A critical review of feature selection methods for machine learning in IoT security

Jing Li* and Mohd Shahizan Othman

Faculty of Computing,
Universiti Teknologi Malaysia (UTM), Malaysia
Email: jinglihz225@163.com
Email: goldboy_225@163.com
Email: shahizan@utm.my
*Corresponding author

Hewan Chen

Digital Reform Research Center,
China Jiliang University, China
Email: chw@cjlu.edu.cn

Lizawati Mi Yusuf

Faculty of Computing,
Universiti Teknologi Malaysia, Malaysia
Email: lizawati@utm.my

Abstract: In the internet of things (IoT) era, the security of connected devices and systems is critical. Machine learning models are commonly used for IoT attack detection, where feature selection (FS) plays an important role. However, FS for IoT security differs from traditional cybersecurity due to the uniqueness of IoT systems. This paper reviews FS methods for effective machine learning-based IoT attack detection. We identify five research questions and systematically review 1,272 studies, analysing 63 that meet inclusion criteria using the preferred reporting items for systematic review and meta-analysis (PRISMA) guidelines. We categorised the studies to address the research questions regarding FS methods, trends, practices, datasets and validation used. We also discussed FS limitations, challenges, and future research directions for IoT security. The review can serve as a reference for researchers and practitioners seeking to incorporate effective FS into machine learning-based IoT attack detection.

Keywords: internet of things; IoT; feature selection; IoT dataset; attack detection; classification; IoT security; systematic literature review; SLR; machine learning; deep learning.

Reference to this paper should be made as follows: Li, J., Othman, M.S., Chen, H. and Yusuf, L.M. (2024) ‘A critical review of feature selection methods for machine learning in IoT security’, *Int. J. Communication Networks and Distributed Systems*, Vol. 30, No. 3, pp.264–312.

Biographical notes: Jing Li is currently pursuing his PhD in Computer Science at the Universiti Teknologi Malaysia (UTM). He received his Master's in Management Information Systems from the Zhejiang University, China in 2012 and Bachelor's in Computer Science from China Jiliang University in 2003. He has over 15 years of experience in the ICT industry, with expertise in networking, cybersecurity and IoT. His research interests include internet of things, cybersecurity, digital forensics, big data, high-performance computing, machine learning and deep learning. He is also an IEEE member and actively working on emerging applied machine learning technologies.

Mohd Shahizan Othman is a Senior Lecturer and Deputy Director at the Centre for Information & Communication Technology, Universiti Teknologi Malaysia (UTM). He has over 15 years of experience in teaching, research and university administration. He received his PhD in Information Science from the Universiti Kebangsaan Malaysia in 2008. Prior to that, he obtained his Master's in Information Technology from the same university in 2001 and Bachelor's in Computer Science from UTM in 1998. He has taught over 20 courses at the undergraduate and post-graduate levels, covering areas of information systems, software development and IT management.

Hewan Chen is an associate researcher and staff engineer at the Digital Reform Office of China Jiliang University. She obtained her Bachelor's in Computer Science from the China Jiliang University in 2003 and Master's in Software Engineering from Hangzhou Dianzi University in 2008. She has over 15 years of experience in digitalisation and smart campus development. Her research focuses on digital reform, digital campus construction, information systems and data-driven decision making. She has published papers on high-efficiency wireless networks, digital campus development, data transmission, digital transformation and innovation in universities.

Lizawati Mi Yusuf received her BSc in Computer Science with a major in Industrial Computing from the Universiti Teknologi Malaysia (UTM), Malaysia in 2000, and MSc in Information Technology from Universiti Kebangsaan Malaysia (UKM), Malaysia. She is currently a Lecturer with the Faculty of Computing, UTM. Her research interests include optimisation, web information extraction and retrieval, web data mining, machine learning, social learning, business intelligence, high-performance computing and numerical analysis.

1 Introduction

Internet of things (IoT) provides a promising opportunity to seamlessly bring the real world and worlds together to form a larger, more intelligent network. Originally, the term IoT was introduced by Ashton (2009) to describe a network of interconnected devices that are uniquely identifiable and able to communicate with each other using RFID technology. After development and evolution for many years, IoT has become a compound technology involving embedded devices with sensors, wireless sensor network, operating system, software, data communication, middleware, big data and AI technologies for various applications over the internet (Xu et al., 2014). By 2030, there will be an estimated 26 billion connections on the IoT, according to a recent report from Statista (2022). These IoT devices are integrated into appliances based on IoT infrastructure that support a variety of protocols for communication over a public network. The characteristics of IoT, including multiple-layer infrastructure, ubiquitous interconnected IoT devices, and less powerful capabilities in IoT systems, cause IoT infrastructure to be more vulnerable to various attacks compared with traditional IT infrastructure.

Many factors contribute to the vulnerability of IoT networks. IoT infrastructure comprises four layers: perception, network, middleware, and application, each of which has its own security vulnerabilities, including the gateways that connect them. Cybercriminals can exploit these vulnerabilities, making IoT security a major concern (Hassija et al., 2019). In addition, IoT has extensive applications in various sectors, including smart homes, healthcare, manufacturing, agriculture, logistics, autonomous vehicles, and smart cities, with the ability to exchange data between the real and digital worlds. However, these devices are susceptible to security threats due to the large amount of confidential user data they carry. Ensuring the integrity, confidentiality, and availability of the IoT system is critical to protecting user data (Kouicem et al., 2018). Moreover, the increasing demand for IoT devices has led to their deployment worldwide, but their low-cost design, coupled with limited resources such as bandwidth, battery, computational resources, and memory, restricts the integration of security applications (Hassija et al., 2019). Therefore, the above concerns on IoT security, like many attack surfaces with multiple layers in IoT infrastructure, extensive applications among all sectors, and limited resources on IoT devices, make IoT vulnerable to various attacks by cyber criminal (Ahmad and Alsmadi, 2021).

Attack detection ahead of time is quite crucial in the IoT security domain, and IDS is one of the most effective methods to protect IoT networks from attacks. Lately, many researchers have been focusing on detecting attacks in IoT datasets, which can be either real or simulated IoT networks. This field of study has gained significant attention, and effective classification models are being developed to classify unseen IoT data after training the model with a specific training dataset. However, due to the unique characteristics and challenges of IoT security, it is essential to identify the most relevant features from the data to build an effective machine learning (ML) model. IoT devices are characterised by their limited computational resources, low-power processors and small memory size. These devices are typically designed to collect data from various sensors and transmit it to other devices or the cloud for analysis. The data collected by IoT devices is often high-dimensional and noisy, making it challenging to extract meaningful features for use in ML models (Leevy et al., 2022). Moreover, IoT devices are vulnerable to security threats, including hacking, malware attacks and privacy breaches. Since the amount of data generated by IoT devices is huge, it is not feasible to process all the data for detecting security threats (Ahmad and Alsmadi, 2021). Hence, feature selection (FS) becomes critical for reducing the dimensionality of the data and selecting the most relevant features that can improve the accuracy of ML models.

In addition to the above challenges, FS in IoT security also needs to consider the scalability and interpretability of the selected features. Since IoT devices are often deployed in large-scale environments, the selected features must be scalable to handle large amounts of data (Al-Garadi et al., 2020). Furthermore, the selected features must be interpretable so that security experts can understand the significance of the features and identify potential security threats (Disha and Waheed, 2022). Thus, FS is critical in ML for IoT security because IoT devices generate high-dimensional, noisy data and are vulnerable to security threats. FS helps in reducing the dimensionality of the data, selecting relevant features, and improving the accuracy and scalability of ML models while ensuring the interpretability of the selected features. As a result, many researchers have dedicated significant resources towards developing FS methods that can improve the accuracy of classification, reduce computation time, and rely on fewer features to detect attacks in IoT networks.

Review studies have been conducted in the area of IoT security, specifically pertaining to the implementation of ML and deep learning (DL) techniques. The purpose of these studies is to identify patterns and classify different types of attacks within the IoT environment. Nagaraja and Kumar (2018) reviewed early research on intrusion detection, highlighted the lack of specificity regarding the measures used to detect intrusion, and presents various methods for FS and computation of high-dimensional data for identifying network intrusion. Then, Hussain et al. (2020) presented the potential impact of IoT on our lives and the security challenges posed by resource-constrained IoT networks, and proposed the use of ML and DL techniques to address security problems. After that, Bojarajulu et al. (2021) discussed how ML models with optimal FS can mitigate these attacks by detecting malicious network traffic, however, there is just a cursory analysis of FS in IoT data. Recently, Verma et al. (2022) investigated FS for network intrusion detection systems (NIDS) and presented an overview of the majority of techniques proposed in the FS research for NIDS and a classification and comparative study of FS algorithms. Ahmetoglu and Das (2022) discussed the growing amount of cyberattacks and how ML may automate the detection and prediction of attacks in network traffic using techniques including detection, classification, clustering, and anomaly analysis, but they did not concentrate on IoT-specific data. As a result, there are few reviews that specifically focused on FS techniques for IoT datasets in IoT security. Kalakoti et al. (2022) applied FS methods and ML to detect botnet attacks on IoT devices across the botnet lifecycle. They found with few features, high detection accuracy is possible, wrapper methods produce optimal feature sets consistently, channel features best detect latter lifecycle stages, and host features identify initial bot attacks.

In this research, the aim of this study is to help other researchers by making a systematic literature review (SLR) of related studies that used FS in ML-based attack classification models in IoT security in the last five years. Also, this research will help to specify the current situation, challenges and future directions in FS for IoT security. The main contributions of this systematic review can be summarised as follows:

1 Comprehensive literature searches and investigations are conducted, with a focus on FS using IoT data for attack detection in IoT security. There are 1,272 papers collected with the specified keywords search strategy from six databases (Web of Science, IEEE Xplore, Scopus, ScienceDirect, ACM, SpringerLink and Wiley Online Library) in the literature published from January 2018 to December 2022 on FS in IoT data for IoT security.

2 An extensive literature review using the methodology based on the standard preferred reporting items for systematic review and meta-analysis (PRISMA) process is employed. This study proposes five research questions (12 sub-questions in total). We initially formulate research questions and motivations, collect the related studies, define the including and excluding criteria, and finally identify the primary studies focusing on the topics with an acceptable quality score. Data items for each research

question are extracted for intensive data analysis to provide answers and discussion to the proposed research questions.

3 Intensive explanation and discussion have been implemented in the primary studies. Each paper is reviewed based on the extracted data items to answer the proposed research questions, involving the current situation and the objectives of FS, FS methods, IoT datasets, FS validation methods, limitations, challenges, and future directions. This aims to provide researchers and practitioners who want to pursue research on FS using IoT data to build ML or DL-based attack classification models in IoT networks.

The structure of this study is as follows: Table 1 lists all the acronyms used in the paper. Section 2 outlines the research methodology which includes the research protocols and research questions. The literature review results, including discussion and answers to the research questions, are presented in Section 3. Limitations of this study are discussed in Section 4. Lastly, Section 5 provides conclusions.

Table 1 Acronyms and their explanations

Acronym	*Explanation*	*Acronym*	*Explanation*
IoT	Internet of things	RFID	Radio frequency identification
IDS	Intrusion detection system	IPS	Intrusion prevention system
ML	Machine learning	DL	Deep learning
FS	Feature selection	MLP	Multilayer perceptron
EFS	Ensemble feature selection	FA	Firefly optimisation
KNN	K-nearest neighbours	MI	Mutual information
CS	Chi-squared test	GR	Gain ratio
CFS	Correlation-based feature selection	FE	Forward elimination
BE	Backward elimination	RFE	Recursive feature elimination
AWO	Augmented whale optimisation	OCSVM	One class support vector machine
FPR	False positive rate	GA	Genetic algorithm
RFE	Recursive feature elimination	SFS	Sequential feature selection
PSO	Particle swarm optimisation	KS	Kolmogorov-Smirnov test
PCC	Pearson correlation coefficient	SU	Symmetric uncertainty
RNN	Recurrent neural network	LSTM	Long short-term memory networks
GRU	Gated recurrent unit	PCA	Principal component analysis
SVM	Support vector machine	NN	Neural networks
SHAP	Shapley additive explanations	PFI	Permutation feature importance
DNN	Deep neural network	D-FES	Deep-feature extraction and selection
TSO	Transient search optimisation algorithm	AQU	Aquarium optimiser
HGS	Hunger games search (HGS) optimisation algorithm	GTO	Game theory optimisation

Table 1 Acronyms and their explanations (continued)

Acronym	*Explanation*	*Acronym*	*Explanation*
CLS	Classifier	VIM	Variable importance measures
CorrAUC	Correlation and area under the curve	TOPSIS	Technique for order of preference by similarity to ideal solution
DT	Decision tree	NB	Naive Bayes
ET	Extended trees	RF	Random forest
XGB	Extreme gradient boosting	AE	Auto encoder
SMOTE	Synthetic minority over-sampling technique	SDN	Software-defined networking (SDN)
SBFE	Backward feature elimination	SFFS	Sequential forward selection
DoS	Denial of service	DDoS	Distributed denial of service
XSS	Cross-site scripting (XSS) attacks	MITM	Man in the middle attack
RPL	Routing protocol for low-power and lossy networks	Acc	Accuracy
Prec	Precision	Rec	Recall
F1	F1-score	DR	Detection rate
FAR	False alarm rate	TPR	True positive rate
TNR	True negative rate	FPR	False positive rate
FNR	False negative rate	MCC	Matthews correlation coefficient
G-mean	A combination of sensitivity (TPR) and specificity (TNR)	TTB	Time to build the models
TTP	Time to predict the models	CM	Confusion matrix
AUC	Area under curve	ROC	R of curve
TP	True positive	TN	True negative
FP	False positive	FN	False negative

2 Methodology

In order to accomplish the objectives of the current SLR study, we adhered to the traditional and unique recommendations made by Keele et al. (2007). The approach utilised to carry out the current SLR of FS utilising IoT data for IoT security is presented in this part. Our methodology follows the framework outlined in Figure 1. The key steps include:

1 *Planning stage:* Developing a systematic plan for how the study will be conducted.

2 *Identifying research questions and motivations:* Determining the specific questions and goals that the study aims to address.

3 *Searching process:* Conducting a comprehensive search of relevant literature and data sources.

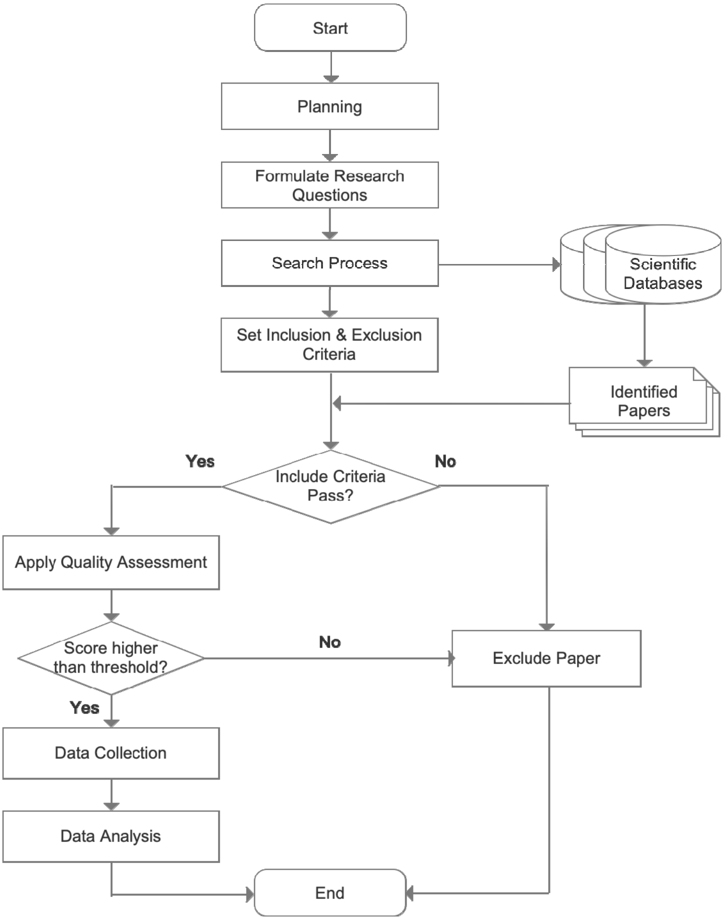
4 *Applying inclusion and exclusion criteria:* Screening the searched results to filter for relevant and high-quality sources based on predetermined criteria.

5 *Quality assessment:* Evaluating the methodology and credibility of the selected sources.

6 *Collecting data:* Extracting relevant data and insights from the sources.

7 *Analyzing data:* Synthesizing and making sense of the accumulated data to draw conclusions that answer the research questions.

Figure 1 Search process flowchart



2.1 *Planning stage*

In the initial planning stage of our study, we identified the necessary steps to accomplish our research objectives. Our study focuses on the impact of FS on ML or DL-based security models in IoT security. We made sure to establish both strategic and technical strategies to ensure that the rest of our proposed technique could be executed in a systematic and consistent manner. This planning stage served as the foundation for the successful implementation of our SLR methodology.

2.2 Research questions and motivations

In this section, we present the research questions investigated in the current SLR study, as well as the motivations behind them. The motivations come from the noteworthy achievements of the work using FS approaches for attack classification in the IoT security domain. For instance, most studies have indicated that FS is essential to processing heterogenous IoT datasets to improve the performance of attack detection and classification. Thus, the research questions RQs investigated in this study can be found in Table 2.

Table 2 Research questions and the motivations

No.	*Research questions*	*Motivations*
RQ1	What is current situation of FS approaches applied for machine learning or deep learning-based attack classification model for IoT security?	
RQ1.1	What is the trend of the studies that applied FS for IoT security in recent five years?	The motivation of RQ1 is to identify highly related empirical studies during past five years, in order to acquire the situations of the studies on the topic in recent years
RQ1.2	What are the distributions of the studies according to databases and publishers?	
RQ1.3	What are the main objectives of applying feature selection for IoT security?	
RQ2	What are the FS methods and techniques applied on attack classification models for IoT security?	
RQ2.1	What are the main types of feature selection approaches applied for attack classification model?	RQ2 is motivated by the need to identify the main objectives and the FS methods applied in recent studies.
RQ2.2	What are the specific techniques utilised for each type of feature selection used in IoT security models?	
RQ3	What are the characteristics of related factors for FS methods for IoT security?	
RQ3.1	What are the IoT datasets as the benchmark by the studies when applying FS method?	RQ3 is motivated by the need to the idea on how the feature selection method can be applied concerning to the characteristics of datasets and attacks.
RQ3.2	What are mapping of datasets and attacks to various FS methods among the studies?	
RQ4	What are the verification methods to evaluate the effectiveness of proposed FS approaches?	
RQ4.1	What are the traditional machine learning and deep learning algorithms mapping to FS methods?	RQ4 is motivated by the need to the idea of how to verify the effectiveness of proposed FS methods.
RQ4.2	What are the performance metrics used for validation of FS approaches?	
RQ4.3	What are the methods of the validation of FS in studies?	
RQ5	What are the challenges and future directions using FS to the classification models in IoT security?	
RQ5.1	What are the limitations of the proposed FS in studies?	RQ5 is motivated by the need to find the limitations, challenges, and the research in future direction.
RQ5.2	What are the major challenges of applying FS methods?	
RQ5.3	What are the future research directions of FS in terms of the classification model for IoT security?	

2.3 Searching process

This section explains how the articles were selected for the study. To find relevant experimental studies on FS methods using IoT data for attack classification in IoT security, various digital scientific databases were examined. Table 3 shows the list of databases, their fields, search strings, and the initial number of studies found. To extract each article from the digital databases, a manual search process was used for journal articles and conference proceedings.

Table 3 Repositories and the corresponding search strings

Digital database	*Field*	*Search strings*	*No.*
Web of Science	All	"feature selection" AND ("iot" OR "internet of things") AND "security" AND ("machine learning" OR "deep learning")	178
IEEE Xplore	All	"feature selection" AND ("iot" OR "internet of things") AND "security" AND ("machine learning" OR "deep learning")	113
Scopus	TITLE-ABS-KEY	"feature selection" AND ("iot" OR "internet of things") AND "security" AND ("machine learning" OR "deep learning")	258
ScienceDirect	All	"feature selection" AND "iot security" AND ("machine learning" OR "deep learning")	168
ACM Digital Library	All	("feature selection") AND ("iot" OR "internet of things") AND ("security") AND ("machine learning") 2018–2022	338
SpringerLink	All	"feature selection" AND "iot security" AND ("machine learning" OR "deep learning") 2018-2022	183
Wiley Online Library	All	"feature selection" AND "iot security" AND ("machine learning" OR "deep learning")	34
Overall			1,272

2.4 Inclusion and exclusion criteria

To ensure that only relevant studies were included in this SLR, specific criteria were established to determine the eligibility of each study. In order to be included in the review, an article had to meet various conditions, such as being written in clear and precise English. Any articles written in a language other than English were not considered for inclusion as they may be challenging to comprehend. A comprehensive list of the criteria for inclusion and exclusion is presented in Table 4.

Table 4 Inclusion and exclusion criteria

Inclusion criteria	*Exclusion criteria*
a Each article must be focused and related to the topic of feature selection applied in machine learning or deep learning-based classification model for IoT security.	a The studies that are not related to the topic, or only related to any one sub-topic like feature selection, machine learning or deep learning-based attack classification, or IoT security but not all above.

Table 4 Inclusion and exclusion criteria (continued)

Inclusion criteria		*Exclusion criteria*	
b	Each article must be a proof of an empirical study addressing the research questions of the related topic.	b	Technical reports, government reports, letters and editorials, short notes, book chapters, survey or review papers, and experimental papers that deviate from answering the research questions.
c	The dataset utilised by each article must be based on at least one public IoT dataset or the IoT data extracted from IoT scenarios.	c	The studies focusing on datasets not generated from IoT scenarios.
d	Each article must be written in a simple and understandable English reported in a publication article, which can be accessed.	d	Article must not be written in a different language than English, or cannot be accessed.
e	Each article must be published within January 2018–December 2022.	e	Be published outside the period of time specified.

2.5 Quality assessment

In addition to applying inclusion and exclusion criteria, a quality assessment was conducted to refine the scope of data collection and analysis. The focus of the quality assessment was to evaluate how well the authors addressed the research questions posed in the SLR. This assessment aided in the precise extraction of relevant data while eliminating irrelevant studies. Table 5 outlines the five quality assessment questions used to formulate the quality assessment criteria.

Table 5 Quality assessment questionnaire

Quality assessment question		*Relevant to the research question*
QA1	Whether the complete data items can be extracted and how does the author(s) explain their research problems?	RQ1
QA2	How does the author(s) present the implementation of feature selection methods the studies?	RQ2
QA3	How does the author(s) present the concerning factors to feature selection methods in research methodology?	RQ3
QA4	How does the author(s) conduct comprehensive validation for the proposed research method?	RQ4
QA5	How does the author(s) present the study findings, limitations and future direction?	RQ5

Table 6 Quality assessment scoring matrix

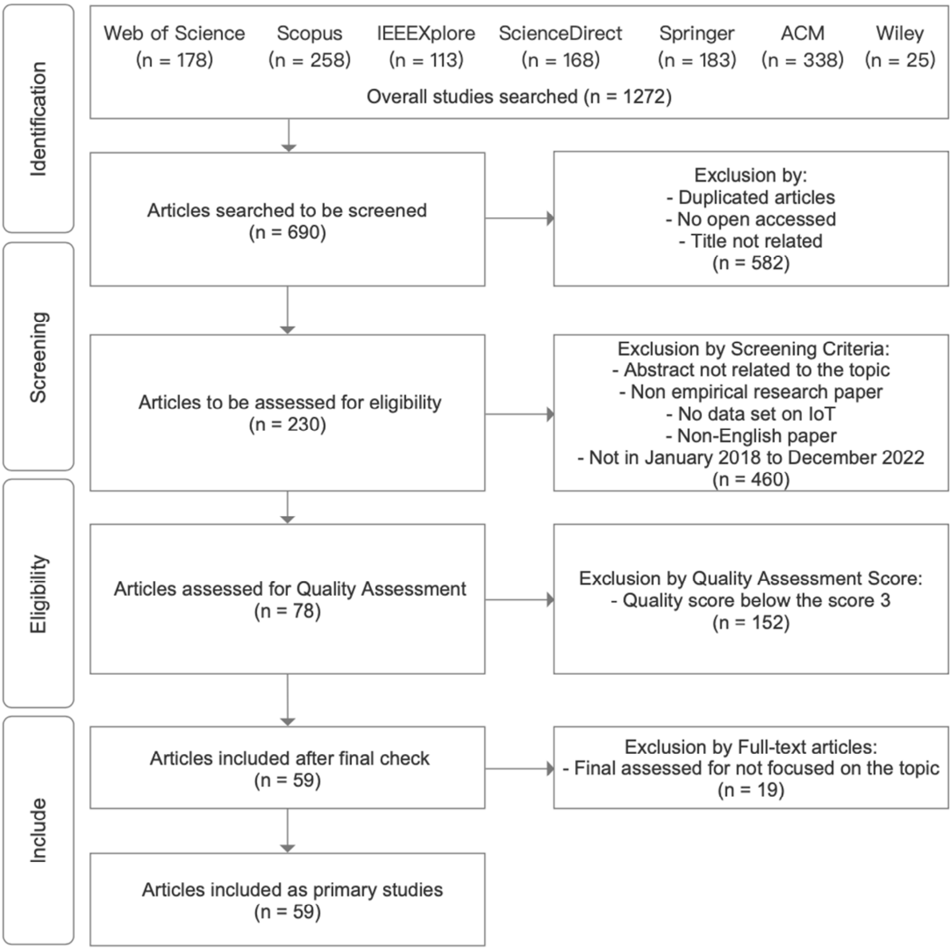
Quality assessment scoring criteria	*Score*
The author(s) have presented a comprehensive, clear, and unambiguous explanation of the answers to the specific RQ.	High = H = 1
The author(s) have provided some explanation, but it is not specific, detailed, or clear enough to the specific RQ.	Medium = M = 0.5
The author(s) have given little or no technical information in response to the specific RQ.	Low = L = 0

The research papers underwent an evaluation process based on the quality assessment questions mentioned earlier. Table 6 was used as a scoring matrix to assign a score to each paper. Only papers with a score greater than 3 were deemed acceptable and included in this research review, while those with a lower score were excluded.

2.6 Data collection

Once the quality of the research papers has been assessed, those that are unrelated to our study questions will be removed. The process of data extraction will be initiated, which involves a comprehensive analysis, identification, and gathering of significant data from every research paper that has passed the quality assessment. This generates a shortlist of papers with specific metadata that can be used for paper classification and subsequent analysis. The extracted information and metadata from the primary research studies are summarised in Table 7.

Figure 2 PRISMA diagram


Identification
Screening
Eligibility
Include
Web of Science (n = 178)
Scopus (n = 258)
IEEEXplore (n = 113)
ScienceDirect (n = 168)
Springer (n = 183)
ACM (n = 338)
Wiley (n = 25)
Overall studies searched (n = 1272)
Articles searched to be screened (n = 690)
Exclusion by: - Duplicated articles - No open accessed - Title not related (n = 582)
Articles to be assessed for eligibility (n = 230)
Exclusion by Screening Criteria: - Abstract not related to the topic - Non empirical research paper - No data set on IoT - Non-English paper - Not in January 2018 to December 2022 (n = 460)
Articles assessed for Quality Assessment (n = 78)
Exclusion by Quality Assessment Score: - Quality score below the score 3 (n = 152)
Articles included after final check (n = 59)
Exclusion by Full-text articles: - Final assessed for not focused on the topic (n = 19)
Articles included as primary studies (n = 59)

To achieve our goal, the PRISMA was applied (Page et al., 2021) in this SLR study. The PRISMA was employed to provide comprehensive details about the number of articles assessed in this study, as shown in Figure 2.

Table 7 Data item collection form

Data fields	*Description*	*Research questions*
Reference ID	It provides the unique ID of each primary study.	For documentation purpose
No. of primary studies	It provides the number of studies qualified after quality scoring scheme.	RQ1
Year	Year of publication.	RQ1
Publication source	This information includes the type of study and the name of the publication where the primary study was conducted.	RQ1
Databases	It provides the digital database name for each primary study.	RQ1
Objectives	It provides the major objectives of FS implemented in each primary study.	RQ2
FS approaches	It provides the type of feature selection utilised in each primary study.	RQ2
FS techniques	It provides FS technique in its FS direction from the primary study.	RQ2
Datasets	It provides the IoT dataset used for analysis.	RQ3
Attacks	It presents the types of attacks detection or classification in each study.	RQ3
No. of feature sets	It introduces the original features from dataset and list the number of features.	RQ3
No. of Instances	It introduces the network flow instances of datasets.	RQ3
Machine learning algorithm(s)	It provides the type of machine learning algorithms.	RQ4
Deep learning algorithms(s)	It provides the type of deep learning algorithms.	RQ4
Performance metrics	It provides the metrics used for FS validation.	RQ4
Compared with that of full features	It provides the result compared with that of full feature sets.	RQ4
Compared with existing FS techniques	It provides the result compared with that of the-state-of-the-art FS techniques.	RQ4
Limitations	It describes the limitations of the proposed FS in the primary studies.	RQ5
Major challenges	It introduces the major challenges for FS applied.	RQ5
Future direction	It introduces the future direction for FS applied for attack classification for IoT security.	RQ5

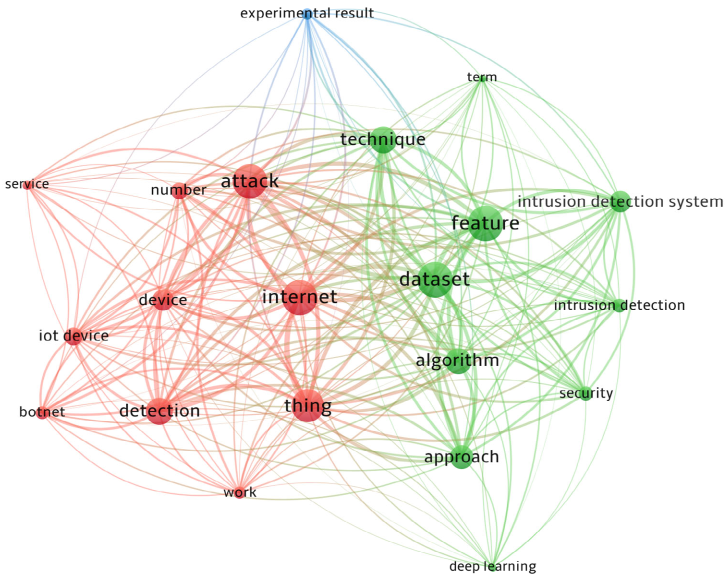
2.7 Data analysis

This subsection is the final step of the SLR methodology: data analysis to utilise the primary studies and the data extracted from each study to conduct data analysis in order to answer the six main research questions raised in this research study. The quality assessment report can be found in Appendices 1, 2 and 3, which presents the primary studies, the main idea, and the quality score for each study.

3 Results and analysis

In this SLR, a thorough search in multiple scientific databases (Web of Science, IEEE Xplore, Scopus, ScienceDirect, ACM, SpringerLink and Wiley Online Library) was conducted and initially identified 1,272 studies. Following the PRISMA process, we narrowed down our selection to 63 papers that were relevant to our research questions.

Figure 3 The key items clustering and network visualisation of primary studies by VOSviewer (see online version for colours)



VOSviewer was used to conduct a brief data analysis on the key terms found in the title and abstract fields of 63 primary studies in order to determine the key aspects and relationships between them. As shown in Figure 3, there are three clusters with red, blue, and green colour highlighted. For the red flag items, ‘internet’, ‘thing’, ‘device’, ‘IoT device’ means the term ‘internet of things’ or IoT in academics and industry; additionally, ‘attack’, ‘detection’ and ‘botnet’ mean security terms; thus, the output of the above means IoT security. Among the green flag terms are ‘dataset’, ‘feature’, ‘technique’, ‘algorithm’, and ‘deep learning’, with the additional words ‘intrusion detection system’ and ‘intrusion detection’, or IDS in academics and industry. As for the blue cluster, one term is ‘experimental result’, which means the experimentation and validation of the proposed system. Therefore, we can conclude that the brief background and methodology used in primary studies are valid, and the results showed that the primary studies are topic-focused, and the review based on these studies is valid.

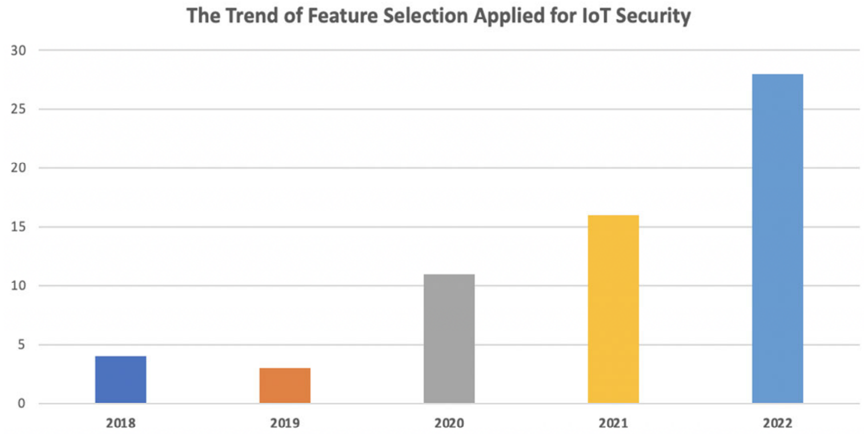
RQ1 What is current situation of FS approaches applied for ML or DL-based attack classification model for IoT security?

RQ1.1 What is the trend of the studies that applied FS for IoT security in recent five years?

After learning from the studies, two main factors contribute to this increasing trend. The first is the growing development of AI or ML-based cyber security models in IoT networks, which is driven by the limitations of traditional security models, which can only detect and classify known attacks and are ineffective at recognising unknown or zero attacks. Since the massive IoT devices deployed all over the world can create any possible variant of a known attack, any type of zero-day attack could threaten the critical infrastructure of IoT networks. Furthermore, followed by the second factor, the high performance of a security model using ML algorithms is highly dependent on the representative features needed to map to any type of attack. While the optimal features can be selected using various FS techniques in various manners, in the last five years, appropriate FS methods and ML algorithms have contributed to more effective and efficient security models in the IoT.

According to Figure 4 and the discussion above, FS research in IoT security has been expanding since it started in 2020, and it is still a hot issue among researchers in the field of IoT security.

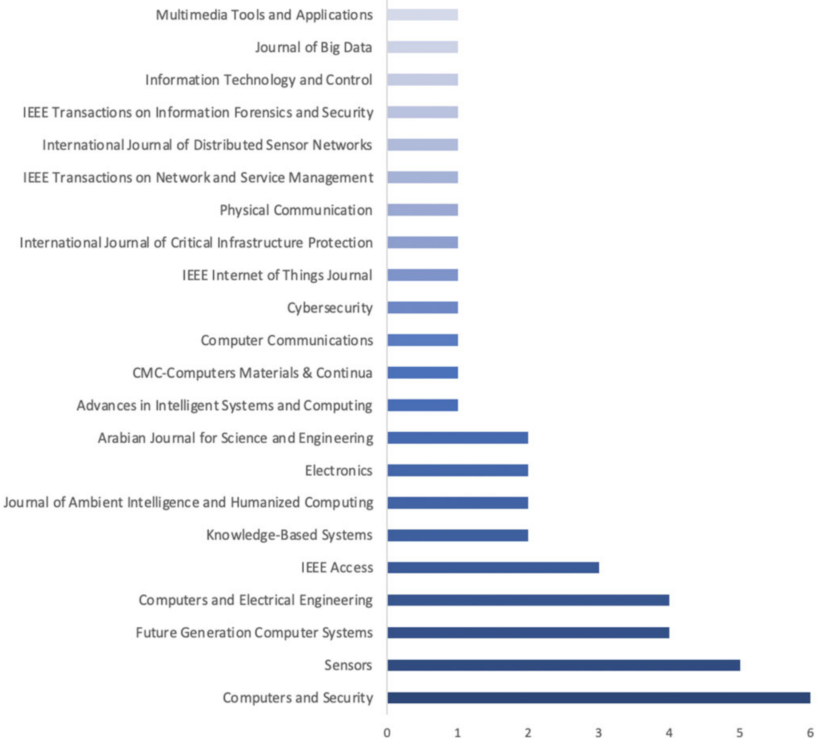
Figure 4 The trend of FS applied for IoT security over the years (see online version for colours)



RQ1.2 What are the distributions of the studies according to databases and publishers?

From Figure 5, the distribution of the number of primary studies in each journal is presented. Three groups of journals can be classified; the journals that published equal or more than five primary studies are *Computer and Security* and *Sensors*, which are in the first group. The second group of journals has equal to or more than three published primary studies involving *Future Generation Computer Systems*, *Computers and Electrical Engineering* and *IEEE Access*. Besides, the third group of journals below the three primary studies involves *Knowledge-Based Systems*, *Electronics*, *International Journal of Distributed Sensor Networks*, and so on. Based on Figure 5 and the explanation above, the result shows that which journals focus more on the topic of FS in IoT security and which journals can be future candidates for paper publication in the same domain.

Figure 5 The number of PS from each journal (see online version for colours)



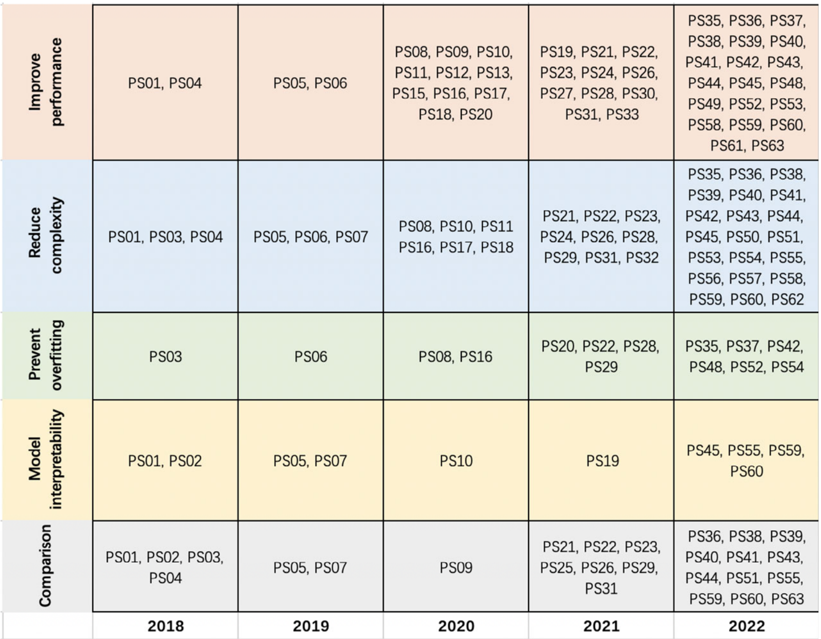
RQ1.3 What are the main objectives of applying FS for IoT security?

Generally, the purpose of FS in ML is to identify a subset of the most relevant features from the original feature set, which can then be used to train a model. This can improve the performance of the model and reduce overfitting, as well as make the model more interpretable by identifying the most important factors that contribute to the outcome. Additionally, it can also help in reducing the computational cost and time of training a model.

Figure 6 presents the distribution of the primary studies according to purpose over the past five years. The primary studies are classified by five categories: improving performance, reducing complexity, preventing overfitting, model interpretability and comparison.

Many purposes are described with various terms; thus, the rules for categorising studies are as follows: studies focusing on an effective attack detection model, improving the detection rate, achieving high accuracy, lowering the misclassification rate, and so on are considered first class. Studies that use FS techniques to reduce model cost and time, model prediction time, and model efficiency in resource-constrained IoT systems are considered to fall under the category of reducing complexity. While the works emphasising overfitting problems are classified as being of the third class, some studies focusing on the model's interpretability after using FS are classified as being of the fourth class. Finally, some studies that employed various FS techniques with various ML algorithms for effective models are classified as the last class. Since some studies employed FS to improve the performance and reduce the complexity of the proposed model as well, they fall into multiple categories with corresponding purposes.

Figure 6 The purpose of FS for IoT security in recent years (see online version for colours)



	2018	2019	2020	2021	2022
Improve performance	PS01, PS04	PS05, PS06	PS08, PS09, PS10, PS11, PS12, PS13, PS15, PS16, PS17, PS18, PS20	PS19, PS21, PS22, PS23, PS24, PS26, PS27, PS28, PS30, PS31, PS33	PS35, PS36, PS37, PS38, PS39, PS40, PS41, PS42, PS43, PS44, PS45, PS48, PS49, PS52, PS53, PS58, PS59, PS60, PS61, PS63
Reduce complexity	PS01, PS03, PS04	PS05, PS06, PS07	PS08, PS10, PS11 PS16, PS17, PS18	PS21, PS22, PS23, PS24, PS26, PS28, PS29, PS31, PS32	PS35, PS36, PS38, PS39, PS40, PS41, PS42, PS43, PS44, PS45, PS50, PS51, PS53, PS54, PS55, PS56, PS57, PS58, PS59, PS60, PS62
Prevent overfitting	PS03	PS06	PS08, PS16	PS20, PS22, PS28, PS29	PS35, PS37, PS42, PS48, PS52, PS54
Model interpretability	PS01, PS02	PS05, PS07	PS10	PS19	PS45, PS55, PS59, PS60
Comparison	PS01, PS02, PS03, PS04	PS05, PS07	PS09	PS21, PS22, PS23, PS25, PS26, PS29, PS31	PS36, PS38, PS39, PS40, PS41, PS43, PS44, PS51, PS55, PS59, PS60, PS63

Based on the data extracted in Figure 6, we can see that the primary studies mostly fell into improving performance (45 out of 62), which means the performance metrics on attack detection and classification are the most concerning points for the academics. Followed by the second category is reducing complexity (42 out of 62), which show that producing lightweight models is also vital, particularly for resource-limited IoT networks in recent years. The interesting point is that more studies are focusing on developing lightweight models with significant performance metrics, rather than focusing solely on performance. Since there are so many FS techniques that can be employed before training learning models, many studies have tried to employ various FS techniques combined with different ML and DL algorithms to build state-of-the-art models, particularly in the past two years.

FS can prevent overfitting and contribute to a model that can be generalised to the same scenarios; thus, the implementation of the most primary studies can address overfitting to some extent; however, not many studies emphasise overfitting in their studies (14 out of 62). Few studies (10 out of 62) argued for model interpretability in their proposed FS approaches; however, there is an increasing trend toward the implementation of model interpretability in 2022.

RQ2 What are the FS methods and techniques applied on attack classification models for IoT security?

RQ2.1 What are the main types of FS approaches applied for attack classification model?

The process of FS involves various methods for selecting the most relevant features, which can be categorised into filter, wrapper, embedded, and hybrid methods based on the mechanism used for selecting the optimal features. The filter method assesses the importance of each feature using statistical tests and selects the subset of the most relevant features, such as the chi-squared test, mutual information, and correlation-based feature selection (CFS). The wrapper method utilises a ML algorithm to assess the performance of different feature subsets and chooses the best subset based on a performance metric, such as forward selection, backward elimination and recursive feature elimination (RFE). Embedded methods use a ML algorithm to select features as part of the model training process, such as Lasso and Ridge regression, which incorporate a built-in FS process through the regularisation term.

Hybrid methods combine the strengths of multiple FS methods to achieve better performance. Examples include combining filter and wrapper FS to construct a more powerful FS method. Ensemble approaches combine multiple FS techniques that use the same, different parts, or even the entire dataset, and then make decisions using algorithms such as interaction or majority voting based on the candidate feature list from multiple FS techniques. Some studies tried to explore various FS techniques to obtain the model with the best performance; we classify these types of studies into the comparison category.

Table 10 shows the distribution of primary studies over various FS approaches applied for IoT security. We found there are six types of FS methods used to identify the most informative features before building a security model. The result shows that the filter-based FS method is the top FS approach used in attack classification for IoT security. Most of the studies used filter FS by using various statistical techniques to select the feature sets based on two rules: one was to eliminate the features that have high correlation with each other, while the other was to obtain the features that have high correlation with the target classes for model training and prediction (Soe et al., 2020a). The proposed method performs feature representation and selection based on APT behaviour data and trained a multiclass model named SMOTE-RF to deal with imbalance and multiclassification problems. Furthermore, the feature sets of the two rules may overlap, so appropriate threshold settings for the correlation are vital for determining the final feature sets for building high performance models (Saurabh et al., 2022). Moreover, considering most of the datasets for IoT security are large volumes of network datasets with big data characteristics (Koroniotis et al., 2022), while most IoT systems are equipped with limited computational and storage resources, filter FS was chosen in the majority of research because it is computationally light, which fulfils the need for making the overall model lightweight for IoT networks (Awad et al., 2022).

Wrapper FS was the primary study's second method, followed by the filter method. Wrapper FS selects the optimal feature subsets rather than identifying individual features implemented by the filter method. Furthermore, wrapper works with ML algorithms to evaluate feature subsets based on the performance metrics required by the model. Since the feature subsets that are evaluated and identified are performance-oriented, the wrapper method can achieve better performance and contribute to higher generalisation capability than filter FS; however, its demerit is that it requires much more computational resources than filter FS, which can be a significant concern for resource-constrained IoT devices. Vigoya et al. (2021) employed a RFE method to evaluate the feature subsets among all the features of the dataset exhaustively. It uses a specific ML algorithm to iteratively remove the least important features based on a performance metric until the desired number of features is reached. Because the search space of feature subsets is extremely large for IoT datasets, which contain too many features with a large number of instances in network flow records, heuristic algorithms were mostly applied with learning algorithms using the wrapper method. One instance where the augmented whale optimisation (AWO) algorithm search algorithm was proposed by Al Shorman et al. (2020) to find the most appropriate feature subset with OCSVM as the learning algorithm to attain the ideal false positive rate (FPR). Halim et al. (2021) came up with an advanced genetic algorithm (GA) which proved to be more efficient than RFE, sequential feature selection (SFS) and CFS. Lastly, Chohra et al. (2022) proposed the particle swarm optimisation (PSO) algorithm, which combined swarm intelligence and ensemble learning techniques to establish the best settings for feature subsets and model hyperparameters. In order to address the limitations like inefficient FS, binary classification, and slow prediction, Masoudi-Sobhanzadeh and Emami-Moghaddam (2022) proposed a two-step ML approach using world competitive contests (WCC) optimisation algorithm and SVM to address these issues. Boopathi (2022) proposed a competitive swarm Henry optimisation (CSHO)-based deep maxout network for IoT intrusion detection. The method identifies 95% of intrusions while reducing energy use, outperforming prior approaches. Nonetheless, more attention needs to be given to attaining a balance between searching efficiency in feature space and performance metrics such as accuracy or F1-score.

Hybrid FS method is a combination of multiple FS methods to achieve better performance. The idea behind hybrid methods is to leverage the strengths of multiple FS techniques to achieve a more accurate and robust solution. For example, a hybrid method might first use a filter method to reduce the number of features based on a statistical test, then use a wrapper method to further refine the feature set based on the performance of a ML model. For example, Guerra-Manzanares et al. (2019a) proposed a hybrid FS by first using filter FS and then employing wrapper FS to identify the optimal feature subset based on the features obtained by filter FS. Similarly, Li et al. (2020) employed a two-step hybrid FS using the Kolmogorov-Smirnov (KS) test to select important features from the candidate feature set, then used Pearson correlation to remove redundant features to obtain the informative features. Moreover, Padmashree and Krishnamoorthi (2022), Zhou et al. (2022) and Malik et al. (2022) implemented the same idea of hybrid

FS to identify optimal feature subsets by combining the strengths of multiple FS methods, resulting in improved performance and robustness.

Ensemble FS is a hybrid method that involves combining the outputs of multiple FS techniques to create a final feature set. With this technique, multiple FS methods are applied to the same data, or subsets of the data, and the results are merged to create a final feature set. The combination can be achieved through various methods, such as taking the union or intersection of the feature sets produced by each method or using a voting scheme. For instance, in a study (Kumar et al., 2021), three feature sets were generated using correlation coefficient, random forest mean decrease accuracy, and gain ratio (GR) techniques, which were then combined using a designed mechanism to obtain a single optimised feature set. In another study, Guo (2021) combined five FS techniques involving, information gain (IG), gain ratio (GR), chi-square (CS), Pearson correlation coefficient (PCC), and symmetric uncertainty (SU) through majority voting to extract the final feature sets for the subsequent model training. Alamiedy et al. (2021) proposed an ensemble FS approach for detecting DDoS attacks in RPL networks, combing three bio-inspired algorithms with SVM to detect DDoS attacks on RPL, a protocol enabling IoT device communication. However, the choice of FS techniques and the combination approach must be carefully considered to achieve optimal results.

In embedded FS, the FS process is incorporated into the optimisation objective of the ML model. Doshi et al. (2018), Shi et al. (2021) and Disha and Waheed (2022) employed random forest as the algorithm for selecting the feature sets based on Gini impurity scores, then use multiple ML algorithms respectively to implement attack classification. Embedded methods can produce models with improved interpretability, as the most important features are automatically identified and selected as part of the training process. Alternatively, some studies that used different techniques to obtain feature sets are classified as others. For example, Ozer et al. (2021) iteratively selected and evaluated only two features, named feature pairs, from the original 12 features using multiple ML algorithms to build and evaluate a lightweight model, respectively. Suresh et al. (2019) proposed improved weighted random forest feature selection (IW-RFI) by evaluating mutual information between 41 attributes in the dataset to choose optimal features for ML. By selecting the most relevant features, their model accurately detects 95% of IoT threats and allows secure transmission, outperforming approaches without IW-RFI. Ravi et al. (2022) bypassed the FS process and directly used DL algorithms named RNN, LSTM, and GRU to extract and select features for model building. However, Carter et al. (2022) employed principal component analysis (PCA) to reduce the features, and the results showed a significant advantage to using PCA for both traditional ML algorithms (SVM) and neural network-based DL algorithms for anomaly detection.

Considering there are various FS approaches and so many specific techniques that can be selected for various IoT datasets to build models, some primary studies implement comparison using various FS methods to evaluate and obtain the best feature sets. For example, Parker et al. (2019) and Guerra-Manzanares et al. (2019b) implemented an FS comparison of filter, wrapper, and hybrid methods, and the results showed hybrid produced the best accuracy results. Moreover, Samdekar et al. (2021) evaluated multiple FS methods involving filter and wrapper using one ML algorithm named SVM to determine the best model. Gaber et al. (2022) compared filter and wrapper FS, which involved constant removal and constant removal combined with RFE. Furthermore, Illy et al. (2022) evaluated the impact of various selected features and various ML algorithms on the accuracy of the models, and the result showed that the accuracy of the detection model depends more on the feature sets than the ML methods.

Table 8 Primary studies based on FS methods

FS types	*# of PS*	*Primary studies*
Filter	18	PS01, PS08, PS09, PS10, PS14, PS17, PS20, PS21, PS29, PS37, PS41, PS42, PS54, PS56, PS57, PS58, PS59, PS61
Wrapper	13	PS03, PS12, PS13, PS16, PS19, PS33, PS34, PS36, PS39, PS43, PS48, PS52, PS63,
Embedded	3	PS02, PS24, PS38,
Hybrid	10	PS06, PS11, PS15, PS18, PS27, PS45, PS47, PS49, P50, PS60
Ensemble	6	PS04, PS22, PS23, PS28, PS35, PS44,
Comparison	10	PS05, PS07, PS25, PS26, PS30, PS31, PS40, PS51, PS53, PS55
Others	3	PS32, PS46, PS62

We investigated the trends further by looking at the distribution over the years. From Figure 7 that there were limited studies for each type of FS in the first two years because most of the public IoT datasets were generated in 2018. Then, over the last three years, there has been a consistent use of filter, wrapper, and hybrid FS because researchers proposed various ML-based frameworks for various objectives, such as performance metrics-oriented models, lightweight models, or maintaining the balance between two objectives. Embedded FS was introduced from 2021 to 2022, since AI interpretability or model transparency had been a concern for academics in recent years. Furthermore, other types of FS were also introduced in the past two years. It is worth noticing that FS comparison was consistently conducted over the past five years, because many various FS techniques with different methods can be used to identify final features, moreover, many factors such as the objectives of the proposed models, characteristics of datasets, and classifiers trained by various learning algorithms can affect the results of the proposed FS methods.

Figure 7 The trend of FS approach (see online version for colours)

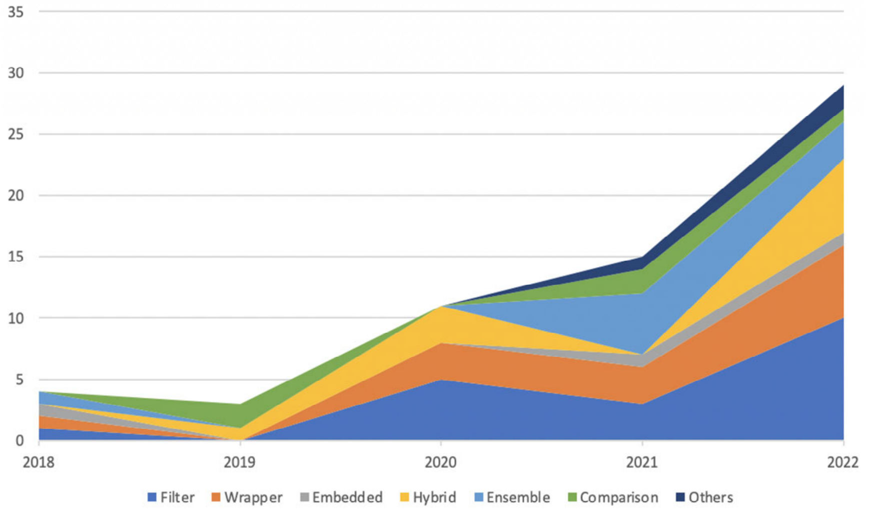


Table 9 Comparison of various FS methods used in IoT networks

FS method	*Description*	*Strengths*	*Weakness*	*Applicability*
Filter	Assesses feature importance using statistical tests and selects most relevant features.	Computationally efficient, easy to interpret.	Limited to linear relationships, may select redundant features.	Small to medium datasets with linear relationships.
Wrapper	Uses a machine learning algorithm to assess the performance of feature subsets and selects the best subset based on a performance metric.	Considers feature interactions, selects nonlinear relationships.	Computationally expensive, prone to overfitting.	Medium to large datasets with nonlinear relationships.
Embedded	Incorporates feature selection into the model training process using regularisation.	Simultaneously optimises feature selection and model performance.	Limited to specific models, may select biased features.	Large datasets with specific models.
Hybrid	Combines the strengths of multiple feature selection methods to achieve better performance.	Can improve performance compared to individual methods.	May be computationally expensive, difficult to interpret.	Medium to large datasets with complex relationships.
Ensemble	Combines multiple feature selection techniques using interaction or majority voting.	Can improve performance and reduce bias compared to individual methods.	May be computationally expensive, difficult to interpret.	Medium to large datasets with complex relationships.
Comparison	Compares various feature selection methods to identify the best-performing method.	Provides insights into the strengths and weaknesses of different methods.	May be limited by the evaluation metric, may not generalise well.	Depends on the specific dataset and problem.

Table 9 provides an overview of various FS methods used in IoT networks, including filter, wrapper, embedded, hybrid, ensemble and comparison methods. Table 9 summarises the strengths, weaknesses, and applicability of each method in terms of the number of instances and feature sets. The filter method is best suited for small to medium-sized datasets, and is useful for identifying highly relevant features based on statistical tests (Soe et al., 2020b). The wrapper method, which involves using a ML algorithm to select features based on a performance metric, is ideal for medium to large datasets (Chohra et al., 2022). The embedded method is appropriate for medium to large datasets, and involves incorporating FS into the model training process (Disha and Waheed, 2022).

Hybrid methods combine the strengths of multiple FS techniques, such as combining filter and wrapper methods to construct a more powerful FS method (Padmashree and Krishnamoorthi, 2022). Ensemble approaches combine multiple FS techniques to make decisions using algorithms such as interaction or majority voting based on the candidate feature list from multiple FS techniques (Kumar et al., 2021). Comparison studies explore various FS techniques to obtain the model with the best performance (Gaber et al., 2022). Thus, the choice of FS method depends on the specific characteristics of the IoT network dataset and the use case. By understanding the strengths, weaknesses, and applicability of each method, researchers and practitioners can make informed decisions about which FS method to use for their particular IoT network application.

RQ2.2 What are the techniques for each type of FS applied for IoT security models?

Based on the FS approaches, we further investigated the specific techniques utilised based on each FS category. From Table 10, the techniques employed in the primary studies.

Table 10 Primary studies based on FS techniques

FS types	*Techniques/algorithms*	*# of PS*	*Primary studies*
Filter	Fisher's score	2	PS01, PS08
	CS	5	PS09, PS20, PS21, PS42, PS54
	IG	6	PS09, PS37, PS41, PS57, PS58, PS59
	GR	1	PS09
	SHAP	1	PS10
	PCC	5	PS14, PS17, PS54, PS56, PS59
	MI	2	PS29, PS56
	PFI	1	PS61
Wrapper	D-FES	1	PS03
	AWO	1	PS12
	Bijective soft set	1	PS13
	GWO	2	PS16, PS48
	TSO	1	PS19

Table 10 Primary studies based on FS techniques (continued)

FS types	*Techniques/algorithms*	*# of PS*	*Primary studies*
Wrapper	GA	1	PS33
	RFE	1	PS34
	GWO	1	PS36
	AQU	1	PS39
	HGS	1	PS43
	GTO	1	PS63
	PSO	1	PS52
Embedded	Gini impurity	2	PS02, PS38
	VIM	1	PS24
Hybrid	KST + PCC	1	PS11
	Cooperative game theory and Shipley value	1	PS15
	GA + GWO	1	PS18
	CorrAUC + TOPSIS and Shannon entropy	1	PS27
	PCC + RFE	1	PS47, PS50, PS60
	RFE + PCC	1	PS45, PS49
Ensemble	Hopkins + variance, then based on entropy	1	PS04
	IG + GR + CS + PCC + SU, then majority voting	1	PS22
	PCC + MI, then the threshold respectively	1	PS23
	PCC, RF and GR, then intersection	1	PS28
	SVM, DT and NB, then top ranked	1	PS30
	RF + PCC, then intersection	1	PS31
	DT + ET + RF + XGB, then top ranked	1	PS35
	(WRAPPER + CLS + PCC) + AE, then combined	1	PS40
	IG + GR + CS, then top ranked	1	PS44
Comparison	Filter: MI and hybrid: MI + J48	1	PS05
	Filter: Fisher's score, PCC; wrapper: SFFS, SBFE; and hybrid: filter + wrapper	1	PS06
	Filter: PCC and wrapper: SFFS + DT	1	PS25
	CS, ET, FA and PCA	1	PS26
	IG, CS and EFS + DT	1	PS51
	Constant removal and that with RFE	1	PS53
	Manually selecting and evaluating each type of features	1	PS55
Others	Feature pairs	1	PS32
	Deep learning algorithms, RNN, LSTM and GRU	1	PS46
	PCA	1	PS42

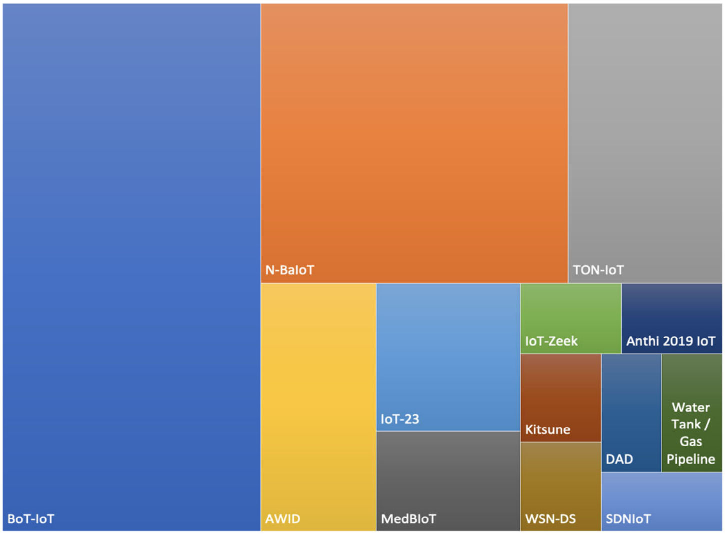
In filter FS, IG, PCC, and CS techniques were widely used as feature ranking techniques to identify final feature sets. The second tier used by primary studies to select features was MI and Fisher's score. The terms GR, SHAP, and PFI were only used once. One point that needs to be mentioned is that the techniques used in filter FS were also utilised in other types of FS, such as PCC, IG, CS, GR, and MI, and were widely used as one step of FS in hybrid, ensemble, and comparison modes, particularly for PCC, which was the most commonly employed in the primary studies. PCC is a measure of the linear relationship between two continuous variables. In wrapper FS, the techniques categorised in Table 10 are searching algorithms searching for the optimal feature subsets. The results showed that most of the searching techniques are based on heuristic algorithms, which are more efficient for handling large IoT datasets with high-dimensional feature spaces. In hybrid FS, the combination of PCC as the feature ranking technique and RFE as the searching technique was widely used.

RQ3 What are the characteristics of related factors for FS methods for IoT security?

RQ3.1 What are the IoT datasets as the benchmark by the studies when applying FS method?

Since the IoT datasets with representative information can be the benchmark for validation of the attack detection and classification models, Table 12 describes a set of publicly used IoT datasets with basic information such as the year created, the number of features, the total number of instances, and the mapping of each dataset to the primary studies. From the visualised Figure 8, we can argue that BoT-IoT (19 out of 63) was the mostly used datasets among the studies, following by N-BaIoT (12 out of 63), TON-IoT (4 out of 63), AWID (4 out of 63), and IoT-23 (3 out of 63). Most of other studies were investigated by just one study except by MedBIoT which was created for medical industry.

Figure 8 The IoT datasets investigated by primary studies (see online version for colours)



Among the datasets, Bot-IoT dataset was the mostly used and evaluated dataset by the primary studies, and it has the largest volume of instances (72,000,000) for studies to create and evaluate attack detection models. Followed by N-BaIoT which has more than one hundred features (115) to describe the information of each instance, was the secondly studied by researchers. Six studies worked on TON-IoT created in 2021 with its characteristics of heterogeneous sources and multiple layers, to create attack detection models.

RQ3.2 What are mapping of datasets and attacks to various FS methods among the studies?

Since FS is the key process of data processing in the ML pipeline, the characteristics of the data, particularly the attacks to be detected and classified, are highly related to the FS method to be utilised. Therefore, we investigated the IoT datasets used in the primary studies and what types of FS methods were applied to each of them. Table 11 shows the primary studies based on various IoT datasets, the attack classes in the datasets, and the corresponding FS methods. One point that needs to be mentioned is that the primary studies classified in FS comparison are reclassified into specific FS methods in this section. Since many FS methods are involved in FS comparison, one primary study may be classified into two FS categories. For example, PS25 has implemented both the filter and wrapper methods for comparison; thus, PS25 is added to both the filter and wrapper FS in Table 11, and the same rule applies to other primary studies that have implemented FS comparison, so the total number of PS in Table 11 is more than 63.

Table 11 The primary studies based on various IoT datasets

Dataset	*Attack classes*	*FS*	*# of PS*	*Primary studies*
BoT-IoT	DoS, DDoS, reconnaissance, information theft	Filter	24	PS09, PS25, PS26, PS41, PS51, PS56, PS57, PS61
		Hybrid		PS27, PS45, PS49, PS60
		Ensemble		PS28, PS44
		Wrapper		PS25, PS26, PS33, PS39, PS63, PS48, PS51
		Others		PS32
TON-IoT	Scanning, XSS, DoS, DDoS, backdoor, injection, password cracking, MITM, ransomware	Filter	6	PS20，PS54, PS58, PS59
		Ensemble		PS22
		Embedded		PS38
N-BaIoT	Botnet, Gafgyt, Mirai	Filter	13	PS01, PS07, PS08, PS14, PS21
		Wrapper		PS07, PS12, PS16, PS36
		Hybrid		PS06, PS07, PS60
		Ensemble		PS04

Table 11 The primary studies based on various IoT datasets (continued)

Dataset	*Attack classes*	*FS*	*# of PS*	*Primary studies*
AWID	Injection, flooding, impersonation	Filter	4	PS10
		Hybrid		PS18
		Ensemble		PS30
		Wrapper		PS03
IoT-23	Mirai, Torii, Trojan, Gagfyt, Kenjirro, Hakai, Hajime, Okiru	Filter	3	PS21, PS42
		Ensemble		PS35
IoT-Zeek	Malware	Wrapper	1	PS52
Anthi 2019 IoT	Scanning, DoS, IoT-toolkit and MITM	Others	1	PS55
Kitsune	Mirai, SYN DoS, SSDP flood, etc.	Filter	1	PS21
MedBIoT	Mirai, Bashlite and Torii	Filter	2	PS21
		Hybrid		PS50
WSN-DS	Grayhole, Blackhole, flooding, and TDMA scheduling	Ensemble	1	PS23
DAD	Duplication, interception and modification on the MQTT message	Wrapper	1	PS34
Water tank and gas pipeline	Naive malicious response injection, complex malicious response injection, malicious state command injection, malicious parameter command injection, malicious function code injection, denial of service, reconnaissance	Ensemble	1	PS40
SDNIoT	DoS, DDoS, port scanning, OS fingerprinting and fuzzing	Others	1	PS46
Private datasets	Ransomware, Cryptominer	Others	4	PS62
	SYN flood, LowRate, Mirai	Hybrid		PS47
	DOS, DDoS, reconnaissance, exploits, fuzzes, backdoors, generic, DoS, Shellcode	Filter		PS37
	Routing protocol for low-power and lossy networks (RPL)	Ensemble		PS31
	Decreased rank (DR)			
	Sinkhole (SH)			
	Blackhole (BH)			
	Selective forwarding (SF)			
	Hello flooding (HF)			
	Version number (VN)			

From Table 11, the dataset named BoT-IoT was produced by Koroniotis et al. (2019) and was mostly studied by researchers (24 out of 63). As the FS method to implement FS for attack classification, filter and wrapper FS methods dominate, because the dataset contains a large amount of data concerning normal and typical abnormal IoT activities. Many researchers have worked on this dataset as an IoT scenario benchmark to validate their proposed intrusion detection systems, followed by the N-BaIoT dataset, which was produced by Meidan et al. (2018) as public IoT dataset for researchers working on the models for IoT security. The data was collected with real commercial IoT devices involved, and it includes traffic information for Gafgyt and Mirai, two of the most well-known IoT-based botnet attacks. Many researchers (13 out of 63) employed filter and wrapper FS to figure out the most appropriate feature sets for the attacks in the dataset in recent years.

TON-IoT was produced recently by Moustafa (2021) and was also an IoT-specific dataset. The datasets were collected from heterogeneous sources, including telemetry from IoT devices, networking flows, and system logs of the operating system, across multiple layers such as edge, fog and cloud layers. Some studies have implemented various FS methods to identify the features for various attacks in this data, while the filter method was the most commonly used by studies compared with ensemble and embedded FS. AWID was produced by Kolias et al. (2016), focusing on wireless data with the Wi-Fi protocol as one of the communication protocols for IoT networks. Except for embedded FS, other methods were used to identify the most suitable feature for classification models.

Similarly, there are increasingly more IoT datasets created and studied by researchers using various FS methods for various attack classifications. For example, Gandhi and Li (2021) and Kumar et al. (2022a) implemented filter FS for IoT datasets named IoT-23, Kitsune and MedBIoT, respectively. Filter mode can make the FS process more lightweight, and to be specific on the technique, CS was used to identify independent features that can be informative for the models to learn the pattern of attack classes. Similarly, ensemble FS was used by Ismail et al. (2021), Alanazi and Aljuhani (2022) and Jayalaxmi et al. (2022) on datasets named, WSN-DS, IoT-23, and water tank and gas pipeline, to combine the individual capabilities of FS techniques. Moreover, some researchers created their own datasets for specific purposes. For example, Medjek et al. (2021) created the dataset focusing on routing type attacks, and proposed ensemble FS mode by combining random forest and Pearson correlation, followed by interaction to select the features.

RQ4 What are the verification methods to evaluate the effectiveness of proposed FS approaches?

RQ4.1 What are the ML and DL methods used in each type of FS?

Because FS is an essential component of the data processing pipeline in ML, the effectiveness of the FS approach can only be assessed when combined with ML algorithms to contribute to classification models. Among the primary studies, we investigated ML, DL, and both algorithms used in each type of FS method. Table 12 shows that the ML and DL were applied for each type of FS method. The results showed that most studies combined FS with ML algorithms to build the models, while a few studies only employed FS with DL algorithms. It means classic ML algorithms need processed data after FS so that lightweight models with high performance can be built.

Table 12 ML and DL applied in each type of FS method

FS method	*ML(s)*	*DL(s)*	*ML(s) + DL(s)*
Filter	PS01, PS04, PS05, PS07, PS08, PS09, PS10, PS17, PS20, PS21, PS29, PS42, PS54, PS57, PS58, PS59, PS61	PS56, PS37	PS41, PS46, PS62
Wrapper	PS03, PS12, PS13, PS16, PS33, PS34, PS36, PS39, PS43, PS63		PS52, PS19, PS48
Embedded	PS02, PS24		PS38
Hybrid	PS06, PS07, PS11, PS18, PS27, PS47, PS50, PS60	PS45, PS49	PS15
Ensemble	PS04, PS22, PS23, PS28, PS30, PS31, PS35, PS44		PS40
Comparison	PS05, PS26, PS32, PS51, PS53, PS55		PS25

Some studies employed both ML and DL when implementing the FS method. Classical ML algorithms dominate all types of FE methods, since FS can affect the final classifiers learned by various ML models; thus, multiple ML algorithms were often used with the proposed FS methods. As for DL applied with FS, there are two categories of applying DL algorithms in primary studies: one type uses DL as the model training algorithms to build classifiers, while the FS method was independently implemented to generate the feature subsets (Moizuddin and Jose, 2022; Saurabh et al., 2022). Moreover, Luo et al. (2021) proposed a novel ensemble DL-based web attack detection system (EDL-WADS) to address the challenges of detecting web attacks in IoT networks. The system uses three DL models to detect web attacks separately, and an ensemble classifier is used to make the final decision based on the results obtained from the three models. However, the other type is using DL (Jayalaxmi et al., 2022; Moizuddin and Jose, 2022; Cao et al., 2022) as feature extraction based on original feature sets, taking the place of FS, and combining it with the feature sets selected by FS methods, to comprehensively identify the features for model training.

RQ4.2 What are the performance metrics used for validation of FS approaches?

Evaluating the effect of a FS technique on a classification model involves comparing the performance of the model with and without the FS. Comparing the performance metrics of the model with and without the FS technique can provide insight into the effect of the FS on the model's performance. If the performance metrics improve after applying the FS technique, it can be concluded that the FS has a positive effect on the model. On the other hand, if the performance metrics are degraded after applying the FS, it can be concluded that the FS has a negative effect on the model.

Table 13 investigated the common performance metrics used by the primary studies to evaluate the performance of a classification model in IoT security.

Accuracy is calculated as the number of correct predictions made by the model divided by the total number of instances in the dataset. The metric provides a general evaluation of the performance of a model, but it can be misleading in cases where the dataset is imbalanced or has a skewed distribution of positive and negative instances (Disha and Waheed, 2022). Precision is the proportion of true positive (TP) predictions among all positive predictions made by the model. It measures the ability of the model to correctly identify positive or attack instances and avoid false positive (FP) or attack predictions in IoT security model. Recall: the fraction of TP predictions among all positive instances in the dataset, and it is the same as sensitivity, true positive rate (TPR), or detection rate. F1-score means the harmonic mean of precision and recall. The metrics of accuracy, precision, recall, and F1-score were often used together to evaluate classification models, because each metric has its limitation for model evaluation, thus, most studies evaluated all the four metrics to obtain a comprehensive picture of the model's performance.

Table 13 Performance metrics evaluated for FS

Metrics	*# of PS*	*Primary studies*
Accuracy	61	PS01~PS15, PS17~PS43, PS45~PS63
Precision	40	PS01, PS08~PS10, PS13, PS15, PS18~PS22, PS24~PS28, PS31, PS34~PS35, PS37~PS39, PS41~PS43, PS45~PS54, PS51~PS61, PS63
Recall (sensitivity/DR/TPR)	49	PS01, PS03, PS08~PS11, PS13, PS15, PS16, PS18~PS31, PS33~PS43, PS45~PS54, PS57~PS61, PS63
F1-score	40	PS01, PS04, PS07~PS11, PS15, PS18~PS22, PS24~PS26, PS28~PS32, PS34, PS35, PS37, PS39, PS41~PS43, PS45~PS50, PS52~PS54, PS51~PS61
Specificity (TNR)	5	PS13, PS27, PS37, PS51, PS57
AUC-ROC	8	PS21, PS23, PS25, PS29, PS44, PS45, PS48, PS58
FPR	16	PS02, PS16, PS18, PS20, PS23, PS29, PS30, PS36~PS40, PS45, PS48, PS54, PS57
FNR	2	PS37, PS57
MCC	3	PS30, PS37, PS43
G-mean	1	PS16
Model size	1	PS23
TTB	21	PS04, PS08~PS12, PS15, PS18, PS21~PS23, PS30, PS32, PS35, PS43, PS45, PS50, PS56, PS57, PS61~PS63
TTP	9	PS08, PS16, PS21, PS23, PS29, PS35, PS50, PS57, PS62
CM	6	PS08, PS10, PS19, PS25, PS46, PS54

FPR measures the proportion of negative instances that are incorrectly classified as positive by the model, in contrast, false negative rate (FNR) is equals (1 – FPR), which means the positive case that are incorrectly identified as negative one. Since after FPR is calculated, FNR can be obtained, while only two primary studies evaluated FNR, however the two studies also identified FNR, in fact, there is no need to evaluate it since FPR is obtained. Moreover, AUC and ROC are commonly used performance metrics in binary classification tasks to evaluate the ability of a model to distinguish between positive and negative classes. The ROC curve provides a visual representation of the trade-off between the TPR and FPR for different classification thresholds, while the AUC provides a single scalar value that summarises the overall performance of the model across all possible classification thresholds.

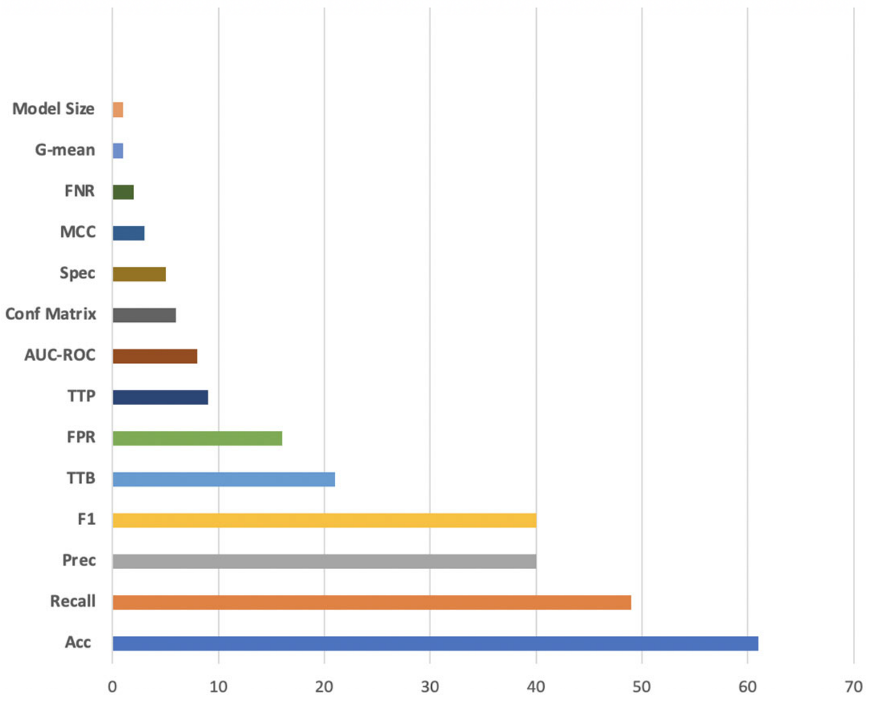
Matthews correlation coefficient (MCC) is also a performance metric used to evaluate the performance of binary classification models. The MCC takes into account the TP, FP, false negative (FN), and true negative rates (TNRs), and it provides a more comprehensive evaluation of the model's performance than accuracy, precision, recall, or F1-score alone. A value of 1 indicates perfect prediction, a value of –1 indicates perfect anti-correlation, and a value of 0 indicates random prediction. However, few primary studies (3 out of 63) used this metric for evaluation. Because the choice of performance metrics will depend on the specific problem being solved and the goals of the evaluation. For example, in some cases (Shafiq et al., 2021; Saurabh et al., 2022), accuracy may be more important than sensitivity or specificity, while in other cases (Abdulkareem et al., 2022; Malik et al., 2022), precision or F1-score may be more relevant. In addition, different metrics may be more or less appropriate for different types of datasets. For example, the studies that used highly imbalanced datasets (Vigoya et al., 2021), metrics such as precision and recall may be more appropriate than accuracy, while in datasets with balanced class distribution, accuracy may be a more appropriate metric. Similarly, G-Mean is a combination of sensitivity (TPR) and specificity (TNR), and provides a single scalar value that summarises the overall performance of the model. It can be especially useful in situations where both TPR and TNR are important. Only 1 out of 63 primary studies investigated G-mean as the performance evaluator.

What is more, model size in memory (bytes) was identified and compared among various classification models only in Ismail et al. (2021), in order to identify the most efficient model for wireless sensor network. Besides, the evaluators using time to build (TTB), or train models and time to predict (TTP), or test models are other aspects to evaluate the efficiency of the models. There are clearly more primary studies focusing more on TTB (21 out of 63) rather than TTP (9 out of 63), because TTB evaluated based on seconds, dominates more time on model training, while TTP evaluated based on μ seconds, takes less time just on test data prediction after the model is built.

Specificity or TNR is a performance metric used in classification tasks to measure the proportion of true negatives (TNs) among all negative instances in the dataset. In classification for IoT security, it means the ability of a model to correctly identify normal case in network flow. Only five primary studies evaluated this metric, because most studies focused their effort on attacks rather than normal cases detection and classification, however, the benchmark dataset named BoT-IoT researched by the studies, has high imbalanced class distribution between attack and normal cases, which means, very few normal instances while attack flows dominate the cases. Thus, TNR is the metric to evaluate the capability of classifying the normal cases in highly imbalanced class. Other studies (6 out of 63) evaluated the performance of models using confusion matrix (CM), which is a table that summarises the number of TP, TN, FP, and FN predictions made by the model.

From Figure 9 for the visualised distribution of the performance metrics discussed above among the primary studies. Accuracy dominates the most, followed by precision, recall, and F1-score to achieve comprehensive evaluators for classification models. FPR is an important indicator since the cases that are falsely identified as attack classes can lead to more resources to follow up on, such as attack mitigation and preventing intrusions into intrusion prevention systems (IPSs). Moreover, TTB is a significant indicator to evaluate for the lightweight classification model in resource-limited IoT systems since the number of selected features can directly lead to the cost of building the model. Furthermore, to be specific, the cost for searching, identifying, and selecting the optimal features employed by the methods of FS and the FS techniques are another key to the overall cost of ML-based classification systems.

Figure 9 Performance metrics validation by primary studies (see online version for colours)



RQ4.3 What are the methods of the validation of FS in studies?

We further investigated how primary studies validate the proposed FS to see if comprehensive validation is conducted for each study, besides performance metrics, processing time searching for optimal features, and time for training models and implementing predictions. Table 14 presents the distribution of validation methods for the proposed FS methods of each primary study.

Here are the shortcut names for each character in Table 14: ‘Multi-DS’ means validated using multiple datasets; in Table 14, one IoT dataset with any traditional networking, or a non-IoT dataset, is also considered as multiple datasets. ‘Multi-FS’ means various FS techniques were used and compared. Similarly, ‘Multi-MLs’ and ‘Multi-DLs’ mean multiple ML algorithms and multiple DL algorithms were used and compared with the proposed FS in studies. ‘Full features’ means the performance of the models based on selected features is compared with the models with full features. Finally, ‘recent works’ means the proposed FS and the models were compared with recent studies on their performance using the same dataset.

The validation of the proposed FS technique using multiple ML algorithms is the most validated item. Different algorithms may have different requirements for the input features and may perform better or worse on different types of data. By using and comparing multiple algorithms, the researchers can compare different models using various ML algorithms and identify the most effective model.

From Table 14 are for detailed information on the validation for each study. Some studies used extensive FS validation methods to consolidate performance results and claim contributions. For example, Kumar et al. (2021) verified the results except the comparison of multiple DL classifiers. Similarly, Disha and Waheed (2022) validate all the check points in Table 14 except for making comparisons with other FS in the study. Some studies focused more on performance metrics but did not validate the proposed FS method compared with the results of full features and recent studies on the same dataset. For example, Rahman et al. (2021) proposed an ensemble FS to combine the ranked features by three ML algorithms, and the proposed FS outperformed any other individual wrapper FS with results of 99.95%, 99.95%, and 99.90% accuracy respectively, however, the study does not validate the same model with full features and the results of recent studies.

Table 14 Validation methods for the proposed FS method of each primary study

FS validation by	*# of PS*	*Primary studies*
Multi-DS	20	PS09, PS12, PS21, PS25, PS28, PS33, PS38~PS42, PS46~PS48, PS50, PS52, PS54, PS55, PS60, PS63
Multi-FS	12	PS07, PS09, PS11, PS12, PS19, PS26, PS29, PS30, PS45, PS51, PS53, PS56, PS59
Multi-MLs	36	PS01~PS08, PS11~PS14, PS17, PS20, PS22~PS24, PS27~PS29, PS31~PS34, PS38, PS41, PS42, PS44, PS46, PS51, PS53~PS55, PS57~PS61
Multi-DLs	8	PS15, PS37, PS38, PS41, PS46, PS48, PS49, PS56,
Full features	22	PS05, PS06, PS08, PS10, PS17, PS22, PS26, PS28, PS32, PS33, PS36~PS38, PS43, PS49, PS50, PS53~PS55, PS57~PS59, PS61~PS63
Recent works	22	PS08, PS12, PS16, PS19, PS28, PS33, PS35~PS39, PS43, PS45, PS46, PS48~PS50, PS53, PS56, PS57, PS59~PS61, PS63

RQ5 What are the limitations, challenges and future directions of FS to the models in IoT security?

RQ5.1 What are the limitations in current researches?

The IoT data samples included in studies' FS techniques may influence the results of the studies. As we concluded from the answers to RQ3, most studies used public IoT dataset to validate their proposed FS methods and ML algorithms, while few studies used private data extracted by their experimental environment for specific attack detection. However, the samples varied among some studies even using the same dataset. For example, Motylinski et al. (2022), Moizuddin and Jose (2022) and Ozer et al. (2021) used 5% of the whole BoT-IoT dataset, in addition, only ten features of the original features (45) was used as the candidate features before implementing the proposed FS method. Similarly, Abdulkareem et al. (2022) and Leevy et al. (2022) used 5% instances of BoT-IoT, with 36 and 29 features, respectively as the sample data. In addition, the proposed model that uses low-frequency IoT datasets gathered in responses to RQ3 requires additional validation using popular datasets.

Moreover, data pre-processing with the domain knowledge of IoT was omitted by some studies, which may cause the performance results of the modes invalid. For example, Fatani et al. (2022) proposed meta-heuristic algorithms AQU searching for the optimal feature subsets, but there is no pre-processing explained in the study. Furthermore, Ozer et al. (2021) involved the irrelevant features to build anomaly detection systems. Abdulkareem et al. (2022) conducted dimensionality reduction but did not consider the imbalance class distribution of the BoT-IoT dataset. Illy et al. (2022) focused on attack and feature analysis and evaluation of manually selected features, however, solid domain knowledge is required to implement manually FS. Kumar et al. (2021) extensively used manual data pre-processing work which may be labour-consuming, and the number of features in the reduced set of features can be further optimised to increase overall accuracy and detection rate.

Various objectives of the classification model drive the implementation of the FS methods. Different objectives, such as the chosen performance metrics-oriented model, attacks to be detected and classified, an efficient or lightweight model focused with high accuracy, and so on, may directly influence the FS and ML algorithms used for the proposed classification model. For example, the binary classification result can be quite different from that of multi-classification in the same dataset (Fatani et al., 2022). Some studies conducted limited performance evaluation, Ahmed and Tjortjis (2022) evaluated the models with limited performance metrics, while Awad et al. (2022) and Saurabh et al. (2022) did not evaluate the effect of the proposed FS with that of original features. Some studies focus only on the specific attacks detection, Prasad and Chandra (2022) and Kumar et al. (2022a) focused on binary classification of DDoS and botnet attack among the datasets. Similarly, there is no one FS method or technique that fits all scenarios. Since there are various FS methods applied in primary studies, involving filter, wrapper, embedded, hybrid, and ensemble FS methods, each FS method has its strengths and weaknesses based on the objectives and scenarios.

RQ5.2 What are the major challenges of FS in the primary studies on the IoT security model?

The characteristics of IoT datasets, which are constantly changing, make implementing FS methods and techniques difficult. Large size and high dimensionality are the intrinsic aspects of IoT datasets. For example, BoT-IoT has the maximum of 72,000,000 instances, while the extracted features of N-BaIoT and AWID exceed 100, which can be a challenge for the FS method. Besides, the heterogeneity of IoT datasets can contain a mix of different types of data, such as numerical, categorical, and text data, which can make them challenging to process and analyse. Moreover, IoT datasets can be imbalanced, meaning that the distribution of the target variable may not be evenly distributed. This can pose a challenge for classification models, as they may not accurately reflect the minority class. Furthermore, IoT datasets can be noisy, with errors or missing data points, which can affect the accuracy of the classification models. Finally, since the dynamic characteristics of IoT datasets can change over time, with new data points involving new attack types or zero-day attacks being added or existing data points being updated, this can affect the performance of the classification models that had outstanding performance in previous datasets.

Another significant problem is that the optimised feature scheme lacks sufficient discriminative ability to identify all classes of assaults even with a single dataset. For example, Shafiq et al. (2021) proposed identified 5 from 45 original features by using hybrid FS, which contribute to an effective attack detection performance, however, the sensitivity of specific attack such as data theft attack only achieved 66.67%, compared with more than 99% of other type attacks such as DDoS attack. Moreover, the same FS approach may contribute to opposite output of classification for different datasets. For example, in Disha and Waheed (2022), the performance of output of UNSW-NB15 and TON-IoT are quite opposite after applying the same FS method, since the class distribution is quite different for this two datasets. Thus, the dataset and the objective of the classification model should be carefully considered before applying the proposed FS method.

Finally, the other challenge is that any FS may have its side effect. Any effective FS approach achieving high performance by using specific ML algorithm or DL algorithm, does not mean the FS scheme provide beneficial effect with other learning algorithms. For example, in Shafiq et al. (2021), the performance results of C4.5 DT and RF outperform the results of SVM and NB with the same FS technique. The result showed the proposed FS technique can cause quite different performance result with different ML algorithms. In addition, in Shafiq et al. (2021), the performance results of C4.5 DT and RF outperform the results of SVM and NB with the same FS technique. The result showed the proposed FS technique can cause quite different performance result with different ML algorithms. Similarly, with the same FS approach in Medjek et al. (2021), RF achieved the best performance compared with other classic ML algorithms involving DT, kNN, NB, also outperform the performance of DL algorithm MLP, which may be caused by the characteristics of the dataset. Similarly, in Disha and Waheed (2022), the proposed embedded weighted Gini-based FS showed positive effect on tree-based classifiers, while reduced the performance of neural-based algorithms in terms of accuracy and FAR.

RQ5.3 What are the future research directions of FS in terms of the classification performance of IoT security model?

Since IoT devices are increasingly vulnerable to security threats and attacks, making it vital to develop methods for detecting and classifying these attacks. Various studies applied various FS methods and ML or DL-based frameworks for attack classification in IoT security, which is still a hot area of research, thus, we investigated the future directions after this review study as following:

- *Diversity and representative of datasets* is vital for building generative models for IoT security. Because various zero-day attacks are becoming more common in IoT networks, a dataset that can represent real-world scenarios can be used as a benchmark for attack detection models. Motylinski et al. (2022), Abdulkareem et al. (2022) and Kumar et al. (2022b) suggested multiple public IoT datasets validation is necessary while retaining the distribution of the IoT data in real scenarios when implementing data pre-processing. Moreover, for the specific attacks such as botnet, MITM, and routing attacks, self-created dataset can be used (Prasad and Chandra, 2022; Malik et al., 2022; Medjek et al., 2021).
- *Integration with DL models:* The integration of FS algorithms with DL models is a promising direction, as it can provide a more effective way of selecting features for large and complex datasets (Ahmed and Tjortjis, 2022). DL algorithms to extract

additional features with more characteristics to target attack classes. For example, Rahman et al. (2021) used auto encoder to extract more characteristics of the original features prior to FS to improve classification performance. In addition, efficient FS to reduced feature sets can contribute DL model with larger architectures to improve the performance result with lower computational cost (Ozer et al., 2021). Lastly, Gad et al. (2022) and Gaber et al. (2022) argued using more DL methods with hyperparameters optimised to create more efficient models.

- *Semi-supervised and unsupervised FS:* There is a growing interest in developing semi-supervised and unsupervised FS methods, which can be used when labelled data is scarce or unavailable. Halim et al. (2021) suggested unsupervised learning algorithms such as clustering to make the machine self-learn new kinds of attacks. Guo (2021) suggested PCA as the dimensionality reduction technique to examine its performance in IoT IDSs. Moreover, since the existing IDSs have limitations in designing anomaly detection models for specific sets of traffic attributes, which makes it difficult to identify emerging threats in the IoT environment. To solve this problem, Hu et al. (2021) suggested an IDS based on multiple-kernel clustering (MKC) algorithms to improve clustering accuracy, reduce sensitivity to FS, and has better tolerance for poor-quality traffic sampled data.
- *Multi-objective optimisation:* Multi-objective optimisation is a growing area of research in FS, as it provides a way of balancing different objectives, such as accuracy, interpretability, and computational efficiency (Kareem et al., 2022). Optimised meta-heuristic algorithms such as adaptive PSO can be employed (Chohra et al., 2022). Kumar et al. (2022b) suggested highly efficient meta-heuristic methods considering limited energy resource. In addition, improving the effect of FS to predict malicious activities by adjusting the importance score for statistic-based techniques, such as PCC (Awad et al., 2022). Trade-off between the speed and detection rate can be a direction for FS in the future. For example, Shafiq et al. (2021) discussed and proposed an algorithm to evaluate and select many feature subsets considering the trade-off between complexity of the model and attack detection performance. Kareem et al. (2022) proposed hybrid meta-heuristic algorithms to search for the most optimal feature subsets with reduced searching time, while multi-objective optimisation can further be used for hyperparameters of learning algorithms.
- *Explainability and interpretability:* Explain ability and interpretability are becoming increasingly important in FS, as it is important to understand why a model is making certain predictions, and to ensure that the results are not biased or influenced by irrelevant factors. For example, Guerra-Manzanares et al. (2019b) proposed a filter method using Fisher's score and local interpretable model-agnostic explanation (LIME) at FS and post-hoc interpretation phases, respectively. Moreover, Bhandari et al. (2020) conducted a tree-based model with a focus on feature analysis, knowledge of these important features can be used to remove irrelevant features and also to better understand how the models work and what data should be collected in the future. Furthermore, in Shafiq et al. (2021) and Kumar et al. (2021), it is promising to observe that the direction of class-wise FS, where different results are obtained for different classes using the same FS and ML techniques, might increase the performance of a particular attack type.

- *Integration with domain knowledge:* The integration of domain knowledge with FS is a promising direction, as it can provide a more effective way of selecting features that are relevant to a specific application domain. In order to handle the majority of IoT data, which involve missing values, categorical features, irrelevant features, and distribution imbalance, suitable pre-processing with domain expertise is required. Siddiqi and Pak (2021) proposed a statistic way to identify the most suitable normalisation method for IoT datasets and suggest a direction of hybrid method for normalisation to improve ML-based IDS. In addition, data pre-processing of handling class imbalance should keep reflecting the class distribution of real scenarios (Motylinski et al., 2022). Moreover, mitigation of the correctly identified attacks implemented as a module in security framework is a promising direction for historic security model in IoT networks (Prasad and Chandra, 2022; Khater et al., 2021).
- *IoT characteristics and infrastructure:* Lightweight (energy-efficient) with considerable performance metrics in intrusion detection systems is paramount instead of inefficient and heavyweight intrusion detection systems. Ozer et al. (2021) intensively reduced the original 12 features optimised by original author, to only two features by using feature pair technique. The model with minimal selected features toward specific attack class can contribute to highly efficient or real-time attack detection system. Moreover, reducing FPR is vital to IoT security (Carter et al., 2022), security teams are frequently distracted by false identified attacks because they still require a lot of labour to mitigate in additional IPSs. Moreover, industrial scale with large attack span should be evaluated for the models created from the public datasets (Saurabh et al., 2022; Illy et al., 2022). Finally, online and incremental FS methods are becoming increasingly important, as they can handle large-scale and streaming data in real-time, making them well suited for applications in areas such as sensor networks, social media, and the IoT. Kumar et al. (2021) and Ravi et al. (2022) advocate using the optimised models to deploy online for real-time anomaly detection in realistic IoT circumstances.

In addition to the future directions suggested by the primary studies, many more potential research directions will likely emerge in the near future, including the following:

- *Energy-efficient FS for IoT security:* As IoT devices become more pervasive, there is a growing need for energy-efficient approaches to FS that can reduce the computational and energy requirements of security tasks. One potential research direction is to investigate energy-efficient FS methods that can be applied to IoT security tasks, such as anomaly detection and intrusion detection. For example, Hu et al. (2021) proposed deep-green, a dispersed energy-efficient computing paradigm for the industrial internet of things (IIoT) that merges data transmission and processing. The proposed method optimises computing and network resources, and reduces computing load and communication overhead on the cloud-side server. This could involve exploring techniques such as sparse FS algorithms, which prioritise the most important features while minimising computational complexity, and low-power ML algorithms that can run efficiently on resource-constrained devices. Another potential approach is to consider hardware-accelerated FS, where specialised hardware can be used to accelerate FS tasks, potentially reducing energy consumption and improving performance. By developing energy-efficient FS methods for IoT security, researchers can help to improve the scalability and sustainability of security applications in the IoT, while reducing the overall energy consumption of these systems.

- *Multiple-layer FS for IoT security:* IoT environments consist of multiple layers of infrastructure, including edge IoT devices, gateways, cloud servers, and network communication protocols. For example, Khedr et al. (2023) proposed an SDN-based four-module framework for detecting and mitigating DDoS attacks in IoT networks. FS methods can be applied to each layer of this infrastructure to improve the overall security of the IoT system. One potential research direction is to investigate the use of FS methods at multiple layers of the IoT infrastructure, and to explore how these methods can be combined to create effective ML-based security systems. This could involve investigating how FS can be applied to edge devices to reduce the amount of data that needs to be transmitted to the cloud for processing, and how FS can be applied to communication protocols to identify and filter out malicious traffic. Additionally, research could focus on developing methods for combining FS results across different layers of the infrastructure to create a more comprehensive security system. By exploring the application of FS at multiple layers of the IoT infrastructure, researchers can help to improve the effectiveness and efficiency of security systems in IoT environments.
- *Attacks-oriented FS for IoT security:* IoT security systems must be able to detect and classify a wide range of attacks, including malware, DDoS attacks, insider attacks, and many others. FS methods can be applied to the data collected from IoT devices to identify the most important features for each type of attack, improving the accuracy and efficiency of detection and classification. One potential research direction is to investigate the use of FS methods for detecting and classifying different types of attacks in IoT environments. This could involve comparing the effectiveness of different FS methods for each type of attack, and developing new methods that are specifically designed for IoT security. Researchers could also explore how FS can be used in conjunction with other ML techniques, such as anomaly detection and DL, to create more effective and robust security systems. By focusing on the application of FS on various types of attacks detection and classification, researchers can help to improve the accuracy and reliability of security systems in IoT environments.
- *Privacy-preserving FS with federated learning for IoT security:* As the number of interconnected IoT devices continues to grow, federated learning is becoming an increasingly popular approach for building ML models that can detect security threats across multiple devices while preserving data privacy. However, selecting the most relevant features from distributed data sources in a federated learning setting presents a unique set of challenges, such as maintaining model accuracy while minimising communication overhead and preserving the privacy of sensitive data. One potential research direction is to explore the effectiveness of different FS methods in federated learning settings for IoT security, and to develop new approaches that are specifically tailored to the challenges of distributed data and privacy-preserving ML. This could involve investigating techniques such as differential privacy, federated FS algorithms, and context-aware FS methods. By addressing these challenges, researchers can help to ensure that federated learning

remains a viable approach for improving IoT security while preserving the privacy of user data.

- *Adversarial attacks and defenses for IoT security:* As ML-based security systems become more widespread in IoT environments, the risk of adversarial attacks that attempt to evade or disrupt these systems also increases. One potential research direction is to explore the vulnerabilities of FS methods to adversarial attacks and to develop new methods for defending against these attacks. This could involve investigating techniques such as adversarial FS, where attackers attempt to influence the FS process to compromise the security of the system, and adversarial training, where the system is trained on adversarial examples to improve its robustness. Additionally, new FS methods that are specifically designed to be resistant to adversarial attacks could be developed. By addressing the vulnerabilities of FS methods to adversarial attacks, researchers can help to improve the overall security and reliability of ML-based security systems in IoT environments.
- *FS applied with blockchain for IoT security:* Blockchain is a distributed and decentralised ledger technology that provides a tamper-evident and transparent mechanism for recording and verifying transactions. When combined with FS methods, blockchain can enhance the security of IoT systems by providing a secure and immutable record of the selected features used in ML models. For example, Liu et al. (2023) proposed a semi-centralised trust management system architecture based on blockchain to mitigate the impact of malicious devices in IoT data exchange. One potential research direction is to investigate the use of blockchain-based FS methods for IoT security. This could involve exploring the design of blockchain-based FS algorithms that can be integrated with ML models for detecting and mitigating attacks. Another direction is to investigate the privacy implications of using blockchain-based FS methods, as sensitive data could be stored on the blockchain. Additionally, researchers could investigate how blockchain-based FS methods can be used to enhance the security of IoT devices and networks, including edge devices and gateways. By focusing on the application of FS with blockchain techniques, researchers can help to enhance the security and privacy of IoT systems.

4 Limitation of the study

This study conducted a SLR about the application of FS methods in ML or DL-based attack classification models for IoT security based on 63 primary studies between 2018 until 2022. The result of this SLR may have been affected by the coverage of search strategy, the researchers' bias, and inaccuracy of data extraction. These have been discussed and addressed below.

The coverage of search strategy in this study was determined by limited set of keywords that targeted an overview of FS methods applied using ML or DL algorithms for IoT security from the selected academic databases. Thus, there may be the possibility where related studies that using various keywords or the studies from other databases, were not included in this search result.

Another threat to validity is related to the possibility of bias of the researchers. All the primary studies used the at least one dataset which was generated in specific IoT environment, as a result, the studies that also employed FS and ML or DL-based attack classification were filtered and not entered into following evaluation of quality score criteria. Besides, the score criteria may cause the bias of the quality of the primary studies, because the quality score is designed based on the expected findings on FS from the title, abstract, keyword, and full text, but not only general quality of academic study.

Finally, there may be the possibility of inaccuracy of data item extraction on taxonomy of FS in this study, such as the category of the purpose of FS, FS methods, FS validation methods, and performance metrics. However, the data items were extracted based on comprehensive understanding of the studies, and the accuracy of this study can be guaranteed by providing detailed searching coverage, data items, and criteria for research question findings.

5 Conclusions

FS is crucial for developing efficient and accurate ML and DL-based models that detect and prevent IoT security threats. As IoT networks become more heterogeneous and high-dimensional data becomes more available, FS becomes increasingly important for improving model performance by reducing complexity. However, a comprehensive review of current FS research and applications for IoT security has been lacking. The core contribution of this work is conducting the first SLR of FS methods for ML in IoT security, considering the uniqueness of IoT systems. This SLR paper focuses on the contribution of FS to improving the performance of ML and DL-based classification models for IoT security. The study collected 1,272 studies and provided a quality scoring scheme for 63 primary studies published from 2018 to 2022 from six research databases: Web of Science, IEEE Xplore, Scopus, ScienceDirect, ACM, SpringerLink and Wiley Online Library. The study then presented the current situation of FS methods, an applied FS trend, benchmark IoT datasets, FS validation methods, and metrics of FS for IoT security. Finally, the paper investigated the limitations, challenges, and future directions for FS. This study contributes a systematic reference for incorporating effective FS and ML methods to build high-performance IoT security models and aims to help researchers understand the recent progress and provide a comprehensive roadmap for FS in IoT security.

References

Abdulkareem, S.A., Foh, C.H., Carrez, F. and Moessner, K. (2022) ‘FI-PCA for IoT network intrusion detection’, in *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, pp.1–6 [online] https://doi.org/10.1109/ISNCC55209.2022.9851723.

Ahmad, R. and Alsmadi, I. (2021) ‘Machine learning approaches to IoT security: a systematic literature review’, *Internet of Things*, June, Vol. 14, p.100365 [online] https://doi.org/10.1016/j.iot.2021.100365.

Ahmed, A. and Tjortjis, C. (2022) ‘Machine learning based IoT-BotNet attack detection using real-time heterogeneous data’, in *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp.1–6 [online] https://doi.org/10.1109/ICECET55527.2022.9872817.

Ahmetoglu, H. and Das, R. (2022) 'A comprehensive review on detection of cyber-attacks: data sets, methods, challenges, and future research directions', *Internet of Things* [online] https://doi.org/10.1016/j.iot.2022.100615.

Al Shorman, A., Faris, H. and Aljarah, I. (2020) 'Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for IoT botnet detection', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 7, pp.2809–2825 [online] https://doi.org/10.1007/s12652-019-01387-y.

Alamiedy, T.A., Anbar, M.F.R., Belaton, B., Kabla, A.H. and Khudayer, B.H. (2021) 'Ensemble feature selection approach for detecting denial of service attacks in RPL networks', in Anbar, M., Abdullah, N. and Manickam, S. (Eds.): *Communications in Computer and Information Science 1487 CCIS*, pp.340–360, Springer Science and Business Media Deutschland GmbH, ISBN: 9789811680588, https://doi.org/10.1007/978-981-16-8059-5_21.

Alanazi, M. and Aljuhani, A. (2022) 'Anomaly detection for internet of things cyberattacks', *CMC – Computers Materials & Continua* [online] https://doi.org/10.32604/cmc.2022.024496.

Alazab, M. (2022) 'A discrete time-varying Greywolf IoT Botnet detection system', *Computer Communications*, Vol. 192, pp.405–16, https://doi.org/10.1016/j.comcom.2022.06.016.

Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I. and Guizani, M. (2020) 'A survey of machine and deep learning methods for internet of things (IoT) security', *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 3, pp.1646–1685 [online] https://doi.org/10.1109/COMST.2020.2988293.

Alqahtani, M., Mathkour, H. and Ismail, M.M.B. (2020) 'IoT Botnet attack detection based on optimized extreme gradient boosting and feature selection', *Sensors*, Vol. 20, No. 21, p.6336, https://doi.org/10.3390/s20216336.

Aminanto, M.E., Choi, R., Tanuwidjaja, H.C., Yoo, P.D. and Kim, K. (2018) 'Deep abstraction and weighted feature selection for wi-fi impersonation detection', in *IEEE Transactions on Information Forensics and Security*, March, Vol. 13, No. 3, pp.621–636, doi: 10.1109/TIFS.2017.2762828.

Asadi, M., Jamali, M.A.J., Parsa, S. and Majidnezhad, V. (2020) 'Detecting Botnet by using particle swarm optimization algorithm based on voting system', *Future Generation Computer Systems*, June, Vol. 107, pp.95–111, https://doi.org/10.1016/j.future.2020.01.055.

Ashton, K. (2009) 'That 'internet of things' thing', *RFID Journal*, Vol. 22, No. 7, pp.97–114.

Awad, M., Fraihat, S., Salameh, K. and Al Redhaei, A. (2022) 'Examining the suitability of netflow features in detecting IoT network intrusions', *Sensors* [online] https://doi.org/10.3390/s22166164.

Bahşi, H., Nõmm, S. and La Torre, F.B. (2018) 'Dimensionality reduction for machine learning based IoT Botnet detection', *2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, Singapore, pp.1857–1862, doi: 10.1109/ICARCV.2018.8581205.

Baig, Z.A., Sanguanpong, S., Firdous, S.N., Vo, V.N., Nguyen, T.G. and So-In, C. (2020) 'Averaged dependence estimators for DoS attack detection in IoT networks', *Future Generation Computer Systems*, Vol. 102, pp.198–209, https://doi.org/10.1016/j.future.2019.08.007.

Bhandari, S., Kukreja, A.K., Lazar, A., Sim, A. and Wu, K. (2020) 'Feature selection improves tree-based classification for wireless intrusion detection', in *SNTA 2020 – Proceedings of the 3rd International Workshop on Systems and Network Telemetry and Analytics*, Association for Computing Machinery, Inc., pp.19–26 [online] https://doi.org/10.1145/3391812.3396274.

Bojarajulu, B., Tanwar, S. and Rana, A. (2021) 'A synoptic review on feature selection and machine learning models used for detecting cyber attacks in IoT', in *2021 6th International Conference on Computing, Communication and Security (ICCCS)*, pp.1–7 [online] https://doi.org/10.1109/ICCCS51487.2021.9776344.

Bojarajulu, B., Tanwar, S. and Singh, T.P. (2022) 'Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model', *Computers & Security*, p.103064, https://doi.org/10.1016/j.cose.2022.103064.

Boopathi, M. (2022) 'Henry MaxNet: Tversky index based feature selection and competitive swarm Henry gas solubility optimization integrated deep maxout network for intrusion detection in IoT', *International Journal of Intelligent Robotics and Applications*, Vol. 6, No. 2, pp.365–383 [online] https://doi.org/10.1007/s41315-022-00234-2.

Cao, B., Li, C., Sun, J. and Song, Y. (2022) 'IoT intrusion detection technology based on deep learning', in *2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA)*, pp.284–289 [online] https://doi.org/10.1109/CVIDLICCEA56201.2022.9825291.

Carter, J., Mancoridis, S. and Galinkin, E. (2022) 'Fast, lightweight IoT anomaly detection using feature pruning and PCA', in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, SAC '22*, Association for Computing Machinery, New York, NY, USA, pp.133–138 [online] https://doi.org/10.1145/3477314.3508377.

Chohra, A., Shirani, P., Karbab, E.B. and Debbabi, M. (2022) 'CHAMELEON: optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection', *Computers & Security* [online] https://doi.org/10.1016/j.cose.2022.102684.

Davahli, A., Shamsi, M. and Abaei, G. (2020) 'Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 11, pp.5581–5609, https://doi.org/10.1007/s12652-020-01919-x.

Disha, R.A. and Waheed, S. (2022) 'Performance analysis of machine learning models for intrusion detection system using Gini impurity-based weighted random forest (GIWRF) feature selection technique', *Cybersecurity*, Vol. 5, No. 1 [online] https://doi.org/10.1186/s42400-021-00103-8.

Doshi, R., Apthorpe, N. and Feamster, N. (2018) 'Machine learning DDoS detection for consumer internet of things devices', *2018 IEEE Symposium on Security and Privacy Workshops (SPW 2018)* [online] https://doi.org/10.1109/SPW.2018.00013.

Fatani, A., Dahou, A., Al-Qaness, M.A.A., Lu, S. and Elaziz, M.A. (2022) 'Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system', *Sensors*, Vol. 22, No. 1 [online] https://doi.org/10.3390/s22010140.

Fatani, A., Elaziz, M.A., Dahou, A., Al-Qaness, M.A.A. and Lu, S. (2021) 'IoT intrusion detection system using deep learning and enhanced transient search optimization', *IEEE Access*, https://doi.org/10.1109/ACCESS.2021.3109081.

Gaber, T., El-Ghamry, A. and Hassanien, A.E. (2022) 'Injection attack detection using machine learning for smart IoT applications', *Physical Communication* [online] https://doi.org/10.1016/j.phycom.2022.101685.

Gad, A.R., Haggag, M., Nashat, A.A. and Barakat, T.M. (2022) 'A distributed intrusion detection system using machine learning for IoT based on ToN-IoT dataset', *International Journal of Advanced Computer Science and Applications*, Vol. 13, No. 6, pp.548–63, https://doi.org/10.14569/IJACSA.2022.0130667.

Gad, A.R., Nashat, A.A. and Barkat, T.M. (2021) 'Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset', *IEEE Access*, Vol. 9, pp.142206–17, https://doi.org/10.1109/ACCESS.2021.3120626.

Gandhi, R. and Li, Y. (2021) 'Comparing machine learning and deep learning for IoT botnet detection', *2021 IEEE International Conference on Smart Computing (SMARTCOMP 2021)* [online] https://doi.org/10.1109/SMARTCOMP52413.2021.00053.

Guerra-Manzanares, A., Bahsi, H. and Nõmm, S. (2019a) 'Hybrid feature selection models for machine learning based botnet detection in IoT networks', in *2019 International Conference on Cyberworlds (CW)*, pp.324–327 [online] https://doi.org/10.1109/CW.2019.00059.

Guerra-Manzanares, A., Nõmm, S. and Bahsi, H. (2019b) 'Towards the integration of a post-hoc interpretation step into the machine learning workflow for IoT botnet detection', in *2019 18th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp.1162–1169 [online] https://doi.org/10.1109/ICMLA.2019.00193.

Guo, G. (2021) 'A machine learning framework for intrusion detection system in IoT networks using an ensemble feature selection method', in Chakrabarti S. P.R. (Ed.): *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2021*, Institute of Electrical and Electronics Engineers Inc., pp.593–599 [online] https://doi.org/10.1109/IEMCON53756.2021.9623082.

Halim, Z., Yousaf, M.N., Waqas, M., Sulaiman, M., Abbas, G., Hussain, M., Ahmad, I. and Hanif, M. (2021) 'An effective genetic algorithm-based feature selection method for intrusion detection systems', *Computers & Security*, November, Vol. 110, p.102448 [online] https://doi.org/10.1016/j.cose.2021.102448.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019) 'A survey on IoT security: application areas, security threats, and solution architectures', *IEEE Access*, Vol. 7, pp.82721–82743 [online] https://doi.org/10.1109/ACCESS.2019.2924045.

Hu, N., Tian, Z., Lu, H., Du, X. and Guizani, M. (2021) 'A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks', *International Journal of Machine Learning and Cybernetics*, Vol. 12, No. 11, pp.3129–44, https://doi.org/10.1007/s13042-020-01253-w.

Hussain, F., Hussain, R., Hassan, S.A. and Hossain, E. (2020) 'Machine learning in IoT security: current solutions and future challenges', *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 3, pp.1686–1721 [online] https://doi.org/10.1109/COMST.2020.2986444.

Illy, P., Kaddoum, G., Kaur, K. and Garg, S. (2022) 'ML-based IDPS enhancement with complementary features for home IoT networks', *IEEE Transactions on Network and Service Management* [online] https://doi.org/10.1109/TNSM.2022.3141942.

Ismail, S., Khoei, T.T., Marsh, R. and Kaabouch, N. (2021) 'A comparative study of machine learning models for cyber-attacks detection in wireless sensor networks', in Paul, R. (Ed.): *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* [online] https://doi.org/10.1109/UEMCON53757.2021.9666581.

Jayalaxmi, P.L.S., Saha, R., Kumar, G. and Kim, T-H. (2022) 'Machine and deep learning amalgamation for feature extraction in industrial internet-of-things', *Computers & Electrical Engineering*, Vol. 97, p.107610 [online] https://doi.org/10.1016/j.compeleceng.2021.107610.

Kalakoti, R., Nomm, S. and Bahsi, H. (2022) 'In-depth feature selection for the statistical machine learning-based botnet detection in IoT networks', *IEEE Access*, Vol. 10, pp.94518–94535 [online] https://doi.org/10.1109/ACCESS.2022.3204001.

Kareem, S.S., Mostafa, R.R., Hashim, F.A. and El-Bakry, H.M. (2022) 'An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection', *Sensors*, Vol. 22, No. 4, p.1396 [online] https://doi.org/10.3390/s22041396.

Keele, S. et al. (2007) *Guidelines for Performing Systematic Literature Reviews in Software Engineering*, Technical report, ver. 2.3, EBSE technical report, EBSE.

Khater, B.S., Abdul Wahab, A.W., Idris, M.Y.I., Hussain, M.A., Ibrahim, A.A., Amin, M.A. and Shehadeh, H.A. (2021) 'Classifier performance evaluation for lightweight IDS using fog computing in IoT security', *Electronics* [online] https://doi.org/10.3390/electronics10141633.

Khedr, W.I., Gouda, A.E. and Mohamed, E.R. (2023) 'FMDADM: a multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks', *IEEE Access*, Vol. 11, pp.28934–54, https://doi.org/10.1109/ACCESS.2023.3260256.

Kolias, C., Kambourakis, G., Stavrou, A. and Gritzalis, S. (2016) 'Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset', *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 1, pp.184–208 [online] https://doi.org/10.1109/COMST.2015.2402161.

Koroniotis, N., Moustafa, N. and Slay, J. (2022) ‘A new intelligent satellite deep learning network forensic framework for smart satellite networks’, *Computers and Electrical Engineering*, Vol. 99, p.107745 [online] https://doi.org/10.1016/j.compeleceng.2022.107745.

Koroniotis, N., Moustafa, N., Sitnikova, E. and Turnbull, B. (2019) ‘Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset’, *Future Generation Computer Systems*, November, Vol. 100, pp.779–796 [online] https://doi.org/10.1016/j.future.2019.05.041.

Kouicem, D.E., Bouabdallah, A. and Lakhlef, H. (2018) ‘Internet of things security: a top-down survey’, *Computer Networks*, August, Vol. 141, pp.199–221 [online] https://doi.org/10.1016/j.comnet.2018.03.012.

Kumar, A., Shridhar, M., Swaminathan, S. and Lim, T.J. (2022a) ‘Machine learning-based early detection of IoT botnets using network-edge traffic’, *Computers & Security*, Vol. 117, p.102693 [online] https://doi.org/10.1016/j.cose.2022.102693.

Kumar, R., Malik, A. and Ranga, V. (2022b) ‘An intellectual intrusion detection system using hybrid hunger games search and remora optimization algorithm for IoT wireless networks’, *Knowledge-Based Systems*, Vol. 256, p.109762 [online] https://doi.org/10.1016/j.knosys.2022.109762.

Kumar, P., Gupta, G.P. and Tripathi, R. (2021) ‘Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks’, *Arabian Journal for Science and Engineering*, Vol. 46, No. 4, pp.3749–3778 [online] https://doi.org/10.1007/s13369-020-05181-3.

Leevy, J.L., Hancock, J., Khoshgoftaar, T.M. and Peterson, J.M. (2022) ‘IoT information theft prediction using ensemble feature selection’, *Journal of Big Data*, Vol. 9, No. 1 [online] https://doi.org/10.1186/s40537-021-00558-z.

Li, T., Hong, Z. and Yu, L. (2020) ‘Machine learning-based intrusion detection for IoT devices in smart home’, *2020 IEEE 16TH International Conference on Control & Automation (ICCA)*.

Liu, Y., Zhang, C., Yan, Y., Zhou, X., Tian, Z. and Zhang, J. (2023) ‘A semi-centralized trust management model based on blockchain for data exchange in IoT system’, *IEEE Transactions on Services Computing*, Vol. 16, No. 2, pp.858–871 [online] https://doi.org/10.1109/TSC.2022.3181668.

Luo, C., Tan, Z., Min, G., Gan, J., Shi, W. and Tian, Z. (2021) ‘A novel web attack detection system for internet of things via ensemble classification’, *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 8, pp.5810–5818 [online] https://doi.org/10.1109/TII.2020.3038761.

Mafarja, M., Heidari, A.A., Habib, M., Faris, H., Thaher, T. and Aljarah, I. (2020) ‘Augmented whale feature selection for IoT attacks: structure, analysis and applications’, *Future Generation Computer Systems*, Vol. 112, pp.18–40, https://doi.org/10.1016/j.future.2020.05.020.

Malik, K., Rehman, F., Maqsood, T., Mustafa, S., Khalid, O. and Akhunzada, A. (2022) ‘Lightweight internet of things botnet detection using one-class classification’, *Sensors* [online] https://doi.org/10.3390/s22103646.

Masoudi-Sobhanzadeh, Y. and Emami-Moghaddam, S. (2022) ‘A real-time IoT-based botnet detection method using a novel two-step feature selection technique and the support vector machine classifier’, *Computer Networks*, Vol. 217 [online] https://doi.org/10.1016/j.comnet.2022.109365.

Medjek, F., Tandjaoui, D., Djedjig, N. and Romdhani, I. (2021) ‘Fault-tolerant AI-driven intrusion detection system for the internet of things’, *International Journal of Critical Infrastructure Protection* [online] https://doi.org/10.1016/j.ijcip.2021.100436.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A. and Elovici, Y. (2018) ‘N-BaIoT: network-based detection of IoT botnet attacks using deep autoencoders’, *IEEE Pervasive Computing*, Vol. 17, No. 3, pp.12–22 [online] https://doi.org/10.1109/MPRV.2018.03367731.

Moizuddin, M.D. and Jose, M.V. (2022) 'A bio-inspired hybrid deep learning model for network intrusion detection', *Knowledge-Based Systems* [online] https://doi.org/10.1016/j.knosys.2021.107894.

Motylinski, M., MacDermott, A., Iqbal, F. and Shah, B. (2022) 'A GPU-based machine learning approach for detection of botnet attacks', *Computers & Security* [online] https://doi.org/10.1016/j.cose.2022.102918.

Moustafa, N. (2021) 'A new distributed architecture for evaluating AI-based security systems at the edge: network TON_IoT datasets', *Sustainable Cities and Society*, September, Vol. 72, p.102994 [online] https://doi.org/10.1016/j.scs.2021.102994.

Nagaraja, A. and Kumar, T.S. (2018) 'An extensive survey on intrusion detection – past, present, future', in *Proceedings of the Fourth International Conference on Engineering & MIS 2018. ICEMIS '18*, Association for Computing Machinery, New York, NY, USA [online] https://doi.org/10.1145/3234698.3234743.

Nõmm, S. and Bahşi, H. (2018) 'Unsupervised anomaly based Botnet Detection in IoT Networks', *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Orlando, FL, USA, pp.1048–1053, doi: 10.1109/ICMLA.2018.00171.

Ozer, E., Iskefiyeli, M. and Azimjonov, J. (2021) 'Toward lightweight intrusion detection systems using the optimal and efficient feature pairs of the Bot-IoT 2018 dataset', *International Journal of Distributed Sensor Networks* [online] https://doi.org/10.1177/15501477211052202.

Padmashree, A. and Krishnamoorthi, M. (2022) 'Decision tree with pearson correlation-based recursive feature elimination model for attack detection in IoT environment', *Information Technology and Control*, Vol. 51, No. 4, pp.771–785 [online] https://doi.org/10.5755/j01.itc.51.4.31818.

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L. et al. (2021) 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *BMJ*, Vol. 372 [online] https://doi.org/10.1136/bmj.n71.

Parker, L.R., Yoo, P.D., Asyhari, T.A., Chermak, L., Jhi, Y. and Taha, K. (2019) 'DEMISe: interpretable deep extraction and mutual information selection techniques for IoT intrusion detection', *14th International Conference on Availability, Reliability and Security (ARES 2019)* [online] https://doi.org/10.1145/3339252.3340497.

Prasad, A. and Chandra, S. (2022) 'VMFCVD: an optimized framework to combat volumetric DDoS attacks using machine learning', *Arabian Journal for Science and Engineering* [online] https://doi.org/10.1007/s13369-021-06484-9.

Rahman, M.A., Asyhari, A.T., Wen, O.W., Ajra, H., Ahmed, Y. and Anwar, F. (2021) 'Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection', *Multimedia Tools and Applications*, Vol. 80, No. 20, pp.31381–31399 [online] https://doi.org/10.1007/s11042-021-10567-y.

Ravi, V., Chaganti, R. and Alazab, M. (2022) 'Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system', *Computers and Electrical Engineering*, Vol. 102, p.108156 [online] https://doi.org/10.1016/j.compeleceng.2022.108156.

Samdekar, R., Ghosh, S.M. and Srinivas, K. (2021) 'Efficiency enhancement of intrusion detection in IoT based on machine learning through bioinspire', in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, Tirunelveli, India, pp.383–387 [online] https://doi.org/10.1109/ICICV50876.2021.9388392.

Saurabh, K., Kumar, T., Singh, U., Vyas, O.P. and Khondoker, R. (2022) 'NFDLM: a lightweight network flow based deep learning model for DDoS attack detection in IoT domains', in *2022 IEEE World AI IoT Congress (AIIoT)*, pp.736–742 [online] https://doi.org/10.1109/AIIoT54504.2022.9817297.

Shafiq, M., Gu, Z., Nazir, S. and Yadav, R. (2022) 'Analyzing IoT attack feature association with threat actors', *Wireless Communications & Mobile Computing*, https://doi.org/10.1155/2022/7143054.

Shafiq, M., Tian, Z., Bashir, A.K., Du, X. and Guizani, M. (2020) 'IoT malicious traffic identification using wrapper-based feature selection mechanisms', *Computers and Security*, Vol. 94, https://doi.org/10.1016/j.cose.2020.101863.

Shafiq, M., Tian, Z., Bashir, A.K., Du, X. and Guizani, M. (2021) 'CorrAUC: a malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques', *IEEE Internet of Things Journal*, Vol. 8, No. 5, pp.3242–3254 [online] https://doi.org/10.1109/JIOT.2020.3002255.

Shi, L., Wu, L. and Guan, Z. (2021) 'Three-layer hybrid intrusion detection model for smart home malicious attacks', *Computers & Electrical Engineering*, Vol. 96, p.107536 [online] https://doi.org/10.1016/j.compeleceng.2021.107536.

Siddiqi, M.A. and Pak, W. (2021) 'An agile approach to identify single and hybrid normalization for enhancing machine learning-based network intrusion detection', *IEEE Access* [online] https://doi.org/10.1109/ACCESS.2021.3118361.

Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R. and Sakurai, K. (2020a) 'Machine learning-based IoT-Botnet attack detection with sequential architecture dagger', *Sensors* [online] https://doi.org/10.3390/s20164372.

Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R. and Sakurai, K. (2020b) 'Implementing lightweight IoT-IDS on raspberry pi using correlation-based feature selection and its performance evaluation', in Xhafa, F., Takizawa, M., Enokido, T. and Barolli, L. (Eds.): *Advances in Intelligent Systems and Computing*, Vol. 926, pp.458–69, https://doi.org/10.1007/978-3-030-15032-7_39.

Statista (2022) *Statista, 'Cybersecurity – Market Data Analysis & Forecasts'* [online] https://www.statista.com/study/124902/cybersecurity-report/ (accessed 20 December 2022).

Suresh, B., Venkatachalam, M. and Saroja, M. (2019) 'Towards improved random forest based feature selection for intrusion detection in smart IOT environment', *International Journal of Innovative Technology and Exploring Engineering*, Vol. 8, No. 11, pp.749–757 [online] https://doi.org/10.35940/ijitee.F1446.0881119.

Verma, J., Bhandari, A. and Singh, G. (2022) 'Feature selection algorithm characterization for NIDS using machine and deep learning', in *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp.1–7 [online] https://doi.org/10.1109/IEMTRONICS55184.2022.9795709.

Vigoya, L., Fernandez, D., Carneiro, V. and Novoa, F.J. (2021) 'IoT dataset validation using machine learning techniques for traffic anomaly detection', *Electronics* [online] https://doi.org/10.3390/electronics10222857.

Xu, L.D., He, W. and Li, S. (2014) 'Internet of things in industries: a survey', *IEEE Transactions on Industrial Informatics*, Vol. 10, No. 4, pp.2233–2243 [online] https://doi.org/10.1109/TII.2014.2300753.

Zhou, L., Zhu, Y., Zong, T. and Xiang, Y. (2022) 'A feature selection-based method for DDoS attack flow classification', *Future Generation Computer Systems*, Vol. 132, pp.67–79 [online] https://doi.org/10.1016/j.future.2022.02.006.

Appendix 1

Primary studies from 2018 to 2020

Index	*Title*	*Ref.*	*Publisher*	*Type*	*Quality assessment scoring*					
					QA1	*QA2*	*QA3*	*QA4*	*QA5*	*Score*
PS01	Dimensionality reduction for machine learning based IoT botnet detection	Bahsi et al. (2018)	Scopus	Conference	1	1	0.5	0.5	0.5	3.5
PS02	Machine learning DDoS detection for consumer internet of things devices	Doshi et al. (2018)	IEEE	Conference	0.5	1	0.5	0.5	1	3
PS03	Deep abstraction and weighted feature selection for Wi-Fi impersonation detection	Aminanto et al. (2018)	IEEE	Journal	1	1	1	1	0.5	4.5
PS04	Unsupervised anomaly based botnet detection in IoT networks	Nomm and Bahsi (2018)	IEEE	Conference	1	1	0.5	0.5	0.5	3.5
PS05	DEMISe: interpretable deep extraction and mutual information selection techniques for IoT intrusion detection	Parker et al. (2019)	Scopus	Conference	1	1	1	0.5	0.5	4
PS06	Hybrid feature selection models for machine learning based botnet detection in IoT networks	Guerra-Manzanares et al. (2019a)	IEEE	Conference	1	1	1	0.5	0.5	4
PS07	Towards the integration of a post-hoc interpretation step into the machine learning workflow for IoT botnet detection	Guerra-Manzanares et al. (2019b)	IEEE	Conference	1	1	1	0.5	0.5	4
PS08	IoT botnet attack detection based on optimized extreme gradient boosting and feature selection	Alqahtani et al. (2020)	Scopus	Journal	1	1	1	0.5	0.5	4
PS09	Averaged dependence estimators for DoS attack detection in IoT networks	Baig et al. (2020)	ScienceDirect	Journal	0.5	1	0.5	0.5	0.5	3
PS10	Feature selection improves tree-based classification for wireless intrusion detection	Bhandari et al. (2020)	Scopus	Conference	1	1	1	0.5	0.5	4
PS11	Machine learning-based intrusion detection for IoT devices in smart home	Li et al. (2020)	IEEE	Conference	1	0.5	1	0.5	0.5	3.5
PS12	Augmented whale feature selection for IoT attacks: structure, analysis and applications	Mafarja et al. (2020)	ScienceDirect	Journal	1	1	0.5	0.5	0.5	3.5
PS13	IoT malicious traffic identification using wrapper-based feature selection mechanisms	Shafiq et al. (2020)	ScienceDirect	Journal	1	1	0.5	0.5	0.5	3.5
PS14	Implementing lightweight IoT-IDS on Raspberry Pi using correlation-based feature selection and its performance evaluation	Soe et al. (2020)	Springer	Journal	1	1	0.5	1	0.5	4
PS15	Detecting botnet by using particle swarm optimization algorithm based on voting system	Asadi et al. (2020)	ScienceDirect	Journal	1	1	1	1	0.5	4.5
PS16	Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for IoT botnet detection	Al Shorman et al. (2020)	Springer	Journal	1	1	0.5	0.5	0.5	3.5
PS17	Machine learning-based IoT-botnet attack detection with sequential architecture dagger	Soe et al. (2020)	Scopus	Journal	1	1	0.5	1	0.5	4
PS18	Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks	Davahli et al. (2020)	Springer	Journal	1	1	0.5	1	0.5	4

Appendix 2

Primary studies in 2021

Index	*Title*	*Ref.*	*Publisher*	*Type*	*Quality assessment scoring*					
					QA1	*QA2*	*QA3*	*QA4*	*QA5*	*Score*
PS19	IoT intrusion detection system using deep learning and enhanced transient search optimization	Fatani et al. (2021)	IEEE	Journal	0.5	1	1	0.5	0.5	3.5
PS20	Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset	Gad et al. (2021)	IEEE	Journal	1	1	0.5	0.5	0.5	3.5
PS21	Comparing machine learning and deep learning for IoT botnet detection	Gandhi and Li (2021)	IEEE	Conference	0.5	1	0.5	0.5	0.5	3
PS22	A machine learning framework for intrusion detection system in IoT networks using an ensemble feature selection method	Guo (2021)	Scopus	Conference	0.5	1	0.5	0.5	0.5	3
PS23	A comparative study of machine learning models for cyber-attacks detection in wireless sensor networks	Ismail et al. (2021)	IEEE	Conference	0.5	1	0.5	0.5	0.5	3
PS24	Three-layer hybrid intrusion detection model for smart home malicious attacks	Shi et al. (2021)	ScienceDirect	Journal	0.5	1	1	0.5	0.5	3.5
PS25	An agile approach to identify single and hybrid normalization for enhancing machine learning-based network intrusion detection	Siddiqi and Pak (2021)	IEEE	Journal	0.5	0.5	1	0.5	0.5	3
PS26	Efficiency enhancement of intrusion detection in IoT based on machine learning through bioinspire	Samdekar et al. (2021)	IEEE	Conference	0.5	0.5	1	0.5	0.5	3
PS27	CorrAUC: a malicious Bot-IoT traffic detection method in IoT network using machine-learning techniques	Shafiq et al. (2021)	IEEE	Journal	1	1	1	0.5	0	3.5
PS28	Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks	Kumar et al. (2021)	Springer	Journal	1	1	0.5	1	0.5	4
PS29	Classifier performance evaluation for lightweight IDS using fog computing in IoT security	Khater et al. (2021)	Scopus	Journal	1	0.5	0.5	0.5	1	3.5
PS30	Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection	Rahman et al. (2021)	Springer	Journal	0.5	1	1	0.5	0.5	4
PS31	Fault-tolerant AI-driven intrusion detection system for the internet of things	Medjek et al. (2021)	Web of Science	Journal	0.5	1	0.5	0.5	0.5	3
PS32	Toward lightweight intrusion detection systems using the optimal and efficient feature pairs of the Bot-IoT 2018 dataset	Ozer et al. (2021)	Springer	Journal	1	1	0.5	0.5	0.5	3.5
PS33	An effective genetic algorithm-based feature selection method for intrusion detection systems	Halim et al. (2021)	Web of Science	Journal	1	1	0.5	0.5	0.5	3.5
PS34	IoT dataset validation using machine learning techniques for traffic anomaly detection	Vigoya et al. (2021)	Scopus	Journal	0.5	1	0.5	0.5	0.5	3

Appendix 3

Primary studies in 2022

Index	*Title*	*Ref*	*Publisher*	*Type*	*Quality assessment scoring*					
					QA1	*QA2*	*QA3*	*QA4*	*QA5*	*Score*
PS35	Anomaly detection for internet of things cyberattacks	Alanazi and Aljuhani (2022)	Scopus	Journal	1	0.5	0.5	0.5	0.5	3
PS36	A discrete time-varying greywolf IoT botnet detection system	Alazab (2022)	ScienceDirect	Journal	1	1	1	0.5	0.5	4
PS37	Intelligent IoT-botnet attack detection model with optimized hybrid classification model	Bojarajulu et al. (2022)	ScienceDirect	Journal	0.5	1	0.5	1	0.5	3.5
PS38	Performance analysis of machine learning models for intrusion detection system using Gini impurity-based weighted random forest (GIWRF) feature selection technique	Disha and Waheed (2022)	Springer	Journal	1	1	0.5	1	0.5	4
PS39	Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system	Fatani et al. (2022)	Scopus	Journal	1	1	1	0.5	0.5	4
PS40	Machine and deep learning amalgamation for feature extraction in industrial internet-of-things	Jayalaxmi et al. (2022)	Web of Science	Journal	1	0.5	1	0.5	0.5	3.5
PS41	A new intelligent satellite deep learning network forensic framework for smart satellite networks	Koroniotis et al. (2022)	ScienceDirect	Journal	1	1	0.5	0	0.5	3
PS42	Machine learning-based early detection of IoT botnets using network-edge traffic	Kumar et al. (2022a)	ScienceDirect	Journal	1	0.5	0.5	0.5	0.5	3
PS43	An intellectual intrusion detection system using hybrid hunger games search and remora optimization algorithm for IoT wireless networks	Kumar et al. (2022b)	ScienceDirect	Journal	1	1	0.5	1	0.5	4
PS44	IoT information theft prediction using ensemble feature selection	Leevy et al. (2022)	Springer	Journal	1	1	0.5	0.5	0.5	4
PS45	Decision tree with Pearson correlation-based recursive feature elimination model for attack detection in IoT environment	Padmashree and Krishnamoorthi (2022)	Scopus	Journal	0.5	1	0.5	0.5	0.5	3
PS46	Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system	Ravi et al. (2022)	ScienceDirect	Journal	1	1	0	0.5	0.5	3
PS47	A feature selection-based method for DDoS attack flow classification	Zhou et al. (2022)	ScienceDirect	Journal	1	1	0	0.5	0.5	3
PS48	A bio-inspired hybrid deep learning model for network intrusion detection	Moizuddin and Jose (2022)	Web of Science	Journal	1	1	0.5	0.5	0.5	3.5
PS49	IoT intrusion detection technology based on deep learning	Cao et al. (2022)	IEEE	Conference	1	1	0.5	0.5	0	3

Primary studies in 2022 (continued)

Index	*Title*	*Ref*	*Publisher*	*Type*	*Quality assessment scoring*					
					QA1	*QA2*	*QA3*	*QA4*	*QA5*	*Score*
PS50	Lightweight internet of things botnet detection using one-class classification	Malik et al. (2022)	Scopus	Journal	1	1	0	0.5	0.5	3
PS51	Analyzing IoT attack feature association with threat actors	Shafiq et al. (2022)	Wiley	Journal	1	1	0.5	0	1	3.5
PS52	CHAMELEON: optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection	Chohra et al. (2022)	Web of Science	Journal	1	1	0.5	1	1	4.5
PS53	Injection attack detection using machine learning for smart IoT applications	Gaber et al. (2022)	Web of Science	Journal	1	1	0.5	1	0.5	4
PS54	A distributed intrusion detection system using machine learning for IoT based on ToN-IoT dataset	Gad et al. (2022)	Scopus	Journal	0.5	1	0.5	1	0.5	3.5
PS55	ML-based IDPS enhancement with complementary features for home IoT networks	Illy et al. (2022)	IEEE	Journal	1	1	0	0.5	0.5	3
PS56	NFDLM: a lightweight network flow based deep learning model for DDoS attack detection in IoT domains	Saurabh et al. (2022)	IEEE	Conference	1	1	0	0.5	0.5	3
PS57	FI-PCA for IoT network intrusion detection	Abdulkareem et al. (2022)	IEEE	Conference	1	1	0.5	0.5	0.5	3.5
PS58	Machine learning based IoT-BotNet attack detection using real-time heterogeneous data	Ahmed and Tjortjis (2022)	IEEE	Conference	0.5	1	0.5	0.5	0.5	3
PS59	Examining the suitability of NetFlow features in detecting IoT network intrusions	Awad et al. (2022)	Scopus	Journal	1	1	0.5	1	0.5	4
PS60	VMFCVD: an optimized framework to combat volumetric DDoS attacks using machine learning	Prasad and Chandra (2022)	Springer	Journal	1	1	0.5	1	0.5	4
PS61	A GPU-based machine learning approach for detection of botnet attacks	Motylinski et al. (2022)	Web of Science	Journal	0.5	1	0.5	0.5	0.5	3
PS62	Fast, lightweight IoT anomaly detection using feature pruning and PCA	Carter et al. (2022)	ACM	Conference	0.5	1	0.5	0.5	0.5	3
PS63	An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection	Kareem et al. (2022)	Scopus	Journal	0.5	1	0.5	1	1	4