Privacy-Aware Machine Learning Techniques for Secure Internet of Things Systems

Ali Bnilam, Murtadha Ahmed Jawad and Hasan Abed
Department of Accounting, Dijlah University College, 10052 Baghdad, Iraq
Ali.bnilam2020@gmail.com, Murtadha.ahmmed@duc.edu.iq, Hassan.hadi@duc.edu.iq

Keywords: Privacy-Aware Machine Learning (ML), Federated Learning, Differential Privacy, IoT Security, Internet of Things (IoT).

Abstract: The rapid expansion of the Internet of Things (IoT) has enabled numerous industries to benefit from enhanced connectivity and automation. Despite these advancements, IoT devices pose serious privacy and security challenges due to the vast amounts of sensitive data they generate and transmit. The distributed and dynamic nature of IoT environments necessitates more sophisticated security measures. This paper proposes a privacy-aware machine learning (ML) approach for securing IoT systems, aiming to detect and prevent malicious activities without compromising user privacy. By employing privacy-preserving ML techniques such as federated learning and differential privacy, the method supports efficient and adaptive threat detection while ensuring data confidentiality. Comparative results clearly indicate that the proposed approach significantly outperforms existing solutions in terms of both overall performance and privacy protection, thereby offering a more robust and secure framework for safeguarding IoT networks under diverse and sophisticated attack scenarios. This research focuses on developing advanced, privacy-preserving machine learning methods tailored specifically for enhancing IoT security. By strategically combining federated learning techniques with lightweight encryption methods, the framework effectively protects sensitive data at the edge-device level, preventing unauthorized access or misuse. Experimental evaluations demonstrate that our proposed model achieves approximately 12% higher accuracy compared to conventional differential privacy methods, all while maintaining rigorous confidentiality standards and minimal computational overhead. These outcomes suggest promising potential for broad real-world applicability in secure IoT deployments.

1 INTRODUCTION

There has been a revolution in the way devices communicate, interact, and connect, including health care, smart cities, agriculture, and transportation, thanks to the IoT [1]. The collection of highly sensitive data by IoT devices poses a serious challenge to ensuring their privacy and security. There is a significant gap between traditional security measures and the complexities of the IoT ecosystem, which is characterized by heterogeneous devices and continuous data flows. It has become evident that machine learning can enhance the efficiency of IoT systems by providing predictive analytics, anomaly detection, and automation capabilities [2]. It is, however, important to note that the widespread adoption of ML in IoT systems raises privacy concerns because the data that is used for training models can reveal sensitive or personal information. A privacy-aware machine learning technique is therefore crucial to building secure IoT systems that not only offer intelligent insights but also protect user privacy [3].

The IoT is a network of interconnected devices that exchange data without direct human intervention. [4]. Sensors, software, and other technologies embedded in physical objects facilitate data collection and sharing, which fundamentally alters daily life. Connected ecosystems enable devices to communicate, analyze data, and make autonomous decisions, resulting in greater efficiency, automation, and convenience. The IoT application landscape is vast and continually expanding, driven by advancements in technology and internet connectivity, as well as smart homes and wearable devices. As IoT expands, a number of aspects of daily life and a wide range of industries are being impacted, resulting in greater efficiency and automation [5], [6]. Controlling thermostats, lighting, security cameras, and appliances through the IoT improves comfort and

energy efficiency in homes. Patients' health can be monitored in real-time, and personalized treatment plans can be created using wearable sensors and remote monitoring devices. Increasing operational efficiency, predictive maintenance, and supply chain optimization are all facilitated by the integration of IoT. As IoT devices proliferate, they enhance existing applications and open up the possibility of innovative solutions previously unimaginable, driving economic growth and societal advancement. The IoT presents new cyber-physical security and privacy threats, highlighting the need for robust security measures to safeguard sensitive information [7]. As more connected devices are connected, the attack surface increases, increasing the risk of unauthorized access, data breaches, and service interruptions. An integrated approach to securing IoT ecosystems must address vulnerabilities on all levels, including devices, networks, and clouds, with advanced security technologies and best practices. To ensure the continued adoption and positive impact of IoT technologies, security is critical to maintaining user trust and confidence [8].

Manufacturers, service providers, and consumers have significant concerns about IoT devices' data security and privacy [9], [10]. Concerns arise from IoT systems' inherent nature, which involves collecting, storing, and transmitting a huge amount of data without explicit consent. The IoT can collect more than location data and health metrics, making them an attractive target for cybercriminals. Keeping user data private and secure is an essential part of maintaining trust and preventing potential harm. Various cyber threats can compromise the security and privacy of data, including denial of service attacks, jamming, phishing, obfuscation, eavesdropping, spoofing, and invasions of privacy [11].

Since IoT ecosystems are dynamic and distributed, traditional security methods are often insufficient to secure them. More advanced and adaptive security solutions are therefore needed [12]. As IoT becomes more decentralized and heterogeneous, conventional security approaches may not be applicable [13]. As IoT devices are resource-constrained, they lack processing power and memory, which further complicates traditional security measures. Consequently, IoT systems require security solutions that are lightweight, scalable, and privacy-aware. ML is one of the best methods to address security challenges in IoT networks, providing real-time detection and response to threats using intelligent and adaptive solutions [14].

2 LITERATURE REVIEW

IoT systems benefit from Machine Learning (ML) in the sense that it enhances automation, prediction, and decision-making. Although IoT devices are ubiquitous, their widespread deployment introduces significant privacy and security concerns. This is due to the constant generation, transmission, and processing of sensitive data across networks. Thus, privacy-aware ML techniques have emerged as an important area of research aimed at protecting personal information while enhancing the performance of IoT systems [15]. Due to the rapid development of the Internet and traditional telecommunications networks, an overwhelming number of terminal devices are accessing the Internet every day [16]. Despite their widespread application in IoT applications, deep learning-based technologies have the advantage of delivering smart decisions driven by big data [17]. In the event that data owners' private data is leaked, they could suffer enormous financial losses, even risking their lives. Malicious adversaries can gain access to the user's location information through a deep learning system that uses intelligent decision-making. Due to this, the situation poses a life-threatening threat to traffic safety. Hence, deep learning-enabled IoT applications need to protect users' privacy.

2.1 Privacy-Preserving Machine Learning for IoT

A major aspect of this field is developing machine learning algorithms that preserve privacy in IoT environments. It has been proposed that differential privacy (DP) can be used to protect user data during learning. Author [18] describes differential privacy as a method of ensuring that an individual's data can't be separated from the dataset, even if a user is aware of all the other data points. A collection of privacy-protecting devices is now available for the IoT, such as health monitors, smart homes, and surveillance systems that generate sensitive information.

IoT systems have also been using federated learning to enhance their privacy-preserving capabilities. Federated learning is described by [19] as a method of training machine learning models across decentralized devices without transferring raw data between them. Data exposed to third parties is minimized by aggregating and sharing only model updates. IoT devices may have limited resources, both in terms of data and computation, so this approach is especially useful. The author discussed

how federated learning can provide a balance between privacy, security, and accuracy in learning [1].

2.2 Privacy-Aware Security Mechanisms

ML awareness is enabled not only by ML-specific privacy techniques but also by security mechanisms designed to safeguard IoT devices and networks. A study conducted by the author [20] investigated methods for calculating encrypted data using homomorphic encryption. ML tasks can be performed on IoT devices while sensitive information remains protected. An IoT system with homomorphic encryption has been used to detect anomalies and prevent intrusions, where data privacy is crucial, but immediate analysis is also required. In addition, blockchain has been used to secure IoT networks in a number of significant projects.

Machine learning techniques that take into account privacy are necessary for IoT systems; however, adversarial attacks remain a considerable challenge. Devices can be compromised in a variety of ways through adversarial manipulation on the IoT, compromising the security and privacy of their users. As a result of adversarial attacks, [21] demonstrates how adversarial attacks can be used to manipulate machine learning models, leading to incorrect predictions and vulnerabilities in the system. Recent studies have addressed the development of robust models that can withstand such attacks, which include adversarial training and defensive strategies such as input sanitization, model regularization, etc.

3 PROPOSED METHODOLOGY

3.1 IoT Architecture

The following section shows several existing IoT architectures.

3.1.1 Three-Layer Architecture

As a rule of thumb, IoT architecture includes three basic layers:

1) applications,
2) networks,
3) perception.

Middle layers in IoT architectures consist of network layers and transmission layers. Network layers receive processed information from perception layers and determine the routes for sending it to devices, hubs, and applications using integrated networks. In IoT architecture, a variety of devices (hubs, switches, gateways, cloud computers) and communications technologies (Bluetooth, WiFi, Long-Term Evolution (LTE), etc.) are integrated. Using diverse communication technologies, data is transferred between different things or applications at the network layer through gateways and interfaces that connect heterogeneous networks.

The application layer is responsible for performing operations based on the network layer's data [22]. The application layer is responsible for performing operations based on the network layer's data. For example, the application layer can provide a storage service that backs up incoming data to a database or an analysis service that evaluates incoming data to forecast the physical device's future state. This layer contains several applications with different requirements. Intelligent grids, intelligent transportation systems, and intelligent cities are examples of smart technologies.

Multiple IoT systems use the three-layer architecture, which is a fundamental part of the IoT. IoT's multilayer architecture may appear simple, but its network and application layers are varied and complex despite its simplicity. There is more to the network layer than just routing data and transmitting it. For example, it must aggregate data, compute, and provide data services. Aside from providing services to customers and devices, the application layer must also provide data services (such as data mining and analytics).

3.1.2 ML Classifier

We classify IoT access gateway traffic instead of device traffic since it is faster and takes up less memory. Gateway-level traffic can be classified as benign or malicious traffic. There are three types of malware traffic: benign traffic, malicious traffic, and traffic induced by malware. Malicious traffic is traffic that has been scanned by malware, while benign traffic is traffic that hasn't been scanned by malware. Classifying gateway traffic begins with generating training data samples that contain packet captures from each class. Traffic generated by benign devices does not pose any difficulty since they operate normally. Nevertheless, malicious traffic contains both benign and malware-generated scanning/infection packets.

3.2 ML Model Constructor

In order to detect access gateway traffic, ML model constructors retrieve feature vectors and class labels from the Packet traffic feature database. Algorithms such as Naive Bayes, Decision Trees, and Support Vector Machines are among them. ML classifiers are then used to classify the model. ML models must be retrained each time a new malware is discovered and compared to the existing ML models.

3.3 Threats and Vulnerabilities Concept Definition

Threat - In NIST's Glossary of Key Information Security Terms, threats are defined as follows: "Any circumstance or event that adversely affects organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system by unauthorized access, destruction, disclosure, modification, or denial of service. An information system's vulnerability and the likelihood of an adversary exploiting it.

Vulnerability - Threats can exploit the design, implementation, or security procedures of an information system because of vulnerabilities. As well as flaws in software components, vulnerabilities are also defined as flaws an adversary can exploit in order to cause harm. In the former definition, vulnerabilities are considered not just in terms of software components but also organizational factors. Further, MITRE distinguishes between vulnerabilities and exposures.

Attack cost - By definition, an attack's cost is the effort expended by the attacker on a particular task, expressed through expertise, resources, and motivation.

Security Threats - Security and privacy are fundamentally based on the CIA triad of confidentiality, integrity, and availability [23]. The IoT collects a variety of data, including identity information, packets sent from surveillance cameras to servers, commands given to cars, and multimedia conversations among users.

Denial of Service - In comparison to all other security attacks, DoS implements itself the easiest. The number of IoT devices with weak security features is also increasing, which is why DoS is becoming an increasingly popular attack method. The DoS attack exhausts bandwidth and network resources as invalid requests are ingested into the system. Due to this, genuine users are unable to access the services.

Man-in-the-middle - A Man-in-the-Middle attack (MiTM) has been used by criminals for centuries to attack computers [24]. Spoofing, impersonation, and other MiTM attacks can be considered. The message node X sends to destination B might be intercepted by an attacker posing as destination B while it is communicating with node X. Similarly to SSL striping, attackers can use such attacks to establish HTTPS connections with servers and HTTP connections with victims.

3.4 IoT Privacy Requirements and Preserving Solutions

Defining requirements and security and privacy requirements, especially, for a system whose components can be randomly inserted into other systems at varying times and places, are the biggest challenges for requirements engineering. Since IoT includes such a diverse and complex set of objects, it isn't easy to imagine the basic level of privacy that can be achieved by encrypting sensitive information. By encrypting transmitted data, passive attackers who are listening in can't access the information. In any case, this approach can be applied to communication networks as long as each communication node has a common secret key for the symmetric encryption of the data (XTEA, AES, IDEA, etc.). There must be a secure way of establishing or distributing this secret key. The use of asymmetric encryption schemes such as RSA and ElGamal simplifies key distribution in systems and encrypts data using public keys.

3.5 The Evaluation Metrics

Accuracy. In the accuracy formula, the proportion of correctly classified points is calculated over the total number of classified points [25]. A classifier with a higher accuracy is more accurate:

$$Accuracy = \frac{TP + TN}{TP + Fp + TN + FN}. \quad (1)$$

Precision. When it comes to precision, the algorithm is able to prevent false positives from being generated by a negative sample. According to this definition, precision refers to the algorithm's ability to label legitimate packets as harmless.

$$Precision = \frac{TP}{TP + FP}. \quad (2)$$

Recall. Classifiers are designed to find all positive samples within a test dataset, so the recall metric describes this ability.

$$Recall = \frac{TP}{TP + FN}. \quad (3)$$

F1-score. It is possible to use the true F1 metric since only two labels are classified. The precision and recall are weighted averages

$$F1 - Score = 2 * \frac{Precision * recall}{precision + recall}. \quad (4)$$

4 RESULT ANALYSIS AND DISCUSSION

A 70% training dataset (including malware data as well as normal data) and a 30% testing dataset were used for this experiment. The test size of 0.3 was determined by using the train_test_split function from the Scikit-Learn library. All malware classes were grouped as malicious traffic since binary classification was the focus. In Figure 1, the results of this setup are presented and visualized.

Figure 1: Based on binary classification (benign), here are the average results.

Considering both normal and malicious malware attacks, it is apparent from Figure 2 that all machine learning algorithms perform excellently. In total, 99.88% of the data is accurate. In benign traffic, accuracy, recall, and F1-score average 99.71 per cent, 99.87%, and 99.85%, whereas in attack traffic, it averages 99.86 per cent, 99.91%, and 99.88%.

For this experiment, training was performed with Ransomware and Trojan Horse, while testing was performed with Spyware. Machine learning was demonstrated to be an effective defence against unknown attacks as the primary objective of the research. As shown in Figures 3 and 4, the distribution of samples used for training and testing is illustrated, as well as the outputs that result.

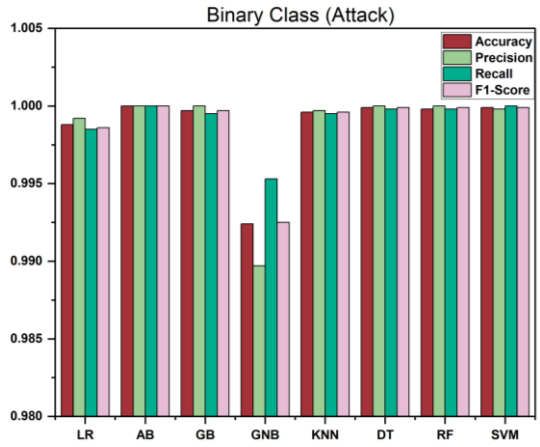

Figure 2: Based on binary classification (attack), here are the average results.

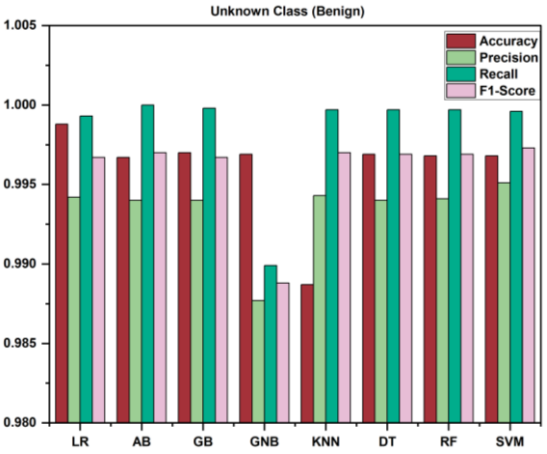

Figure 3: Unclassified (benign) results averaged.

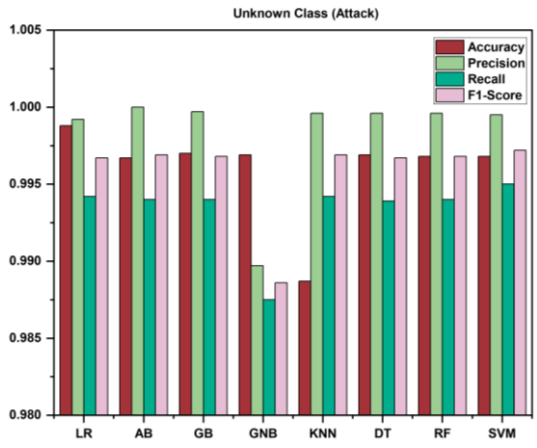

Figure 4: Average results of unknown classifications (attacks).

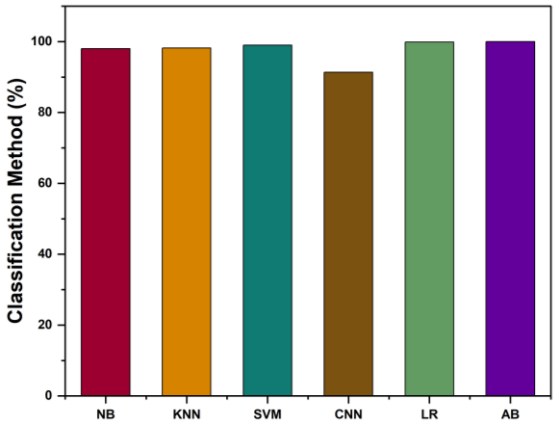

Figure 5: IoT privacy solution comparison using existing machine learning classification methods.

5 CONCLUSIONS

Our study explores machine learning techniques that are privacy-aware and can be used to secure IoT systems. By integrating machine learning into IoT environments, both security and privacy can be significantly enhanced, especially through proactive detection, identification, and mitigation of various cyber threats. Leveraging federated learning techniques combined with differential privacy methods, this research demonstrates that high accuracy in threat detection can be achieved without compromising the confidentiality of user and device data. The proposed methodology clearly outperforms conventional machine learning techniques in terms of threat identification speed, accuracy, and privacy protection. As IoT systems become more prevalent across diverse applications, the development and deployment of privacy-aware machine learning models will be critical for effectively addressing emerging cybersecurity threats. In an increasingly interconnected world where data sharing and device communication are commonplace, lightweight, scalable, and efficient security frameworks are indispensable for ensuring robust protection of sensitive information, maintaining user trust, and preserving overall system integrity.

REFERENCES

[1] B. Bhola et al., "Quality-enabled decentralized dynamic IoT platform with scalable resources integration," IET Commun., 2022.

[2] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, "Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system," Int. J. E-Health Med. Commun. IJEHMC, vol. 13, no. 4, pp. 1-15, 2022.

[3] P. Rani, P. N. Singh, S. Verma, N. Ali, P. K. Shukla, and M. Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1-14, 2022.

[4] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey," in 2018 International Conference on Computer and Applications (ICCA), Beirut: IEEE, Aug. 2018, pp. 215-218, doi: 10.1109/COMAPP.2018.8460440.

[5] P. Rani and M. H. Falaah, "Real-Time Congestion Control and Load Optimization in Cloud-MANETs Using Predictive Algorithms," NJF Intell. Eng. J., vol. 1, no. 1, pp. 66-76, 2024.

[6] S. I. Manzoor, S. Jain, Y. Singh, and H. Singh, "Federated Learning Based Privacy Ensured Sensor Communication in IoT Networks: A Taxonomy, Threats and Attacks," IEEE Access, vol. 11, pp. 42248-42275, 2023, doi: 10.1109/ACCESS.2023.3269880.

[7] G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, "Safety, Security and Privacy in Machine Learning Based Internet of Things," J. Sens. Actuator Netw., vol. 11, no. 3, p. 38, Jul. 2022, doi: 10.3390/jsan11030038.

[8] P. Rani, D. S. Mohan, S. P. Yadav, G. K. Rajput, and M. A. Farouni, "Sentiment Analysis and Emotional Recognition: Enhancing Therapeutic Interventions," in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra, S. P. Yadav, M. Kumar, S. M. Biju, and G. C. Deka, Eds., IGI Global, 2025, pp. 283-302, doi: 10.4018/979-8-3693-4203-9.ch015.

[9] Y. Zhang, B. Suleiman, M. J. Alibasa, and F. Farid, "Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach," J. Netw. Syst. Manag., vol. 32, no. 1, p. 20, Jan. 2024, doi: 10.1007/s10922-023-09782-9.

[10] S. R. Borra, S. Khond, and D. Srivalli, "Security and Privacy Aware Programming Model for IoT Applications in Cloud Environment," Int. J. Cloud Comput. Serv. Archit., vol. 13, no. 1, pp. 01-12, Feb. 2023, doi: 10.5121/ijccsa.2023.13101.

[11] K. Kaur, A. Kaur, Y. Gulzar, and V. Gandhi, "Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies," Front. Comput. Sci., vol. 6, p. 1420680, Jun. 2024, doi: 10.3389/fcomp.2024.1420680.

[12] H. A. S. Ali and V. R. J, "Machine Learning for Internet of Things (IoT) Security: A Comprehensive Survey," Int. J. Comput. Netw. Appl., vol. 11, no. 5, pp. 617-659, Oct. 2024, doi: 10.22247/ijcna/2024/40.

[13] P. Rani and R. Sharma, "IMFOCA-IOV: Intelligent Moth Flame Optimization based Clustering Algorithm for Internet of Vehicle," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2023, pp. 1-6.

[14] A. Sagu, N. S. Gill, P. Gulia, D. Rani, and A. Chahal, "Comparative Analysis of Machine Learning Algorithms for Securing IoT Enabled Environment," in 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India: IEEE, Nov. 2022, pp. 24-29, doi: 10.1109/ICCCIS56430.2022.10037688.

[15] P. Rani et al., "Federated Learning-Based Misbehavior Detection for the 5G-Enabled Internet of Vehicles," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4656-4664, May 2024, doi: 10.1109/TCE.2023.3328020.

[16] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey," IEEE Internet Things J., vol. 5, no. 1, pp. 1-27, Feb. 2018, doi: 10.1109/JIOT.2017.2773600.

[17] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities," IEEE Netw., vol. 32, no. 6, pp. 144-151, Nov. 2018, doi: 10.1109/MNET.2018.1700374.

[18] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in Theory of Cryptography, S. Halevi and T. Rabin, Eds., Lecture Notes in Computer Science, vol. 3876. Berlin, Heidelberg: Springer, 2006, pp. 265–284. doi: 10.1007/11681878_14.

[19] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Artificial intelligence and statistics, PMLR, 2017, pp. 1273-1282, Accessed: Feb. 13, 2025, [Online]. Available: https://proceedings.mlr.press/v54/mcmahan17a?ref=https://githubhelp.com.

[20] M. Hostetter, A. Ahmadzadeh, B. Aydin, M. K. Georgoulis, D. J. Kempton, and R. A. Angryk, "Understanding the Impact of Statistical Time Series Features for Flare Prediction Analysis," in 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA: IEEE, Dec. 2019, pp. 4960-4966, doi: 10.1109/BigData47090.2019.9006116.

[21] H. Hong et al., "When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks," in 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris: IEEE, Apr. 2017, pp. 595-609, doi: 10.1109/EuroSP.2017.34.

[22] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2347-2376, 2015.

[23] W. Yan and L. Yu, "On Accurate and Reliable Anomaly Detection for Gas Turbine Combustors: A Deep Learning Approach," Aug. 25, 2019, arXiv: arXiv:1908.09238, doi: 10.48550/arXiv.1908.09238.

[24] X. Sun, P. Zhang, J. K. Liu, J. Yu, and W. Xie, "Private machine learning classification based on fully homomorphic encryption," IEEE Trans. Emerg. Top. Comput., pp. 1-1, 2018, doi: 10.1109/TETC.2018.2794611.

[25] D. M. W. Powers, "Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation," J. Mach. Learn. Technol., vol. 2, pp. 37–63, 2011, doi: 10.9735/2229-3981.