Insights of machine learning-based threat identification schemes in advanced network system

Thanuja Narasimhamurthy, Gunavathi Hosahalli Swamy
Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, Affiliated to Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Aug 12, 2023
Revised May 8, 2024
Accepted May 12, 2024

Keywords:

Advanced network system
Collaborative
Machine learning
Security
Threat identification

ABSTRACT

An advanced network system (ANS) is characterized by extensive communication features that can support a sophisticated collaborative network structure. This is essential to hosting various forms of upcoming modernized and innovative applications. Security is one of the rising concerns associated with ANS deployment. It is also noted that machine learning is one of the preferred cost-effective ways to optimize the security strength and address various ongoing security problems in ANS; however, it is still unknown about its overall effectivity scale. Hence, this paper contributes to a systematic review of existing variants of machine learning approaches to deal with threat identification in ANS. As ANS is a generalized form, this discussion considers the impact of existing machine learning approaches on its practical use cases. The paper also contributes towards critical gap analysis and highlights the study's potential learning outcome.

Corresponding Author:

Thanuja Narasimhamurthy
Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru,
Affiliated to Visvesvaraya Technological University
Belagavi, Karnataka, India
Email: nthanuja@bit-bangalore.edu.in

1. INTRODUCTION

With the evolving new demands of applications and enterprises, the network and communication system area has consistently changed to meet the demands [1]–[3]. This led to the evolution of the advanced networking system (ANS), which is meant to improve communication services in manifold aspects [4] significantly. Adoption of advanced networking systems leads to better connectivity and communication among devices, organizations, and individuals, thereby facilitating reliable transmission of data with speedy networks where instantaneous information sharing is facilitated [5]. Another significant role of ANS is towards internet of things (IoT), where a vast array of devices is connected to facilitate aggregation and analysis of data as well as automation [6]. With increasing futuristic planning towards modernized and innovative transportation systems, industries, and smart cities, IoT is gaining its adoption in the commercial market faster. The importance of ANS can also be realized in its deployment area of cloud computing, where many sophisticated operations can be relayed to users hosted on a cloud platform using varied services [7]. Additionally, ANS facilitates cloud computing towards forming a collaborative network with higher scalability and high-speed networks. It is also noted that the importance of big data is gaining in the current era. It can provide data storage and mapping, transmission, and efficient collection, followed by applying a wide range of analytics to derive meaningful information [8]. The applicability of big data analytics contributes towards ANS in the perspective of data exchange supportability that can be used in scientific research, healthcare, and business intelligence. ANS also improves business operations by offering innovative mechanisms to share resources within an organization, forming a customized collaborative network, and offering seamless communications [9]. With more preference towards virtual meetings, ANS can offer a collaborative platform that supports real-time streaming, sharing of necessary files, and interactive conferences, minimizing geographical barriers. Hence, productivity and performance are well-balanced and improved with such innovation ANS.

Further, ANS is potentially helpful for all emerging technologies towards their deployment and development; therefore, ANS can offer a better form of supportive backbone towards autonomous systems, virtual reality, artificial intelligence, edge computing, and 5G/6G network-based operations [10]. Such a form of technology requires a sophisticated network architecture that can deliver high-performance yield with reliability. However, all the discussion about the application mentioned above/services associated with ANS is more witnessed under the roof of research and significantly less in the commercial market. This eventually means that ANS is witnessed with significant beneficial characteristics, attracting scientific communities to continue its investigation. In contrast, there are certain eventual impediments towards its success rate.

Despite the increasing dimension of research contribution in the area of ANS, there are various impending challenges, which are required to be addressed as follows: i) The primary challenges in ANS are associated with cyber threats and security breaches, viz. unauthorized access, denial of service (DoS) attacks, data breaches, and malware. More robust and innovative intrusion detection systems, firewalls, and encryption strategies are needed to circumvent such threats. Unfortunately, conventional security schemes are ineffective in identifying or resisting such innovative lethal threats. ii) The following issues in ANS are associated with capacity and scalability over many connected devices with increasing data traffic. Balancing scalability demands along with reliability and optimal performance is something that ANS has yet to be witnessed. iii) Network congestion is another potential challenge in ANS with an exponential rise in data traffic. A potential bottleneck arises when its assigned network capacity cannot hold up servicing enormous traffic volumes, eventually leading to packet loss and latency. Further, conventional traffic management schemes needed a severe revision to mitigate evolving network congestion issues for optimal service quality. iv) interoperability among the devices, protocols, and multiple technologies is essential with the rise of integrated and collaborative services in ANS. v) Various intrinsic and extrinsic attributes, e.g., network disruption, device failures, power outages, and natural disasters, potentially affect ANS-based services' resiliency, and reliability. vi) The management of ANS has a higher likelihood to be complex, which demands skilled administrators of the network along with specialized devices to address troubleshooting issues, monitoring, and configuring. vii) The most significant challenge associated with ANS is related to data protection and privacy issues. Privacy is the biggest concern in ANS because a vast amount of susceptible and personal data is collected, propagated, processed, and stored by different devices. Although there are various evolving solutions towards addressing the issues mentioned above, there is still no report of any benchmarked solution at present.

After reviewing some relevant literature, all the above-identified challenges and issues linked with ANS have been cross-verified. It is noted that ANS is mainly studied concerning IoT scenarios as a use-case where varied methodologies have evolved to address some of its issues [11], [12]. Further, it is noted that various evolving studies have also been concentrated towards addressing challenges in cyber-physical systems (CPS), where security and privacy a critical concern [13], [14]. Various research has also been carried out towards the 5G network system, one of the dependable systems towards ANS, to find the distinct set of security problems with varied solutions [15], [16]. Further, a review of studies in vehicular networks is carried out to see that a significant number of research works towards mitigating security threats in ANS is noticed [17], [18]. All these research works are evidence that a potential number of research works have already been started in the current era towards paving the path of effective ANS implementation. However, each study has its uniqueness as well as limiting characteristics. Apart from this, it is also noted that security identification and mitigation is a bigger deal of problems in ANS, where existing claimed security solutions are not proven to be fully proved.

Irrespective of all the above-reviewed methodologies, there is still an ambiguity associated with the best solution to date with better clarity and measurable applicability discussion of existing systems towards ANS. Apart from this, it is also noted that machine learning has potentially contributed to leveraging ANS's security characteristics. Undoubtedly, various deep learning and encryption-based methodologies also contribute to optimal security characteristics in ANS. However, the proposed study emphasizes only machine-learning-based security solutions as this paper's scope. Therefore, the proposed study presents compact, yet pinpointed highlights of the current and latest machine learning methodologies associated with addressing security threats in ANS concerning various use cases. This manuscript's core notion highlights the strengths and weaknesses of existing security solutions using machine learning approaches towards ANS. The novel value-added points of the proposed research are the following contributions viz. i) Varied machine learning scheme is specifically studied that is meant for upgrading the security performance in discrete use-cases of ANS; ii) The paper reviews the use-cases of IoT, CPS, vehicular network, and other associated use-cases of ANS to review the effectiveness of machine learning approaches on them; iii) The paper highlights a unique research trend to showcase the distinct inclination of usage/adoption of machine learning methods; iv) The manuscript highlights the significant open-ended research issues in the form of the gap, which demands immediate attention by research communities; and v) Finally, the paper offers a summary of the learning outcomes associated with this study.

2. METHOD

The core agenda of the proposed study is to assess the effectiveness and applicability of the existing machine learning approach towards threat mitigation in ANS. Therefore, a compact and systematic planning of reviewing the existing methodologies has been adopted to carry out this review work. Initially, issues measuring the effectiveness of machine learning approaches towards solving security problems in ANS have been studied. This is accomplished by reviewing all the research journals published to date associated with the same issues. Primary filtering is carried out by screening the abstract to ensure that it deals with the same identified issues, while this step is controlled by exclusion and inclusion criteria. The exclusion criteria involve non-machine learning approaches mainly, while the inclusion criteria involve machine learning-based papers published from 2018 to till date. The exclusion criteria also involve any discussion paper or articles that do not have a complete discussion of methodologies. This dual criterion is used for further removing the duplicates from the primary filtered papers. The duplicates are identified to be those papers dealing with precisely the same dataset or the same methodologies. The same author also writes papers in multiple places dealing with the same architecture or vice versa, i.e., two concepts presented by different authors have been eliminated based on recent publication dates. The dual criteria are also used for screening adopted methodology and results accomplished. Only papers with detailed methodology and algorithms with precise numerical or graphical outcomes information have been shortlisted as unique papers for reviewing. This is because no conclusive inference can be offered without clearly understanding the methodology and outcome accomplished. This principle is finally used for secondary filtering, which further reduces the number of distinct and unique research articles. Finally, based on secondary filtered research journals, the complete observation is carried out exclusively towards identifying the enlisted research problems being addressed, adopted methodology to solve them, and accompanied beneficial factors and limitations connected to each study. Finally, the research gap is extracted based on a systematic review of secondary filtered research journals, leading to the extraction of learning outcomes. All the involved steps of observation further contribute towards identifying the research trend to understand the frequently used machine learning models or adoption trends of use cases of the ANS system. Figure 1 pictorially showcases the adopted methodology.

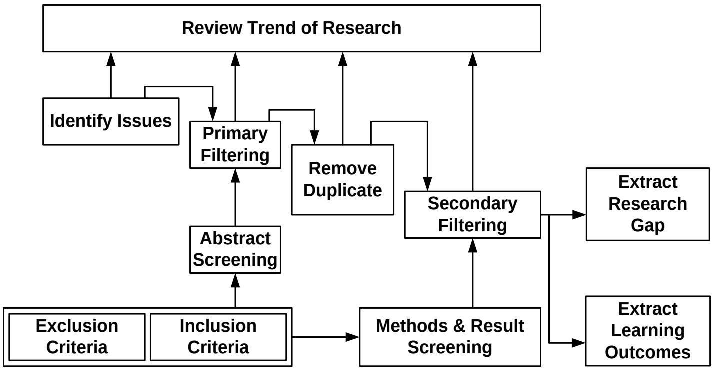

Figure 1. Adopted method

3. RESULTS

Different types of networking terminologies evolve at present in the context of advanced networking systems, viz. internet of things (IoT), cyber-physical system (CPS), advanced long-term evolution (LTE)-based networks, and advanced vehicular network (AVN). It should be noted that various security schemes towards protecting data and varied services are being executed over such advanced networking systems; however, this part of the study will be limited to adopting a learning-based scheme to optimize the security performance.

3.1. Existing studies in IoT security

Various machine learning-based approaches are adopted to address various security threats in IoT. Zhao and Kuerban [19] have used the k-nearest neighbor (KNN) approach to identify malware in cross architectures of IoT. Further study towards malware detection is also carried out by El-Ghamry *et al.* [20], where a machine learning approach has been integrated with swarm intelligence towards optimizing the detection performance. The study used a support vector machine (SVM) and ant colony optimization (ACO), which improvised the feature selection process to detect IoT malware. The SVM model is further tuned using particle swarm optimization (PSO) for improved classification performance. Yerima [21] have used a machine learning scheme to develop a botnet detection scheme to capture malware details in mobile devices. Ahanger *et al.* [22] have developed a scheme for resisting ransomware attacks in IoT devices by deploying hybrid machine learning. The study model integrated ElasticNet with the XGBoost algorithm to protect every IoT device executed over the PureOS operating system. The adoption of a machine learning approach with the Ensemble algorithm is noted in the work of Tomer and Sharma [23] and Alotaibi and Ilyas [24] towards the detection of distributed denial-of-service (DDoS) attacks on fog devices in IoT. Ullah *et al.* [25] carried out further studies towards the detection of and classification of DDoS attacks. The technique has used multiple machine learning approaches to develop a selection process of dynamic attributes, contributing to reducing computational effort in security operations. A study towards identifying and extracting potential features associated with intruders in IoT is carried out by Musleh *et al.* [26]. The study model has investigated the applicability of multiple learning approaches to realize their effectiveness in intrusion detection systems. Work carried out by Aljabri *et al.* [27] has used multiple machine learning approaches towards constructing unique feature engineering methods for contributing towards identifying attacks in IoT. The recent work by Koirala *et al.* [28] has used machine learning to detect botnets in healthcare system-based IoT devices. Further, a statistical evaluation has been carried out using entropy and correlation to extract potential features for identifying botnets in IoT environments.

3.2. Existing studies in CPS security

Existing studies towards securing CPS consist of multiple machine learning approaches to optimize attacks' detection performance. The recent work carried out by Alrowais *et al.* [29] has used the fuzzy c-means (FCM) approach integrated with artificial bee colony (ABC) optimization to detect the presence of attacks in medical information. The security model presented by Demelie and Deriba [30] has developed a unique learning mechanism towards specifically identifying and resisting structured query language injection (SQLI) attacks, a malware variant. Multiple machine learning schemes have been used to discover that combining artificial neural networks and SVM offers higher accuracy while naïve Bayesian performs sub-optimally. Another recent study discussed by Selvarajan *et al.* [31] used machine learning integrated with a blockchain to leverage privacy protection in industrial IoT applications. The study model has used analysis with an authentic intrinsic to minimize intrusion's influence by obtaining encoded data over transformed features. Alzahrani *et al.* [32] have used machine learning to offer higher privacy and security over medical data. A unique study model towards constructing a threat intelligence is presented by Dalal *et al.* [33], where a neural network-based analytical model is designed for predicting cyber-attacks present in the cloud ecosystem. According to the study model, the neural network-based model is witnessed with superior threat detection performance. The existing study has also witnessed the usage of reinforcement learning towards threat analysis as witnessed in the work of Ibrahim and Elhafiz [34], where an augmented graph is designed to represent the security loophole of the system followed by allocation of incentives and penalty based on adopted actions. A similar adoption of reinforcement systems is also seen in the work of Wolgast *et al.* [35] towards unknown threat detection in power systems. Vulnerability analysis of CPS in nursing homes is studied by Zhou *et al.* [36], where a gradient boosting technique has been adopted to develop a unique intrusion detection model. The model's outcome is witnessed to resist multiple potential threats considered via the standard dataset of the threat model.

3.3. Existing studies in vehicular networks

At present, various machine learning approaches are targeted towards improving the security perspective of the vehicular system, primarily meant for running using an advanced network system. Alsaade and Al-Adhaileh [37] have used an autoencoder-based learning scheme to detect cyber-attacks in-vehicle networks. According to this study, the modelling is carried out using KNN, autoencoders, long-short-term memory (LSTM), and decision tree (DT) to identify the threats. Khanna and Sharma [38] have used an improved SVM to categorize various threats in vehicular ad hoc networks, followed by a feed-forward backpropagation algorithm for classification. Ercan *et al.* [39] conducted a study to detect the misbehavior associated with counterfeited position-based attacks. A similar problem associated with position falsification threat is also addressed by Uprety *et al.* [40], where authors have used a federated machine learning approach. The authors have considered the use-case of internet-of-vehicle (IoV), where machine learning has been used to detect misbehavior. The authors have ensembled machine learning approaches using random forest (RF) and KNN algorithm to enhance detection performance. Rashid *et al.* [41] have developed a scheme for detecting malicious behavior in vehicular networks that works in real-time mode. Considering the detection case of a DDoS attack, the scheme has used multiple machine learning classifiers to classify binary forms of attacks. An interesting study has been conducted by Sun *et al.* [42], where machine learning has been used to improve the security features in IoV running over 6G networks. The core idea of this paper is to construct a dataset consisting of multiple network conversations to investigate the security loopholes more closely. Another recent and unique assessment-based security study model has been presented by Bari *et al.* [43], where the idea is to detect threats in the controller area network of a vehicle with the assistance of machine learning. The authors have used KNN, DT, and SVM for learning systems to classify intrusion during cyber-attacks. Apart from this, certain studies have also integrated blockchain with machine learning to offer more resiliency (Singh *et al.* [44]). Ayaz *et al.* [45] have used federated learning and blockchain to secure IoV running over a 6G network system. Another unique study is presented by Li *et al.* [46], where a federated learning approach is designed considering a multiparty computation system to upgrade privacy attributes in vehicular networks.

3.4. Other approaches

From the perspective of advanced network technologies, there is also the inclusion of technologies, e.g., software defined networks (SDN), fiber optic broadband, satellite network communication, and telemetry. Prabhakaran *et al.* [47] have developed a predictive scheme for intrusion in SDN networks using DT, C4.5, naïve Bayes (NB), and Bayesian networks to identify the attacks over virtual network function in SDN. Further studies towards securing SDN networks have also been carried out by Althobiti *et al.* [48], Alheeti *et al.* [49], Alamri and Thayananthan [50], Batra *et al.* [51], Guo and Bai [52], and Mohammadi *et al.* [53]. All these research approaches are used for modelling the control strategy based on the input of an attacker on various use cases where machine learning is used to learn and classify the attacks. A study towards securing optical fiber from DDoS has been carried out by Alwabisi *et al.* [54] using multiple machine learning models. The adoption of the neural network is used over an experimental prototype towards optical fiber by Ruzicka *et al.* [55] to perform safety event classification. Adoption of an autoencoder and k-means clustering is used for anomaly detection in acoustic sensing associated with optical fiber, as witnessed in the work of Xie *et al.* [56]. Lollie *et al.* [57] have used an encryption process integrated with machine learning to secure optical fiber communication. Tomasov *et al.* [58] and Abdeli *et al.* [59] have presented a scheme of anomaly analyzers where machine learning improves the detection rate with a polarization analyzer.

Further, with the evolving 6G, there is also an increasing trend towards satellite network communication, where machine learning is witnessed to play a crucial role [60]–[62]. However, this is ultimately a novel field of advanced networking systems, where the applicability of artificial intelligence is yet to encounter issues and challenges [63]. Network telemetry is another essential part of an advanced network system, which mainly aggregates network traffic data for analysis to identify threat possibilities. Some of the notable discussions were carried out by Sutariya and Pramanik [64], Sivanathan *et al.* [65], and Li *et al.* [66]. However, these study approaches are not much different from conventional approaches, where the main idea is to subject the data to analytical operation to extract specific typical patterns of intrusion or threats.

Therefore, it can be observed that various forms of machine-learning-based approaches are deployed on advanced network systems. While some technologies, e.g., IoT, IoV, CPS, and SDN, have witnessed a more significant number of contributions, other associated technologies associated with telemetry, fiber optics, and satellite-based communication systems have witnessed much less attention from the inclusion of machine learning-based approaches. Table 1 summarizes the notable research contribution of existing times concerning strengths and limitations.

3.5. Research trend

It should be noted that prior sections have discussed only the recent publications dealing with varied machine learning-based approaches for leveraging ANS security systems. However, there are various research publications whose individual discussion is out of the scope of this paper. Hence, this section presents a compact picture of existing research trends in which the research journals published between 2018 and 2023 (till date) are used. A total of 106,461 research journals have addressed security loopholes associated with various use cases of ANS. Table 2 highlights this trend of overall publications. From Table 2, it can be noted that there are a total of 64,089 research journals on varied reputed publishers related to the non-machine learning-based approach. In comparison, there are 42,372 research journals relating to discretely machine learning-based security approaches in ANS.

Table 1. Summary of existing approaches

Authors	Problem	Methodology	Advantage	Limitation
Zhao and Kuerban [19]	Cross-architecture malware detection	KNN	95% accuracy	Need prior attack definition
El-Ghamry *et al.* [20]	IoT malware detection	SVM, ACO, PSO	96% accuracy in detection	Sob-optimal convergence rate
Yerima [21]	Mobile malware detection	KNN, SVM, and DT	Very simplified model	Need prior attack definition
Ahanger *et al.* [22]	Ransomware attacks	ElasticNet, XGBoost	90% accuracy, low false positives	Specifically designed for ransomware
Tomer and Sharma [23]	DDoS attacks on fog nodes	Ensemble machine learning	Supports real-time detection	Designed explicitly for DDoS attack
Alotaibi and Ilyas [24]	Binary classification of intruder	KNN, Logistic regression (LR), DT, RF	Enhances outcome reliability, 98.67% of accuracy	This leads to highly non-uniform iterative operation
Ullah *et al.* [25]	DDoS attack detection and classification	RF, KNN, LR, Gaussian naïve Bayes, DT	99.98% of accuracy	Designed explicitly for DDoS attack
Musleh *et al.* [26]	Feature extraction towards intruders	SVM, KNN, and RF	98% of accuracy	Study outcome specific to the dataset
Aljabri *et al.* [27]	Attack identification	Multi-layer perceptron (MLP), LR, RF, J48, KNN, Bagging	Random forest excels better performance with 99.9% accuracy	Not accessed over a large-scale network
Koirala *et al.* [28]	Botnet detection	Entropy, Pearson correlation, multi-layer perceptron, gradient boost, KNN, RF, NB, LR, DT	99.98% accuracy	It is not meant for dynamic attack detection
Alrowais *et al.* [29]	Attack detection in medical information	FCM, ABC algorithm	Simplified threat detection approach	It is not meant for identifying complex forms of attacks
Demelie and Deriba [30]	SQLI attack	ANN, SVM, LR, RF, DT, NB	99% accuracy exhibited by ANN and SVM, simplified assessment model	Accuracy depends on increased training data
Selvarajan *et al.* [31]	Privacy and security	Transformation using autoencoder, neural network, blockchain	99.8% of accuracy	The study does not consider the heterogenous environment in IoT
Alzahrani *et al.* [32]	Privacy and security	Fuzzy logic, DT, RF, neural network-based models	Comprehensive feature extraction, 92% accuracy	Demands Apriori information of attacks
Dalal *et al.* [33]	Detection of cyber attacks	Extremely boosted neural network	99.72% of accuracy, supports real-time communication	Study explicitly to the adopted dataset
Ibrahim and Elhafiz [34]	Threats in cybersecurity	Reinforcement learning	Effective attack graph design	Narrowed applicability towards dynamic attacks
Wolgast *et al.* [35]	Threat detection in power system	Reinforcement learning	Can detect unknown attacks	Scalability issues
Zhou *et al.* [36]	Potential attacks in the nursing system	Gradient boosting machine	Offers significant communication security	Study explicitly to adopt dataset
Alsaade and Al-Adhaileh [37]	Cyber attacks	KNN, DT, LSTM, autoencoder	99.98% of accuracy, simplified design implementation	Study explicitly to adopt dataset
Khanna and Sharma [38]	Replay attack, Sybil attack, DoS attack in vehicular network	Improved SVM, feed-forward backpropagation	Satisfactory throughput	Cannot sustain multiple heterogeneous concurrent attacks
Ercan *et al.* [39]	Position falsification attacks	Ensemble machine learning (RF, KNN)	Low computational time	Centralized scheme
Uprety *et al.* [40]	Position falsification attacks	Federated machine learning (SVM, KNN, LSTM))	Satisfactory attack detection accuracy (~94%)	Narrowed extensive analysis of dynamic threats
Rashid *et al.* [41]	DDoS attack in vehicular ad-hoc network	SVM, RF, multilayered perceptron, LR	RF to offer 98% accuracy	Study applicable only for DDoS attack
Sun *et al.* [42]	Network security in IoV	Machine learning-based fusion of data	Applicable for multiple domains	Model not evaluated on the concurrent and dynamic form of attacks in 6G
Bari *et al.* [43]	Cyber-attacks in the controller area network of vehicle	SVM, KNN, DT	99.9% accuracy in threat detection	Outcome specific to vehicular dataset
Ayaz *et al.* [45]	Security of IoV in 6G network	Federated learning, blockchain	Decentralized approach towards security	Involved complexity associated with blockchain management
Li *et al.* [46]	Privacy issues in vehicular network	Federated learning, multiparty computation	Reduce overhead, ensure high-quality data	Higher memory complexity
Prabhakaran *et al.* [47]	Intrusion in SDN	DT, C4.5, Bayesian network, NB	Bayesian network to exhibit higher accuracy of 93%	Not applicable for dynamic attacks
Althobiti *et al.* [48], Alheeti *et al.* [49], Alamri and Thayananthan [50], Batra *et al.* [51], Guo and Bai [52], Mohammadi *et al.* [53].	Security issues in SDN	Analytical model	Simplified architecture, flexible control plane-based operation	Not benchmarked, attack-specific solution
Alwabisi *et al.* [54]	DDoS in optical fiber	RF, DT, NB, SVM, KNN, LR	SVM and RF show 100% of accuracy	Solution specific to attack
Ruzicka *et al.* [55]	Classification of abnormal events in optical fiber	Neural network, experimental prototype	99% accuracy	No extensive evaluation towards model applicability in large-scale
Xie *et al.* [56]	Anomaly detection in optical fiber in high-speed rail	K-mean clustering, autoencoder	91% of accuracy	Model specific to use-case
Lollie *et al.* [57]	High-dimensionality issues	Encryption, ANN	Light-weight encryption	Demands higher training data
Tomasov *et al.* [58]	Anomaly detection in optical fiber	Machine learning	Faster detection	It depends upon the state of polarization
Abdeli *et al.* [59]	Anomaly detection	Autoencoder, attention-based bidirectional gated recurrent unit	98.2% of accuracy	Tested only on eavesdropping and fiber cuts

Table 2. Trend of total research publication on ANS security

Publication	Non-machine learning approach	Machine learning approach
IEEE	171	15
ScienceDirect	32,585	12,002
Springer	1,372	5
Elsevier	1,256	1,372
MDPI	232	52
ACM	28,473	28,926

The non-machine learning approaches deal with encryption, trust, reputation, and cryptography, while the machine learning-based schemes mainly deal with supervised, unsupervised, and hybrid learning techniques. Apart from this, it is also noted that there is no specific work towards future internet architecture or ANS exclusively; however, this count has been arrived at after summing up individual use-case-based research methodologies. Further, it is noted that machine learning-based approaches are consistently on the rise, while the adoption of non-machine learning-based approaches has its own pace towards cryptography. To obtain a clear notion of the adoption of unique use cases, the aggregated papers are further filtered to ensure that no similar approaches are to be considered. For example, it has been noted that a similar methodology is used in two research publications associated with one use-case of ANS. Hence, all the redundant methodologies have been filtered to explore the adoption trend of specific use case preferences. This observation results in Table 3.

Table 3. The trend of unique implementation of ANS security use cases

Uses cases of ANS	Non-machine learning approach	Machine learning approach
IoT	350	244
CPS	241	143
IoV	60	31
Miscellaneous	98	72

Table 3 shows the smaller number of machine learning approaches because more adoption of deep learning is also witnessed in current times; however, the present paper restricts its observation only to machine learning as it is its sole objective. Hence, Table 3 concludes that a more significant number of IoT based use-cases are preferred for research work, followed by CPS, while the adoption of IoV and others is relatively less. Although it cannot be concluded that IoT is the best use-case in the context of CPS, it is observed that applications hosted on IoT and IoV networks are more supportability of upcoming applications that demand ANS systems to be used. In short, IoT and IoV are the frequently observed use cases for addressing security problems in ANS. Hence, a clear picture of adopting machine learning-based approaches is finally required to be investigated concerning its trend. A similar methodology is adopted, where individual machine-learning approaches' unique/dominant usage is sought. This is quite challenging as most of the existing machine learning-based schemes are found to implement multiple machine learning algorithms. Hence, it is difficult to assess the effectiveness of one single scheme towards leveraging security. For this purpose, the papers with integrated machine learning schemes are collected and studied, and only the papers that have claimed of better contribution of machine learning with comparative analysis are finally selected. The sub-optimal performance of other learning schemes is opted out. This filtering exercise is carried out towards all the machine learning-based methodologies for all the use-cases of ANS to finally arrive at the outcome of the research trend shown in Table 4.

Table 4. The trend of adopted machine learning approaches in ANS security

Machine learning approaches	No. of publication
SVM	99
DT	99
RF	89
MLP/ANN	92
LR	42
RL	31
KNN	11
NB	12
Hybrid/Ensemble/Federated	15

Table 4 highlights the breakdown of all the 490 distinct research publications using machine learning to find that SVM, DT, RF, and ANN are the most preferred machine learning schemes where the researchers have claimed for unique work implementation with better results towards detection and classification of security threats in multiple use-cases of ANS. This outcome of research trend eventually showcases these four machine learning approaches to be most preferred with maximum use cases while researchers claim other approaches to yield sub-optimal accuracy. It should be noted that this does not imply that other methods, especially hybrid/ensemble methods, cannot yield better results. That is why they have not yet been explored in a more dynamic assessment scenario of threats in ANS. Hence, more research towards dynamic tests is further demanded.

3.6. Research gap

The existing machine learning methodologies were designed mainly to strengthen the base of security systems that can further identify and resist potential security threats in ANS. After reviewing existing methodologies, it is noted that there are various claimed beneficial factors, while there are limiting factors. Hence, this section outlines all the primary critical open-ended research issues that are found missing to be addressed in existing research works. Following are the description of identified research gaps:

a. Lack of extensive evidence of sustainability: Existing machine learning approaches in their varied forms have proven their effectiveness in detection, classification, and training operations over the defined set of threat considerations in ANS use cases. However, this is not enough as ANS is anticipated with constantly evolving threats, and there is a need for consistent monitoring by the learning algorithms to keep track of all temporal emerging forms of threats. This raises a question about the applicability of machine learning in its present form concerning its sustainability.

b. Biased emphasis on privacy factors: Available as well as reviewed security approaches has handled the privacy issues too; however, while performing training operation in the distributed environment of ANS, there is higher likelihood of data leakage leading to serious privacy concerns. Unfortunately, few studies have been carried out using multiparty computation or federated learning approach, which is quite capable enough to deal with this situation.

c. Issues relating to interpretability: There is no denying that neural network, SVM, and RF offer some cost-effective, robust solution towards threat identification in use cases reported in the literature about advanced networking system security. However, these outcomes cannot offer a concrete explanation towards the adoption of the decision being made during each iteration. Lack of inclusion of trust or statistical valuation of behavior is witnessed in existing schemes, which suffer from interpretability issues. Because of this issue, the applicability of the same model on a different trajectory of attacks cannot be justified by existing models.

d. Lack of emphasis towards data quality: A successful deployment of machine learning towards threat mitigation calls for quality data, meaning that data should offer higher degree of representation to undergo training. As most of the experiments have been carried out on publicly available datasets, it is still unclear how the model will react when exposed to real-time data. Further, owing to the lack of consideration of progressive attacks or concurrent intrusion in any research work, it increases sensitivity, so acquiring labelled data for training is quite challenging. Further, existing studies have also not addressed issues about data poisoning attacks capable of controlling the entire learning algorithm.

e. Lack of adaptability: A machine learning model can be justified as adaptable if it can determine the threats whose forms are very different compared to the trained dataset. However, most of the higher claims of accuracy in existing models are because of their extensive training operation or consideration of a higher quantity of similarly trained biased data. In such cases, the model's applicability is limited to only considered attacks reported in respective papers and cannot detect novel attacks.

f. Less focus on computational complexity: Most devices running on the ANS system are anticipated to be resource-limited from the energy and processor capability context. Hence, a cost-effective learning model can only be tagged if the model is capable of offering higher accuracy in less iteration and does not introduce time or space complexity. Unfortunately, none of the reported works are benchmarked, nor have they been assessed from the computational complexity perspective to ascertain this fact.

Hence, a conclusive remark of the research gap is that-although more studies are using different variants of machine learning approaches, they have not been witnessed to address those above open-ended issues. With the rising trends of research activities towards adopting deep learning, machine learning has advantages. Hence, there is a need for further research contributions that can address the impending issues by identifying the prominent indicators of practical training algorithms connecting with the broader applicability of solving the security threat identification issues in ANS. The following section discusses the summary of the presented review work's learning outcomes.

4. CONCLUSION AND FUTURE SCOPE

The importance of ANS is anticipated to be realized more for its potential characteristic towards supporting futuristic applications and services. The significance of ANS can be understood from its inherent characteristics of high-end connectivity, collaboration and data sharing, optimization of resources, distributed cloud computing, telecommunication, and multimedia services. However, ANS suffers from a severe security concern that is the prime highlight of this paper. The contribution of this paper is stated in the form of the following novel learning outcomes: i) The conventional encryption-based security mechanism can only offer security towards a specific form of threat, while adoption of machine learning can induce a capability towards identifying a more significant number of anomalies and threats. ii) From the context of approach and model complexity, machine learning models are simpler to implement compared to deep learning approaches and hence, more upcoming works are using deep learning owing to its independence from feature engineering. This calls for more extensive research towards machine learning approaches as all the deep learning models extensively demand larger datasets while this aspect can be controlled in machine learning models. From the perspective of usage of resource-constrained devices in ANS, machine learning approaches are more beneficial compared to evolving deep learning approaches are they can offer better training efficiency, flexibility in feature engineering, highly transparent outcomes, less prone to overfitting issues, demand only more minor data requirements, and is computationally efficient compared to deep learning. Hence, machine learning-based approaches require more attention from an ANS security perspective. iii) Most of the existing approaches in ANS are carried out considering its use cases, and there is no generalized framework for this. This has resulted in a use-case use-case-specific mode of investigation. However, there is a possibility that a generalized machine learning model can be developed, which can be implied in multiple use cases of ANS. Unfortunately, there is no such model reported. iv) Existing learning models offer computational complexity when exposed to the large-scale scenario, and v) SVM, DT, RF, and ANN are witnessed to offer optimal threat mitigation performance. Yet, they have limiting factors associated with them, which demand more finetuning to apply to the ANS framework. Therefore, our future work direction will address the open-end research problems identified in the current review work. Our upcoming work's prime focus will be developing a novel machine learning framework that can offer consistent performance towards multiple threat mitigation over multiple use cases of ANS.

REFERENCES

[1] J. J. L. Escobar, R. P. D. Redondo, and F. Gil-Castiñeira, “In-depth analysis and open challenges of mist computing,” *Journal of Cloud Computing*, vol. 11, no. 1, Nov. 2022, doi: 10.1186/s13677-022-00354-x.

[2] M. M. Rad, A. M. Rahmani, A. Sahafi, and N. N. Qader, “Social internet of things: vision, challenges, and trends,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, Dec. 2020, doi: 10.1186/s13673-020-00254-6.

[3] T. Rajmohan, P. H. Nguyen, and N. Ferry, “A decade of research on patterns and architectures for IoT security,” *Cybersecurity*, vol. 5, no. 1, Dec. 2022, doi: 10.1186/s42400-021-00104-7.

[4] J. Tian, H. Xiao, Y. Sun, D. Hou, and X. Li, “Energy efficiency optimization-based resource allocation for underlay RF-CRN with residual energy and QoS guarantee,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, Dec. 2020, doi: 10.1186/s13638-020-01824-z.

[5] M. W. Akhtar, S. A. Hassan, R. Ghaffar, H. Jung, S. Garg, and M. S. Hossain, “The shift to 6G communications: vision and requirements,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, Dec. 2020, doi: 10.1186/s13673-020-00258-2.

[6] A. Kumar Sangaiah, A. Chaudhary, C.-W. Tsai, J. Wang, and F. Mercaldo, “Cognitive computing for big data systems over internet of things for enterprise information systems,” *Enterprise Information Systems*, vol. 14, no. 9–10, pp. 1233–1237, Nov. 2020, doi: 10.1080/17517575.2020.1814422.

[7] A. Aliyu *et al.*, “Mobile cloud computing: taxonomy and challenges,” *Journal of Computer Networks and Communications*, vol. 2020, pp. 1–23, Jul. 2020, doi: 10.1155/2020/2547921.

[8] D. Kozjek, R. Vrabič, B. Rihtaršič, N. Lavrač, and P. Butala, “Advancing manufacturing systems with big-data analytics: a conceptual framework,” *International Journal of Computer Integrated Manufacturing*, vol. 33, no. 2, pp. 169–188, Feb. 2020, doi: 10.1080/0951192X.2020.1718765.

[9] J. Mendling, B. T. Pentland, and J. Recker, “Building a complementary agenda for business process management and digital innovation,” *European Journal of Information Systems*, vol. 29, no. 3, pp. 208–219, 2020, doi: 10.1080/0960085X.2020.1755207.

[10] L. F. de S. Cardoso, B. Y. L. Kimura, and E. R. Zorzal, “Towards augmented and mixed reality on future mobile networks,” *Multimedia Tools and Applications*, vol. 83, no. 3, pp. 9067–9102, Jan. 2024, doi: 10.1007/s11042-023-15301-4.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “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, 2020, doi: 10.1109/COMST.2020.2988293.

[12] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, “Security, privacy and trust for smart mobile-internet of things (M-IoT): a survey,” *IEEE Access*, vol. 8, pp. 167123–167163, 2020, doi: 10.1109/ACCESS.2020.3022661.

[13] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You, and X. Xu, “A survey of network attacks on cyber-physical systems,” *IEEE Access*, vol. 8, pp. 44219–44227, 2020, doi: 10.1109/ACCESS.2020.2977423.

[14] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, “Physical safety and cyber security analysis of multi-agent systems: a survey of recent advances,” *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021, doi: 10.1109/JAS.2021.1003820.

[15] J. Suomalainen, J. Julku, M. Vehkapera, and H. Posti, “Securing public safety communications on commercial and tactical 5G networks: a survey and future research directions,” *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1590–1615, 2021, doi: 10.1109/OJCOMS.2021.3093529.

[16] J. Sanchez-Gomez *et al.*, "Integrating LPWAN technologies in the 5G ecosystem: a survey on security challenges and solutions," *IEEE Access*, vol. 8, pp. 216437–216460, 2020, doi: 10.1109/ACCESS.2020.3041057.

[17] N. I. Shuhaimi and T. Juhana, "Security in vehicular ad-hoc network with Identity-based cryptography approach: a survey," in *2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, Oct. 2012, pp. 276–279, doi: 10.1109/TSSA.2012.6366067.

[18] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A survey on privacy-preserving authentication schemes in VANETs: attacks, challenges and open issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/ACCESS.2021.3125521.

[19] Y. Zhao and A. Kuerban, "MDABP: a novel approach to detect cross-architecture IoT malware based on PaaS," *Sensors*, vol. 23, no. 6, Mar. 2023, doi: 10.3390/s23063060.

[20] A. El-Ghamry, T. Gaber, K. K. Mohammed, and A. E. Hassanien, "Optimized and efficient image-based IoT malware detection method," *Electronics*, vol. 12, no. 3, Jan. 2023, doi: 10.3390/electronics12030708.

[21] S. Y. Yerima, "High accuracy detection of mobile malware using machine learning," *Electronics*, vol. 12, no. 6, Mar. 2023, doi: 10.3390/electronics12061408.

[22] T. A. Ahanger, U. Tariq, F. Dahan, S. A. Chaudhry, and Y. Malik, "Securing IoT devices running PureOS from ransomware attacks: leveraging hybrid machine learning techniques," *Mathematics*, vol. 11, no. 11, May 2023, doi: 10.3390/math11112481.

[23] V. Tomer and S. Sharma, "Detecting IoT attacks using an ensemble machine learning model," *Future Internet*, vol. 14, no. 4, Mar. 2022, doi: 10.3390/fi14040102.

[24] Y. Alotaibi and M. Ilyas, "Ensemble-learning framework for intrusion detection to enhance internet of things' devices security," *Sensors*, vol. 23, no. 12, Jun. 2023, doi: 10.3390/s23125568.

[25] S. Ullah, Z. Mahmood, N. Ali, T. Ahmad, and A. Buriro, "Machine learning-based dynamic attribute selection technique for DDoS attack classification in IoT networks," *Computers*, vol. 12, no. 6, May 2023, doi: 10.3390/computers12060115.

[26] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion detection system using feature extraction with machine learning algorithms in IoT," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, Mar. 2023, doi: 10.3390/jsan12020029.

[27] M. Aljabri *et al.*, "Machine learning-based detection for unauthorized access to IoT devices," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, Mar. 2023, doi: 10.3390/jsan12020027.

[28] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT device security through network attack data analysis using machine learning algorithms," *Future Internet*, vol. 15, no. 6, Jun. 2023, doi: 10.3390/fi15060210.

[29] F. Alrowais, H. G. Mohamed, F. N. Al-Wesabi, M. Al Duhayyim, A. M. Hilal, and A. Motwakel, "Cyber attack detection in healthcare data using cyber-physical system with optimized algorithm," *Computers and Electrical Engineering*, vol. 108, May 2023, doi: 10.1016/j.compeleceng.2023.108636.

[30] W. B. Demilie and F. G. Deriba, "Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques," *Journal of Big Data*, vol. 9, no. 1, Dec. 2022, doi: 10.1186/s40537-022-00678-0.

[31] S. Selvarajan *et al.*, "An artificial intelligence lightweight Blockchain security model for security and privacy in IIoT systems," *Journal of Cloud Computing*, vol. 12, no. 1, Mar. 2023, doi: 10.1186/s13677-023-00412-y.

[32] A. Alzahrani, M. Alshehri, R. AlGhamdi, and S. K. Sharma, "Improved wireless medical cyber-physical system (IWMCPS) based on machine learning," *Healthcare*, vol. 11, no. 3, Jan. 2023, doi: 10.3390/healthcare11030384.

[33] S. Dalal *et al.*, "Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment," *Journal of Cloud Computing*, vol. 12, no. 1, Jan. 2023, doi: 10.1186/s13677-022-00356-9.

[34] M. Ibrahim and R. Elhafiz, "Security analysis of cyber-physical systems using reinforcement learning," *Sensors*, vol. 23, no. 3, Feb. 2023, doi: 10.3390/s23031634.

[35] T. Wolgast, E. M. Veith, and A. Nieße, "Towards reinforcement learning for vulnerability analysis in power-economic systems," *Energy Informatics*, vol. 4, no. S3, Sep. 2021, doi: 10.1186/s42162-021-00181-5.

[36] F. Zhou, X. Du, W. Li, Z. Lu, and J. Wu, "NIDD: an intelligent network intrusion detection model for nursing homes," *Journal of Cloud Computing*, vol. 11, no. 1, Dec. 2022, doi: 10.1186/s13677-022-00361-y.

[37] F. W. Alsaade and M. H. Al-Adhaileh, "Cyber attack detection for self-driving vehicle networks using deep autoencoder algorithms," *Sensors*, vol. 23, no. 8, Apr. 2023, doi: 10.3390/s23084086.

[38] H. Khanna and M. Sharma, "An improved security algorithm for VANET using machine learning," *Journal of Positive School Psychology*, vol. 6, no. 3, pp. 7743–7756, 2022.

[39] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2022, doi: 10.1109/ACCESS.2021.3136706.

[40] A. Uprety, D. B. Rawat, and J. Li, "Privacy preserving misbehavior detection in IoV using federated machine learning," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2021, pp. 1–6, doi: 10.1109/CCNC49032.2021.9369513.

[41] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An adaptive real-time malicious node detection framework using machine learning in vehicular ad-hoc networks (VANETs)," *Sensors*, vol. 23, no. 5, Feb. 2023, doi: 10.3390/s23052594.

[42] B. Sun, R. Geng, L. Zhang, S. Li, T. Shen, and L. Ma, "Securing 6G-enabled IoT/IoV networks by machine learning and data fusion," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, 2022, doi: 10.1186/s13638-022-02193-5.

[43] B. S. Bari, K. Yelamarthi, and S. Ghafoor, "Intrusion detection in vehicle controller area network (CAN) bus using machine learning: a comparative performance study," *Sensors*, vol. 23, no. 7, Mar. 2023, doi: 10.3390/s23073610.

[44] P. K. Singh, S. Nandi, S. K. Nandi, U. Ghosh, and D. B. Rawat, "Blockchain meets AI for resilient and intelligent internet of vehicles," *arXiv preprint arXiv:2112.14078*, 2021.

[45] F. Ayaz, Z. Sheng, D. Tian, M. Nekovee, and N. Saeed, "Blockchain-empowered AI for 6G-enabled internet of vehicles," *Electronics*, vol. 11, no. 20, Oct. 2022, doi: 10.3390/electronics11203339.

[46] Y. Li, H. Li, G. Xu, T. Xiang, and R. Lu, "Practical privacy-preserving federated learning in vehicular fog computing," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 4692–4705, May 2022, doi: 10.1109/TVT.2022.3150806.

[47] S. Prabakaran *et al.*, "Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network," *Sensors*, vol. 22, no. 3, Jan. 2022, doi: 10.3390/s22030709.

[48] A. Althobiti, R. Almohayawi, and O. Bamsag, "Machine learning approach to secure software defined network: machine learning and artificial intelligence," in *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, Nov. 2020, pp. 1–8, doi: 10.1145/3440749.3442597.

[49] K. M. A. Alheeti, A. Alzahrani, M. Alamri, A. K. Kareem, and D. Al-Dosary, "A comparative study for SDN security based on machine learning," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 11, pp. 131–140, Jun. 2023, doi: 10.3991/ijim.v17i11.39065.

[50] H. A. Alamri and V. Thayananthan, "Analysis of machine learning for securing software-defined networking," *Procedia Computer Science*, vol. 194, pp. 229–236, 2021, doi: 10.1016/j.procs.2021.10.078.

[51] R. Batra, V. K. Shrivastava, and A. K. Goel, "Anomaly detection over SDN using machine learning and deep learning for securing smart city," in *Green Internet of Things for Smart Cities*, New York: CRC Press, 2021, pp. 191–204.

[52] X. Guo and W. Bai, "ML-SDNIDS: an attack detection mechanism for SDN based on machine learning," *International Journal of Information and Computer Security*, vol. 19, no. 1/2, 2022, doi: 10.1504/IJICS.2022.126759.

[53] R. Mohammadi, C. Lal, and M. Conti, "HTTPScout: a machine learning based countermeasure for HTTP flood attacks in SDN," *International Journal of Information Security*, vol. 22, no. 2, pp. 367–379, Apr. 2023, doi: 10.1007/s10207-022-00641-3.

[54] S. Alwabisi, R. Ouni, and K. Saleem, "Using machine learning and software-defined networking to detect and mitigate DDoS attacks in fiber-optic networks," *Electronics*, vol. 11, no. 23, Dec. 2022, doi: 10.3390/electronics11234065.

[55] M. Ruzicka, L. Jabloncik, P. Dejdar, A. Tomasov, V. Spurny, and P. Munster, "Classification of events violating the safety of physical layers in fiber-optic network infrastructures," *Sensors*, vol. 22, no. 23, Dec. 2022, doi: 10.3390/s22239515.

[56] Y. Xie, M. Wang, Y. Zhong, L. Deng, and J. Zhang, "Label-free anomaly detection using distributed optical fiber acoustic sensing," *Sensors*, vol. 23, no. 8, Apr. 2023, doi: 10.3390/s23084094.

[57] M. L. J. Lollie *et al.*, "High-dimensional encryption in optical fibers using spatial modes of light and machine learning," *Machine Learning: Science and Technology*, vol. 3, no. 3, Sep. 2022, doi: 10.1088/2632-2153/ac7f1b.

[58] A. Tomasov, P. Dejdar, P. Munster, T. Horvath, P. Barcik, and F. Da Ros, "Enhancing fiber security using a simple state of polarization analyzer and machine learning," *Optics & Laser Technology*, vol. 167, Dec. 2023, doi: 10.1016/j.optlastec.2023.109668.

[59] K. Abdelli, J. Y. Cho, F. Azendorf, H. Griesser, C. Tropschug, and S. Pachnicke, "Machine learning-based anomaly detection in optical fiber monitoring," *Journal of Optical Communications and Networking*, vol. 14, no. 5, May 2022, doi: 10.1364/JOCN.451289.

[60] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: a survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, Oct. 2022, doi: 10.1016/j.comnet.2022.109246.

[61] F. Fourati and M.-S. Alouini, "Artificial intelligence for satellite communication: a review," *Intelligent and Converged Networks*, vol. 2, no. 3, pp. 213–243, Sep. 2021, doi: 10.23919/ICN.2021.0015.

[62] A. Bhattacharyya, S. M. Nambiar, R. Ojha, A. Gyaneshwar, U. Chadha, and K. Srinivasan, "Machine learning and deep learning powered satellite communications: enabling technologies, applications, open challenges, and future research directions," *International Journal of Satellite Communications and Networking*, vol. 41, no. 6, pp. 539–588, Nov. 2023, doi: 10.1002/sat.1482.

[63] J. J. Garau-Luis, S. Eiskowitz, N. Pachler, E. Crawley, and B. Cameron, "Towards autonomous satellite communications: an AI-based framework to address system-level challenges," *arXiv preprint arXiv:2112.06055*, 2021.

[64] K. Sutariya and K. K. Pramanik, "Managing IoT cyber-security using programmable telemetry and machine learning," in *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, Jan. 2023, pp. 1323–1328, doi: 10.1109/AISC56616.2023.10085343.

[65] A. Sivanathan, H. H. Gharakheili, and V. Sivaraman, "Managing IoT cyber-security using programmable telemetry and machine learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 60–74, Mar. 2020, doi: 10.1109/TNSM.2020.2971213.

[66] Y. Li, G. Huang, C. Wang, and Y. Li, "Analysis framework of network security situational awareness and comparison of implementation methods," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1506-1.

BIOGRAPHIES OF AUTHORS

Thanuja Narasimhamurthy assistant professor, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, India. She completed graduation and post-graduation from Visvesvaraya Technological University in information/computer science and engineering stream. Published papers in international journals and conferences in the domain of machine learning and internet of things. Research focuses on networking systems, internet of things and machine learning. She can be contacted at email: nthanuja@bit-bangalore.edu.in.

Gunavathi Hosahalli Swamy associate dean, Skill Development and Assistant professor, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru. She has published many research papers in international journals and international conferences. Actively involved in organizing events/conferences, also organized many workshops/FDPs. Major areas of research interest are image processing, pattern recognition, artificial intelligence, machine learning, data science and IoT. She can be contacted at email: gunavathihs@bit-bangalore.edu.in.