Hamad	C, A, I	◑	●	●	◑	◕	◑
[14], 2020, Kayode	C, I	○	●	●	●	◑	◑
[15], 2021, Zhu	C	◑	◑	●	◕	●	●
[16], 2021, Jiang	C	◑	◑	◑	◑	●	○
[17], 2021, Chowdhury	I, A, C	○	●	●	●	○	◑
[18], 2021, Jourdan	C	◑	◔	◕	◑	◑	◑
[19], 2022, V. Ngo,	I, C	●	◔	●	●	●	◕

Table 4: Comparison of papers using ML to address IoT security or efficiency (High: ●, Medium: ◑, Low: ○)

not taken into account.

Privacy enhancing methods

The paper by **Jourdan** et al. [18] demonstrates how modifying or normalizing the data of certain features that are prone to re-identification and training the machine learning algorithm to still detect activities (e.g. walking) based on all features can result in better privacy (lower re-identification accuracy) and high (87%) activity recognition. Random forest was used for both the raw data input and the feature removed, normalized input.

Jourdan et al. address the problem of a central server data breach and preserving the privacy of the users. Reducing the user re-identification percentage by normalizing the features that are prominent for user identification and keeping the features that are prominent for task recognition. The advantages are better privacy while maintaining a high (87%) activity recognition, compared to other approaches. The utility-privacy trade-off is favorable for their approach compared to the baseline suppression and perturbation, where features useful for re-identification are deleted and an increasing amount of fixed noise is added per point respectively. Compared to the suppression, the normalization approach also allows higher control over the feature weight in the protection. Finally the approach shifts the computational cost to the user, lowering the cost for the central application server. In terms of the disadvantages only higher power devices (mobile phones) are considered. The approach should also be evaluated on IoT devices with less computational power.

Heda [15] is a framework proposed by **Zhu** et al. to preserve the privacy while training ML models in an aggregated form. The operations use partial homomorphic encryption and are the foundation for the protocols used to train the logistic regression, support vector machine and naive bayes models. In comparison with related work Heda does not lose model accuracy, collusion is not possible in the majority of situations and no untrusted servers are required.

Zhu et al. propose to solve privacy issues in shared data aggregation scenarios, where there exists data owners with IoT devices and model demander that aggregates the data from multiple data owners. With the use of partial homomorphic encryption the privacy of the data is preserved while operations for training the classifiers are executed on the encrypted data. The advantages of this approach are the low loss in accuracy when training on encrypted data. No un-trusted server is required as in related work. In terms of scalability the record number has no effect on the time consumption and the number of data owners does not have an effect for the Logistic Regression (LR) and the Support Vector Machine (SVM), while the Naive Bayes has a less than linear increase. The disadvantages of the proposed approach is the existence of computational overhead for both the data owner and the model demander. The use of 4 core, 8gb ram computers is not applicable to the scenario where IoT devices and model demander interface and communicate directly without an intermediary data owner. Furthermore the highest level of semantic security is not possible due to requiring homomorphism. Finally insider and side-channel attacks against homomorphic encryption are possible [21] and the communication is prone to eavesdropping. The secure two-party communication is addressed by the paper.

The proposed solution by **Jiang** et al. [16] to create a privacy-preserving approach, that utilizes collaborative learning and Gaussian random projection is presented. Independent IoT devices generate random Gaussian matrix R_i which is kept secret and used to create a projection of the training data. In a collaborative environment these projects are collected by the coordinator who then trains the deep learning model on the projected training data. An unsupervised learning method is used to combat distortion.

Jiang et al. focus on the problem of data confidentiality in collaborative learning scenarios (i.e. privacy-preserving collaborative learning PPCL) in an IoT scenario, where computational resources are limited. They propose independent random projection of model input features to hide or obfuscate the data rather than encrypting it, saving computational overhead. The deep neural network then trains its classifier on the projected data. Compared to the other random projection methods and noise additions Gaussian random projections, paired with deep neural network classification gives a higher accuracy. The additional advantages of this approach is the good scalability on the four data sets used and the general practicality. Confidentiality is improved and the possibility of collusion is reduced in the honest-but-curious coordinator model. The disadvantages of the approach are that the data used in the paper is homogeneous, which does not address the heterogeneous nature of IoT data. Furthermore high complexity patterns are not easily recognizable, due to the increased complexity in the data patterns from the generated independent projection matrices. Finally the

computation overhead vs accuracy trade-off varies between different random projection types.

5 Discussion and Future Work

This section gathers the results of the previous sections. The future research directions are then derived from the results of the review and comparison.

5.1 Discussion

The reviewed papers in section 4 create an overview of the current state of ML-based IoT security and efficiency research. Various techniques are discussed in the papers such as GAN-DQN, partial homomorphic encryption, network-flow based detection, independent random projections, and hierarchical edge computing with autoencoders.

The key advantages encompass the high accuracy of these techniques, with a subset of papers [12] [17] mentioning accuracy rate of 0.90 to 0.99. In terms of real-time systems, some papers [14] [19] targeting RTS applications show good detection capabilities. These techniques are well-suited for time critical IoT infrastructure.

Nevertheless limitations of these techniques persist. The high resource consumption and computational overhead of some approaches [15] [18] limits the practical implementation in resource constrained networks. Additionally the datasets in some papers [12] [17] are sub-optimal due to being imbalanced and homogeneous at times. Furthermore providing limited variety in malicious traffic can reduce the robustness of the solution.

The review of the ML-based IoT security solutions provides a valuable insight into the current approaches and their limitations. It is evident that the approaches do not individually target all of the potential attack vectors and efficiency requirements. Therefore the challenge in future research is addressing the crucial aspects of security, efficiency, and privacy and improving the robustness of the ML-based solutions.

5.2 Future Work

The future research directions proposed follow from the limitations found during the study of papers. Limitations of the studied approaches include but are not limited to the following aspects of the security and privacy approaches.

- *Dataset availability and balance* is a key component of ML-based solutions. Improvements to the dataset entail also incorporating heterogeneous data to reflect the characteristics of real IoT networks and their traffic. More realistic datasets also require re-balancing by for example over or under-sampling [22]. Finally realistic simulated data generation frameworks [23] have potential to alleviate these problems and need further consideration.
- *Targeting multiple attack vectors* is a key for a robust solution. Anomaly and intrusion detection does not cover all the attack vectors. Therefore combining ML-methods for multiple IoT vulnerabilities in an intelligent way, while taking computational limitations into account, is suggested.
- *Addressing the computational limitations of IoT devices* is essential for adoption into industry. Consequently techniques that adapt the distributed ML-model based on the memory and processing power of IoT devices is beneficial. This can be done through ML algorithm selection or model size, since some algorithms are better suited for low resource environments. Further research into the performance vs resource use [24] and leveraging adaptive cloud, edge and node computing is advisable.
- *Preserving privacy* is an important task in certain applications. This differs based on usage and data breach damages. Furthermore detection methods, such as partial homomorphic encryption [15], can loose accuracy. Further research into the trade-off between privacy and detection accuracy is recommended.

6 Responsible Research

While conducting and presenting research a number of factors increase the reliability and quality of the work. Factors such as reproducibility and risks are important to reflect on and will be discussed in this section.

Some of the research conducted and discussed could potentially cause damages. Especially research on ML-based smart attacks and offensive security exploits can be used by malicious actors for personal gain. On the one hand understanding the technologies and using open source exploits to improve security and evaluate current security methods is immensely beneficial. On the other hand a certain risk is involved within this process.

The survey papers and articles reviewed in this paper are from reputable sources. The literature search was conducted on IEEE (Institute of Electrical and Electronics Engineers) and ACM (Association for Computing Machinery) conference and article papers. With a reliable and rigorous review process compared to other publishers these publications are well suited for a literature review.

In terms of the reproducibility this paper is more difficult to judge, given that this paper is a literature review rather than an experiment. Still the literature search process, review methodology, quality of argumentation and use of references can be evaluated. As mentioned above for the literature search the publications used are referenced and available. The review methodology is described in the introduction yet there are slight differences in approach per paper. In general the quality of argumentation is a limiting factor of this paper. Lastly the references are used as basis for conclusions and aid researchers in reproducing the work.

7 Conclusions

This paper provides a review of the surveys and state-of-the-art literature on ML-based IoT security and efficiency. With the background of IoT attack vectors and machine learning algorithms, the use of ML for improving security is the target. To answer the research question of how ML can be used to enhance the security of IoT system, the reviewed papers provide various approaches. Detection methods can be used to identify malicious nodes, network traffic and attacks. Privacy preserving methods can use ML training on encrypted

data or training the model on local nodes close to the data. Adversarial networks can be used to provide privacy by reducing re-identification and train improved ML security models. Future research into dataset quality, solution robustness, computational limitations and privacy preserving methods is desirable. The reviewed literature indicates the promising potential of ML methods, to advance the security and efficiency of IoT networks, therefore further research is beneficial.

References

[1] Lionel Sujay Vailshery. Iot connected devices by use case 2030, Nov 2022.

[2] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: Application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.

[3] Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain. Machine learning in iot security: Current solutions and future challenges. *IEEE Communications Surveys amp; Tutorials*, 22(3):1686–1721, 2020.

[4] Ismail Butun, Patrik Osterberg, and Houbing Song. Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys amp; Tutorials*, 22(1):616–644, 2020.

[5] Timo Steffens. *Attribution of advanced persistent threats*. Springer Vieweg Berlin, 2020.

[6] Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. A survey of machine and deep learning methods for internet of things (iot) security. *IEEE Communications Surveys amp; Tutorials*, 22(3):1646–1685, 2020.

[7] Zhiyan Chen, Jinxin Liu, Yu Shen, Murat Simsek, Burak Kantarci, Hussein T. Mouftah, and Petar Djukic. Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. *ACM Computing Surveys*, 55(5):1–37, 2022.

[8] Jiang Bian, Abdullah Al Arafat, Haoyi Xiong, Jing Li, Li Li, Hongyang Chen, Jun Wang, Dejing Dou, and Zhishan Guo. Machine learning in real-time internet of things (iot) systems: A survey. *IEEE Internet of Things Journal*, 9(11):8364–8386, 2022.

[9] Emilie Bout, Valeria Loscri, and Antoine Gallais. How machine learning changes the nature of cyberattacks on iot networks: A survey. *IEEE Communications Surveys amp; Tutorials*, 24(1):248–279, 2022.

[10] Ibrahim Ghafir, Konstantinos G. Kyriakopoulos, Sangarapillai Lambotharan, Francisco J. Aparicio-Navarro, Basil Assadhan, Hamad Binsalleeh, and Diab M. Diab. Hidden markov models and alert correlations for the prediction of advanced persistent threats. *IEEE Access*, 7:99508–99520, 2019.

[11] Statista: Main types of cyberattacks in italy in 2018, Feb 2020.

[12] Rohan Doshi, Noah Apthorpe, and Nick Feamster. Machine learning ddos detection for consumer internet of things devices. *2018 IEEE Security and Privacy Workshops (SPW)*, 2018.

[13] Salma Abdalla Hamad, Wei Emma Zhang, Quan Z. Sheng, and Surya Nepal. Iot device identification via network-flow based fingerprinting and learning. *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019.

[14] Olumide Kayode and Ali Saman Tosun. Deep q-network for enhanced data privacy and security of iot traffic. *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020.

[15] Liehuang Zhu, Xiangyun Tang, Meng Shen, Feng Gao, Jie Zhang, and Xiaojiang Du. Privacy-preserving machine learning training in iot aggregation scenarios. *IEEE Internet of Things Journal*, 8(15):12106–12118, 2021.

[16] Linshan Jiang, Rui Tan, Xin Lou, and Guosheng Lin. On lightweight privacy-preserving collaborative learning for internet of things by independent random projections. *ACM Transactions on Internet of Things*, 2(2):1–32, 2021.

[17] Morshed Chowdhury, Biplob Ray, Sujan Chowdhury, and Sutharshan Rajasegarar. A novel insider attack and machine learning based detection for the internet of things. *ACM Transactions on Internet of Things*, 2(4):1–23, 2021.

[18] Theo Jourdan, Antoine Boutet, Amine Bahi, and Carole Frindel. Privacy-preserving iot framework for activity recognition in personal healthcare monitoring. *ACM Transactions on Computing for Healthcare*, 2(1):1–22, 2021.

[19] Mao V. Ngo, Tie Luo, and Tony Q. Quek. Adaptive anomaly detection for internet of things in hierarchical edge computing: A contextual-bandit approach. *ACM Transactions on Internet of Things*, 3(1):1–23, 2022.

[20] Statistics: Google ipv6 adoption, Jan 2023.

[21] Furkan Aydin and Aydin Aysu. Exposing side-channel leakage of seal homomorphic encryption library. *Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security*, 2022.

[22] Omar Elghalhoud, Kshirasagar Naik, Marzia Zaman, and Nishith Goel. Data balancing and hyper-parameter optimization for machine learning algorithms for secure iot networks. *Proceedings of the 18th ACM International Symposium on QoS and Security for Wireless and Mobile Networks on 18th ACM International Symposium on QoS and Security for Wireless and Mobile Networks*, 2022.

[23] Andreas Meyer-Berg, Rolf Egert, Leon Böck, and Max Mühlhäuser. Iot dataset generation framework for evaluating anomaly detection mechanisms. *Proceedings of*

the 15th International Conference on Availability, Reliability and Security, 2020.

[24] Davy Preuveneers, Ilias Tsingenopoulos, and Wouter Joosen. Resource usage and performance trade-offs for machine learning models in smart environments. *Sensors*, 20(4):1176, 2020.

A Appendix: Comparison of surveys

Survey, Year	**Specialization**	**ML**	**DL**	**Security**	**Authentication**	**Efficiency**	**Privacy**
[3], 2020	General	●	●	●	●	●	●
[6], 2020	General	●	●	●	◑	○	●
[7], 2022	APT	◑	●	●	◑	○	○
[8], 2022	RTS IoT	◑	◑	○	○	●	○
[9], 2022	ML-based attacks	◑	◑	◑	○	○	●

Table 5: Comparison of surveys (High: ●, Medium: ◑, Low: ○)