International Journal of Humanities and Information Technology (IJHIT)
e-ISSN: 2456 –1142, Volume 6, Issue 4, (December 2024), www.ijhit.info

A Review of Intelligent Cybersecurity Solutions for Network Threats Using Machine Learning and Federated Learning

Naveen Shrivastava[1], Mahesh Marri[2], Khaja Moiezuddin Mohammed[3], Rashmika Jalagam[4], Sridevi Allu[5], Sivaraju Kuraku[6]

[1] T-Mobile
[2] Amazon Web Services, Senior Electrical Engineer
[3] IQVIA
[4] Matilda Cloud
[5] American Airlines
[6] University of the Cumberlands

Abstract

A lot of decision-support systems have gotten quicker, more accurate, and more efficient thanks to machine learning models. As compared to other fields, network security applications of machine learning confront a more disproportionate threat of active adversarial assaults. The reason behind this is that machine learning programs used for network security, like detecting malware, intrusions, and spam, are inherently hostile. The exponential rise of digital networks and connected devices has led to the proliferation of dangers such as malware, phishing, denial-of-service (DoS), advanced persistent threats (APTs), insider threats, and zero-day vulnerabilities. Traditional cybersecurity techniques, although successful to a certain extent, can't keep up with these threats because they are always evolving. Emerging possibilities for improved detection, prevention, and response tactics in intelligent cybersecurity are derived from ML and FL. Results in intrusion and anomaly detection using ML techniques (including deep learning, semi-supervised, supervised, and unsupervised learning) have been encouraging. Important sectors like healthcare, finance, and government systems have voiced concerns about data security and privacy; nevertheless, FL offers a decentralized paradigm that protects privacy and permits collaborative model training without revealing critical raw data. Also covered are the reasons for doing this research, the obstacles we've encountered, and the potential avenues for future study that might help us build cybersecurity frameworks that are smart, robust, and privacy-preserving, and that could handle the ever-changing nature of cyber threats.

Keywords: Federated Learning, Anomaly Detection, Privacy Preservation, Cybersecurity, Machine Learning, Intrusion Detection, Network Threats, Adversarial Defense.

DOI: 10.21590/dcfs25es

I. INTRODUCTION

The increasing integration of the Internet into social, economic, and industrial activities, cyberspace has become a critical infrastructure that shapes the way individuals learn, work, and interact. However, this reliance also exposes users and organizations to a growing number of cybersecurity threats, ranging from phishing and spam to advanced persistent attacks and ransomware [1]. The dynamic and evolving nature of cyber risks makes it challenging to design static defense mechanisms, particularly against zero-day attacks that exploit previously unseen vulnerabilities [2]. Consequently, developing intelligent and adaptive solutions for threat detection and mitigation has emerged as an urgent research priority.

Protecting computer systems, networks, and data from unauthorized access, modification, or destruction is the goal of "cybersecurity" initiatives [3][4]. Firewalls, antivirus programs, and Intrusion Detection Systems (IDSs) are some of the more conventional methods that detect and prevent known harmful patterns. However, these methods struggle to scale against the volume, variety, and velocity of modern cyberattacks [5]. The increasing machine-to-machine interactions and ubiquitous connectivity in computing environments have further amplified the sophistication and frequency of cybercrimes, making conventional signature-based techniques insufficient.

Machine Learning (ML) and Deep Learning (DL) have become widely used due to their ability to analyze large amounts of different data and uncover patterns of malicious activity that were previously undiscovered [6]. ML-driven cybersecurity applications include phishing detection, malware classification, intrusion detection, and anomaly-based network monitoring. Compared to traditional rule-based solutions, ML approaches enable adaptive learning, automated feature extraction, and real-time threat recognition, thereby reducing the workload of human analysts and improving the resilience of security systems [7]. Additionally, attackers are using ML to improve the efficiency of their attacks, which highlights the necessity for defensive tactics that are just as advanced. Federated Learning (FL) is a promising new paradigm that allows remote nodes to collaborate on ML model training without revealing any raw data, which is a boon for data sharing and privacy concerns [8]. There is a scalable and privacy-preserving way to do intrusion detection, log analysis, and share threat intelligence when FL is integrated with ML-based cybersecurity frameworks [9]. In addition, ML and FL solutions can make better use of SIEM systems to filter and aggregate data, which allows for timelier and context-aware warnings.

A. Structure of the Paper

The structured of the paper is as follows: Section II discusses cybersecurity solutions for network threats, highlighting major attack types and defense strategies. Machine learning and federated learning are discussed in Section III, which focusses on cybersecurity. Various tasks, approaches, and architectures are covered. Section IV provides a discussion on the comparative advantages, challenges, and limitations of existing approaches. Section V presents the paper's main conclusions and suggests avenues for further research.

II. CYBERSECURITY SOLUTIONS FOR NETWORK THREATS

A computer system or mobile device could be breached in a number of ways, including, but not limited to, unauthorized access, data destruction, or malicious data tampering. Any attempt to breach any of these

security measures is referred to as an attack [10], and the risk and danger associated with each of these breaches is known as a threat. The term "cyber security" has multiple possible meanings. Protecting one's computer, server, and data stored on a network or mobile device from harmful attacks is an important part of cyber security. Separated cyber defenses into subfields such as information and network security. The rate at which attackers develop and implement new strategies to breach systems is outpacing the rate at which defenses can identify and counteract such incursions and attacks [11]. Figure 1 shows a variety of cyber-security risks that need to be managed and addressed.

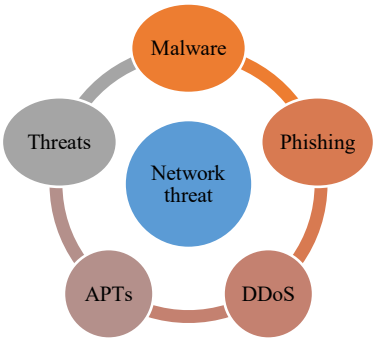


Fig. 1. Cybersecurity Issues

The basics of cyber threats and attacks are discussed below and shown in table I.

A. Malware (Viruses, Worms, Ransomware)

Static, dynamic, and hybrid malware detections are the three main categories. Without actually running the programs, static malware detection looks for dangerous patterns. Nevertheless, programs undergo dynamic detection while they are in operation [12]. Hybrid detection combines the best features of both methods. Malware encompasses a wide range of forms, including viruses, Trojan horses, and worms. An malevolent program that secretly takes data from a computer is known as a virus. Worms are malicious programs that stealthily proliferate and use system resources. A trojan horse is malicious software that steals sensitive information by impersonating legitimate software. No, it's not possible for a Trojan horse to reproduce. Spam messages distributed by email or text message also pose a significant threat to the network and computer resources. A lot of bandwidth and memory is used up by spam communications.

B. Phishing and Social Engineering Attacks

Phishing is a technique whereby an unauthorized individual gains access to sensitive information by masquerading as a trusted user. One kind of phishing involves sending a link to a website that looks like a real one but really contains links that ask for sensitive information. The opposite is true with malware, which is intentionally created software whose goal is to infiltrate a target machine and disrupt its normal operation.

C. Denial of Service (DoS/DDoS)

A DOSs attack occurs when a hacker causes a system overload or memory resource scarcity on a network, making it unable to process access requests from valid users [13]. In a remote-to-local (R2L) attack, an attacker from afar utilizes a network's weaknesses in an effort to gain access to the local area

network. U2R attacks occur when a legitimate user with limited network access tries to gain root user privileges.

D. Advanced Persistent Threats (APTs)

The goal of APTs is to disrupt governmental and corporate systems. APTs can only be effective if they maintain a high level of stealth for an extended period of time while operating [14]. Even after critical systems have been compromised and the attackers have accomplished their initial goals, the compromised systems remain operational, and the assault objectives usually go beyond immediate financial gain.

E. Insider Threats

A zero-day attack is a kind of cyberattack in which the developers of the affected software were either unaware of the vulnerability or did not realize that a patch was available.

TABLE I. COMPARISON OF MAJOR CYBERSECURITY THREATS

Attack Type	**Definition / Characteristics**	**Techniques Used**	**Impact**
Malware (Viruses, Worms, Ransomware, Trojan Horse)	Computer programs with malicious intent that can damage, disrupt, or even take over whole systems. Contains methods for both static and dynamic detection as well as hybrid configurations.	Virus: destroys or alters data Worm: replicates itself, consumes resources Trojan Horse: disguises as legitimate software to steal data (non-replicating) Ransomware: encrypts files and demands payment	Data corruption, system slowdown, unauthorized access, financial loss
Phishing & Social Engineering	An effort at fraud using the impersonation of a trusted entity in order to gain sensitive information. Typical methods of distribution include email, phoney websites, or messaging.	Fake login pages Deceptive links Social engineering manipulation	Credential theft, identity fraud, unauthorized access to accounts
Denial of Service (DoS/DDoS), R2L & U2R	Overwhelms a target system with traffic or exploits vulnerabilities to deny legitimate access. Variants include: R2L: remote attacker gaining local access U2R: local user escalating privileges to root	Flooding network with requests Exploiting system memory Privilege escalation	Service unavailability, resource exhaustion, unauthorized system control
Advanced Persistent	Long-term, stealthy, and targeted cyberattacks typically	Spear phishing Zero-day exploits	Data exfiltration,

Threats (APTs)	aimed at governments or enterprises. Attackers maintain persistence even after breaching systems.	Stealth malware and backdoors	espionage, long-term infiltration of networks
Insider Threats & Zero-Day Attacks	Threats originating from within an organization or from previously unknown vulnerabilities (zero-day). Exploited before patches are available.	Malicious insiders Exploiting unpatched vulnerabilities	Unauthorized system access, data theft, disruption before defenses exist

F. Techniques to Avoid Cyber Threats

Risk Mitigation Strategies for Cyberspace Take these vital steps to strengthen cybersecurity and protect manually from cybercriminals.

- **Use Secure and complicated Passwords:** Avoid using the same password for several websites. Instead, should be protect online accounts by making complex passwords [15]. A password manager is a great tool to help securely generate and remember complex passwords for all online accounts.
- **Maintain Software Updates:** Stay protected from known vulnerabilities and the latest security patches by periodically updating operating system, programmers, and antivirus software.
- **Backup Data Regularly:** Make sure important files and data are backed up on a standard basis. Keep data backups up to date [16]. In the event of data loss or ransomware assaults, it is crucial to have backups stored on accessible and secure cloud or offline drives.
- **Use Secure Wi-Fi Connections:** Choose encrypted (WPA2 or WPA3), password-protected Wi-Fi networks when connect to them. Never do financial transactions or access sensitive information while using an unsecured or public Wi-Fi network.
- **Monitor and Activity:** Keep an eye on and review account activities frequently. Reviewing online account activity, credit card statements, and bank statements might help spot any questionable or unauthorized purchases. If notice anything out of the ordinary, should notify the relevant authorities immediately.

III. MACHINE LEARNING AND FEDERATED LEARNING IN CYBERSECURITY

Malicious network activity that compromises the availability, confidentiality, or integrity of a network's systems can be detected using Network Intrusion Detection (NID) systems [17]. Machine learning is the backbone of many intrusion detection systems due to its ability to learn from mistakes and adapt to new sorts of threats.

A. Machine learning tasks in cybersecurity

Machine learning (ML) is commonly considered a branch of "Artificial Intelligence" (AI), having connections to analytics, data mining, computational statistics, data science, and the capacity to teach computers to learn from instances [18]. This article covers a variety of methods for solving machine learning challenges and how those methods relate to cybersecurity problem areas.

1) Supervised Learning

A task-driven technique, in which a set of predefined goals is used as inputs, is an example of supervised learning. Among machine learning's supervised learning approaches, classification and regression algorithms are by far the most used. A lot of people use these methods to categories or foretell future security issues. Example applications of classification techniques in cybersecurity include yes/no predictions of DOS attacks and the identification of various network attack types, including scanning and spoofing.

2) Unsupervised Learning

The data-driven strategy, which is central to unsupervised learning issues, aims to discover knowledge, structures, or patterns in unlabeled data [19]. Malware and other forms of cyberattack can change their behaviour in real time and independently to evade detection. In order to detect signs of such complex attacks, clustering techniques—a kind of unsupervised learning—can assist in revealing the dataset's latent patterns and structures.

3) Other Learning Techniques

Combining supervised and unsupervised techniques, semi-supervised learning can handle both labelled and unlabeled data. If it's necessary to automatically categorize data without human involvement, it could help cybersecurity models perform better. Another subfield of machine learning, reinforcement approaches define an agent as one that learns by its interactions with its environment.

4) Neural Networks and Deep Learning

DL is a subfield of ML within AI. It's a computer model that takes its cues from the way the human brain's neural networks work. One of the most common methods used in DL is backpropagation, an ANN [20]. It trains using a multi-layer feed-forward NN, which consists of an input layer, a hidden layer (or layers), and an output layer.

B. Machine Learning Techniques For Cyber-Security

This section and Figure 2 describe a small number of popular ML approaches. There is a cyber security application for every single method [21].

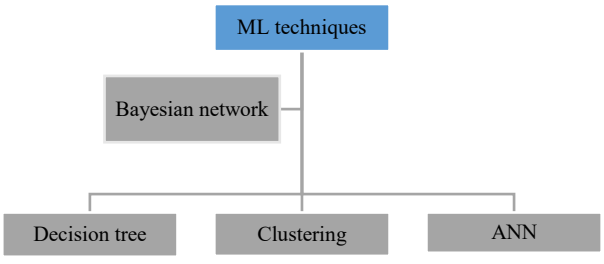


Fig. 2. Machine Learning Techniques For Cyber-Security

1) Bayesian Network

A directed acyclic graph is used to construct the network, which consists of a random set of variables and their conditional relationships [22]. Each node keeps track of the conditional probability form's and

the random variable's states, while the nodes that represent the child rely on the parent nodes. When comparing streaming data with known attack signatures and trends, a Bayesian network can be employed for anomaly detection.

2) Decision Trees

The DT looks a lot like a tree. Trees stand for different types of classifications, with leaves representing each, and branches representing the features that connect and lead to those types of classifications.

3) Clustering

It is an unsupervised learning technique that uses a similarity metric to classify data. With audit data, clustering algorithms can learn to identify distinct types of attacks without the need for the system administrator to explicitly describe them. A density-based clustering approach called SLCT generated the normal and abnormal network data.

4) Artificial Neural Networks (ANN)

The ANN mostly mimics the way the human brain works. A NN is structured with layers. Data activates the neuron in the network's second layer. Which in turn outputs to the next layer of the hierarchy. After this process is complete, the output is generated by the final network layer. "Hidden layers" refer to the internal network that is crucial to the neural network and is shielded from the outside world.

C. Federated Learning (FL)

FL stands for decentralized learning and is a notion in ML. By enabling users to train a model together without ever exchanging data, it helps to safeguard their privacy [23]. Those in possession of really sensitive information, like health records, financial data, transcripts of intimate conversations, and other personally identifiable data (PID), may find this method very attractive.

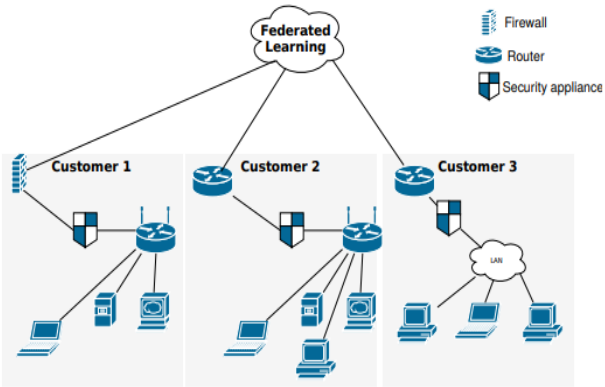


Fig. 3. Federated Learning in Threat Detection

The scenario being investigated, as shown in Figure 3, involves three customers operating on various services on slightly different infrastructure. Without combining customer data, want to create a common threat detection model that is more secure than learning individual models for each client.

D. Types of Federated Learning

In a federated learning architecture, many forms of collaboration take place in response to data needed to train a model. As a result of data structure and access limits, solutions that work for different data partitioning scenarios have been developed [24]. Figure 4 depicts three possible solutions: HFL, VFL, and FTL.

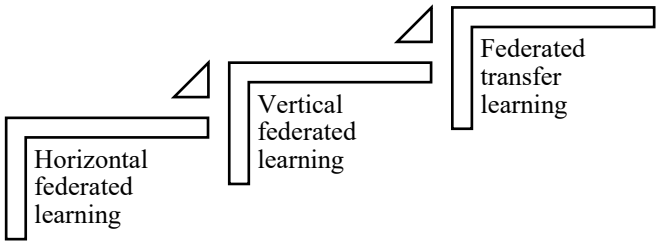


Fig. 4. Types of Federated Learning

- **Horizontal federated learning:** Data is horizontally distributed between several clients in this manner, which constitutes a federated learning paradigm. Here, combine datasets that share the same set of characteristics but use different samples.
- **Vertical federated learning:** Data is vertically partitioned across several clients in this FL approach. Databases with identical samples but distinct features are encompassed. Multiple clients (e.g., an IDS set up on a company network and another IDS set up on user devices) share different kinds of data that belongs to the same people (samples).
- **Federated transfer learning:** Using this FL, can increase learning by sharing knowledge between clients, even when the features and instances in the two datasets are very different [25]. One can use this strategy to partition datasets in both the horizontal and vertical directions.

E. Motivations of FL for Cybersecurity

Reasons Behind FL in Cybersecurity Conventional cybersecurity approaches make it more difficult to gather and share data in a way that invades people's privacy [26]. Data consolidation from several data providers is an equally complicated undertaking. It is possible to use FL to accomplish data privacy and security while reducing cyber-attacks. Figure 5 shows the various elements that impact the cybersecurity applications of FL and the strategies employed by FL to accomplish these goals. The following are some reasons to use FL for cybersecurity:

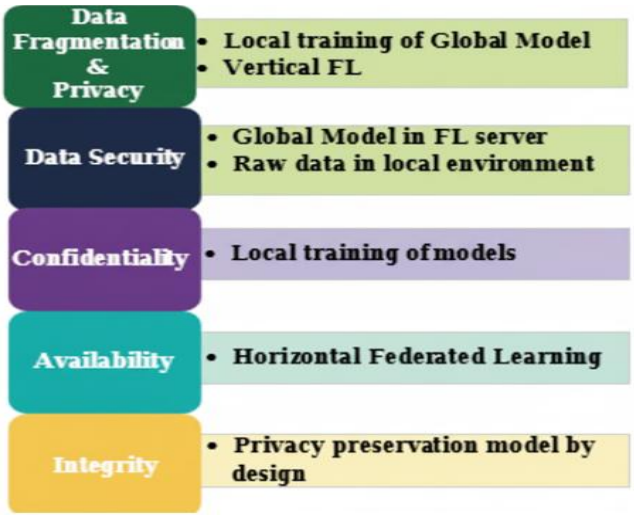


Fig. 5. Federated Learning for Cybersecuity-Motivations

- **Data Fragmentation and Data Privacy:** Objects in the feature space vertically divide user data from an organisation, with each object carrying a unique data feature for all users. Instead of sending the raw data to the server, each node in the core network delivers the parameters of a local model that was developed using features taken from data that was acquired locally. Lessening privacy issues is one benefit of this.
- **Data Security:** Security flaws such as SQL injection, man-in-the-middle, and denial-of-service attacks can be prevented with FL by sending only updates to the server across the network instead of the original data and information.
- **Confidentiality:** Data breach and cyberthreat occur when any unauthorised access misuses data. Confidential and sensitive information can only be accessed by authorised individuals. While using FL, local model training in edge devices guarantees authorised access.
- **Availability:** Users must be granted access to their information when necessary. Cyberattacks and other harmful concerns can affect system uptime and dependability, which in turn affects availability. When FL is used, the edge device has access to the local model, and the user has access to the global model in the cloud.
- **Integrity:** A crucial part of cybersecurity is maintaining data consistency, accuracy, and completeness. It is possible for hackers to modify the sender's data before it reaches the receiver. Since the FL model is designed to safeguard privacy and does not transmit sensitive information outside the local region, the data is secure.

F. Privacy And Security

Novel privacy and security concerns have emerged, despite the fact that the original focus in FL was on achieving stringent privacy safeguards through avoiding data sharing [26]. More recent investigations have shown that sending out model updates can still expose valuable customer data and, worse, cause security breaches. This section provides an overview of the relevant methods for dealing with these issues.

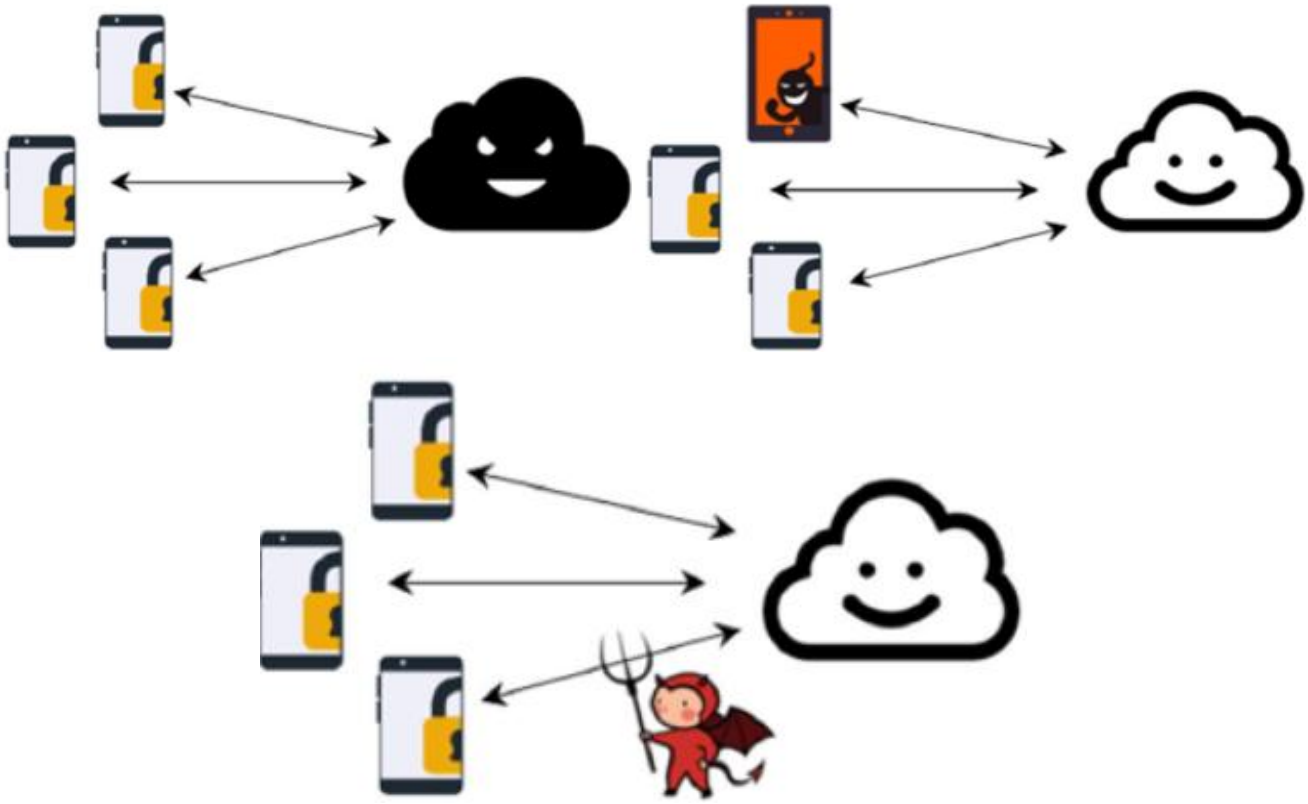


Fig. 6. Different Malicious Actors in Vulnerable FL System

Figure 6 displays the latter, which are categorised as follows:

- **Malicious Server:** An innocent-looking server that is curious about user updates can look at them without modifying the model. On the other hand, malevolent servers can potentially alter the model and examine the modifications. In order to discriminate based on user identity, the suggested architecture employs multi-task Generative Adversarial Networks that target client-level privacy.
- **Insider adversary:** Participants in the learning rounds can range from genuinely interested parties to those with ulterior motives, much as the aforementioned actors.
- **Outsider adversary:** The trusted clients and server are communicating updates, however eavesdroppers on the channel could potentially reveal.

IV. LITERATURE REVIEW

Recent studies on Network Threats Using ML and FL. Table II reviews the research on Network threat using machine and federated learning by study, approach, key findings, challenges, and suggested future research topics.

Suomalainen et al. (2020) the 5G network could unwittingly expose itself to major security risks including unfair resource exploitation, denial of service, and the disclosure of sensitive data if these ML systems are launched. So, to help prepare for 5G, we've broken down the shortcomings of the leading ML systems that are being studied extensively right now. To further avoid these problems using ML in 5G networks, categorize them and then survey potential remedies [27].

Liu et al. (2020) suggest a safe FL framework built on the blockchain for smart contract creation that eliminates the possibility of participation from trustworthy or malevolent parties. By carrying out smart contracts to protect against poisoning assaults, the central aggregator identifies members who are abusive or untrustworthy. For added security, guard against membership inference attacks by implementing local differential privacy measures. Quantitative findings indicate that the suggested architecture can successfully prevent poisoning and membership inference attacks, strengthening the safety of FL in 5G networks [28].

Khramtsova et al. (2020) Smaller organisations and clients frequently face challenges when trying to utilize ML due to the fact that ML functions better with larger datasets. The reason behind this is that due to limited resources for data sharing and collaboration, their machine learning threat detection model not able to compete with that of larger organisations. studies revolve on a common cyber defence assignment: using security-as-a-service providers' monitoring of network traffic to detect harmful URLs [23].

Sharma et al. (2019) Federated Transfer Learning has only looked at the semi-honest approach. In this study, present an enhanced version of the earlier approach, together with an FTL model that includes the ability for malevolent actors to arbitrarily violate the protocol. If suppose that all parties adhere strictly to the protocol, as in the semi-honest model, then it collapses. In order to make model work efficiently with any number of parties, even while dealing with a dishonest majority, employ SPDZ, one of the realistic MPC protocols. Furthermore, as compared to earlier work, the models tested in environment exhibit far superior performance with regard to both communication cost and runtime [29].

Preuveneers et al. (2018) Security researchers are increasingly turning to AI techniques like DL and ML to bolster tried-and-true ways of system monitoring and threat identification. The time-to-detection of these covert assaults can be increased with the use of interconnected and federated learning systems that pool monitoring data and work together to improve hazardous behaviour detection. fundamental worry is that an adversary may manipulate the federated learning outcomes while going unnoticed in a federated learning system by infecting one of the local ML models with malicious training samples [30].

McElwee et al. (2017) The detection of cyberattacks on computer networks is a common goal of network intrusion detection systems. In order to decide the necessary actions, security analysts must manually evaluate the numerous security alerts generated by these systems. Security analysts may get tired from reviewing all of these warnings, especially if they work long shifts. In order to alleviate the heavy workload of DOD cyber defence security analysts, this article examines a case study that demonstrates how ML was used to prioritize security warnings [31].

TABLE II. SUMMARY OF LITERATURE REVIEW BASED ON NETWORK THREAT USING MACHINE AND FEDERATED LEARNING

References	Study On	Approach	Key Findings	Challenges	Future Work
Suomalainen et al., (2020) [7]	ML vulnerabilities in 5G networks	Survey and classification of ML weaknesses in	ML deployment in 5G may lead to unfair resource use, DoS, and	Ensuring robustness and resilience of ML models in	Develop secure ML frameworks tailored for 5G

		5G	privacy leakage	adversarial settings	
Liu et al., (2020) [8]	Secure Federated Learning (FL) in 5G	Blockchain-based FL with smart contracts + local differential privacy	Protects 5G users against poisoning and membership inference attacks while enhancing FL security	Overhead of blockchain integration and contract execution	Optimize scalability and efficiency of blockchain-FL integration
Khramtsova et al., (2020) [9]	Data sharing for ML-based threat detection	Experiments on unwanted URL detection in network traffic	Larger organizations benefit from more data; smaller ones face weaker ML performance	Lack of collaboration among organizations; data silos	Design privacy-preserving data-sharing mechanisms to support smaller organizations
Sharma et al., (2019) [10]	Federated Transfer Learning (FTL) with malicious participants	Use of SPDZ secure MPC protocol for FTL	Supports dishonest majority, improves runtime and communication efficiency	Handling malicious participants in FL remains complex	Extend framework for large-scale deployment across multiple industries
Preuveneers et al., (2018) [11]	Poisoning attacks in Federated Learning for cybersecurity	FL systems for collaborative malicious behavior detection	FL improves detection by data sharing but vulnerable to poisoning	Adversaries can inject malicious samples into local training	Develop robust aggregation and poisoning-resistant FL techniques
McElwee et al., (2017) [12]	ML for triage of security alerts in NIDS	Case study on ML-assisted alert triage in DoD systems	ML reduces manual burden on analysts, speeding up triage	Analyst fatigue and high alert volume	Enhance explainability and trust of ML triage systems

V. CONCLUSION AND FUTURE WORK

The increasing sophistication and complexity of network threats has elevated cybersecurity to the status of a top digital security concern. Attack methods are always changing, and traditional defences aren't always up to the task of stopping new kinds of malware, phishing, DOS, APTs, insider assaults, and zero-day vulnerabilities. To improve detection, prevention, and reaction tactics, intelligent systems powered by ML and FL provide promising capabilities in this context. ML techniques provide

adaptability for identifying new and unknown threats, while FL introduces a privacy-preserving paradigm that enables collaborative threat intelligence without requiring centralized data sharing. Together, these approaches present a strong foundation for building resilient and intelligent cybersecurity systems.

Future work in this domain will focus on several key directions. First, enhancing the robustness of ML and FL models against adversarial attacks and data poisoning is essential for ensuring trustworthy cyber defines. Second, incorporating explainable AI (XAI) will improve the interpretability and transparency of automated threat detection, thereby fostering greater trust among users and stakeholders. Third, lightweight and resource-efficient models must be designed to suit IoT and edge computing environments with limited computational capabilities. Additionally, the development of standardized datasets, evaluation frameworks, and cross-domain collaboration mechanisms will be crucial for benchmarking, validating, and deploying intelligent cybersecurity solutions at scale.

REFERENCES

1. M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Comput. Networks*, vol. 169, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
2. H. P. Kapadia, “Cross-Platform UI/UX Adaptions Engine for Hybrid Mobile Apps,” *Int. J. Nov. Res. Dev.*, vol. 5, no. 9, pp. 30–37, 2020.
3. Y. Xin *et al.*, “Machine Learning and Deep Learning Methods for Cybersecurity,” *IEEE Access*, vol. 6, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
4. S. S. S. Neeli, “Serverless Databases: A Cost-Effective and Scalable Solution,” *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 6, p. 7, 2019.
5. J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014, doi: 10.1016/j.jcss.2014.02.005.
6. G. Tsochev, R. Trifonov, O. Nakov, S. Manolov, and G. Pavlova, “Cyber security: Threats and Challenges,” in *2020 International Conference Automatics and Informatics (ICAI)*, IEEE, Oct. 2020, pp. 1–6. doi: 10.1109/ICAI50593.2020.9311369.
7. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends,” *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.
8. J. B. Fraley and J. Cannady, “The promise of machine learning in cybersecurity,” in *SoutheastCon 2017*, 2017, pp. 1–6. doi: 10.1109/SECON.2017.7925283.
9. S. S. S. Neeli, “Decentralized Databases Leveraging Blockchain Technology,” vol. 8, no. 1, pp. 1–8, 2020.
10. K. Thakur, M. Qiu, K. Gai, and M. L. Ali, “An Investigation on Cyber Security Threats and Security Models,” in *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*, 2016. doi: 10.1109/CSCloud.2015.71.
11. K. R. S. Dubey, “Network Security and Threats in Modern Era-Review,” *Issn*, vol. 2, no. 2, pp. 107–117, 2014.
12. K. Shaukat *et al.*, “Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity,” *Energies*, vol. 13, no. 10, May 2020, doi: 10.3390/en13102509.

13. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
14. I. Ghafir and V. Prenosil, "Advanced Persistent Threat Attack Detection: An Overview," *Int. J. Adv. Comput. Networks Its Secur.*, vol. 4, no. 4, 2014.
15. M. Jouini, L. B. A. Rabai, and A. Ben Aissa, "Classification of Security Threats in Information Systems," *Procedia Comput. Sci.*, vol. 32, pp. 489–496, 2014, doi: 10.1016/j.procs.2014.05.452.
16. A. Thapliyal, P. S. Bhagavathi, T. Arunan, and D. D. Rao, "Realizing Zones Using UPnP," in *2009 6th IEEE Consumer Communications and Networking Conference*, 2009, pp. 1–5. doi: 10.1109/CCNC.2009.4784867.
17. D. D. Rao, "Multimedia Based Intelligent Content Networking for Future Internet," in *2009 Third UKSim European Symposium on Computer Modeling and Simulation*, 2009, pp. 55–59. doi: 10.1109/EMS.2009.108.
18. I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, 2020, doi: 10.1186/s40537-020-00318-5.
19. A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," *Int. J. Distrib. Cloud Comput.*, vol. 4, no. 2, pp. 1–9, 2016.
20. V. M. L. G. Nerella, "Automated Cross-Platform Database Migration And High Availability Implementation," *Turkish J. Comput. Math. Educ.*, vol. 9, no. 2, pp. 823–835, 2018.
21. R. Das and T. H. Morris, "Machine Learning and Cyber Security," in *2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE)*, IEEE, Dec. 2017, pp. 1–7. doi: 10.1109/ICCECE.2017.8526232.
22. V. M. L. G. Nerella, "Observability-Driven SRE Practices for Proactive Database Reliability and Rapid Incident Response," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 7, no. 8, pp. 32–38, Aug. 2019, doi: 10.17762/ijritcc.v7i8.11710.
23. E. Khramtsova, C. Hammerschmidt, S. Lagraa, and R. State, "Federated Learning For Cyber Security: SOC Collaboration For Malicious URL Detection," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, Nov. 2020, pp. 1316–1321. doi: 10.1109/ICDCS47774.2020.00171.
24. P. Kairouz *et al.*, "Advances and Open Problems in Federated Learning," 2019. doi: 10.48550/arXiv.1912.04977.
25. M. Śmietanka, H. Pithadia, and P. Treleaven, "Federated Learning for Privacy-Preserving Data Access," *SSRN Electron. J.*, pp. 1–16, 2020, doi: 10.2139/ssrn.3696609.
26. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020, doi: 10.1109/MSP.2020.2975749.
27. J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, "Machine Learning Threatens 5G Security," *IEEE Access*, vol. 8, pp. 190822–190842, 2020, doi: 10.1109/ACCESS.2020.3031966.

28. Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., Ragireddy, U. K., & Addepalli, P. V. (2023). Data-Driven Approaches for Forecasting Cost Overruns in Infrastructure Projects. *European Journal of Technology*, *7*(5), 23-34.
29. Dhuli, S., Prabu, M., Muzaffer, H. S., Uday Kumar, R., & Prasanth Varma, A. (2023). A Survey on Critical Success Factors Influencing Project Success Across Multiple Industries. *J Contemp Edu Theo Artific Intel: JCETAI-106*.
30. Ragireddy, U. K., Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., & Syed, M. H. (2023). An Overview of Different Automation Strategies Used in Cloud-Based CI/CD Pipelines for Software Deployment. *International Journal of Technology, Management and Humanities*, *9*(01), 116-127.
31. Addepalli, P. V., Bandaru, S. R., Shyam, D., Manoharan, P., Syed, M. H., & Ragireddy, U. K. (2023). Performance Analysis of Machine Learning Models for Cybersecurity Risk Classification in IT Projects. *Universal Library of Engineering Technology*, (Issue).
32. Mylavarapu, K. B., Pilli, J., Jannu, P. K., Mohammad, J. A., & Panchali, S. H. (2023). Artificial Intelligence for Continuous Quality Assurance in Cloud-Native Applications: A Review. *European Journal of Technology*, *7*(5), 35-49.
33. Jannu, P. K., Mohammad, J. A., Panchali, S. H., Mylavarapu, K. B., & Pilli, J. (2023). A Survey on Energy-Efficient Microarchitecture Design Strategies for Mobile CPUs and GPUs: Techniques and Future Directions. *International Journal of Technology, Management and Humanities*, *9*(04), 137-151.
34. Taluri, R. (2021). Cloud-Native Architectures for Enterprise Financial Data Management, Analytics, and Regulatory Reporting Compliance. International Journal of Emerging Trends in Computer Science and Information Technology, 2(2), 101-111. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I2P112
35. Taluri, R. (2022). Cloud Data Engineering Strategies for Large-Scale Financial Data Integration and Intelligent Corporate Performance Reporting. International Journal of Emerging Research in Engineering and Technology, 3(4), 176-188. https://doi.org/10.63282/3050-922X.IJERET-V3I4P119
36. Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., & Chilakapati, V. K. (2023). An AI-Based Framework for Detecting IoT Botnets Through Network Traffic Analysis and Modeling. *Universal Library of Engineering Technology*, (Issue).
37. Kavuluri, H. V. R., Pathani, A. K., Dasari, A., Chilakapati, V. K., Keshireddy, S. R., & Nagumotu, V. T. (2023). Cloud Data-Center Network Verification: Approaches, Algorithms and Toolchains. *American Journal of Computing and Engineering*, *6*(2), 18-32.
38. Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., & Dasari, A. (2023). A Survey on 5G/6G Radio Access Networks: Technologies, Protocols, and Performance Metrics. *International Journal of Technology, Management and Humanities*, *9*(02), 79-93.
39. Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., Pathani, A. K., Dasari, A., & Chilakapati, V. K. (2023). An AI-Based Framework for Detecting IoT Botnets Through Network Traffic Analysis and Modeling. *Universal Library of Engineering Technology*, (Issue).
40. Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, "A Secure Federated Learning Framework for 5G Networks," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 24–31, Aug.

2020, doi: 10.1109/MWC.01.1900525.

41. S. Sharma, C. Xing, Y. Liu, and Y. Kang, "Secure and Efficient Federated Transfer Learning," in *2019 IEEE International Conference on Big Data (Big Data)*, IEEE, Dec. 2019, pp. 2569–2576. doi: 10.1109/BigData47090.2019.9006280.
42. D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E. Ilie-Zudor, "Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study," *Appl. Sci.*, vol. 8, no. 12, Dec. 2018, doi: 10.3390/app8122663.
43. S. McElwee, J. Heaton, J. Fraley, and J. Cannady, "Deep learning for prioritizing and responding to intrusion detection alerts," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, IEEE, Oct. 2017, pp. 1–5. doi: 10.1109/MILCOM.2017.8170757.